Privasi dalam Rumah Kaca: Menuntut Akuntabilitas Penggunaan *Spyware* di Indonesia



ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT

2026

Privasi dalam Rumah Kaca: Menuntut Akuntabilitas Penggunaan *Spyware* di Indonesia

2026

Privasi dalam Rumah Kaca: Menuntut Akuntabilitas Penggunaan *Spyware* di Indonesia

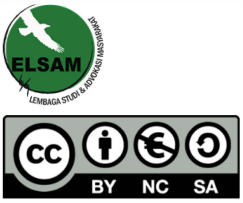
Tim Peneliti:
Kezia Khatwani
Adzkar Ahsinin
Gurnadi
Parasurama Pamungkas
Nurul Izmi

Tim Editor edisi Bahasa Indonesia:
Sungeb
Ferinda Khairunissa Fachri

Design & Layout:
Dodi Sanjaya
Samuel Johanes

Pertama kali dipublikasikan dalam Bahasa Indonesia oleh **Lembaga Studi dan Advokasi Masyarakat (ELSAM)** dengan berkolaborasi bersama **Seknas FITRA** dan **FIND**

April 2026



Daftar Isi

Kata Pengantar	3
A. Pendahuluan	11
B. Pertanyaan Penelitian	50
C. Metode Penelitian	51
D. Karakteristik Perangkat, Operasi *Spyware, dan Bentuk Ancaman terhadap Target*	56
E. *Spyware* dan Kepentingan Kekuasaan Negara: Operasi *Spyware* di Berbagai Negara	76
F. Ancaman Perangkat *Spyware* terhadap Demokrasi dan Hak Asasi Manusia: Konstruksi Struktur Norma HAM dalam Merespons Dinamika Relasi Teknologi dan Hak Asasi Manusia	108

G. Pertarungan Daud *versus Jalut (Goliath)*: *Publik yang Nirkuasa melawan Kekuatan Gigantik Korporasi Teknologi dalam Bingkai Lanskap Norma Bisnis dan HAM* 142

H. Tantangan dalam Penyelesaian Kasus bagi Korban *Spyware*: Keterbatasan Pelindungan HAM yang Ada untuk Memberikan Pelindungan atas Kelahiran Hak-Hak Digital 184

I. Urgensi Pengembangan Ekosistem Akuntabilitas Penggunaan *Spyware* di Indonesia Berbasis Hak Asasi Manusia 237

I.1. Kekosongan Hukum Penggunaan *Spyware* Komersial dan Pengadaan *Spyware* Komersial 237

I.2. Kesenjangan Transparansi dalam Pengadaan Barang dan Jasa Teknologi Intelijen dan *Surveilance* 276

I.3. Jejak-Jejak Penggunaan Perangkat *Spyware* di Indonesia dan Ancamannya Terhadap HAM: Refleksi dari Kasus 298

J. Penutup 328

J.1. Kesimpulan 328

J.2. Rekomendasi 330

Daftar Pustaka 333

Profil ELSAM 359



Kata Pengantar

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan mendasar dalam cara manusia berinteraksi, bekerja, dan membangun relasi sosial. Namun, di balik kemajuan tersebut, muncul pula ancaman yang semakin kompleks terhadap hak atas privasi dan keamanan individu. Salah satu bentuk ancaman yang semakin mengemuka adalah penggunaan perangkat lunak mata-mata atau *Spyware*, yang memungkinkan pengumpulan data secara diam-diam, invasif, dan sering kali tanpa persetujuan pengguna.

Sebagaimana ditunjukkan dalam berbagai kajian mengenai privasi, praktik *Surveilans* tidak lagi terbatas pada konteks keamanan negara, melainkan telah meluas ke berbagai aspek kehidupan sehari-hari. Fenomena ini semakin diperkuat dengan hadirnya teknologi *Spyware* yang mampu mengakses hampir seluruh aktivitas digital seseorang, mulai dari komunikasi pribadi hingga data lokasi secara *real-time*. Dalam banyak kasus, penggunaan teknologi ini

tidak hanya menimbulkan persoalan teknis, tetapi juga menyentuh dimensi hak asasi manusia, demokrasi, dan relasi kekuasaan.

Riset ini disusun untuk memberikan pemahaman yang lebih komprehensif mengenai *Spyware*, termasuk karakteristik, mekanisme kerja, serta implikasinya terhadap privasi dan kebebasan sipil. Selain itu, riset ini juga berupaya menelaah bagaimana praktik penggunaan *Spyware* berkembang dalam konteks global maupun nasional, serta sejauh mana kerangka hukum yang ada mampu mengantisipasi dan mengendalikan potensi penyalahgunaannya.

Dalam konteks yang lebih luas, meningkatnya penggunaan teknologi *Surveilans* menunjukkan adanya pergeseran dalam relasi antara individu, negara, dan korporasi. Pengumpulan data yang masif dan praktik pengawasan yang tidak transparan berpotensi menciptakan ketidakseimbangan kekuasaan, di mana individu semakin kehilangan kendali atas informasi pribadinya. Oleh karena itu, penting untuk menempatkan isu *Spyware* tidak hanya sebagai persoalan teknologi, tetapi juga sebagai

bagian dari diskursus hak asasi manusia dan tata kelola digital.

Oleh sebab itu, riset ini diharapkan dapat memberikan kontribusi bagi pengembangan pemahaman kritis mengenai *Spyware* serta mendorong diskusi yang lebih luas mengenai pentingnya perlindungan privasi di era digital. Dengan meningkatnya kesadaran publik dan penguatan regulasi yang berorientasi pada hak asasi manusia, diharapkan praktik penggunaan teknologi *Surveilans* dapat dikendalikan secara lebih akuntabel dan transparan.

Genealogi Metafora: Privasi dalam Rumah Kaca

Pemilihan judul Privasi dalam Rumah Kaca lahir dari sebuah resonansi sastra yang terasa begitu relevan dengan kondisi zaman ini. Judul tersebut terinspirasi dari novel keempat tetralogi Buru karya Pramoedya Ananta Toer, Rumah Kaca (1988), yang mengisahkan pengawasan sistematis yang dilakukan negara kolonial Belanda terhadap Minke tokoh utama yang mewakili gerakan nasionalisme awal di Hindia Belanda.

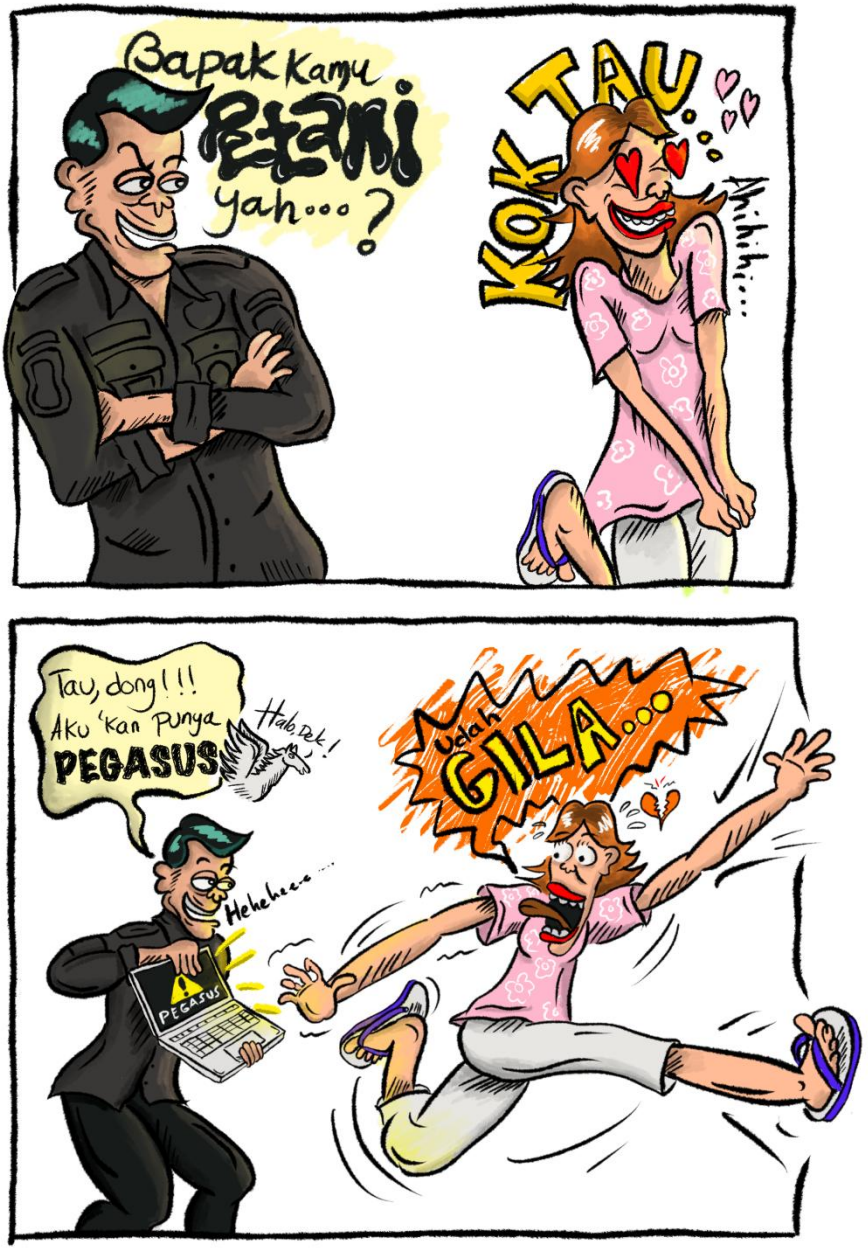
Dalam novel tersebut, "rumah kaca" menjadi metafora yang kuat untuk menggambarkan kondisi seseorang yang hidup di bawah tatapan kuasa yang tak pernah bisa dihindari, setiap gerak-gerik terekam, setiap kata tercatat, setiap relasi dipetakan oleh aparat intelijen kolonial. Minke tidak pernah benar-benar bebas, sebab kebebasannya hanya ilusi di dalam struktur pengawasan yang transparan dari luar namun membelenggu dari dalam. Ia bisa melihat dunia, tetapi dunia atau lebih tepatnya, kekuasaan juga terus-menerus melihat dirinya.

Lebih dari seabad setelah latar waktu yang digambarkan Pramoedya, kondisi yang dialami Minke terasa bukan sekadar sejarah. Teknologi *Spyware* hari ini mereplikasi logika "rumah kaca" itu ke dalam genggaman tangan kita, perangkat yang kita pikir adalah alat kebebasan justru bisa menjadi jendela yang memungkinkan pihak lain mengintip tanpa sepengetahuan kita. Nama-nama berbeda, teknologinya berbeda, tetapi relasi antara pengawas dan yang diawasi tetap menyimpan struktur yang serupa asimetri kekuasaan yang dalam, di mana satu pihak memiliki visibilitas penuh sementara pihak lain tak menyadari bahwa dirinya sedang diamati.

Dengan meminjam gambaran Pramoedya, riset ini ingin menegaskan bahwa persoalan *Surveilans* digital bukanlah fenomena baru yang lahir dari kecanggihan silikon. Ia adalah kelanjutan dari sebuah genealogi kekuasaan yang panjang hasrat untuk melihat, mengetahui, dan mengendalikan. Menyebutnya "Privasi dalam Rumah Kaca" adalah pengingat bahwa kita tidak sedang berhadapan dengan masalah teknis semata, melainkan dengan sesuatu yang jauh lebih tua dan lebih dalam pertarungan antara hak untuk tidak terlihat dan keinginan kuasa untuk tidak melewatkan satu pun.

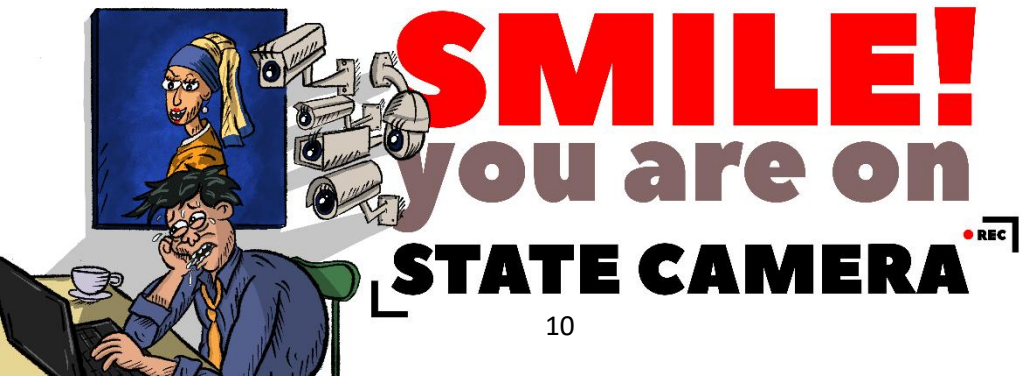
Selain itu, riset ini diharapkan dapat memberikan kontribusi bagi pengembangan pemahaman kritis mengenai *Spyware* serta mendorong diskusi yang lebih luas mengenai pentingnya perlindungan privasi di era digital. Dengan meningkatnya kesadaran publik dan penguatan regulasi yang berorientasi pada hak asasi manusia, diharapkan praktik penggunaan teknologi *Surveilans* dapat dikendalikan secara lebih akuntabel dan transparan.

Desiana Samosir
Direktur Eksekutif ELSAM


Bapak Kamu Petani Yah...?
KOK TAU..
Ahihihi...
Tau, dong!!! Aku 'kan Punya PEGASUS
Hah Dek!
Udah GILA..
Hehehee....
PEGASUS

“Kalian boleh bebas, tapi kalian dalam pantauanku.”

– Pramoedya Ananta Toer, Rumah Kaca (1988)


SMILE!
you are on
STATE CAMERA
REC

"Kita punya badan-badan yang mengawasi kamar tidur orang melalui webcam, dan mereka mengumpulkan miliaran catatan lokasi ponsel setiap hari. Mereka tahu di mana Anda naik bus, ke mana Anda pergi bekerja, di mana Anda tidur, dan ponsel apa saja yang Anda gunakan saat tidur."[1]



Edward Snowden

A. Pendahuluan

Pemerintah di berbagai belahan dunia tengah memperkuat represi terhadap suara kritis dengan menyasar pembela HAM, jurnalis, dan aktivis melalui *Surveilans* digital yang ditargetkan (*targeted digital surveillance*). Praktik ini bekerja melalui peretasan perangkat yang dirancang untuk menghambat aktivitas kemanusiaan, yang pada akhirnya mencederai prinsip demokrasi dan supremasi hukum. Sebagai taktik yang kian sentral, *Surveilans* tersebut menjadi instrumen utama negara dalam

[1] Amnesty International UK, "Evidence of Global Opposition to US Mass Surveillance," 16 Januari, 2026, https://www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq. Diakses pada 16 Desember 2025

membungkam perbedaan pendapat secara luas dan terorganisir, terutama melalui penggunaan perangkat lunak mata-mata (*Spyware*) seperti Pegasus produksi NSO Group maupun teknologi serupa lainnya Teknologi *Spyware* merupakan teknik yang ampuh dan fleksibel yang kehadirannya justru menjadi ancaman yang unik dan serius terhadap privasi dan keamanan.[2] Pada 2021, Forbidden Stories dan Amnesty International melalui *Pegasus Project* memperoleh akses daftar daftar berisi 50.000 nomor telepon yang dipilih sebagai target oleh klien NSO Group. Dari analisis terhadap daftar tersebut, terungkap identitas lebih dari 1.000 individu yang tersebar di lebih dari 50 negara. Para target tersebut mencakup figur penting, termasuk anggota keluarga kerajaan Arab, 65 eksekutif bisnis, 85 aktivis HAM, 189 jurnalis, serta lebih dari 600 politisi dan pejabat pemerintah, termasuk menteri kabinet, diplomat, hingga personel militer dan keamanan.[3]

---

[2] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure" (Amnesty International Ltd, 2021).

[3] Steven Feldstein dan Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*, Carnegie Endowment for International Peace, 14 Maret 2023, https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses.

Pegasus, produk unggulan NSO Group saat ini mungkin merupakan bentuk *Spyware* paling canggih di pasaran. Perangkat lunak ini dapat mengumpulkan semua data dari perangkat target dari jarak jauh, termasuk foto dan video, berkas, teks, kontak, dan log panggilan. Perangkat lunak ini dapat mengendalikan kamera dan mikrofon ponsel pintar untuk melihat dan mendengarkan target, serta memantau lokasi, mencatat penekanan tombol, dan menyadap panggilan telepon atau video.[4]

Bahkan dalam perkembangannya, perangkat *Surveilans* tidak lagi sebatas mengendalikan berbagai aplikasi pada ponsel pintar, namun dalam praktik yang lebih ekstrem penggunaannya ini dapat disalahgunakan sebagai perangkat untuk menargetkan masyarakat sipil, seperti membunuh puluhan ribu warga sipil yang terjadi di Gaza, Palestina. Situasi genosida di Palestina membuktikan perangkat lunak mata-mata adalah senjata perang yang mengancam tidak hanya warga Palestina di Gaza,

[4] Mike Sexton, "What Is Spyware and Why Should Policymakers Care?," Third Way, 9 Maret 2023, https://www.thirdway.org/memo/what-is-spyware-and-why-should-policymakers-care. Diakses pada 6 Agustus 2025

tetapi seluruh umat manusia.[5] Perusahaan-perusahaan Israel seperti NSO Group, Candiru, Intellexa, Paragon, dan lainnya telah menciptakan *Spyware* kelas militer, seperti Pegasus, Predator, dan Graphite, yang dapat menyusup ke ponsel, mengekstrak data pribadi, dan bahkan mengubah menjadi perangkat *Surveilans*. Teknologi ini dilaporkan telah diuji coba di lapangan pada warga Palestina oleh unit intelijen Israel sebelum dikomersialkan dan dipasarkan secara global. *Spyware* adalah senjata yang digunakan oleh rezim otoriter dan rezim yang menyebut diri mereka "demokratis" untuk membungkam perbedaan pendapat dan oposisi, menargetkan jurnalis dan pengacara, serta merobek-robek rajutan nilai-nilai HAM.[6]

Teknologi *Surveilans* baru ini yang sebagian besar dikembangkan oleh perusahaan swasta tidak diatur dan tidak transparan. Titik kritis ini memungkinkan peretas untuk menyusup ke ponsel pintar dari jarak jauh tanpa sepengetahuan individu yang menjadi target. Setelah masuk ke dalam ponsel, Pegasus dapat mengaktifkan kamera dan mikrofon,

---

[5] "The Dangerous Rise of Military-Grade Spyware – a Global Day of Action," BDS Movement, 18 Juni 2025, https://bdsmovement.net/Global-Day-Action-Against-Spyware. Diakses pada 31 Desember 2025.

[6] "The Dangerous Rise of Military-Grade Spyware – a Global Day of Action."

serta mencuri data, termasuk komunikasi, gambar, dan video. Senjata-senjata ini melakukan *Surveilans* yang ditargetkan dan invasif dalam skala yang tidak terbayangkan sebelum munculnya perangkat tersebut. Industri perangkat lunak mata-mata negara tersebut telah diuntungkan dari *Surveilans* setiap aspek kehidupan Palestina. Selanjutnya pengalaman itu oleh sektor swasta dijadikan sebagai dasar untuk merancang, mengembangkan, dan mengekspor teknologi ini ke seluruh dunia, baik ke negara demokratis maupun negara otoritarian. Warga Palestina di wilayah pendudukan kerap menjadi kelinci percobaan dalam pengembangan dan pengujian teknologi militer Israel. Perangkat lunak mata-mata adalah bagian inti dari gambaran ini. Teknologi yang telah teruji terhadap warga Palestina tersebut kemudian dipasarkan secara global dengan klaim *'battle-tested'* guna menarik minat pembeli internasional.[7]

Situasi ini memperlihatkan risiko *Surveilans* yang semakin tinggi seiring pemanfaatan dan penggunaan

[7] Antony Loewenstein, "How Palestine Became Israel's Spyware Test-bed," New Internationalist, 19 Oktober 2023, https://newint.org/features/2023/10/02/spy-games. Diakses pada 31 Desember 2025.

teknologi *Spyware* di tahun-tahun mendatang. Pada saat yang sama teknologi ini tersedia secara komersial dan penggunaannya oleh pemerintah semakin meluas. Organisasi dan individu kemungkinan besar akan kesulitan untuk mencegah dan mengidentifikasi *Spyware* pada perangkat mereka.[8]

Menurut data Carnegie Endowment for International Peace antara tahun 2011 dan 2023, setidaknya terdapat 74 pemerintah melakukan kontrak dengan perusahaan komersial untuk memperoleh perangkat lunak mata-mata atau teknologi forensik digital. Rezim otokratis jauh lebih mungkin membeli perangkat lunak mata-mata komersial atau forensik digital daripada negara demokrasi. Kecenderungan ini terlihat adanya hubungan kontraktual 44 rezim yang diklasifikasikan sebagai otokrasi tertutup atau otokrasi elektoral memperoleh teknologi *Surveilans* yang ditargetkan antara tahun 2011 dan 2023, dibandingkan dengan 30 negara demokrasi elektoral atau demokrasi liberal.[9] Temuan Dragonfly Intelligence memperkuat

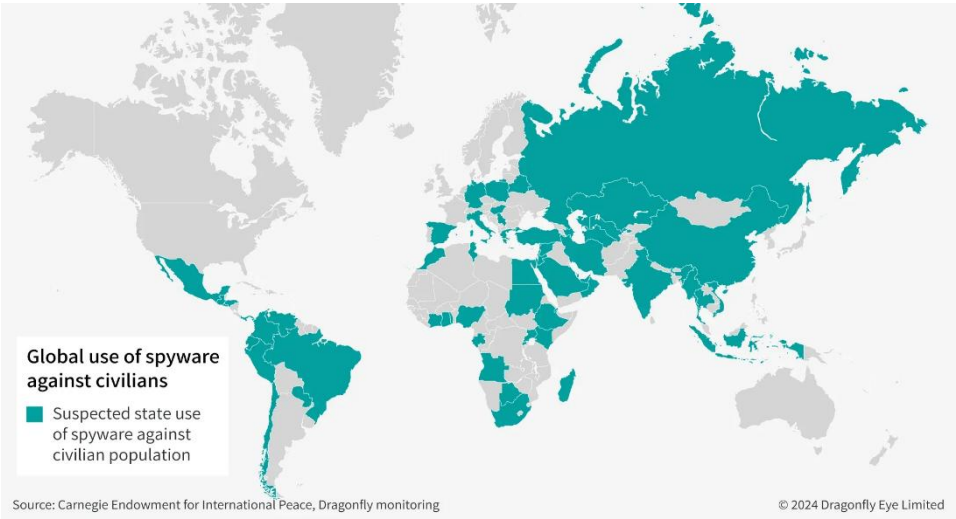
[8] "Risks to organisations from spyware," *Dragonfly Intelligence*, 27 Juni 2024, https://dragonflyintelligence.com/news/global-risks-to-organisations-from-spyware/. Diakses pada 31 Desember 2025

[9] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

fenomena kecenderungan pemerintahan otoriter untuk menargetkan individu yang bekerja di bidang jurnalisme dan organisasi masyarakat sipil (lembaga swadaya masyarakat) dengan memanfaatkan teknologi *Spyware*. *Spyware* biasanya disebarkan melalui taktik spear-phishing, di mana korban dikirimi pesan berisi tautan berbahaya guna menginfeksi perangkat mereka. Otoritas di banyak negara kemungkinan telah memanfaatkan teknologi *Spyware* yang ditujukan bagi individu-individu atau organisasi yang bekerja pada isu yang dianggap sensitif secara politik oleh pemerintah otoriter, seperti isu-isu hak asasi manusia (HAM), pencari suaka politik, atau korupsi. Menurut analisis Dragonfly Intelligence, Azerbaijan, Mesir, Indonesia, Yordania, Kazakhstan, dan Arab Saudi teridentifikasi sangat termotivasi untuk menggunakan *Spyware* terhadap individu dan organisasi di tahun-tahun mendatang.[10]

[10] Dragonfly Intelligence, "Global Risks to Organisations from Spyware," *Dragonfly Intelligence*, 24 Juni 2024, https://dragonflyintelligence.com/news/global-risks-to-organisations-from-spyware/. Diakses pada 13 Agustus 2025

Peta di bawah ini memetakan negara-negara yang diduga menyalahgunakan *Spyware* untuk pengawasan intelijen terhadap warga sipil yang dilandasi motif politik. Hal ini didasarkan pada kumpulan data tentang penggunaan *Spyware* komersial dan penelitian CitizenLab.[11]



Dukungan dari luasnya basis pelanggan pemerintah di pasar global memperkuat posisi perusahaan penyedia perangkat ini, meskipun terdapat berbagai upaya regulasi yang menargetkan rantai pasok *Spyware*. Komersialisasi industri *Spyware*

[11] Dragonfly Intelligence, "Global Risks to Organisations from Spyware."

tersebut tercermin melalui fakta-fakta berikut:[12]

1) Dari 195 negara di dunia, setidaknya 80 negara diketahui telah membeli *Spyware* dari vendor komersial;

2) Sebanyak 14 dari 27 negara anggota Uni Eropa teridentifikasi telah membeli *Spyware* dari satu vendor tunggal, yakni NSO Group;

3) Vendor *Spyware* terindikasi terlibat dalam 50 persen dari total eksploitasi zero-day sepanjang tahun 2023. Angka ini mencakup 64 persen dari seluruh eksploitasi yang menyasar perangkat lunak seluler serta peramban;

4) Meski pendapatan tahunan industri ini sulit dipastikan, skala ekonominya sangat besar; salah satu vendor bahkan pernah memper timbangkan valuasi IPO sebesar $2 miliar.

Israel merupakan eksportir utama teknologi *Spyware* dan alat forensik digital yang tercatat dalam basis data inventaris global. Terdapat 56 dari 74 pemerintah telah membeli *Spyware* komersial dan

[12] Jen Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights" (Atlantic Council, September 4, 2024).

teknologi forensik digital dari perusahaan yang berbasis di atau terhubung ke Israel, seperti NSO Group, Cellebrite, Cytrox, dan Candiru. Selain vendor *Spyware* komersial papan atas seperti NSO Group dan Cytrox, kini berkembang lapisan pemasok sekunder yang mencakup perusahaan *Spyware* spesialis, operasi peretas bayaran, perantara eksploitasi, serta entitas sejenis lainnya. Ketika perusahaan komersial besar menghadapi pengawasan yang lebih ketat dari pemerintah demokratis, pada saat bersamaan terdapat peningkatan permintaan *malware* sumber terbuka dan yang tersedia secara komersial. Kecenderungan ini telah menghasilkan teknologi *Spyware* dengan biaya yang lebih murah bagi pemerintah maupun aktor swasta untuk melakukan serangan dan memungkinkan mereka bersembunyi dalam "kebisingan" kode sumber *Spyware* yang terbuka.[13] Pada sisi yang lain, Israel sebagai pengekspor *Spyware* terkemuka belum cukup memprioritaskan pertimbangan HAM dalam rezim perizinan ekspornya.[14]

Industri *Surveilans* beroperasi secara tertutup,

[13] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

[14] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

meskipun ada seruan berulang untuk transparansi dan akuntabilitas yang lebih besar. Minimnya transparansi ini merupakan tantangan mendasar dalam menuntut akuntabilitas atas pelanggaran HAM yang timbul dari penggunaan *Spyware* tersebut. Tanpa informasi lebih lanjut tentang industri *Surveilans*, misalnya (1) yurisdiksi tempat beroperasinya; (2) identitas dan kepemilikan perusahaan yang memfasilitasi *Surveilans* pemerintah; (3) kemampuan yang ditawarkan; (4) skala penyebaran; atau (5) detail uji tuntas perusahaan atau upaya pemulihan, mustahil untuk memastikan cakupan penuh risiko HAM yang ada, mengurangi risiko tersebut, atau mencari pemulihan ketika terjadi pelanggaran. Pelapor Khusus PBB tentang kebebasan berpendapat dan berekspresi dalam laporannya pada 2019 mencatat, berbagai tuduhan yang berdasar menunjukkan bahwa banyak perusahaan menjual alat pengintai kepada pemerintah untuk memata-matai jurnalis, aktivis, dan tokoh oposisi, serta pihak lain yang memainkan peran penting dalam demokrasi. Karena tuduhan ini sangat serius, perusahaan dituntut untuk terbuka mengenai siapa rekan bisnis mereka dan bagaimana proses kerja mereka.[15]

[15] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."

Lebih jauh, kini industri *Spyware* dan forensik digital global telah memperkuat kapasitas pemerintah demokratis dan otoriter untuk melakukan intrusi tingkat lanjut. Carnegie Endowment for International Peace mengidentifikasi vendor dan klien utama dalam industri *Spyware* global dan menyoroti hubungan antara pemerintah dan pemasok perangkat lunak intrusi.[16] Indonesia dalam data Carnegie Endowment for International Peace, telah menggunakan *Spyware* yang diproduksi FinFisher yang berasal dari Jerman pada 2015. Perangkat sadap ini digunakan untuk mempersekusi kelompok minoritas agama dan kelompok LGBT. Selain itu, antara 2021-2022 Indonesia juga mempergunakan produk dari Candiru, NSO Group, dan Cytrox yang berasal dari Israel. Sebelumnya pada 2020, selain *Spyware*, Indonesia juga mempergunakan teknologi forensik digital yang diproduksi Cellebrite asal Israel.[17] Indikasi penggunaan alat sadap di Indonesia

[16] Steven Feldstein dan Brian Kot, "Mapping the Shadowy World of Spyware and Digital Forensics Sales," *Carnegie Endowment for International Peace*, 27 Februari 2023. https://carnegieendowment.org/features/commercial-spyware?lang=en. Diakses pada 31 Desember 2025

[17] Feldstein dan Kot, "Mapping the Shadowy World of Spyware and Digital Forensics Sales"

juga diungkap oleh Konsorsium IndonesiaLeaks, yang beranggotakan antara lain *Tempo*, jaringan jurnalis global *Forbidden Stories* serta *Organized Crime and Corruption Reporting Project* (*OCCRP*) menemukan operasi *Spyware* Pegasus di Indonesia.[18]

Penelitian Amnesty International mengonfirmasi keberadaan Pegasus yang mengancam ruang sipil di Indonesia. Penelitian ini menemukan bahwa Kepolisian Negara Republik Indonesia (Polri) dan Badan Siber dan Sandi Negara (BSSN) dalam kurun waktu 2017–2023 mengimpor teknologi *Spyware* dari Israel, Yunani, Singapura, dan Malaysia. Pemasok teknologi *Spyware* ke Indonesia, antara lain Q Cyber Technologies yang memiliki keterkaitan dengan NSO Group, konsorsium Intellexa, Saito Tech (Candiru), FinFisher dan anak perusahaan Raedarius M8 Sdn Bhd, dan Wintego Systems. Lembaga-lembaga negara tersebut melakukan pengadaan teknologi *Surveilans* dan *Spyware* melalui perusahaan perantara yang berbasis

---

[18] M. Khory Alfarizi, "Fakta-Fakta Pegasus, Spyware Canggih Yang Disebut Masuk Indonesia," *Tempo*, 20 Juni 2023,https://www.tempo.co/politik/fakta-fakta-pegasus-spyware-canggih-yang-disebut-masuk-indonesia-175195. Diakses pada 31 Desember 2025.

di Singapura. Pencatatan pihak ketiga sebagai pemilik administratif dalam dokumen resmi ini menciptakan hambatan serius dalam mengidentifikasi pemilik yang sebenarnya. Pemanfaatan struktur hukum tersebut memperumit verifikasi rantai pasok teknologi *Surveilans* ini. Kekaburan ini melumpuhkan fungsi pengawasan dalam proses pengadaan barang dan jasa publik karena identitas vendor asli menjadi sulit terlacak.[19]

Selain Pegasus yang diproduksi NSO Group, *Spyware* Predator dari Cytrox, menjadi pilihan favorit bagi banyak pemerintah dan baru-baru ini menjadi subjek investigasi di Yunani, menyusul pengungkapan operator pemerintah menggunakan *malware* Predator untuk meretas ponsel jurnalis Thanasis Koukakis dan pemimpin oposisi serta anggota Parlemen Eropa Nikos Androulakis. Selain Yunani, operator yang didukung negara di Armenia, Pantai Gading, Mesir, Indonesia, Madagaskar, Serbia, dan Spanyol kemungkinan juga menggunakan Predator.[20] Perangkat *Spyware* yang sangat invasif ini dirancang bersifat rahasia dengan

[19] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia," 2024.

[20] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

meninggalkan jejak minimal sehingga sangat sulit untuk terdeteksi. Konsekuensi lebih jauh, situasi ini berisiko menciptakan impunitas yang disengaja untuk pelanggaran hak-hak seperti, hak atas kebebasan berekspresi, berkumpul dan berasosiasi secara damai, keamanan pribadi, dan kebebasan dari penahanan sewenang-wenang.[21] Sementara itu, banyak negara belum memiliki kerangka legislasi yang kuat untuk melindungi warga negara yang berpotensi menjadi korban penyalahgunaan perangkat lunak mata-mata dan teknologi *Surveilans* lainnya yang sangat invasif ini. [22] "Hingga saat ini, Indonesia belum memiliki kerangka legislasi khusus yang mengatur legalitas penggunaan *Spyware* dan teknologi *Surveilans*. Regulasi yang paling relevan saat ini masih terbatas pada aturan penyadapan untuk penegakan hukum sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah beberapa kali diubah, terakhir melalui Undang-Undang Nomor 1 Tahun 2024.[23]

---

[21] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

[22] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia."

[23] Menurut undang-undang ini penyadapan adalah kegiatan mendengarkan, merekam, mengalihkan, mengubah, menghalangi dan/atau

Cakupan dan ragam teknologi *Surveilans* yang tersedia saat ini belum pernah terjadi sebelumnya dalam sejarah manusia karena memungkinkan untuk memantau dan melacak lokasi, komunikasi, riwayat penelusuran individu atau kelompok dalam skala besar. Cakupan *Surveilans* yang semakin luas ini dimungkinkan oleh lompatan terbaru dalam kemampuan teknologi digital dan dipicu oleh peristiwa global, seperti pandemi Covid-19. Menurut Neil M. Richards saat ini manusia tengah memasuki era pengawasan *(age of surveillance)*.[24] Penggunaan teknologi *Surveilans* kini tidak lagi didominasi oleh negara otoriter, tetapi juga telah meluas ke negara-negara demokratis. Fenomena ini menciptakan risiko global terhadap privasi dan hak asasi manusia, karena pengawasan ketat kini terjadi di hampir semua model pemerintahan. *Surveilans* massal juga tidak lagi terbatas dilakukan oleh badan intelijen. *Surveilans* ini tertanam dalam kemitraan publik-swasta, *platform* konsumen, dan kota pintar yang seringkali

mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang bukan bersifat publik, baik melalui jaringan komunikasi kabel maupun jaringan nirkabel, seperti radiasi elektromagnetik atau transmisi frekuensi radio.

[24] Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review*, Vol. 126:1934, 2013, hlm. 1936

diimplementasikan tanpa pengawasan hukum yang memadai atau debat publik yang berarti. Dari kamera pengenalan wajah di jalan-jalan perkotaan hingga algoritma kepolisian prediktif yang menargetkan populasi tertentu, teknologi *Surveilans* telah mencapai tingkat pervasif yang menantang batas-batas pelindungan HAM. Era pasca Edward Snowden memicu kesadaran global tentang praktik *Surveilans* yang didorong oleh negara. Namun, satu dekade kemudian, aktor swasta telah menjadi sama pentingnya dalam membangun dan memelihara infrastruktur *Surveilans* digital global. Perangkat *Surveilans* komersial dijual kepada pemerintah dengan catatan pelanggaran HAM yang buruk dan perusahaan multinasional mengumpulkan, berbagi, dan memonetisasi data pribadi dalam skala yang belum pernah terjadi sebelumnya. *Surveilans* bukan lagi perangkat luar biasa yang digunakan dalam konteks berisiko tinggi. *Surveilans* kini telah menjadi rutinitas, dinormalisasi, dan sering kali tidak transparan.[25]

Alasan utama penggunaan teknologi *Surveilans*

[25] Edmarverson A. Santos, "Human Rights and the Global Digital Surveillance Infrastructure," *Diplomacy and Law* (blog), 3 Juli 2025, https://www.diplomacyandlaw.com/post/human-rights-and-the-global-digital-surveillance-infrastructure. Diakses pada 16 Desember 2025

telah lama didasarkan pada janji peningkatan keamanan. Pemerintah dan aktor swasta seringkali membela penggunaan pemindai biometrik, sistem pengenalan wajah, dan perangkat *Surveilans* berbasis kecerdasan artifisial sebagai respons yang diperlukan terhadap terorisme, kejahatan, dan keresahan sosial. Pembenaran ini dibangun di atas dikotomi kebebasan *versus* keamanan sehingga menyederhanakan masalah yang sangat kompleks dan mengaburkan fungsi *Surveilans* yang berkembang dalam masyarakat kontemporer. Seiring dengan perluasan infrastruktur digital, kemampuan *Surveilans* tumbuh tidak hanya dalam skala tetapi juga dalam tujuan karena tidak lagi terbatas pada ranah kontra-terorisme atau penegakan hukum. *Surveilans* dalam praktiknya saat ini juga melayani berbagai tujuan administratif, komersial, dan politik. Pergeseran ini membutuhkan pembingkaian ulang perdebatan bahwa *Surveilans* bukan hanya perangkat keamanan, tetapi juga mekanisme kontrol. Lebih jauh, penggunaan *Surveilans* untuk rekayasa sosial dan perilaku semakin terlihat baik dalam rezim demokratis maupun otoriter. Sistem berbasis kecerdasan artifisial digunakan untuk mendeteksi perilaku "pra-kejahatan", menilai kelayakan kredit, mengelola akses kesejahteraan, dan menekan perbedaan pendapat. Fungsi-fungsi ini,

meskipun disajikan sebagai alat tata kelola, sering kali bergantung pada algoritma yang tidak transparan dan praktik pengumpulan data yang tidak diatur yang mengikis kepercayaan publik dan mereduksi individu menjadi titik data dalam matriks risiko.[26]

Industri *Spyware* telah menjadi salah satu ancaman terbesar bagi masyarakat sipil, HAM, dan demokrasi saat ini. Fenomena ini muncul di tengah upaya berbagai negara menghadapi penyebaran instrumen *Surveilans* invasif yang beroperasi tanpa regulasi yang memadai.[27] Penggunaan teknologi *Surveilans* seperti *Spyware* tidak hanya menimbulkan risiko pelanggaran hak atas privasi, hak atas ekspresi, hak atas kebebasan berkumpul secara damai secara langsung, tetapi pada saat bersamaan juga menghalangi orang-orang menggunakan hak mereka di masa mendatang. Teknologi *Spyware* merupakan jenis perangkat lunak berbahaya yang dipergunakan untuk mengumpulkan informasi dari suatu perangkat tanpa memberi tahu pengguna dan mengirimkannya

[26] Santos, "Human Rights and the Global Digital Surveillance Infrastructure."

[27] Leyland Cecco, "Spyware Is Huge Threat to Global Human Rights and Democracy, Expert Warns," *The Guardian*, 10 Agustus 2022, https://www.theguardian.com/world/2022/aug/09/spyware-canada-threat-democracy-human-rights. Diakses pada 6 Agustus 2025

ke entitas lain yang tidak berwenang. Teknologi ini sangat invasif karena memungkinkan akses tidak terbatas ke suatu perangkat secara otomatis dan meninggalkan jejak yang sangat minim sehingga hampir mustahil bagi pengguna untuk mengetahui data apa yang telah diambil.[28]

Teknologi *Spyware* seringkali disebut sebagai teknologi intersepsi yang sah (*lawful interception technologies*), konsekuensi logisnya kemudian produk-produk ini sangat rentan disalahgunakan. Pada sisi yang lain, sampai saat ini, belum ada kerangka kerja untuk mencegah penyalahgunaan tersebut dan tidak ada konsekuensi ketika teknologi tersebut digunakan. Perusahaan-perusahaan yang menjual teknologi yang sangat berbahaya lolos begitus saja tanpa hukuman apa pun. Kondisi ini menunjukkan perlu ada pengaturan yang tepat tentang penggunaan teknologi *Spyware* yang dipandu oleh prinsip-prinsip HAM untuk memastikan pelanggaran hak tidak lagi terjadi. [29]

---

[28] Amnesty International, A Web of Surveillance: Unravelling A Murky Network Of Spyware Exports To Indonesia, hlm. 7.

[29] Amnesty International, "When Is Targeted Surveillance Wrong?," 10 Agustus 2023, https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/. Diakses pada 16 Desember 2025.

Teori Michel Foucault yang berkaitan dengan *Surveilans* dikonstruksi berdasarkan relasi pengetahuan-kekuasaan, dan pembentukan kebenaran melalui proses pengarsipan. Pendekatan ini menawarkan lensa yang relevan untuk mengungkap struktur kontrol yang telah tertanam dalam praktik bukti digital. David Lyon mendefinisikan *Surveilans* sebagai perhatian yang terfokus, sistematis, dan rutin terhadap detail pribadi untuk tujuan pengaruh, manajemen, pelindungan, atau pengarahan. *Surveilans* menciptakan relasi antara otoritas (prinsipal) dan individu (subjek) yang dipantau melalui 'tatapan' pengawasan. Kondisi ini memicu pola perilaku antisipatif, di mana subjek secara proaktif menyesuaikan tindakannya agar sejalan dengan ekspektasi otoritas dan melakukan sensor mandiri terhadap perilaku yang dianggap tidak diinginkan. Konsep panoptikon yang diusulkan Michael Foucault, yang berasal dari desain penjara yang diinisiasi Jeremy Bentham berpusat pada internalisasi kontrol melalui *Surveilans*. Penggunaan kerangka ini penting karena *Surveilans* bukanlah pasif, maupun netral. Carissa Véliz menyatakan penerapan *Surveilans* terhadap seseorang merupakan manifestasi tindakan dominasi. Dengan kata lain, *Surveilans* sangat terkait dengan sistem penindasan, termasuk rasisme dan

kolonialisme. Teori *Surveilans* membahas dinamika kekuasaan yang tersirat dalam bukti digital, yaitu kekuasaan dipegang oleh pihak yang berwenang untuk menentukan melalui algoritma dan insentif lainnya informasi apa yang diprioritaskan, dihargai, dan bahkan dianggap benar. Sementara itu, individu yang ditargetkan pengalamannya terefleksikan dalam bukti digital yang mungkin mengalami perampasan hak. Kerugian dan penderitaan yang tercakup dalam bukti digital dan konten digital tidak mendapatkan respons yang berarti. Sistem hukum internasional yang tidak responsif dalam menghadapi begitu banyak bukti. Fenomena ini mengindikasikan bahwa kendali atas bukti dan konten digital telah menjadi instrumen kekuatan global yang menciptakan bentuk dominasi tersendiri.[30]

Dalam keadaan terbatas, penggunaan teknik *Surveilans* yang invasif dapat dibenarkan, seperti mencegah atau menyelidiki kejahatan serius tertentu

[30] Chris Carpenter, "Symposium on Forensic and Counter-Forensic Approaches to International Law: Digital Evidence and the Gaze – a Conceptual Framework for Analyzing Digital Evidence Through a Foucauldian Lens," Opinio Juris, 16 Maret 2026, https://opiniojuris.org/2025/12/10/symposium-on-forensic-and-counter-forensic-approaches-to-international-law-digital-evidence-and-the-gaze-a-conceptual-framework-for-analyzing-digital-evidence-through-a-foucauldian-lens/. Diakses pada 16 Desember 2025.

atau tindakan yang merupakan ancaman serius terhadap keamanan nasional. Hukum internasional menyatakan tindakan *Surveilans* yang ditargetkan harus dirancang secara sempit untuk menyelidiki individu tertentu yang dicurigai melakukan kejahatan serius atau tindakan yang mengancam keamanan nasional. Perangkat *Spyware* harus digunakan sebagai upaya terakhir, setelah semua tindakan yang kurang invasif telah dilakukan atau telah terbukti tidak efektif. Meskipun demikian, durasi serta cakupan penggunaan perangkat *Spyware* harus dibatasi secara ketat hanya pada data yang relevan. Dengan kata lain, pemerintah harus mematuhi prinsip-prinsip legalitas, berdasarkan kebutuhan, dan proporsionalitas ketika menggunakan teknologi *Surveilans*.[31]

Namun demikian, realita justru memperlihatkan pemerintah jarang mematuhi standar ini. Negara tetap mengeksploitasi alasan keamanan nasional atau ketertiban umum untuk memberikan keleluasaan yang luas kepada lembaga penegak hukum untuk menggunakan perangkat lunak invasif terhadap berbagai target, dan sedikit memperhatikan prinsip-prinsip kebutuhan dan proporsionalitas. Setelah

[31] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

lembaga-lembaga tersebut memperoleh perangkat *Spyware* hanya ada sedikit pengaman yang mengatur penggunaannya. David Kaye, pelapor khusus PBB untuk kebebasan berpendapat dan berekspresi mengatakan:[32]

> *"Tidak cukup hanya mengatakan bahwa sistem komprehensif untuk pengendalian dan penggunaan teknologi Surveilans yang ditargetkan telah rusak. Sistem tersebut hampir tidak ada. Meskipun hukum HAM memberikan batasan yang jelas terhadap penggunaan perangkat Surveilans, negara-negara tetap melakukan Surveilans ilegal tanpa takut akan konsekuensi hukum. Kerangka hukum HAM sudah ada, tetapi kerangka kerja untuk menegakkan batasan tersebut belum ada."*

Dalam konteks ini, Pelapor Khusus PBB tentang hak atas kebebasan berkumpul secara damai dan berserikat menyatakan:[33]

---

[32] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

33 International Commission of Jurists, "Digital Technologies and Human Rights: a Legal Framework" (International Commission of Jurists, May 2022), hlm. 4.

"Bagi banyak orang yang menjadi bagian dari masyarakat sipil, internet bukan lagi tempat yang aman, karena mereka telah menjadi target Surveilans dan kekerasan daring yang semakin meningkat. Tindakan ini sering dilakukan oleh agen negara, tetapi difasilitasi oleh penyedia layanan internet swasta."

Setelah bertahun-tahun pengumpulan bukti yang menunjukkan dampak negatif teknologi *Surveilans* digital terhadap HAM, mulai dari laporan penggunaan peralatan pengawasan perusahaan Prancis Amesys di Libya selama Musim Semi Arab hingga pengungkapan terkini tentang penargetan jurnalis secara global, Pelapor Khusus PBB tentang kebebasan berpendapat dan berekspresi baru-baru ini menyimpulkan bahwa industri *Surveilans* terus menyediakan layanannya tanpa pengawasan dan hampir tanpa hukuman.[34]

[34] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."

Terdapat beberapa pendekatan hukum menurut George T. Papademetriou untuk membatasi kemampuan perusahaan *Surveilans* swasta untuk memfasilitasi pelanggaran HAM.

1) Mempertegas penerapan instrumen HAM internasional terhadap perlindungan privasi.

2) Memperketat pengawasan domestik melalui kontrol ekspor dan sanksi: Menciptakan mekanisme penegakan hukum nasional yang lebih kuat melalui rezim kontrol ekspor serta penerapan sanksi pidana bagi penyalahgunaan teknologi.

3) Memperluas akses pemulihan bagi korban: Membuka peluang yang lebih besar bagi korban untuk menuntut ganti rugi di tingkat domestik melalui jalur gugatan perdata (litigasi) terhadap vendor atau perusahaan terkait.

Instrumen-instrumen HAM inti ini sudah ada sebelum teknologi internet berkembang secara revolusioner dan tidak mengantisipasi dampak transformatif yang akan ditimbulkan oleh komunikasi global terhadap kehidupan sehari-hari. Upaya yang lebih baru untuk memperbarui hukum HAM untuk

merespons perubahan-perubahan tersebut yang menghasilkan beberapa kemajuan dalam mengisi kesenjangan tersebut, termasuk menyoroti pentingnya hak atas privasi dalam ekosistem teknologi digital.[35] Kemudian pengembangan pelindungan hukum internasional menghadapi tantangan lain terkait implementasi pada ranah hukum domestik. Meskipun beberapa dokumen, termasuk Laporan Pelapor Khusus untuk Kebebasan Berekspresi, David Kaye pada 2019

[35] Pada 2015, Kantor Komisioner Tinggi Hak Asasi Manusia membentuk Pelapor Khusus tentang Hak atas Privasi, yang bertujuan untuk "meningkatkan kesadaran mengenai pentingnya mempromosikan dan melindungi hak atas privasi, termasuk dengan mempertimbangkan tantangan-tantangan khusus yang muncul di era digital. Resolusi Dewan Hak Asasi Manusia pada tahun 2017, 2018, dan 2019 meletakkan dasar bagi Resolusi Majelis Umum yang inovatif tentang Privasi di Era Digital pada tahun 2020.79 Resolusi ini mengidentifikasi beberapa kekhawatiran khusus tentang privasi dalam konteks digital, termasuk kebutuhan bagi negara untuk mempertahankan mekanisme pengawasan yang memadai yang memastikan akuntabilitas atas pengawasan negara terhadap komunikasi, dan untuk memberikan solusi yang efektif ketika terjadi pelanggaran. Resolusi ini mengidentifikasi beberapa kekhawatiran spesifik tentang privasi dalam konteks digital, termasuk kebutuhan negara untuk mempertahankan mekanisme pengawasan yang memadai yang memastikan akuntabilitas atas surveilans komunikasi yang dilakukan oleh negara dan memberikan pemulihan yang efektif ketika terjadi pelanggaran. Majelis Umum PBB menekankan peran penting yang dimainkan bisnis dalam menjaga hak atas privasi dan menyerukan kepada bisnis yang mengumpulkan data untuk memenuhi tanggung jawab mereka untuk menghormati privasi sesuai dengan Kerangka Kerja "Melindungi, Menghormati, dan Memberikan Pemulihan berdasarkan Prinsip-Prinsip Panduan PBB tentang Bisnis dan HAM. Lihat, George T. Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry," *Harvard Human Rights Journal* 36 (2023), hlm. 205-206

tentang *Surveilans* dan HAM, telah menegaskan bahwa pemerintah yang menggunakan perangkat *Surveilans* memiliki kewajiban untuk memastikan penggunaannya sesuai dengan kerangka hukum domestik yang memenuhi standar yang dipersyaratkan oleh hukum HAM internasional. Selain itu, jika secara formal telah terefleksikan dalam hukum domestik, dampak kewajiban HAM internasional terhadap individu akan bergantung pada kekuatan supremasi hukum dan independensi peradilan, yang bervariasi di setiap negara mengingat badan intelijen cenderung beroperasi secara sembunyi-sembunyi dan dengan pengawasan terbatas.[36]

Sementara itu, belum terbentuk konsensus internasional tentang bagaimana pemerintah harus menyeimbangkan privasi dengan keamanan untuk mengisi celah hukum yang ada. Upaya menutup kesenjangan hukum ini menjadi urgen bagi komunitas HAM internasional karena dua alasan:[37]

---

[36] Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry," hlm. 206-208.

[37] David Kaye dan lainnya yang terlibat dalam debat internasional tentang bagaimana negara dapat mematuhi kewajiban privasi mereka yang terlibat dan berpartisipasi dalam Forum seperti Dewan Hak Asasi Manusia atau Kelompok Pakar Pemerintah PBB untuk Memajukan Perilaku Negara yang Bertanggung Jawab di Dunia Maya dalam Konteks Keamanan Internasional

Pertama, meskipun hak atas privasi yang diakui secara internasional menciptakan kewajiban hukum tertentu bagi negara, kewajiban ini saat ini longgar dan memberikan ruang yang cukup besar untuk variasi dalam praktik negara. Serangkaian interpretasi otoritatif yang lebih ketat (misalnya, dengan memperbarui Komentar Umum 16 tentang hak atas privasi) akan memberikan komunitas internasional alat penting untuk mengidentifikasi dan mengutuk pemerintah dan perusahaan yang melanggar hak atas privasi.

Kedua, jika upaya ini tidak berhasil menciptakan instrumen hukum yang mengikat secara internasional, artikulasi dan kontestasi hak atas privasi dan kewajiban yang

(UN's Group of Governmental Experts for Advancing Responsible State Behaviour in Cyberspace in the Context of International Security) menjadi ruang bagi pemerintah untuk membahas isu-isu pelik dan mencapai konsensus tentang peran mengkhawatirkan perusahaan teknologi surveilans dalam memfasilitasi pelanggaran HAM. Dialog ini pada gilirannya dapat berkembang menjadi praktik negara, termasuk melalui pernyataan interpretatif yang berwenang dari pemerintah. Meskipun agak terbatas oleh kesediaan negara untuk melanggar norma ketika isu keamanan nasional dipertaruhkan, efek praktisnya tetap akan signifikan. Lihat, Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry."

> menyertainya di forum internasional memiliki efek normatif yang penting. Teori proses hukum transnasional menyatakan hukum HAM internasional, meskipun kurang ditegakkan, membentuk perilaku negara dalam tiga fase, yakni interaksi antar negara di mana norma-norma global diperdebatkan, interpretasi prinsip-prinsip hukum yang relevan, dan internalisasi oleh sistem hukum domestik.

Selanjutnya, pengendalian ekspor domestik dan sanksi pidana menyediakan serangkaian mekanisme lain untuk mengendalikan pelaku penyalahgunaan pemanfaatan teknologi *Spyware.* Upaya untuk mengontrol ekspor dan penetapan sanksi berdampak lebih langsung pada profitabilitas perusahaan *Spyware* dibandingkan instrumen HAM internasional. Meskipun demikian, beberapa faktor membatasi potensi transformatif dari pendekatan ini. *Pertama,* karena rezim kontrol ekspor berpotensi dikontestasikan dengan kepentingan politik, bukan komitmen prinsipil terhadap HAM. *Kedua,* mengandalkan sepenuhnya negara sebagai penegak hukum bermasalah karena pertimbangan birokrasi dan kelembagaan tidak mungkin memberikan sanksi kepada aktor swasta

yang memiliki hubungan dengan negara tersebut [38]

Kesulitan-kesulitan ini mencerminkan ketegangan yang mendalam dalam hubungan antara privasi dan keamanan dan mengungkapkan bahwa ketergantungan pada satu negara untuk bertindak sebagai penegak hukum global bukanlah solusi yang langgeng. Kekhawatiran yang lebih praktis dan terkait adalah tantangan sumber daya yang ditimbulkan oleh penegakan hukum. Upaya mempertahankan rezim peraturan yang ketat bergantung pada ketersediaan kapasitas untuk menyelidiki, menilai, dan menuntut perusahaan *Spyware* yang telah melanggar HAM. Upaya ini pada gilirannya bergantung pada alokasi pendanaan politik. [39]

Neil M. Richards mengidentifikasi empat prinsip

[38] Sebagai contoh Amerika Serikat, dalam kasus Edward Snowden, meskipun katalis penting bagi tantangan hukum terhadap program tersebut dan pada akhirnya dinyatakan melanggar hukum, namun penegak hukum di Amerika Serikat memiliki insentif yang kuat untuk mempertahankan hubungan dengan kontraktor swasta. Laporan yang menunjukkan bahwa Biro Investigasi Federal telah mencoba produk NSO Group dan CIA terus melakukan pengawasan di wilayah AS merupakan pengingat penting bahwa lembaga penegak hukum ini seringkali memilih privasi yang lebih sedikit atas nama keamanan nasional. Lihat, Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry."

[39] Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry."

yang memandu pengembangan hukum *Surveilans* (*surveillance law*) di masa depan untuk menciptakan keseimbangan antara biaya dan manfaat *Surveilans* pemerintah *(government surveillance). Pertama, Surveilans* melampaui batasan publik/pribadi. *Surveilans* publik maupun pribadi bermuara pada masalah yang sama, bukan sepenuhnya terpisah. Bahkan jika pada akhirnya titik perhatian difokuskan pada *Surveilans* pemerintah, maka solusi apa pun harus mengatasi kompleksitas hubungan antara *Surveilans* pemerintah dan korporasi. *Kedua, Surveilans* rahasia yang tidak sah dan pembuatan program *Surveilans* domestik apa pun yang keberadaannya dirahasiakan semestinya dilarang secara hukum. *Ketiga, Surveilans* total tidak sah dan gagasan pemerintah untuk merekam semua aktivitas internet tanpa izin semestinya juga dilarang secara hukum. *Surveilans* pemerintah terhadap internet dapat menyebabkan penyalahgunaan kekuasaan dan menyerang kebebasan dasar. Dalam konteks ini, seperti halnya penyadapan telepon, *Surveilans* harus melalui proses peradilan sebelum diizinkan. *Keempat, Surveilans* berbahaya karena mengancam privasi intelektual dan meningkatkan risiko pemerasan, paksaan, dan diskriminasi. Oleh karena itu, *Surveilans* merupakan tindakan berbahaya karena melanggar

konstitusionalitas kebebasan sipil yang mendasar. [40]

Penargetan *Surveilans* digital kepada pembela HAM karena pendapat atau pekerjaan yang mereka lakukan tidak pernah diperbolehkan menurut hukum HAM. Hal itu melanggar hak atas privasi, dan menghambat pelaksanaan kebebasan berpendapat dan berekspresi, terlepas dari apakah data atau komunikasi individu yang ditargetkan benar-benar dicegat. Seringkali sulit untuk membuktikan bahwa *Surveilans* semacam itu sedang terjadi dan menginfeksi perangkat digital atau data pribadi. Upaya infeksi *Spyware* terhadap pembela HAM yang ditargetkan memberikan indikasi pembela HAM telah menjadi sasaran *Surveilans* sekarang atau di masa mendatang. Hal ini menunjukkan Pemerintah perlu menetapkan langkah-langkah uji tuntas dan pelindungan melalui kerangka hukum hukum, baik legislasi maupun regulasi yang ada tidak memadai. Pada saat bersamaan, upaya infeksi perangkat digital pembela HAM menandakan adanya kegagalan dari pihak perusahaan yang memasok perangkat lunak, pemerintah negara asal perusahaan tersebut dan negara tempat *Surveilans* terjadi untuk mengatasi

[40] Richards, "The Dangers of Surveillance," hlm. 1935-1936.

penyalahgunaan perangkat *Spyware*.[41]

Global Justice Clinic, New York University School of Law menegaskan negara perlu menahan diri dan melindungi diri pembela HAM dari pelanggaran hak yang melanggar hukum tersebut dengan:[42]

1) Memastikan adanya kerangka hukum yang memadai untuk mengotorisasi penargetan tersebut, yang tunduk pada tinjauan yudisial independen;

2) Memberlakukan dan menegakkan undang-undang pengendalian ekspor yang mencegah penjualan perangkat lunak berbahaya dan bentuk senjata digital lainnya kepada pemerintah yang tidak memiliki pelindungan hukum minimal tersebut dalam hukum domestik mereka; dan

3) Melakukan uji tuntas yang kuat untuk memastikan, setidaknya, bahwa pembeli

[41] Global Justice Clinic, "Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights," 1 Maret 2019, hlm. 3.

[42] Global Justice Clinic, "Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights."

perangkat lunak tersebut oleh pemerintah memiliki pelindungan hukum dasar tersebut, memberikan dasar hukum untuk menargetkan individu tertentu dengan perangkat lunak *Surveilans* dan memberikan pelindungan prosedural kepada individu terhadap penargetan yang salah.

Dalam konteks Indonesia, Amnesty International melalui penelitiannya telah mendokumentasikan penggunaan *Spyware* untuk menargetkan individu tertentu. Meskipun Amnesty International mengakui tidak memiliki bukti bahwa perangkat *Spyware* telah digunakan untuk menargetkan anggota masyarakat sipil tertentu. Kesulitan ini tidak terlepas dari karakteristik perangkat *Spyware* yang memang dirancang bersifat rahasia sehingga sulit mendeteksi kasus penyalahgunaan perangkat *Spyware* tersebut. Oleh karena itu, situasi ini berisiko menciptakan impunitas pelanggaran HAM akibat penyalahgunaan perangkat ini. Amnesty International memberikan aksentuasi secara khusus kasus pembelian *Spyware* di Indonesia mengingat ruang sipil telah menyusut sebagai akibat serangan yang berkelanjutan terhadap hak atas kebebasan berekspresi, berkumpul dan berasosiasi secara damai, keamanan pribadi, dan

kebebasan dari penahanan sewenang-wenang. Selain itu, ketiadaan transparansi pengadaan perangkat *Spyware* pada dasarnya tidak sesuai dengan HAM sehingga pengadaan perangkat *Spyware* semestinya dilarang.[43]

Berdasarkan uraian pendahuluan di atas, penelitian ini mencoba melakukan analisis penggunaan perangkat *Spyware* oleh Pemerintah Republik Indonesia, penggunaan *Spyware* perlu diletakkan pada kecenderungan kemunduran demokrasi pada 2024. Indonesia telah mulai mengarah pada demokratisasi pasca 1998 seiring kejatuhan rezim Presiden Soeharto dan berlangsung hingga akhir tahun 2000-an. Namun, dalam satu dekade Pemerintahan Presiden Joko Widodo (2014-2024) demokrasi Indonesia terus mengalami kemunduran yang ditandai dengan meningkatnya polarisasi dan *illiberalisme*. Menurut V-Dem Institute situasi ini menunjukkan terjadinya peralihan dari negara demokrasi elektoral sejak tahun 1999 kini menuju zona abu-abu otokrasi elektoral (*autocratic grey zone autocracy*) pada 2024.[44]

---

[43] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia."

44 Fabio Angiolillo, Ana Good God, and Staffan I. Lindberg, "DEMOCRACY REPORT 2025: 25 Years of Autocratization – Democracy Trumped?" (V-Dem Institute, March 2025).

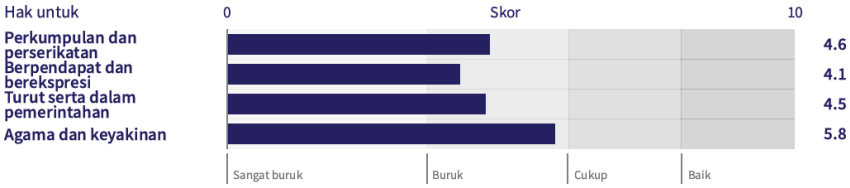
Kecenderungan penurunan demokrasi di Indonesia setidaknya dapat merujuk pada ancaman terhadap kebebasan berekspresi, kebebasan berkumpul secara damai, dan kebebasan berekspresi di Internet tanpa sensor merujuk pada data V-Dem Institute seperti terlihat pada diagram di bawah ini.[45]



[45] Kecenderungan penurunan indeks demokrasi terlihat pada laporan The Economist Intelligence Unit 2025, indeks demokrasi Indonesia 2024 kembali menurun dibandingkan 2023 sehingga masih berada dalam kategori demokrasi cacat. Dari lima dimensi yang diukur, skor terendah ada pada ranah kultur politik dan kebebasan sipil. Berdasarkan laporan The Economist Intelligence Unit (EIU) 2025 mengenai Indeks Demokrasi 2024, Indeks Demokrasi Indonesia mencapai skor 6,44 dari skala tertinggi 10. Raihan itu menempatkan Indonesia pada peringkat ke-59 dari total 167 negara yang diukur indeksnya. Dengan skor tersebut, Indonesia juga berada dalam kategori demokrasi cacat (*flawed democracy*). Posisi Indonesia dalam kategori demokrasi cacat bukan baru terjadi, namun terjadi dalam satu dekade terakhir. Hal ini menunjukkan kecenderungan skor Indeks Demokrasi Indonesia terus menurun.

Lihat Nino Citra Anugrahanto and Kurnia Yunita, "Satu Dekade Tren Indeks Demokrasi Indonesia Menurun," *Kompas.id*, 5 Maret 2025, https://www.kompas.id/artikel/satu-dekade-tren-indeks-demokrasi-indonesia-menurun. Diakses pada 9 Januari 2026.

Situasi HAM yang buruk yang dapat merujuk pada hasil penilaian The Human Rights Measurement Initiative (HRMI). Skor Pemberdayaan Indonesia sebesar 4,4 dari 10 yang menunjukkan bahwa di Indonesia banyak orang tidak dapat menikmati hak-hak sipil dan kebebasan politik mereka, termasuk kebebasan berbicara, berkumpul dan berserikat, serta hak demokratis. Dalam konteks ini, jika dibandingkan dengan negara-negara lain kinerja Indonesia lebih buruk dari rata-rata dalam hal hak-hak pemberdayaan. Skor pemberdayaan Indonesia menurut The Human Rights Measurement Initiative (HRMI) dapat dilihat melalui diagram berikut ini.[46]



[46] Human Rights Measurement Initiative (HRMI), "Indonesia: Rights Tracker," *RightsTracker.org*, https://rightstracker.org/country/IDN. Diakses pada 9 Januari 2026

Apabila merefleksikan tindakan represif dan teror bagi publik yang lantang mengkritik pelbagai kebijakan buruk pemerintah, maka pada 2026 kritik publik akan dibalas dengan tindakan represif yang justru diprediksi semakin menguat.[47] Selain itu, penelitian ini hendak menelisik bagaimana Pemerintah Republik Indonesia merespons penggunaan perangkat *Spyware* melalui pengembangan ekosistem kebijakan, khususnya pengadaan perangkat *Spyware* yang ditopang melalui anggaran publik. Pengadaan publik semestinya menjadi instrumen untuk mengatasi risiko HAM dalam penggunaan teknologi digital, termasuk perangkat *Spyware*. Penggunaan anggaran publik dalam pengadaan teknologi *Spyware* memiliki implikasi hukum yang bermuara pada akuntabilitas kepada publik pengadaan teknologi tersebut karena anggaran publik berasal dari pajak yang dibebankan kepada publik. Akuntabilitas menjadi tanggung jawab semua aktor yang terlibat dalam pengadaan teknologi *Spyware* dan menjadi jalan yang penting untuk pemulihan korban untuk meminta pertanggungjawaban kepada mereka yang menyebabkan pelanggaran HAM.

[47] Bagja Hidayat, "Indonesia 2026: Makin Riuh Makin Represif," *Tempo*, 4 Januari 2026, https://www.tempo.co/prelude/sampul-tempo-edisi-khusus-indonesia-2026-2104222. Diakses pada 8 Januari 2026.

B. Pertanyaan Penelitian

Berdasarkan uraian latar belakang tersebut di atas, penelitian ini berangkat dari beberapa rumusan masalah, sebagai berikut:

1. Bagaimana ekosistem penggunaan *Spyware* di Indonesia ?
2. Bagaimana dampak HAM dari penggunaan *Spyware* di indonesia ?
3. Bagaimana relasi antara negara dan sektor swasta dalam penggunaan *Spyware* dalam lanskap norma bisnis dan HAM untuk mengatur komersialisasi *Spyware* ?
4. Bagaimana mekanisme pertanggung jawaban penggunaan teknologi *Spyware* oleh aparat negara karena pengadaan teknologi tersebut ditopang oleh anggaran publik ?

C. Metode Penelitian

Penelitian ini menjadikan penelitian yang dilakukan Amnesty International dengan judul *A Web of Surveillance: Unravelling A Murky Network of Spyware Exports to Indonesia* sebagai rujukan. Namun demikian, penelitian ini mencoba mengangkat dimensi lain yang belum dielaborasi lebih jauh oleh Amnesty International yakni pengadaan barang publik (*public procurement*), teknologi *Spyware* ditelisik melalui perspektif anggaran publik berbasis pendekatan *human rights budgeting.* Tahapan penelitian pustaka berlangsung dari September 2025-Desember 2025. Temuan awal berdasarkan penelitian pustaka ini divalidasi melalui serangkaian fokus diskusi terpumpun (*focus group discussion*) dengan akademisi, peneliti, dan organisasi masyarakat sipil yang berfokus pada isu teknologi dan HAM, reformasi sektor keamanan, dan transparansi anggaran.

Oleh karena itu, penelitian ini didasarkan pada penelitian pustaka tentang irisan antara pemanfaatan dan penggunaan perangkat *Spyware* dan dampaknya

terhadap HAM. Selain itu, penelitian ini juga mencakup sumber non-akademik dengan merujuk pada laporan tematik serupa, pemberitaan mengenai perangkat *Spyware*, dan sumber-sumber lainnya. Untuk memperdalam gambaran tersebut, penelitian ini juga merujuk pada literatur akademik interdisipliner mengingat sifat dinamika komersialisasi perangkat *Spyware*. Analisis anggaran menjadi salah satu unit analisis pembelian perangkat *Spyware* karena dalam perspektif HAM, pengadaan barang atau jasa publik semestinya mempertimbangkan dan mengatasi risiko HAM serta memperkuat layanan publik yang penting. Telaah anggaran publik dapat dipergunakan untuk menelisik sejauh mana komitmen dan keberpihakan para pembuat kebijakan pengadaan publik, pembeli, dan manajer kontrak mempertimbangkan risiko dan pertimbangan HAM. Pemberian layanan publik yang penting merupakan cara bagi Negara untuk memenuhi kewajiban HAM.[48] Dalam kaitan penggunaan anggaran publik, semestinya penggunaan perangkat *Spyware* tidak ditujukan memata-matai warga negara, khususnya yang kritis terhadap kebijakan negara.

[48] Daniel Morris dan Cathrine Bloch Veiberg, "Public Procurement as a Tool to Address Human Rights Risk in the Use of Digital Technology to Deliver Essential Public Services" (Copenhagen K: The Danish Institute for Human Rights, Februari 2024).

Sistem pajak sangat penting mempertimbangkan perspektif HAM dan pendekatan berbasis HAM menjadikan sistem pajak lebih progresif, transparan, dan adil, dengan tujuan memerangi ketidaksetaraan, mengatasi perubahan iklim, membiayai layanan publik secara adil, mendorong pertumbuhan ekonomi inklusif, tidak mengarah pada penyalahgunaan kekuasaan. Pelapor Khusus PBB tentang kemiskinan ekstrem memberikan aksentuasi pentingnya merancang kebijakan publik, termasuk kebijakan pajak, dengan pendekatan HAM.[49] Oleh karena itu, pendapatan pajak akan mempengaruhi hak karena pajak menjadi sumber utama pendapatan untuk menyediakan layanan kesehatan dan pendidikan, akses transportasi umum, membiayai sistem peradilan yang berfungsi dengan baik dan administrasi hukum serta pemerintahan yang efektif. [50]

---

[49] Rodrigo Uprimny Yepes dan Mariana Matamoros, "A Human Rights-based Approach to Tax Systems," *Dejusticia*, Oktober 2024, https://www.dejusticia.org/en/a-human-rights-based-approach-to-tax-systems/. Diakses pada 9 Januari 2026.

[50] "Inequalities and Democracy and Human Rights," *Tax Justice Network*, 13 November 2020, https://taxjustice.net/topics/inequalities-and-democracy-and-human-rights/. Diakses pada 9 Januari 2026

Hal ini berarti pajak berpotensi memperkuat hak-hak sipil dan politik, ketika individu berkontribusi pada pendapatan negara dengan membayar pajak, maka alokasi dan belanja sumber daya tersebut semestinya mendorong hak untuk berpartisipasi dalam politik dan memperkuat kontrak sosial antara warga negara dan negara. Konsekuensi logis lebih jauh, mendorong akuntabilitas, transparansi, dan daya tanggap pemerintah yang lebih besar untuk mengalokasikan dan membelanjakan sumber daya untuk kebaikan publik (*bonum commune*).[51] Dengan demikian, kebijakan fiskal memiliki dampak langsung terhadap hak-hak. Misalnya, suatu negara memiliki kebijakan untuk membiayai alokasi anggaran yang membahayakan hak-hak warga negara. Demikian pula, negara harus memastikan adanya kondisi agar pihak ketiga tidak melanggar hak-hak melalui penyediaan barang dan jasa yang tidak ditujukan untuk mengurangi penikmatan hak-hak warga negara.[52]

---

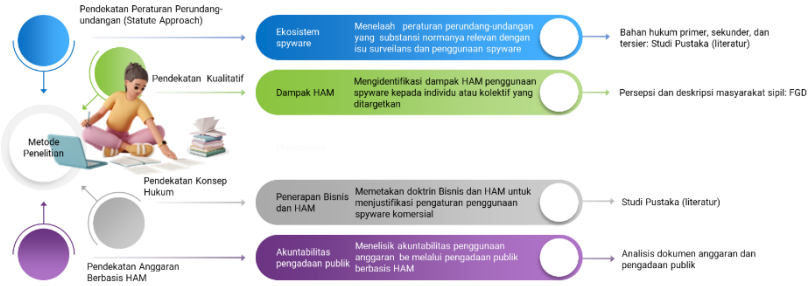
[51] Alexandra Hever, "The Price of Inequality: Why Tax Is a Human Rights Issue," *HRRC* , 27 Juni 2025, https://www.humanrightsresearch.org/post/the-price-of-inequality-why-tax-is-a-human-rights-issue. Diakses pada 9 Januari 2026.

[52] The Initiative for Human Rights Principles in Fiscal Policy, *Principles for Human Rights in Fiscal Policy*, Mei 2021.

Meskipun demikian, upaya mengidentifikasi penyalahgunaan teknologi *Spyware* komersial melalui analisis kebijakan terbukti menjadi masalah yang rumit dan kompleks karena ketiadaan transparansi pengadaan perangkat tersebut. Ketiadaan transparansi pengadaan perangkat *Spyware* bermuara pada keterbatasan data pasar dan aktor yang terlibat dalam rantai pasokan perangkat *Spyware,* termasuk penelusuran alokasi anggaran yang tersebar dalam belanja kementerian/lembaga. Dalam konteks ini, mengingat kerahasian yang menyelimuti penggunaan *Spyware* dan tantangan dalam melakukan penelitian dengan tema semacam ini, maka penelitian ini bersifat eksploratif, bukan upaya untuk memberikan analisis dan tinjauan komprehensif atau definitif tentang *Spyware* dan ancamannya terhadap HAM dan akuntabilitas penggunaan *Spyware* komersial di Indonesia. Konsekuensi dari pendekatan ini, maka setiap informasi yang tersaji dalam penelitian lebihmerupakan indikasi kecenderungan dan perkembangan potensial sehingga membutuhkan penelitian lebih lanjut untuk menata mozaik informasi awal ini. Penelitian lanjutan dengan tema penggunaan *Spyware* di Indonesia menjadi signifikan dilakukan untuk menata mozaik informasi yang masih tersebar agar dapat menciptakan gambaran yang lebih utuh

mengenai penggunaan perangkat *Spyware* dan dampaknya terhadap HAM dan akuntabilitas penggunaan *Spyware* komersial di Indonesia.

Berdasarkan uraian di atas, maka metode penelitian yang dipergunakan dalam penelitian ini dapat digambarkan melalui gambar di bawah ini.



D. Karakteristik Perangkat, Operasi *Spyware*, dan Bentuk Ancaman terhadap Target

Spyware menyediakan akses penuh dan tanpa batas ke setiap perangkat target yang tidak menyadari keberadaannya. Orang-orang yang mengoperasikan *Spyware* kini dapat membaca setiap email dan pesan teks yang dikirim dan diterima, meskipun terenkripsi. Teknologi ini dapat memindai

rol kamera untuk mencari foto-foto pribadi yang memberatkan untuk digunakan sebagai potensi pemerasan dan dapat melacak pergerakan ponsel dengan membaca sistem GPS (*Global Positioning System*). Teknologi ini dapat mengaktifkan kamera dan mikrofon secara diam-diam, mengubah perangkat pribadi tersebut menjadi penyadapan secara real-time. Pada saat bersamaan teknologi ini dapat mengaktifkan fitur penghancuran diri dan menghapus semua jejak panggilan WhatsApp palsu itu sendiri. Apabila dianalogikan dengan tindak pidana, teknologi ini mampu menyapu tempat kejadian perkara untuk menghilangkan sidik jari. Seolah-olah seorang mata-mata yang tidak kasat mata kini telah menyelinap tanpa terdeteksi ke dalam saku target dan melihat dunia melalui mata target dan target tidak tahu ponsel mereka telah diretas.[53]

Sementara, terdapat sekitar 7,64 miliar orang dan hampir tiga perempatnya memiliki setidaknya satu ponsel pribadi. Apa pun merek ponsel pribadi yang dipergunakan, perangkat saku ini menjadi portal elektronik ke dunia luar. Ponsel pribadi yang tersebar

[53] Global Justice Clinic, "Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights."

di seluruh dunia tersebut berpotensi dipilih menjadi target melalui internet, gelombang radio, dan kabel ethernet yang bergerak hampir secepat cahaya dalam keheningan total. Sebuah pesan khusus berisi instruksi yang rumit dikirimkan ke setiap perangkat target dengan cara menyamar sebagai panggilan video pada aplikasi komunikasi populer WhatsApp. Instruksi tersebut mengeksploitasi celah keamanan pada kode aplikasi yang bahkan luput dari perhatian para teknisi WhatsApp paling terlatih. Instruksi ini memicu terjadinya *buffer overflow*, sebuah korsleting digital yang mengacaukan sistem pemrosesan memori aplikasi, membuatnya terganggu seketika, dan membiarkannya terbuka bagi serangan lebih lanjut. Tujuan utamanya adalah membobol kunci sistem dan membiarkannya sedikit terbuka, sehingga program yang lebih rumit dapat menyelinap masuk tanpa terdeteksi.[54]

Spyware merupakan perangkat lunak yang dirancang untuk mengumpulkan data atau memata-matai aktivitas pengguna tanpa izin, lalu mengirimkannya ke pihak ketiga tanpa persetujuan

[54] Ronald J. Deibert, *Chasing Shadows: Cyber Espionage, Subversion, and the Global Fight for Democracy* (Toronto: Simon & Schuster, 2025).

pengguna.[55] Elaine Korzak merumuskan pengertian *Spyware* dengan menambahkan elemen tujuan *Surveilans* atau pengambilan data, sebagai berikut: [56]

> *"Perangkat lunak yang memfasilitasi akses jarak jauh tanpa izin ke perangkat yang terhubung ke internet untuk tujuan Surveilans atau pengambilan data."*

Sementara itu, Giovanni Sartor dan Andrea Loreggia menguraikan *Spyware* melalui berbagai dimensi operasionalnya sebagai berikut:[57]

1) *Spyware* yang dirancang untuk mengumpulkan informasi tentang pengguna tanpa sepengetahuan atau persetujuan

---

[55] "What Is Spyware? Definition, Types and Protection," Fortinet, n.d., https://www.fortinet.com/resources/cyberglossary/spyware.

[56] Perbedaan preferensi individu atau institusional kemudian memunculkan ragam istilah lain yang sering digunakan dalam debat internasional, termasuk teknologi surveilans siber (cyber surveillance technology), peretas bayaran (hacker-for-hire), tentara bayaran siber (cyber mercenaries) atau, yang lebih baru, "kemampuan intrusi siber komersial (commercial cyber intrusion capabilities). Definisi dari semua istilah ini bervariasi di antara berbagai pemangku kepentingan pemerintah dan non-pemerintah. Lihat Elaine Korzak, "Managing Commercial Spyware Through Export Controls: Lesson Learned from the Wassenaar Experience" (Center for Long-Term Cybersecurity (CLTC) UC Berkeley, March 2025).

[57]Giovanni Sartor and Andrea Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes" (European Union, 2022).

pengguna;

2) *Spyware* dapat melacak aktivitas *online* pengguna, mencuri informasi pribadi, atau menampilkan iklan yang tidak diinginkan;

3) *Spyware* dapat menyebar melalui file atau email yang terinfeksi, atau dapat dibundel dengan perangkat lunak lain dan diinstal tanpa sepengetahuan pengguna;

4) *Spyware j*uga dapat mengunduh program berbahaya lainnya dari internet dan menginstalnya di perangkat.

Melengkapi perspektif sebelumnya, Mike Sexton membedah karakteristik *Spyware* dengan memberikan penekanan khusus pada dimensi komersial dan keterlibatan pihak ketiga. Menurut Sexton, karakteristik utama *Spyware* meliputi:[58]

[58] Mike Sexton, "What Is Spyware and Why Should Policymakers Care?," *Third Way*, 9 Maret 2023, https://www.thirdway.org/memo/what-is-spyware-and-why-should-policymakers-care. Diakses pada 16 Desember 2025.

1) Perangkat lunak berbahaya komersial;

2) Terpasang di komputer atau perangkat seluler tanpa persetujuan atau sepengetahuan pengguna;

3) Meretas, men *Surveilans*, dan mengumpulkan data secara diam-diam dari jarak jauh; dan

4) Meneruskan data tersebut ke pihak ketiga.

Berdasarkan karakteristik tersebut, seorang operator dapat melakukan pengumpulan data secara rahasia dari jarak jauh terhadap perangkat yang telah terinfeksi, termasuk telepon seluler dan komputer.[59] *Spyware* adalah teknologi yang memfasilitasi infiltrasi jarak jauh ke dalam komputer pribadi, ponsel pintar, dan perangkat elektronik lainnya, dan akibatnya terjadi eksfiltrasi atau penanaman data, atau penggunaan fitur perangkat, seperti mikrofon, kamera, pesan, dan lainnya untuk mengumpulkan informasi tambahan tentang pemiliknya atau kenalannya, tanpa sepengetahuan

[59] Julie Bloch dkk., "CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent," *Just Security*, 15 Mei 2019, https://www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/. Diakses pada 16 Desember 2025.

mereka.[60]

Tingkat kecanggihan berbagai jenis *Spyware* ditentukan oleh dua parameter: (1) cara *Spyware* menginfeksi perangkat; dan (2) kemampuan *Spyware* untuk mengumpulkan atau mengambil informasi dari perangkat tersebut. Contoh infeksi *Spyware* yang umum dan kurang canggih ketika pengguna mengklik tautan *window pop-up,* atau membuka lampiran email dari sumber yang tidak dikenal, dan komputer *shutdown* atau *restart.* Gangguan pada fungsi komputer tersebut dapat memberi sinyal kepada pengguna bahwa komputer yang digunakan baru saja terinfeksi *malware.* Beberapa bentuk *Spyware* hanya melakukan satu fungsi, seperti melacak lokasi perangkat atau penekanan tombol pada komputer. Di puncak hierarki *Spyware* adalah Pegasus[61], yang memiliki

[60] Tamar Megiddo, "Spyware Exports: Recognizing the Limits of Human Rights Law." SSRN, 3 April 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123661

[61] Spyware Pegasus dapat menginfeksi perangkat pengguna menggunakan kerentanan *zero-click,* yaitu jenis kerentanan yang tidak memerlukan interaksi atau intervensi pengguna. Di masa lalu, *spyware* membutuhkan pengguna untuk membuka file yang terinfeksi atau mengklik tautan berbahaya untuk mengakses perangkat. Pemanfaatan kerentanan *zero-click,* malware dapat masuk ke perangkat hanya dengan mengeksploitasi kelemahan pada sistem operasi, perangkat lunak, atau koneksi jaringan perangkat. Karenanya pengguna tidak menyadari adanya infeksi, lebih sulit

kemampuan untuk membuka kunci dan mengirimkan seluruh isi perangkat seluler, selain mengambil kendali mikrofon dan kamera perangkat, tanpa perlu input pengguna.[62]

Selanjutnya, apabila mempertimbangkan analisis kerentanan dan eksploitasi korban yang ditargetkan terdapat dua jenis serangan yang berbeda: [63]

1) Serangan tanpa klik *(zero-click attacks)* yang tidak memerlukan intervensi apa pun dari pengguna. Serangan ini sering kali didasarkan pada kerentanan *zero-day*, dan sangat berbahaya karena pengguna biasanya tidak menyadari serangan tersebut, sehingga tidak dapat menangkalnya atau mengurangi dampaknya.

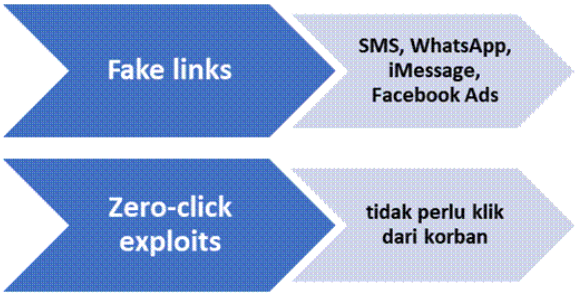
untuk mengenali dan melindungi diri dari serangan semacam itu. Lihat, Sartor dan Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

[62] Katherine Kuhl, "Pegasus Spyware in Hungary: Analyzing Hungary's use of Pegasus on journalists with Lessig's Four Modalities of Regulation" (Senior Theses, Fordham University, 2024).

[63] Sartor dan Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

2) Serangan satu klik *(one-click attacks)* memerlukan tindakan dari pengguna yang menjadi sasaran, yang biasanya berupa mengklik tautan atau tombol yang ditampilkan melalui aplikasi web. Korban, meskipun diharuskan untuk melakukan tindakan, mungkin tidak mengetahui apa yang terjadi karena tertipu oleh tampilan pesan atau antarmuka yang menyesatkan yang diberikan oleh penyerang.

Metode operasi perangkat *Spyware* terbagi menjadi dua seperti terlihat pada gambar di bawah ini.[64]



[64] Gambar hasil pengolahan data yang dilakukan FITRA

Spyware telah beredar di internet sejak pertengahan 1990-an, dan badan keamanan serta intelijen pemerintah diduga telah memproduksi dan menyebarkan perangkat lunak untuk mencegat komunikasi digital selama bertahun-tahun. Dalam perkembangannya kemudian, *Spyware* juga diproduksi dan dipasarkan oleh perusahaan komersial. Perangkat lunak yang mereka produksi kini menjadi semakin canggih serta invasif. Saat ini, beberapa perangkat *Spyware* memungkinkan pengambilan input audio dan visual serta komunikasi secara *real-time* dan jarak jauh, memungkinkan operator perangkat yang melakukan infeksi untuk memata-matai target dan orang-orang di sekitarnya. Perusahaan seperti NSO Group di Israel, Finfisher di Inggris dan Jerman, dan Hacking Team di Italia menjadi pemain kunci dalam industri yang berkembang pesat dan diselimuti kerahasiaan. Pada 2019 yang lalu, NSO menjual Pegasus seharga $1 miliar dan Moody's memperkirakan industri *Spyware* sebagai pasar yang mencengangkan senilai $12 miliar.[65]

Penyebaran dan penyalahgunaan teknologi *Spyware* komersial kini memicu tantangan serius bagi

[65] Bloch dkk., "CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent."

kebijakan internasional. Pasar *Spyware* yang berkembang pesat kini menyediakan berbagai teknologi dengan kemampuan untuk mengakses dan/atau memantau data komunikasi individu dan kelompok secara diam-diam. Pemerintah dan pemangku kepentingan non-pemerintah di seluruh dunia telah berupaya mengatasi pelanggaran HAM dan risiko keamanan nasional yang terkait dengan penyalahgunaan teknologi *Spyware* komersial.[66] Penggunaan *Spyware* memunculkan ancaman unik karena *Spyware* lebih mengganggu daripada instrumen represi digital lainnya dan sulit, bahkan hampir tidak mungkin, untuk diblokir. *Spyware* beroperasi secara rahasia dan seringkali tidak meninggalkan jejak yang memudahkan upaya penegakkan hukum. Perangkat ini juga lebih mudah digunakan oleh pemerintah daripada metode represi dan paksaan konvensional serta beberapa sistem *Surveilans* pasif yang lebih canggih secara teknologi.[67]

Salah satu perangkat *Surveilans* yang paling terkenal adalah Pegasus. Pegasus merupakan

[66] Bloch dkk., "CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent."

[67]Gail Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa" (Master's thesis, Harvard University, 2023).

perangkat *Spyware* yang dikembangkan oleh perusahaan Israel NSO Group.[68] Pegasus dipasarkan sebagai perangkat untuk memerangi terorisme dan kejahatan, namun fakta empirik menunjukkan Pegasus menjadi perangkat untuk mempersenjatai pemerintah otoriter untuk menargetkan jurnalis, aktivis, tokoh oposisi politik, dan komunitas yang terpinggirkan. Kemampuannya untuk menginfeksi perangkat tanpa interaksi pengguna (*zero click*) telah menjadikannya sebagai perangkat *Surveilans* yang belum pernah ada sebelumnya. Hal ini memberi celah pada negara untuk menekan oposisi sambil menghindari pertanggungjawaban. Penyebaran luas dan tanpa pengawasan terhadap perangkat Pegasus telah mengungkap kesenjangan antara keamanan digital global dan kurangnya pengawasan pengaturan yang mengatur penjualan dan penggunaan perangkat *Surveilans* ini. Dalam konteks wilayah konflik, seperti

[68] NSO Group didirikan pada 2010 oleh pengusaha Israel, yaitu Niv Carmi, Shalev Hulio, dan Omri Lavie. NSO Group melisensikan produk surveilans kepada badan intelijen dan penegak hukum di seluruh dunia. Perusahaan ini terutama dikenal karena produk *spyware* Pegasus perangkat lunak malware invasif yang mampu secara diam-diam mengambil kendali atas ponsel pintar dan mengekstrak kontennya dari jarak jauh. Lihat, Dan M. Kotliar and Elinor Carmi, "Keeping Pegasus on the Wing: Legitimizing Cyber Espionage," *Information, Communication & Society* 27, no. 8 (2024): 1499–1529, https://doi.org/10.1080/1369118X.2023.2245873.

Palestina[69] dan Kashmir, penggunaan dan pemanfaatan perangkat *Spyware* Pegasus memperlihatkan semakin eratnya keterkaitan antara *Surveilans* negara, kepentingan korporasi, dan otoritarianisme digital.[70]

Melalui pemanfaatan kerentanan *zero-day*, Pegasus dapat menyusup ke dalam perangkat secara otomatis tanpa melalui klik sama sekali (*zero-click*).

---

[69] Israel telah memulai kampanye genosida terhadap Palestina dengan mengerahkan berbagai sistem pengawasan, termasuk drone, sistem penyadapan komunikasi, teknologi pengenalan wajah (facial recognition technology), dan sistem penargetan Kecerdasan artifisial, termasuk Gospel, Lavender, dan Where's Daddy. Selain itu, Unit 8200 Israel telah mengembangkan Large Language Model (LLM) untuk menganalisis komunikasi yang disadap dari warga Palestina dan kemungkinan besar memberikan informasi ini kepada sistem lain. Sistem-sistem ini memanfaatkan informasi surveilans massal terhadap warga Palestina di Gaza dan mencari tersangka untuk dijadikan target. Bahkan sistem-sistem ini sengaja digunakan untuk menargetkan tersangka ketika mereka berada di rumah tinggal mereka, dan tanpa memperhatikan kedekatan dengan warga sipil dan infrastruktur sipil. Israel telah memperluas praktik surveilans dan intersepsi di internet, media sosial, telepon, aplikasi pesan, dan platform digital lainnya. Dalam konteks ini, Israel telah mengerahkan perangkat spyware, terutama Pegasus dari NSO Group. Lihat, Mais Qandeel and Özgün Erdener Topak, "Genocidal Surveillant Assemblage in Palestine: A Socio-Legal Analysis," *Journal of Genocide Research* (October 2025): 1–22, https://doi.org/10.1080/14623528.2025.2567372.

[70] Samia Afrose, "Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine" (Bachelors thesis, Harvard University, 2025).

Kerentanan *zero-day* adalah kerentanan dalam perangkat lunak yang belum diidentifikasi atau diperbaiki oleh pengembang perangkat lunak. Pengembang perangkat lunak tidak memiliki waktu satu hari pun untuk menanggapi atau memperbaiki masalah tersebut. Dengan memanfaatkan kerentanan yang belum diungkapkan ini, *Spyware* dapat menghindari deteksi dan mendapatkan akses tidak sah ke perangkat atau jaringan.[71]

Pegasus merupakan perangkat *Spyware* yang mampu mengakses dan meretas ponsel dan mengubah ponsel menjadi alat pendengar tanpa sepengetahuan pengguna. Upaya peretasan ini bergantung pada pengguna yang menginstal malware atau mengklik tautan palsu tanpa disadari agar peretas dapat memperoleh akses. Setelah akses diperoleh, Pegasus dapat membaca pesan teks, melacak panggilan, mengumpulkan kata sandi, melacak lokasi, mengakses mikrofon dan kamera perangkat, serta mengumpulkan informasi dari aplikasi. *Spyware* ini dapat mengakses ponsel pengguna melalui kerentanan sistem, seperti email dan berbagai aplikasi, misalnya Apple Music dan

[71] Sartor dan Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

iMessage sehingga memungkinkan perangkat *Spyware* ini melacak semua bentuk komunikasi dan lokasi melalui kamera dan mikrofon ponsel.[72] Perangkat lunak Pegasus menginfeksi iPhone dan perangkat Android sehingga memungkinkan operator mengekstrak pesan, foto, dan email, merekam panggilan, serta mengaktifkan mikrofon dan kamera secara diam-diam.[73] Bagaimana perangkat Pegasus bekerja menargetkan pengguna dapat dilihat melalui gambar di bawah ini.[74]

[72] Penggunaan teknologi surveilans untuk menyusup ke perangkat pribadi bukanlah hal yang asing. Pengungkapan Edward Snowden pada 2010-an mengungkap kemampuan Badan Keamanan Nasional (National Security Agency/NSA) untuk mengaktifkan perangkat seluler dari jarak jauh, termasuk mengakses mikrofon dan kameranya, bahkan ketika perangkat tersebut dimatikan. Selama baterai masih terpasang di perangkat, perangkat pribadi berisiko diawasi. Ini adalah bagian dari program pengawasan massal NSA, yang memungkinkan pemerintah Amerika Serikat untuk mengumpulkan data komunikasi, metadata, dan konten warga Amerika tanpa surat perintah, dan menyimpan informasi mereka di pusat data dan repositori. Lihat, Sartor dan Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

[73] "Pegasus: Spyware Sold to Governments 'Targeted Activists'," *BBC News*, 19 Juli 2021, https://www.bbc.com/news/world-57891506, diakses pada 6 Januari 2026.

[74] "Pegasus: Who Are the Alleged Victims of Spyware Targeting?"



Dalam kasus Jamal Khashoggi, jika ponselnya atau ponsel salah satu anggota keluarganya diretas oleh Pegasus, percakapan, lokasi, dan informasi

sensitif lainnya dapat dicegat dan diakses. Informasi yang dicegat oleh Pegasus ini memainkan peran penting dalam perencanaan dan pelaksanaan pembunuhan Jamal Khashoggi. Kemampuan Pegasus yang luas memungkinkan perangkat lunak ini untuk mengeksploitasi fungsi ponsel, melanggar privasi individu yang menjadi target, serta privasi individu yang berhubungan dengan target tersebut.[75]

Sejumlah kasus menunjukkan bahwa evolusi *Spyware* Pegasus terletak pada kecanggihan metode infeksi dan skala penyebarannya. Inovasi utama perangkat ini meliputi kemampuannya untuk beroperasi tanpa memerlukan interaksi pengguna dalam bentuk apa pun dan dapat melewati beberapa langkah keamanan paling canggih. Hal ini berbeda dengan operasi Badan Keamanan Nasional (NSA) yang umumnya masih mengandalkan intersepsi berbasis jaringan atau instalasi *malware* yang membutuhkan tingkat kelalaian pengguna tertentu. Sementara itu, penggunaan Pegasus tidak lagi terbatas pada badan intelijen negara. Teknologi ini dijual secara komersial kepada berbagai pemerintah di seluruh dunia, yang pada akhirnya mendorong

[75] Ottavio Marzocchi and Martina Mazzini, Pegasus and surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, 2022.

terciptanya pasar represi digital global.[76]

Perangkat *Spyware* dengan karakteristik seperti Pegasus yang memiliki kemampuan mumpuni untuk mengakses seluruh perangkat dan data yang terhubung dengannya, tanpa pandang bulu, dan tanpa batasan sudah melanggar standar dasar kebutuhan dan proporsionalitas berdasarkan hukum HAM internasional. Menurut David Kaye, karakteristik *Spyware* saat ini menuntut kita untuk melangkah lebih jauh dari sekadar moratorium, yakni dengan mengupayakan pelarangan penuh terhadap teknologi invasif tersebut, baik yang disediakan oleh sektor swasta maupun publik. Mengingat besarnya ancaman perangkat ini terhadap HAM, seharusnya tidak ada satu pun pemerintah atau perusahaan swasta yang diizinkan menjual teknologi serupa kepada pihak mana pun.[77]

Kapasitas teknis yang ditawarkan oleh *Spyware* komersial telah menarik perhatian banyak negara. Amerika Serikat, misalnya, tercatat sebagai salah satu pemerintah yang mempertimbangkan penggunaan

---

[76] "Pegasus: Who Are the Alleged Victims of Spyware Targeting?"

[77] David Kaye, "David Kaye: Here'S What World Leaders Must Do About Spyware," Committee to Protect Journalists, 12 Oktober 2022, https://cpj.org/2022/10/david-kaye-what-world-leaders-must-do-about-spyware/#:~:text=Read%20CPJ's%20complete%20special%20report,to%20hack%20into%20individual%20phones. Diakses pada 2 Januari 2026

teknologi dari vendor seperti NSO Group dan perusahaan lain. Menurut laporan media, Pegasus memungkinkan operator untuk secara jarak jauh dan diam-diam menginstal perangkat lunak pada ponsel pengguna atau perangkat digital lainnya yang dapat secara diam-diam mengakses data pengguna dan memantau semua aktivitas mereka. Pegasus melakukan lebih dari sekadar melacak metadata, seperti statistik penggunaan atau log panggilan; menyediakan akses ke semua data yang ada di ponsel, pemantauan *Global Positioning System* (*GPS*), perekaman audio dan visual secara *real-time* melalui kamera dan mikrofon, dan banyak lagi kemampuannya yang lain. Versi terbaru Pegasus dilaporkan tidak lagi memerlukan tindakan dari target untuk mengklik tautan (*zero click*). Hal ini memungkinkan operator untuk menginfeksi ponsel hanya dengan menggunakan nomor telepon target. Bukti baru muncul mengkonfirmasi kemampuan ini, dengan menggunakan celah keamanan dalam layanan pesan WhatsApp, perangkat lunak mata-mata NSO dapat secara diam-diam menginstal perangkat lunak *Surveilans*, hanya dengan melakukan panggilan ke ponsel target, bahkan jika target tidak mengangkatnya. Karena instalasi Pegasus tidak meninggalkan jejak yang dapat dideteksi oleh pengguna biasa, pencarian bukti

infeksinya membutuhkan forensik digital oleh ahli teknologi terlatih, seperti yang ada di Citizen Lab dan Amnesty International.[78]

Teknologi *Surveilans* digital, termasuk *Spyware,* dikenal sebagai barang dwiguna (*dual-use goods*), yang berarti dapat digunakan untuk tujuan pertahanan dan sipil. Teknologi dwiguna di 42 negara berada di bawah rezim kontrol ekspor multilateral Kesepakatan Wassenaar tentang Kontrol Ekspor untuk Senjata Konvensional dan Barang dan Teknologi Penggunaan Ganda (*Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*) pada 1996. Pada 2013, Kesepakatan Wassenaar diubah untuk memasukkan perangkat lunak intrusi. Meskipun Kesepakatan Wassenaar tidak mengikat secara hukum, para penandatangannya biasanya secara sukarela mengadopsi daftar kontrol tersebut ke dalam peraturan domestik. Hal ini mewajibkan perusahaan yang produknya terdaftar untuk memperoleh lisensi khusus sebelum mengekspor barang-barang tersebut.[79]

---

[78] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

[79] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

E. *Spyware* dan Kepentingan Kekuasaan Negara: Operasi *Spyware* di Berbagai Negara

Meskipun dipasarkan sebagai instrumen netral untuk digunakan oleh penegak hukum atau terkait dengan keamanan nasional, perangkat *Spyware*, alat pengenalan wajah, dan sistem biometrik, diduga dipergunakan untuk memfasilitasi pelanggaran norma HAM. Teknologi *Surveilans* dapat dikatakan telah menjadi instrumen penting kekuasaan negara, terutama dalam konteks kontrol oleh rezim otoriter. Pada saat bersamaan, penggunaan *Surveilans* diduga telah memungkinkan represi transnasional. Para pembangkang yang hidup di pengasingan diduga telah dipantau, dilecehkan, dan bahkan diculik atau dibunuh dengan bantuan alat pelacak digital. Perkembangan ini menimbulkan kekhawatiran hukum dan etika yang serius, terutama ketika perusahaan swasta menyediakan teknologi yang kemudian terlibat dalam represi politik, *Surveilans* ilegal, atau penargetan para pembangkang.[80] Perangkat ini

[80] Vladimir Hrle, "Corporate Responsibility in the Age of Surveillance and Transnational Repression: Legal Obligations and Human Rights Due Diligence," *International Bar Association*, 21 Agustus 2025, https://www.ibanet.org/corporate-responsibility-in-age-of-surveillance-

seringkali memiliki fungsi ganda, artinya alat-alat tersebut memiliki aplikasi yang sah dalam investigasi kriminal atau untuk kepentingan keamanan nasional, tetapi dapat digunakan kembali untuk menekan perbedaan pendapat atau menargetkan kelompok minoritas.

Terdapat beberapa tujuan mengapa pihak ketiga mungkin tertarik untuk mendapatkan akses tanpa izin ke suatu perangkat atau sekelompok perangkat:[81]

1) Mengumpulkan informasi tentang target (pengguna perangkat), termasuk data pribadi, seperti nama, alamat, dan nomor telepon, serta informasi tentang aktivitas dan kebiasaan *online* target;

2) Mengumpulkan informasi tentang kenalan target, termasuk data tentang orang-orang yang berkomunikasi dengan target, serta informasi tentang aktivitas dan kebiasaan online mereka;

3) Mendapatkan akses ke perangkat dengan

---

and-transnational-repression-legal-obligations-human-rights-due-diligence. Diakses pada 11 Januari 2026.

[81] Sartor dan Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

tujuan meminta tebusan. Dalam hal ini, pihak ketiga mungkin mencoba untuk mengambil kendali perangkat dan membuat kontennya tidak dapat diakses dengan mengenkripsi dan kemudian menuntut pembayaran sebagai imbalan untuk mengembalikan kendali perangkat kepada pengguna dan memungkinkan akses ke data;

4) Pencurian identitas, jika pihak ketiga mendapatkan akses ke perangkat, maka ia dapat meniru pemilik perangkat dan mengirim pesan atau melakukan tindakan lain yang tampak berasal dari pemilik yang sah. Hal ini bisa sangat berbahaya jika pihak ketiga dapat mengakses informasi pribadi atau keuangan yang sensitif melalui perangkat tersebut;

5) Membuat target tidak dapat menggunakan perangkat tersebut. Hal ini dapat dilakukan dengan menghapus file penting atau menonaktifkan fungsi-fungsi utama perangkat.

Laporan PEGA Committee merangkum risiko

HAM yang terkait dengan pasar *Spyware* komersial yang tidak diatur sebagai berikut: [82]

> "Penyalahgunaan *Spyware* tidak hanya melanggar hak privasi individu. Hal itu merusak demokrasi dan lembaga demokrasi secara diam-diam. Ia membungkam oposisi dan kritikus, menghilangkan pengawasan, serta memberikan efek gentar (*chilling effect*) terhadap pers bebas dan masyarakat sipil. Ia juga berfungsi untuk memanipulasi pemilihan umum. Istilah *'mercenary Spyware'* (*Spyware* bayaran) merefleksikan dengan sangat baik sifat dari produk dan industri tersebut. Bahkan upaya yang gagal untuk menginfeksi ponsel pintar dengan *Spyware* pun memiliki konsekuensi politik, dan dapat membahayakan individu sekaligus demokrasi. Partisipasi dalam kehidupan publik menjadi mustahil tanpa adanya kepastian untuk menjadi bebas dan tidak diawasi."

Pemanfaatan dan penggunaan perangkat

[82] Costica Dumbrava, *Impact of the Use of Spyware on Fundamental Rights* (Brussels: European Parliamentary Research Service,2023), https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf

Spyware sebagai bagian dari *Surveilans* seringkali dilandasi motivasi kekuasaan. Istilah *Surveilans* (*surveillance*) sendiri dalam bahasa Perancis berarti mengamati dari atas (*watching from above*). Upaya *Surveilans* menyiratkan hubungan kekuasaan. Hal ini bukan sekadar *Surveilans* pasif, melainkan bentuk *Surveilans* yang menilai dan melakukan intervensi untuk membentuk perilaku. Tujuan dari *Surveilans* memang menempatkan seseorang tidak perlu menyadari dinamika kontrol tersebut agar efektif. Dinamika ini akan bekerja lebih efektif jika dianggap sebagai sesuatu yang lumrah, di mana muatan politik di baliknya tersamarkan. Dengan kata lain, *Surveilans* dipahami sebagai upaya pemantauan individu guna mendikte atau mengendalikan perilaku mereka[83]

Di banyak negara *Spyware* kerap disalahgunakan. Penggunaan *Spyware* memiliki implikasi serius terhadap privasi, keamanan data dan kepercayaan publik. Saat ini tercatat terdapat 11 jenis *Spyware* di dunia dengan tingkat kemampuan yang berbeda-beda.[84] Aktivis HAM, jurnalis, dan pengacara

[83] Torin Monahan and David Murakami Wood, "Introduction: Surveillance Studies as a Transdisciplinary Endeavor," dalam *Surveillance Studies: A Reader*, ed. Torin Monahan dan David Murakami Wood (Oxford: Oxford University Press, 2018).
[84] Lihat lampiran I penelitian ini.

di seluruh dunia telah menjadi sasaran pemerintah otoriter yang menggunakan perangkat lunak *Spyware* yang dijual oleh perusahaan *Surveilans* Israel, NSO Group. Pegasus Project mengungkapkan identitas orang-orang yang namanya muncul dalam daftar target, termasuk ratusan eksekutif bisnis, tokoh agama, akademisi, aktivis, pejabat serikat pekerja, dan pejabat pemerintah, termasuk menteri kabinet, presiden, dan perdana menteri.[85] Pegasus Project berhasil mengidentifikasi pola penargetan oleh klien individu melalui data yang bocor, sekaligus mengungkap 10 pemerintah yang diyakini bertanggung jawab atas pemilihan target, yakni Azerbaijan, Bahrain, Kazakhstan, Meksiko, Maroko, Rwanda, Arab Saudi, Hungaria, India, dan Uni Emirat Arab.[86]

Di Afrika, penggunaan *Spyware* Pegasus produksi NSO Group telah terkonfirmasi secara luas. Rwanda dan Maroko diidentifikasi sebagai operator

[85] Stephanie Kirchgaessner dkk., "Revealed: Leak Uncovers Global Abuse of Cyber-surveillance Weapon," *The Guardian*, 18 Juli 2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus. Diakses pada 7 Januari 2026.

[86] Kirchgaessner dkk., "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon."

utama, dengan Maroko tercatat sebagai klien terbesar di kawasan tersebut. *Spyware* Pegasus memperburuk kondisi politik di negara-negara Afrika karena selain digunakan untuk memata-matai teroris dan kriminal digunakan, alat sadap ini juga digunakan untuk memata-matai lawan politik, aktivis HAM dan warga sipil. Aplikasi Pegasus di Afrika telah menargetkan hingga 10.000 nomor telepon, termasuk Raja Mohammed VI sendiri. Zambia juga dicurigai menggunakan teknologi ini untuk memata-matai lawan politik selama masa pemerintahan mantan Presiden Edgar Lungu.[87] Jejak Pegasus di Afrika, negara operator[88] dan yang terinfeksi olehnya, dapat dilihat dalam peta di bawah ini. [89]

---

[87] https://www.brookings.edu/articles/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/

[88] "Likely Pegasus Operator" refers to the five African countries identified either by Citizens Lab or Pegasus Project reporting as a country that licenses or operates Pegasus malware. Pegasus infections have been found in all countries that are suspected operators except for Mozambique. By contrast, there were confirmed infections in eight African countries who are not suspected to be operators.

[89] Peta ini merujuk pada www.brookings.edu

Infections, users, and cross-border targets of Pegasus malware in Africa.



Source: Reporting and data compiled from Citizens Lab and the Pegasus Project.

TECH STREAM

Sementara itu, di kawasan ASEAN sendiri, para aktivis pro-demokrasi di Thailand juga berhadapan dengan *Spyware* Pegasus. Aplikasi ini menargetkan aktivis pro-demokrasi dan reformis monarki di Thailand. Setidaknya 30 individu, termasuk pengunjuk rasa, pengacara dan aktivis gerakan pro-demokrasi,

terinfeksi Pegasus antara Oktober 2020 dan November 2021. Infeksi dilakukan melalui eksploitasi *zero-click*, memungkinkan peretasan tanpa sepengetahuan korban, memberikan akses ke data ponsel seperti pesan, lokasi dan rekaman kamera atau mikrofon. The Citizen Lab, iLaw dan DigitalReach menemukan bukti adanya serangan *Spyware* ke gerakan pro-demokrasi, dengan indikasi bahwa beberapa badan pemerintah Thailand mungkin terlibat, termasuk yang terkait dengan produk NSO lainnya seperti Circles.[90]

Penggunaan *Spyware* Pegasus oleh pihak berwenang terkonfirmasi salah satunya dalam kasus pembunuhan Jamal Khashoggi, jurnalis Arab Saudi. Ponsel milik Jamal Khashoggi diretas dan dimata-matai ketika mengunjungi Konsulat Jenderal Arab Saudi di Istanbul**.** Agnes Callamard, Pelapor Khusus (*Special Rapporteur*) mengenai pembunuhan di luar hukum (*extrajudicial killing*) menyimpulkan bahwa:[91]

---

[90] John Scott-Railton dkk., "GeckoSpy: Pegasus Spyware Used Against Thailand's Pro-Democracy Movement - the Citizen Lab," The Citizen Lab, 7 Juli 2022, https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/.

[91] UN Human Rights Council, *Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi*, A/HRC/41/CRP.1 (19 Juni 2019).

> *"Eksekusi terhadap Jamal Khashoggi merupakan contoh paling nyata sebuah pola yang berbeda, yakni ancaman atau penggunaan kekerasan ekstrateritorial oleh suatu negara terhadap individu di wilayah negara lain, di luar situasi konflik bersenjata, oleh satu Negara terhadap orang-orang yang berada di wilayah Negara lain. Eksekusi ini mengakibatkan pelanggaran HAM, termasuk pembunuhan di luar hukum, penculikan, dan penyerahan paksa yang dapat mengakibatkan penyiksaan, pemenjaraan, penghilangan paksa, dan kematian. Pelanggaran lain yang diakibatkan juga dapat mencakup pelanggaran kebebasan berekspresi atau hak atas privasi. Melarikan diri ke luar negeri untuk mencari keselamatan semakin tidak dapat diandalkan sebagai bentuk pelindungan."*

Laporan Pelapor Khusus tersebut merujuk pada hasil analisis Citizen Labs terkait infiltrasi terhadap Jamal Khashoggi dan orang-orang terdekatnya dengan operator Pegasus yang terkait dengan Arab Saudi. Pegasus perangkat *Spyware* buatan NSO memungkinkan operator yang terkait dengan Arab Saudi untuk mengakses kontak telepon, foto, pesan

teks, log obrolan online, email, dan file pribadi lainnya.[92] Infrastruktur intelijen dan teknologi *Surveilans* merupakan senjata yang sangat berbahaya di tangan negara-negara otokratis dan yang dikenai sanksi internasional, seperti Venezuela dan Arab Saudi, yang telah menggunakan teknologi tersebut untuk menargetkan warga sipil, jurnalis, pembangkang, dan minoritas etnis.[93]

Surveilans massal berada pada nuansa antara melindungi warga negara dan melanggar privasi mereka. Data yang dikumpulkan dalam *Surveilans* massal tidak menghormati batas internasional dan pengumpulan data lintas batas menyentuh sejumlah hak terkait yang dilindungi oleh perlindungan privasi, termasuk hak atas kebebasan berekspresi, kebebasan berhati nurani dan beragama, kebebasan berkumpul, kebebasan berserikat dan hak-hak lainnya.[94] Meskipun

---

[92] UN Human Rights Council, *Investigation into the Unlawful Death of Mr. Jamal Khashoggi*.

[93] Ronnie Rosen Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading," *Georgetown Law*, January 30, 2023, https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading/. Diakses pada 20 Januari 2026.

berhati nurani dan beragama, kebebasan berkumpul, kebebasan berserikat dan hak-hak lainnya.[94] Meskipun perangkat ini bersifat intrusif dan mengancam HAM, perusahaan dari negara-negara seperti Prancis, Jerman, dan Italia telah menjual teknologi invasif kepada rezim seperti pemerintah Suriah. Email dari Hacking Team yang dipublikasikan oleh WikiLeaks pada 2015 mengungkapkan perusahaan Italia menjual perangkat invasifnya ke Ethiopia, Nigeria, Sudan Selatan, Bahrain, Uzbekistan, Azerbaijan, Kazakhstan, Rusia, Arab Saudi, dan banyak pemerintah lain dengan sistem otoriter atau sistem satu partai.[95] Tabel negara-negara pengguna *Spyware* Pegasus dan Predator, sebagai berikut:[96]

[94] Anna W. Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware," *The Brooklyn Journal of International Law* 44, no. 2 (January 7, 2019).
[95] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."
[96] Data diolah FITRA

Spyware	Negara Pengguna
Pegasus	Israel (Pengembang), Mexico, Saudi Arabia, UAE, India, Azerbaijan, Maroko, Rwanda, Togo, Hungaria, Polandia, Spanyol, Thailand, Indonesia (diduga), Kazakhstan, Uzbekistan, Vietnam, Mesir, Bahrain, Oman, AS, Yordania, Pakistan (diduga), Singapura (diduga negara klien), Lebanon.
Predator	UAE, Maroko, Indonesia (diduga), Turki, Yunani, Siprus, Italia, AS.

Meskipun terdapat kemungkinan beberapa pemerintah memproduksi sendiri perangkat untuk melakukan *Surveilans* digital yang ditargetkan, banyak negara membeli teknologi canggih yang memungkinkan *Surveilans* tersebut dari perusahaan swasta. Negara seringkali membenarkan pengadaan teknologi ini dengan dalih untuk menjaga hukum dan ketertiban. Beberapa perusahaan *Surveilans* ini memproduksi dan menjual perangkat *Spyware* atau perangkat serupa lainnya kepada negara-negara. Selain untuk tujuan yang sah, pemanfaatan dan

penggunaan perangkat ini ditujukan sebagai instrumen *Surveilans* sehingga mempersempit ruang bagi perbedaan pendapat dengan menargetkan pembela HAM. Serangan *Surveilans* digital yang ditargetkan semacam ini melibatkan interaksi beberapa aktor negara dan non-negara, termasuk perusahaan swasta, investor, lembaga penegak hukum dan intelijen, otoritas kontrol ekspor nasional, dan rezim kontrol ekspor multilateral seperti yang diwujudkan dalam Perjanjian Wassenaar dan Peraturan Penggunaan Ganda Eropa.[97] Kesenjangan dalam pengaturan, penyalahgunaan oleh agen negara, dan kerahasiaan negara dan perusahaan berkorelasi pada hambatan dan kompleksitas untuk mengidentifikasi, mencegah, atau mencari ganti rugi atas pelanggaran HAM yang disebabkan oleh serangan-serangan ini, termasuk membangun mekanisme pengawasan yang memadai.[98]

Risiko keamanan yang ditimbulkan oleh penyebaran *Spyware* komersial menjadi landasan utama bagi pembaruan ekosistem kebijakan untuk

[97] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."
[98] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."

mencegah penyalahgunaan teknologi *Surveilans* tersebut. Amerika Serikat mengambil dua langkah untuk memelihara keamanan siber yang signifikan sejak 2019, yaitu (1) Bagian 889 dari Undang-Undang Otorisasi Pertahanan Nasional *(National Defense Authorization Act),* John S. McCain, 2019 (NDAA 2019); dan (2) Sertifikat Model Kematangan Keamanan Siber (*Cybersecurity Maturity Model Certificate*). Langkah *pertama,* berupaya melindungi keamanan siber di basis industri pertahanan dengan membatasi secara ketat kemampuan, baik lembaga federal maupun kontraktor federal untuk menggunakan pasokan atau layanan dari *Huawei Technologies Company* (*Huawei*), *Zhongxing Telecommunications Equipment Corporation* (ZTE), dan tiga perusahaan Cina lainnya yang menyediakan layanan dan perangkat keras *Surveilans* dan telekomunikasi. Meskipun merupakan langkah yang bertujuan untuk memastikan keamanan siber, Bagian 889 berupaya mencapai keamanan pasokan (*ensuring procurement supply chains*) dengan memastikan rantai pasokan pengadaan berada di pasar domestik atau pasar sekutu yang dapat diandalkan. Sebaliknya, di bawah Model Kematangan Keamanan Siber, Departemen Pertahanan *(Department of Defense)* mengejar keamanan siber melalui serangkaian praktik

keamanan siber komprehensif yang harus diikuti oleh kontraktor pada basis industri pertahanan, ketika menangani informasi kontrak *Federal dan Controlled Unclassified Information* (*CUI*).[99]

Peningkatan penggunaan *Spyware* komersial bukan hanya masalah di Amerika Serikat, namun juga di kawasan Uni Eropa. Pasca pengungkapan Proyek Pegasus pada 2021 yang membuktikan perangkat peretasan Pegasus digunakan untuk memata-matai jurnalis, politisi, aktivis, dan lainnya di seluruh dunia oleh klien perusahaan Israel NSO Group, Parlemen Eropa membentuk komite penyelidikan (PEGA Committee) untuk menyelidiki lebih lanjut penggunaan perangkat *Spyware* komersial di Uni Eropa. Parlemen Eropa mengadopsi rekomendasi yang menyerukan Komisi Eropa untuk mengatur lebih ketat penggunaan, pembuatan, dan perdagangan *Spyware;* menegakkan hukum yang ada dengan lebih ketat; dan membuat definisi yang jelas tentang keamanan nasional.[100]

---

[99] Stuart Joseph Anderson, "Comparing Section 889's Huawei Ban and the Cybersecurity Maturity Model Certificate: The Challenge of Pursuing Cybersecurity Through Friend-Shoring," *Public Contract Law Journal* 54, no. 2 (2025).

[100] Sophie in 't Veld, "An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?," Digital Front Lines, n.d.,

Pada titik ini, karakteristik irisan antara kepentingan pemerintah dan swasta menpersulit upaya untuk mengatur penggunaan perangkat *Spyware* komersial karena hambatan-hambatan, berikut ini: [101]

> *Pertama,* ekosistem kebijakan, baik legislasi, regulasi, maupun penganggaran yang dicirikan dengan tingkat ketidaktransparan yang tinggi. Sebagian besar perusahaan yang beroperasi di bidang ini tidak dikenal luas atau dipublikasikan sehingga informasi yang tersedia untuk umum tentang bisnis ini sangat terbatas. Transparansi pasar *Spyware* komersial yang masih minimal memengaruhi semua elemen rantai pasok, baik vendor, pembeli, pengguna, serta keputusan terkait lisensi transfer dan ekspor.
>
> *Kedua,* Pemerintah memainkan peran sentral dalam semua aspek siklus hidup produk teknologi *Spyware* komersial sehingga akan berimplikasi secara kritis terhadap ekosistem

https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/. Diakses pada 7 Januari 2026.

[101] Korzak, "Managing Commercial Spyware Through Export Controls: Lesson Learned from the Wassenaar Experience."

kebijakan itu sendiri. Terlebih lagi, pemerintah bukan hanya pembeli dan pengguna teknologi *Spyware* komersial. Justru pemerintah menjadi aktor kunci di semua tahap siklus hidup produk *Spyware* komersial. Pemerintah merupakan manifestasi dari kepentingan negara asal perusahaan *Spyware* yang mengembangkan dan memproduksi teknologi tersebut dan mereka memiliki kuasa untuk membentuk lingkungan bisnis dan investasi secara krusial. Di saat yang sama, negara-negara juga merupakan otoritas pengatur, yang bertanggung jawab untuk mengatur perilaku pemerintah mereka sendiri dan penggunaan teknologi *Spyware,* serta memberikan atau menolak izin ekspor bagi perusahaan yang ingin menjual teknologi ini kepada entitas asing. Peran kunci pemerintah dalam pasar *Spyware* komersial, ditambah dengan peran mereka yang saling bertentangan sebagai pengguna dan regulator menimbulkan ketegangan yang menciptakan tantangan untuk mengatur pembatasan nasional dan internasional terhadap *Spyware* komersial.

Ketiga, Teknologi *Spyware* komersial

memenuhi kebutuhan negara untuk memperoleh kapabilitas yang mampu mengakses dan memanipulasi perangkat, sistem, atau jaringan digital dari jarak jauh tanpa otorisasi. Guna memitigasi risikonya, negara-negara menekankan bahwa perangkat dan layanan ini harus dikembangkan serta digunakan hanya untuk tujuan yang sah (*lawful purposes*) melalui penerapan Kode Etik. Deklarasi Pall Mall Process secara spesifik menyebutkan bahwa penggunaan teknologi tersebut harus tetap berada dalam kerangka hukum, seperti untuk kepentingan keamanan dan pertahanan nasional, investigasi dan pencegahan kejahatan serius, maupun aktivitas keamanan siber..

Teknologi digital, termasuk *Spyware*, umumnya dirancang oleh sektor swasta untuk memenuhi pesanan dan kebutuhan spesifik negara. Indikasi penggunaan Pegasus oleh sejumlah lembaga negara di Indonesia mempertegas adanya keterkaitan negara-swasta (*state-business nexus*) yang berimplikasi langsung terhadap kewajiban perlindungan hak asasi manusia. Hubungan

kontraktual ini sering kali menciptakan celah akuntabilitas (*accountability gaps*), di mana kerahasiaan kontrak pengadaan dan kompleksitas teknologi sering digunakan untuk mengaburkan tanggung jawab atas dampak intrusif yang ditimbulkan.

Dalam praktiknya, otoritas publik dan penyedia swasta kerap berkolaborasi untuk menyesuaikan fitur teknologi sesuai kebutuhan operasional tertentu. Kondisi ini mempertegas kewajiban negara untuk memastikan bahwa teknologi yang diperoleh melalui pengadaan publik tidak merugikan pemegang hak. Prinsip-Prinsip Panduan PBB (UNGPs) memberikan aksentuasi bahwa transaksi komersial negara dengan perusahaan memberikan peluang unik (*unique leverage*). Melalui ketentuan kontrak pengadaan, negara memiliki posisi tawar untuk meningkatkan standar penghormatan HAM oleh perusahaan tersebut. Dengan demikian, pengadaan bukan sekadar transaksi bisnis, melainkan instrumen hukum bagi negara untuk mencegah penyalahgunaan teknologi *Surveilans*.[102]

[102] Morris and Veiberg, "Public Procurement as a Tool to Address Human Rights Risk in the Use of Digital Technology to Deliver Essential Public Services."

Pelapor Khusus PBB untuk Hak atas Kebebasan Berpendapat dan Berekspresi mengartikulasikan keterkaitan pemerintah dengan sektor swasta sebagai kolaborator erat dalam pasar perangkat *Surveilans* digital. Namun, seluruh spektrum kolaborasi ini, mulai dari tahap uji tuntas (*due diligence*) dan penjualan hingga dukungan teknis bagi pengguna akhir, umumnya beroperasi di bawah pengawasan dan transparansi yang sangat terbatas. Dalam kaitan ini, Citizen Lab mengidentifikasi keberadaan pasar kerentanan (*vulnerabilities market*) yang dimanfaatkan secara kolektif oleh pemerintah dan aktor swasta. Pasar ini berfungsi sebagai ruang untuk mengeksploitasi kerentanan *zero-day* demi memperoleh akses ilegal ke komunikasi pribadi dan perangkat individu secara rahasia.[103] Penyebaran dan penyalahgunaan teknologi *Surveilans* menjadi perhatian utama Pelapor Khusus PBB untuk Promosi dan Perlindungan HAM dalam Konteks Kontra-Terorisme. Hal ini disebabkan oleh besarnya risiko terhadap hak-hak fundamental yang muncul akibat definisi tujuan kontra-terorisme dan keamanan yang terlalu luas serta ambigu. Ketidakjelasan definisi

[103] UN 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*, A/HRC/41/35 (28 Mei 2019).

tersebut sering kali dijadikan dalih bagi negara maupun aktor swasta untuk melakukan pengabaian HAM secara sistematis dalam ruang lingkup operasi keamanan.[104]

Infeksi *Spyware* sangat sulit dikonfirmasi secara teknis, sehingga jumlah pasti individu yang menjadi target sulit untuk ditentukan. Di sektor media, sebagai contoh, jurnalis non-investigatif dapat menjadi sasaran hanya karena mereka berkomunikasi dengan sumber yang telah berada di bawah pengawasan. Namun, target yang paling rentan adalah jurnalis yang mempublikasikan artikel yang mengancam rezim otoriter, seperti laporan yang mengungkap kasus korupsi tingkat tinggi.[105] Azerbaijan, negara kaya minyak di pesisir Laut Kaspia, menjadi contoh nyata di mana tekanan terhadap kebebasan berpendapat dan perbedaan pandangan politik terus meningkat sejak 2014. Investigasi yang dilakukan oleh Khadija Ismayilova terhadap kekayaan keluarga penguasa negara tersebut justru menempatkan dirinya sebagai

---

[104] Fionnuala Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, UN Human Rights Special Procedures, April 2023.

[105] Fred Guterl, "Special Report: When Spyware Turns Phones Into Weapons," *Committee to Protect Journalists*, 13 Oktober 2022, https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/. Diakses pada 18 Januari 2026.

target utama *Surveilans* pemerintah. Berdasarkan analisis forensik yang dirilis oleh Laboratorium Keamanan Amnesty International dan Forbidden Stories, ponsel Ismayilova teridentifikasi telah terinfeksi Pegasus secara berkala selama hampir tiga tahun. Kasus ini membuktikan bahwa jurnalis yang mengungkap korupsi di tingkat tertinggi kekuasaan merupakan profil yang paling rentan terhadap serangan *Spyware* lintas tahun.[106]

Sesaat pasca serangan terhadap iPhone Khadija Ismayilova pada 10 September 2019, NSO Group mengumumkan rezim tata kelola perusahaan baru yang diklaim lebih transparan. Langkah-langkah tersebut meliputi: (1) pembaruan kebijakan operasional agar selaras dengan Prinsip-Prinsip Panduan PBB tentang Bisnis dan HAM; (2) pembentukan Komite Tata Kelola, Risiko, dan Kepatuhan; serta (3) penunjukan dewan ahli eksternal untuk menangani isu-isu hak asasi manusia. NSO Group berargumen bahwa inisiatif ini akan memperkuat praktik bisnis etis di industri yang selama

[106] Phineas Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists," *Forbidden Stories*, 18 Juli 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/. Diakses pada 22 Januari 2026

ini mereka klaim telah dijalankan.[107] Namun, NSO Group gagal melaksanakan komitmennya untuk menempatkan HAM sebagai fondasi tata kelola perusahaan. Pada Juli 2021, Proyek Pegasus, konsorsium yang terdiri dari enam belas outlet media global yang dikoordinasikan oleh Forbidden Stories, mengungkapkan bahwa Pegasus tidak hanya digunakan oleh kliennya untuk memata-matai daftar tersangka teroris atau kriminal, seperti yang dijanjikan oleh NSO Group. Investigasi menunjukkan Pegasus telah digunakan secara luas terhadap lebih dari 50.000 anggota masyarakat sipil, termasuk aktivis HAM, jurnalis, akademisi, tokoh agama, dan pengacara.[108] Penyebaran perangkat lunak mata-mata komersial seperti Pegasus bukan hanya ancaman terhadap HAM, tetapi juga juga masuk menjadi bagian masalah keamanan nasional.[109]

---

[107] Laurent Richard dan Sandrine Rigaud, *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy* (New York: Henry Holt and Co., 2023).

[108] Michael Silberman, "Policing Pegasus: The Promise of U.S. Litigation for Commercial Spyware Accountability," *Georgetown Law Technology Review* 8, no. 1 (2024).

[109] Pada 2020 dan 2021, perangkat milik para pejabat di Foreign Commonwealth and Development Office, Inggris diretas dengan Pegasus, bersama dengan sebuah perangkat yang terletak di kediaman Perdana Menteri, 10 Downing Street. Situasi serupa juga terjadi di Amerika Serikat, pada Maret 2023, Gedung Putih mengatakan bahwa setidaknya lima puluh karyawan pemerintahannya diduga atau telah dikonfirmasi menjadi sasaran

Berdasarkan hasil investigasi The Pegasus Project yang dipublikasikan oleh konsorsium Forbidden Stories pada 2021, terungkap bahwa setidaknya 180 jurnalis di seluruh dunia telah dipilih sebagai target potensial oleh klien-klien NSO Group. Temuan ini menegaskan bahwa meskipun perusahaan mengklaim produknya hanya digunakan untuk memerangi terorisme dan kejahatan serius, dalam praktiknya, teknologi *Surveilans* tersebut secara sistematis digunakan untuk membungkam kebebasan pers dan memantau aktivitas jurnalisme investigatif di berbagai negara. Keseluruhan target tersebut tersebar di 20 negara yang 10 diantaranya menjadi klien NSO Group. Klien pemerintah ini berkisar dari pemerintahan yang otokratis, seperti Bahrain, Maroko, dan Arab Saudi hingga pemerintahan yang demokratis, seperti India dan Meksiko. Bahkan perangkat ini telah tersebar di seluruh dunia, dari Hongaria dan Azerbaijan di Eropa hingga Togo dan Rwanda di Afrika. Laporan Pegasus Project memperlihatkan banyak dari pemerintahan tersebut tidak ragu untuk memilih jurnalis, pembela HAM, lawan

perangkat lunak mata-mata komersial. Pada saat yang sama, Presiden Joe Biden mengumumkan larangan penggunaan perangkat lunak mata-mata komersial di seluruh pemerintahan karena masalah keamanan nasional. Presiden Joe Biden menyebut Pegasus secara langsung. Lihat, Silberman, "Policing Pegasus."

politik, pengusaha, dan bahkan kepala negara sebagai target teknologi invasif ini.[110]

Hasil investigasi ini kemudian mendapatkan respons dari NSO Group yang ditujukan kepada Forbidden Stories bahwa atas pertimbangan kontraktual dan keamanan nasional NSO Group tidak dapat mengkonfirmasi atau menyangkal identitas pelanggan (klien) pemerintah.[111] Peta di bawah ini menunjukkan sebaran jurnalis yang ditargetkan perangkat *Spyware*.[112]



[110] Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."
[111] Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."
[112] Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."

Di Maroko, misalnya, Pegasus Project melaporkan jurnalis Soulaiman Raissouni yang dipilih menjadi target sebelum menjadi pemimpin redaksi Akhbar al-Youm, salah satu dari sedikit surat kabar independen di negara itu. Jurnalis ini sekarang menjalani hukuman penjara lima tahun karena pelecehan seksual yang menurut pendukungnya merupakan kasus rekayasa. Editor yang menggantikan Raissouni, Taoufik Bouachrine, juga dilaporkan berada dalam daftar *Surveilans*. Taoufik Bouachrine saat ini menjalani hukuman penjara 15 tahun atas berbagai tuduhan pelanggaran seksual yang diyakini oleh jurnalis lokal dan pendukung kebebasan pers sebagai pembalasan atas pemberitaan kritisnya.[113]

Laporan Citizen Lab menemukan pelibatan teknologi *Spyware* untuk menargetkan individu tertentu di Meksiko. Pemerintah Meksiko memperoleh perangkat lunak *Spyware* dan menggunakannya untuk memata-matai seorang aktivis HAM di negara tersebut dan jurnalis yang secara rutin melaporkan isu-isu terkait korupsi pemerintah. Laporan tersebut mencatat bahwa *Surveilans* tersebut terjadi bertahun-tahun pasca pengungkapan pertama

[113] Guterl, "Special Report: When Spyware Turns Phones Into Weapons."

penggunaan *Spyware* Pegasus di Meksiko dan setelah presiden Meksiko meyakinkan publik pemerintah tidak lagi menggunakan teknologi *Surveilans* digital.[114] Kasus serupa terjadi di El Salvador, *Spyware* dipergunakan untuk mengancam kebebasan pers. Knight First Amendment Institute di Universitas Columbia mengajukan gugatan kepada NSO Group atas nama para jurnalis El Faro.[115] Para jurnalis percaya berdasarkan pola peretasan tersebut mereka menjadi sasaran rezim Nayib Bukele, presiden El Salvador, yang semakin represif. Meskipun El Salvador membantah menjadi klien NSO Group, namun Citizen Lab dan Amnesty International telah memverifikasi temuan tersebut. Kembali NSO Group mengklaim bahwa temuan Citizen Lab dan Amnesty International tidak dapat diandalkan.[116]

---

[114] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

[115] Knight Institute, menjelaskan kelompok jurnalis El Faro membawa kasusnya ke pengadilan Amerika Serikat karena NSO Group menawarkan kepada kliennya kemampuan untuk mengeksploitasi kerentanan dalam perangkat lunak dan layanan perusahaan teknologi Amerika Serikat. Institut tersebut juga mencatat bahwa El Faro banyak dibaca di Amerika Serikat dan salah satu jurnalis yang menjadi target merupakan warga Amerika Serikat. Lihat, Jon Allsop, "Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press," Columbia Journalism Review, 14 Februari 2023, https://www.cjr.org/the_media_today/pegasus_spyware_court_cases.php . Diakses pada 20 Januari 2026.

[116] Allsop, "Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press."

Dalam level yang lebih ekstrim, penggunaan teknologi *Spyware* untuk penargetan massal masyarakat sipil dijumpai di Gaza, Palestina.[117] Apa yang terjadi di Palestina memperkuat fenomena kolonialisme data (*data colonialism*) bagaimana teknologi digital mengubah kehidupan sehari-hari menjadi sumber daya yang diekstraksi untuk keuntungan. Kolonialisme data menciptakan tatanan sosial baru di mana kehidupan manusia diperlakukan sebagai sesuatu yang dapat ditambang, dilacak, dan dimiliki. Wajah, suara, dan gerakan rakyat Palestina diubah menjadi data untuk memperkuat kepolisian yang prediktif dan penargetan otonom. Palestina yang diduduki tidak hanya dianggap sebagai barang sekali pakai, tetapi juga bahan mentah komputasi.[118]

Laporan Francesca Albanese merujuk pada Proyek Nimbus (*Project Nimbus*) dan mengungkapkan sumber pendanaan utama berasal dari Kementerian Pertahanan Israel dengan melibatkan Microsoft, Alphabet, dan Amazon. Seluruh perusahaan ini semuanya memberikan Israel akses hampir penuh ke

---

[117] Suchitra Vijayan, "Technologies of Genocide: How Big Tech Profits From Mass Annihilation," *The Polis Project*, 20 Agustus 2025, https://thepolisproject.com/listen/technologies-of-genocide-how-big-tech-profits-from-mass-annihilation/. Diakses pada 22 Januari 2026

[118] Vijayan, "Technologies of Genocide: How Big Tech Profits From Mass Annihilation."

teknik komputasi awan (*cloud computing techniques*) dan teknologi kecerdasan artifisial mereka untuk meningkatkan kemampuannya dalam pemrosesan data, pengambilan keputusan, *Surveilans* dan analisis. Pada Juli 2024, seorang kolonel Israel menggambarkan teknologi awan sebagai senjata dalam arti kata yang sebenarnya. Peran perusahaan teknologi tidak terbatas pada penyediaan informasi kepada pendudukan Israel dan perangkat genosidanya, tetapi juga meluas hingga memberikan "perisai kekebalan," karena melindungi data penting yang dapat menjadi bukti konklusif di hadapan pengadilan internasional manapun untuk kejahatan perang. Laporan Albanese mengutip Kolonel Racheli Dembinsky, komandan Pusat Komputasi dan Sistem Informasi di angkatan darat Israel, yang bertanggung jawab untuk memproses data angkatan bersenjata, menjelaskan bahwa angkatan darat telah bergantung langsung pada penyimpanan komputasi awan dan layanan kecerdasan artifisial yang disediakan oleh raksasa teknologi dunia: Amazon Web Services, Google Cloud, dan Microsoft Azure.[119]

[119] Vijay Prashad dan Ubai Al-aboudi, "How the World Enriches from the Blood of the Palestinians," Progressive International, 17 November 2025, https://progressive.international/wire/2025-11-17-how-the-world-

Tidak hanya terbatas pada negara-negara otoriter maupun negara yang terlibat dalam konflik bersenjata. Kasus penggunaan *Spyware* juga merambah negara-negara demokratis di Eropa, seperti Yunani, Hongaria, Prancis, Spanyol, Finlandia, Polandia, Siprus, dan Belgia. Laporan investigasi menunjukkan bahwa beberapa negara Eropa telah menggunakan Pegasus atau perangkat *Spyware* serupa untuk memata-matai jurnalis, lawan politik, dan pembela HAM. Perangkat *Spyware* digunakan untuk tujuan yang tidak sah seperti memantau, memeras, mengintimidasi, memanipulasi, dan mendiskreditkan oposisi dan kritikus, menghilangkan pengawasan demokratis dan pers bebas, serta memanipulasi pemilihan umum.[120]

Kondisi serupa juga teramati dalam konteks Indonesia. Gatra Priyandita, ahli kebijakan luar negeri dan politik siber di *Australian Strategic Policy Institute* (ASPI), menyatakan bahwa Indonesia menggunakan perangkat *Spyware* untuk tujuan keamanan nasional

enriches-from-the-blood-of-the-palestinians/en/. Diakses pada 22 Januari 2026.

[120] Agnieszka Bień-Kacała, "Pegasus contra democratic process: experience from Europe," dalam *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World*, ed. Michał Balcerzak dan Julia Kapelańska-Pręgowska (Cheltenham: Edward Elgar Publishing Limited, 2024).

yang sah, seperti pemberantasan terorisme. Namun, Priyandita memberikan catatan kritis bahwa:[121]

> *"Terdapat banyak berita dan anekdot tentang aparat keamanan yang menyalahgunakannya untuk memata-matai jurnalis, tokoh oposisi utama, dan aktivis masyarakat sipil. Kemampuanuntuk memperoleh Spyware komersial menyebabkan penurunan kebebasan sipil dan situasi ini sebagai bagian dari kecenderungan yang lebih luas. Meskipun Spyware hanyalah salah satu metode represi potensial, penggunaannya jelas mempermuda hdan membuat penyalahgunaan kekuasaan oleh para pejabat menjadi lebih leluasa."*

Penggunaan dan pengadaan *Spyware* secara inheren memiliki implikasi yuridis bagi negara. Berdasarkan hukum HAM internasional, setiap negara memiliki kewajiban hukum untuk menghormati dan melindungi HAM, termasuk menjamin adanya upaya pemulihan atau ganti rugi yang efektif atas pelanggaran yang terjadi. Selain itu, negara memegang tanggung jawab untuk mengawasi dan

---

[121] Tom Uren, "Amnesty Flags Possible Spyware Abuse in Indonesia," *Lawfare*, 17 Mei 2024, https://www.lawfaremedia.org/article/amnesty-flags-possible-spyware-abuse-in-indonesia. Diakses pada 20 Januari 2026.

memastikan bahwa perusahaan pemasok mematuhi standar asasi manusia dalam menjalankan bisnisnya, guna mencegah teknologi tersebut digunakan untuk tujuan yang melanggar hukum. Meskipun negara dapat mendelegasikan penyediaan barang dan jasa kepada pihak swasta, kewajiban untuk mematuhi komitmen hukum HAM internasional tetap sepenuhnya berada di tangan negara dan tidak dapat dialihkan. Oleh karena itu, proses pengadaan teknologi digital merupakan modalitas krusial bagi negara untuk mengidentifikasi sekaligus memitigasi risiko pelanggaran HAM yang mungkin timbul dari penggunaan teknologi tersebut dalam layanan publik.[122]

F. Ancaman Perangkat *Spyware* terhadap Demokrasi dan Hak Asasi Manusia: Konstruksi Struktur Norma HAM dalam Merespons Dinamika Relasi Teknologi dan Hak Asasi Manusia

Steven Feldstein mendefinisikan represi digital

[122] Korzak, "Managing Commercial Spyware Through Export Controls: Lesson Learned from the Wassenaar Experience."

sebagai pemanfaatan teknologi informasi dan komunikasi untuk mengawasi, memaksa, atau manipulasi individu dan kelompok. Hal ini dilakukan untuk meredam aktivitas maupun keyakinan yang menantang negara. Represi digital dapat diklasifikasikan ke dalam beberapa kategori, yaitu: *Surveilans* yang ditargetkan (seperti penggunaan *Spyware* dan teknologi ekstraksi data), sensor daring, manipulasi sosial dan disinformasi, pemutusan akses internet (*internet shutdown*), serta persekusi yang ditargetkan terhadap pengguna daring. *Spyware* meretas perangkat yang ditargetkan dari jarak jauh, sementara teknologi ekstraksi data digunakan untuk mengakses dan mengekstrak informasi dari perangkat yang berada dalam kepemilikan fisik operator yang kini digunakan oleh pejabat pemerintah di perbatasan dan pelabuhan masuk di seluruh dunia.[123]

Menurut European Data Protection Supervisor terdapat tiga ciri penting yang membedakan Pegasus dengan perangkat *Spyware* lainnya yang berpotensi menimbulkan risiko dan kerusakan yang belum pernah terjadi sebelumnya. Risiko tersebut tidak

[123] Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa."

hanya pada kebebasan mendasar individu tetapi juga pada demokrasi dan supremasi hukum. Hal ini terjadi karena *Spyware* memiliki kemampuan sebagai berikut:[124]

1) Mendapatkan akses penuh ke perangkat yang ditargetkannya;
2) Melakukan serangan *zero click;*
3) Meninggalkan sedikit atau tanpa jejak.

Penggunaan Pegasus yang tidak sah dapat mengganggu setiap elemen proses demokrasi. Dengan menyasar jurnalis dan aktivis, penggunaan *Spyware* ini menghalangi upaya masyarakat dalam menuntut pertanggungjawaban pemerintah serta lembaga publik lainnya. Selain itu, *Surveilans* telah membuka pintu bagi penindasan, manipulasi, pemerasan, pemalsuan, dan pencemaran nama baik. Tindakan permusuhan tersebut dapat membawa konsekuensi lebih lanjut bagi masyarakat sipil dan partisipasi politik. Warga negara dapat menarik diri dari keterlibatan politik, mengekspresikan pandangan dan pendapat mereka. Penggunaan *Spyware* juga dapat merusak integritas pemilihan umum, atau

[124] Sartor dan Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

setidaknya membuatnya tidak adil. Hal ini terjadi karena pihak penguasa memiliki akses ilegal terhadap informasi rahasia lawan politiknya. Data yang dikumpulkan tersebut kemudian dimanipulasi dan digunakan untuk menyerang kandidat oposisi melalui kampanye fitnah. Kampanye semacam itu dapat membawa konsekuensi lanjutan, kandidat dapat mengurungkan niatnya maju dalam pemilihan.[125] Menurut Winnona DeSombre dkk., *Spyware* merupakan salah satu jenis kemampuan siber ofensif (*offensive cyber capabilities*) yang paling berbahaya. Hal ini dikarenakan *Spyware* mampu memanfaatkan perangkat serta teknik komputasi untuk mengeksploitasi kerentanan jaringan dan sistem komputer secara mendalam. Kemampuan tersebut dikembangkan serta dioperasikan oleh berbagai aktor, mulai dari institusi pemerintah, jaringan kriminal, hingga penyedia layanan *Intrusion-as-a-Service***,** yang menjual jasa peretasan jaringan komputer kepada pihak ketiga.[126] Selama bertahun-

[125] Bień-Kacała, "Pegasus contra democratic process: experience from Europe."

[126] Akses sebagai layanan (Access-as-a-service/AaaS) adalah perluasan yang berkembang dari model kejahatan siber sebagai layanan (cybercrime-as-a-service), di mana pelaku jahat menawarkan titik akses ke jaringan bisnis sebagai produk. Pelaku, yang dikenal sebagai Initial Access Brokers (IAB), beroperasi secara oportunistik, memanfaatkan kerentanan yang teridentifikasi untuk menghasilkan keuntungan. Lihat, UN Interregional

tahun, beberapa kelompok *Access-as-a-Service* telah meniru sektor swasta dan terlibat dengan negara-negara untuk menjual produk dan layanan canggih mereka. Kelompok-kelompok ini telah memperbanyak perangkat kemampuan siber ofensif karena sifat pasar yang semi-teratur.[127]

Industri *Spyware* global terus berekspansi seiring dengan tetap beroperasinya perusahaan seperti Candiru, Cytrox, dan RCS Labs. Pada Juni 2022, peneliti Google memperingatkan sejumlah korban di Kazakhstan dan Italia yang menjadi sasaran program canggih milik RCS Labs bernama Hermit. Perangkat ini tidak hanya mampu mencuri data, tetapi juga dapat merekam suara serta melakukan panggilan secara mandiri. Kemunculan *Spyware* Hermit menunjukkan bagaimana aktor ancaman, yang sering kali bekerja sebagai entitas yang disponsori negara, beralih ke teknologi dan taktik *Surveilans* baru pasca-terungkapnya skandal Pegasus dari NSO Group. Sebelumnya, produk NSO Group tersebut diketahui

---

Crime and Justice Research Institute (UNICRI) dan UN Office of Counter-Terrorism (UNOCT), *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks*, 2024.

[127] Maira Cardillo, Sina Fischer, dan Aditi Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People* (Geneva: Geneva Graduate Institute dan CyberPeace Institute, 2023).

telah disalahgunakan oleh rezim represif untuk menyerang aktivis, organisasi masyarakat sipil, hingga terlibat dalam kasus pembunuhan jurnalis.[128]

Pengaturan yang minimalis di industri ini membuat penyalahgunaan *Spyware* semakin sulit untuk dicegah. Penasihat umum NSO Group, Chaim Gelfand, menolak menyebutkan klien tertentu ketika berbicara di hadapan komite investigasi *Spyware* Parlemen Eropa pada bulan Juni 2022. NSO Group berkilah bahwa penjualan Pegasus kepada pemerintah merupakan tindakan yang sah:[129]

> *"Sistem ini dijual untuk menyelamatkan nyawa, tetapi perangkat ini dapat disalahgunakan"*

Sementara itu, NSO Group sendiri tidak menargetkan individu melalui *Spyware* Pegasus, namun menyediakan sarana bagi negara untuk melakukan *Surveilans*. NSO Group mengakui potensi bahaya tersebut. Pengakuan NSO Group tertuang dalam salah satu laporan perusahaan bahwa NSO group sepenuhnya menyadari bahwa jika pelanggan menyalahgunakan salah satu produk, hal itu dapat

[128] Guterl, "Special Report: When Spyware Turns Phones Into Weapons."
[129] Guterl, "Special Report: When Spyware Turns Phones Into Weapons."

menyebabkan kerugian terhadap HAM individu yang tidak terlibat dalam kejahatan serius atau terorisme, khususnya hak atas privasi atau kebebasan berpendapat dan berekspresi.[130] NSO Group menyatakan tujuan pengembangan Pegasus untuk membantu pihak berwenang menangkap pelaku kriminal yang mungkin berkomunikasi melalui layanan pesan terenkripsi. Namun, perangkat Pegasus juga dapat digunakan untuk tujuan yang tidak sah. Organisasi sipil dan jurnalis investigatif telah mendokumentasikan puluhan kasus *Spyware* Pegasus yang terindikasi melanggar HAM.[131]

Saat ini lebih dari 500 perusahaan mengembangkan, memasarkan, dan menjual perangkat *Surveilans* kepada pemerintah. Oleh karena itu, perlu ada upaya mengatur industri yang yang perkembangannya telah meluas melampaui NSO Group. Pelapor Khusus PBB untuk kebebasan berpendapat dan berekspresi, David Kaye memperingatkan bahwa rezim peraturan untuk

---

[130] Silberman, "The Spyware Exception: How the Foreign Sovereign Immunities Act Protects Foreign State Malware Attacks."

[131] Caitlin Chin-Rothmann, "Cyber Mercenaries: Limiting Government Use of Commercial Spyware," Georgetown Journal of International Affairs, 4 September 2024, https://gjia.georgetown.edu/2024/09/04/cyber-mercenaries-limiting-government-use-of-commercial-spyware/. Diakses pada 25 Januari 2026.

perangkat *Spyware* komersial saat ini sama sekali tidak memadai:

> *"Industri Surveilans swasta komersial merupakan arena bebas yang menciptakan ekosistem yang mempertemukan Negara dan industri berkolaborasi dalam penyebaran teknologi yang menyebabkan kerugian langsung dan teratur bagi individu dan organisasi yang penting bagi kehidupan demokrasi, yakni jurnalis, aktivis, tokoh oposisi, pengacara, dan lainnya."*

Berdasarkan Kovenan Internasional tentang Hak-Hak Sipil dan Politik, pemerintah tidak boleh secara tidak sah atau sewenang-wenang mengganggu kebebasan individu atas privasi, ekspresi, berkumpul, dan berasosiasi.[132]

Penggunaan Pegasus telah menimbulkan kekhawatiran bukan hanya terkait keselamatan jurnalis dan profesional media serta efek mengerikan yang ditimbulkannya pada jurnalisme investigatif, tetapi juga terkait erosi norma-norma demokrasi dan supremasi hukum. Secara khusus, PBB pada 2021

---

[132] Chin-Rothmann, "Cyber Mercenaries: Limiting Government Use of Commercial Spyware."

memberikan atensi khusus melalui Komisaris Tinggi PBB untuk Hak Asasi Manusia, Michelle Bachelet yang menyatakan:[133]

> *"Kekhawatiran atas implikasi yang sangat berbahaya dari penggunaan perangkat Spyware Pegasus terhadap HAM. Kemampuan Surveilans teknologi tersebut menimbulkan risiko serius terhadap kebebasan berpendapat dan berekspresi, yang merupakan hal mendasar bagi demokrasi."*

Pelapor Khusus PBB untuk Hak atas Kebebasan Berpendapat dan Berekspresi merujuk pada kerangka hukum HAM yang melindungi dari *Surveilans* yang ditargetkan. Kovenan Internasional tentang Hak-Hak Sipil dan Politik dan Deklarasi Universal Hak Asasi Manusia melindungi hak setiap orang atas privasi, pendapat, dan ekspresi. Pasal 19 dari kedua instrumen tersebut melindungi hak setiap orang untuk memiliki pendapat tanpa campur tangan dan untuk mencari, menerima, dan menyampaikan informasi dan

---

[133] "Slovakia: Use of Pegasus a Threat to Democracy and Human Rights," *Article19*, 9 September 2024, https://www.article19.org/resources/slovakia-use-of-pegasus-a-threat-to-democracy-and-human-rights/#:~:text=The%20European%20Union%20Agency%20for,use%20of%20Pegasus%20in%20Slovakia. Diakses pada 6 Januari 2026.

gagasan dalam segala bentuk, tanpa memandang batas negara dan melalui media apa pun. Pasal 17 (1) Kovenan, yang menggemakan kembali Pasal 12 Deklarasi Universal Hak Asasi Manusia yang menyatakan bahwa tidak seorang pun boleh dikenai campur tangan sewenang-wenang atau melanggar hukum terhadap privasi, keluarga, rumah, atau korespondensinya. Privasi dan ekspresi saling terkait di era digital, dengan privasi daring berfungsi sebagai gerbang menuju pelaksanaan kebebasan berpendapat dan berekspresi yang aman. Pasal 17 mengizinkan campur tangan terhadap hak atas privasi hanya jika diizinkan oleh hukum domestik yang mudah diakses dan tepat serta sesuai dengan persyaratan Kovenan Internasional tentang Hak-Hak Sipil dan Politik yang dilakukan untuk tujuan yang sah dan memenuhi uji kebutuhan dan proporsionalitas. Pasal 19 merumuskan uji tiga bagian yang mensyaratkan bahwa pembatasan harus diatur oleh hukum dan diperlukan untuk melindungi hak atau reputasi orang lain, keamanan nasional atau ketertiban umum, atau kesehatan masyarakat atau moral.[134]

[134] UN General Assembly, *The right to privacy in the digital age*, UN Doc. A/RES/73/179 (17 Desember 2018).

Selanjutnya Pelapor Khusus merujuk Komite Hak Asasi Manusia dalam kesimpulan pengamatannya pada 2017 tentang laporan periodik keenam Italia. Komite menetapkan hak atas privasi mensyaratkan adanya sistem pengawasan yang kuat dan independen terkait *Surveilans*, penyadapan, dan peretasan, termasuk memastikan lembaga peradilan terlibat dalam otorisasi tindakan tersebut dan memberikan pemulihan yang efektif kepada orang-orang yang terkena dampak penyalahgunaan. Jika memungkinkan, setelah peristiwa *Surveilans*, negara menyampaikan pemberitahuan siapa saja yang telah menjadi target *Surveilans* atau yang datanya telah diretas. Majelis Umum, dalam resolusi 73/179, menekankan bahwa *Surveilans* komunikasi digital harus konsisten dengan kewajiban HAM internasional dan harus dilakukan berdasarkan kerangka hukum yang harus dapat diakses publik, jelas, tepat, komprehensif, dan tidak diskriminatif.[135]

Pelapor Khusus PBB untuk Kebebasan Berkumpul secara Damai dan Berserikat (*Special Rapporteur on Freedom of Peaceful Assembly and of Association*) mendorong semua negara untuk mempromosikan

[135] UN General Assembly, *The right to privacy in the digital age*, UN Doc. A/RES/73/179.

penggunaan dan akses internet yang bebas, terbuka, dapat dioperasikan, andal, dan aman, dengan memfasilitasi kerja sama internasional yang bertujuan untuk pengembangan fasilitas media dan informasi serta komunikasi di semua negara, dengan menghormati dan melindungi HAM, termasuk kebebasan berkumpul secara damai dan berserikat dan hak privasi, dan tidak melakukan pembatasan yang tidak semestinya. Termasuk dalam tindakan pembatasan tersebut di antaranya adalah *internet shutdown, Surveilans* sewenang-wenang atau melanggar hukum, atau sensor daring.[136] Pelapor Khusus menyatakan keprihatinan mendalam atas berbagai kasus di mana aktivitas berkumpul secara damai, termasuk protes damai, justru ditanggapi dengan tindakan represif. Bentuk represi tersebut meliputi penggunaan kekerasan yang melanggar hukum oleh aparat penegak hukum, penyalahgunaan senjata *non-lethal*, serta penangkapan dan penahanan sewenang-wenang. Pelapor Khusus juga menyoroti adanya praktik penyiksaan, perlakuan kejam yang tidak manusiawi, penghilangan paksa, serta *Surveilans* ilegal. Selain itu, represi digital seperti internet shutdown dan pembatasan jaringan juga

[136] UN Human Rights Council, *The Rights to Freedom of Peaceful Assembly and of Association*, Resolusi A/HRC/50/L.20 (4 Juli 2022).

kerap menyasar para pengunjuk rasa, pembela HAM, jurnalis, serta kelompok minoritas dan rentan lainnya yang sedang menjalankan hak mereka atas kebebasan berkumpul secara damai dan berserikat.[137]

Pelapor Khusus dalam laporan sebelumnya mengekspresikan keprihatinan mengenai *Surveilans* yang sewenang-wenang dan melanggar hukum, baik di ruang fisik maupun daring, terhadap individu yang terlibat dalam protes damai, termasuk melalui penggunaan CCTV dan kendaraan *Surveilans* udara, serta melalui penggunaan alat pelacakan digital baru dan yang sedang berkembang, seperti teknologi biometrik, termasuk pengenalan wajah dan emosi serta penangkap identitas pelanggan seluler internasional (*stingray*). Lebih jauh, Pelapor Khusus menyerukan kepada Negara-negara untuk menahan diri untuk melakukan ekspor, penjualan, transfer, penggunaan, atau perawatan barang dan teknologi *Surveilans* yang mungkin digunakan untuk melanggar atau menyalahgunakan HAM, termasuk dalam konteks pertemuan. Bahkan Pelapor Khusus mendesak moratorium global atas penjualan, transfer, dan

[137] UN Human Rights Council, *The Rights to Freedom of Peaceful Assembly and of Association*, Resolusi A/HRC/50/L.20.

penggunaan teknologi *Surveilans* yang ditargetkan tersebut.[138]

Fionnuala Ní Aoláin dalam kapasitasnya sebagai Pelapor Khusus tentang pemajuan dan pelindungan HAM dan kebebasan mendasar dalam memerangi terorisme (*Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*) menarasikan potensi penyalahgunaan perangkat *Surveilans* yang melampaui tujuannya untuk menangkal terorisme:[139]

> *"Teknologi Surveilans canggih yang dikembangkan untuk tujuan kontra-terorisme dan keamanan nasional semakin menjadi fokus perhatian internasional karena terdapat bukti empirik serangkaian pengungkapan yang menunjukkan penggunaan perangkat ini untuk memata-matai politisi, jurnalis, aktivis HAM, pengacara, dan warga biasa yang tidak memiliki*

---

[138] UN Human Rights Council, *The Rights to Freedom of Peaceful Assembly and of Association*, Resolusi A/HRC/50/L.16 (30 Juni 2022).

[139] Fionnuala Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, Laporan Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc. A/HRC/52/39 (1 Maret 2023).

hubungan dengan terorisme dan tidak menimbulkan ancaman keamanan nasional.

Teknologi rahasia yang mengganggu untuk Surveilans isi komunikasi digital individu dan informasi lainnya, termasuk metadata (lokasi, durasi, sumber, dan kontak) yang umumnya dikenal sebagai Spyware telah berkembang pesat secara internasional di luar kendali dan menimbulkan risiko besar terhadap promosi dan pelindungan HAM."

Pelopor Khusus kemudian merujuk pada kasus penyalahgunaan perangkat *Spyware* Pegasus:[140]

"Tantangan mendalam tersebut diilustrasikan oleh skandal terkait penggunaan Pegasus oleh rezim represif, program perangkat lunak Surveilans yang diproduksi oleh perusahaan intelijen siber NSO Group."

Selanjutnya, Pelapor Khusus menekankan bahwa analisis HAM terhadap penggunaan perangkat *Spyware* dalam konteks penanggulangan terorisme

[140] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, UN Doc. A/HRC/52/39.

setidaknya harus memastikan bahwa perangkat tersebut: [141]

1) Memungkinkan pengguna untuk secara spesifik menargetkan data dan metadata tertentu, daripada secara otomatis memantau dan merekam semua data dan metadata;

2) Menghindari akses otomatis ke data yang berkaitan dengan kontak individu yang ditargetkan, kecuali pengguna secara khusus memerlukan informasi tambahan tersebut untuk tujuan investigasi;

3) Menciptakan catatan audit yang tidak dapat dihapus, permanen, dan tidak dapat diedit tentang tindakan apa yang telah dilakukan oleh pengguna *Spyware*, termasuk setiap gangguan/modifikasi data/metadata, kapan hal itu terjadi, dan oleh siapa hal itu dilakukan sehingga penggunaan perangkat tersebut dapat diverifikasi, dan kepatuhannya terhadap HAM dapat dinilai setelah kejadian oleh

[141] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, UN Doc. A/HRC/52/39.

> otoritas peradilan. Perangkat lunak mata-mata yang gagal menampilkan fitur-fitur tersebut, meskipun diatur secara ketat, tidak dapat memenuhi persyaratan HAM.

Laporan situasi Hak atas Privasi oleh Kantor Komisioner Tinggi PBB untuk HAM (*Office of the United Nations High Commissioner for Human Rights*) mengartikulasikan ancaman terhadap HAM yang terdampak akibat pengambilan keputusan yang didasari sistem pengambilan keputusan otomatis, analitik prediktif, dan sistem pengenalan biometrik mengandung bias atau diterapkan dalam konteks yang membuatnya cenderung memilih atau secara tidak proporsional memengaruhi kelompok tertentu. Teknologi *Surveilans* secara historis terkadang digunakan untuk menargetkan kelompok tertentu. Sistem pengenalan biometrik digunakan untuk mengidentifikasi dan melacak demonstran dan pembangkang yang damai dan mendiskriminasi berdasarkan opini politik. Penerapan teknologi *Surveilans* yang sewenang-wenang juga dapat menghambat pelaksanaan kebebasan dan hak-hak lainnya. Serangkaian aktivitas pengawasan yang dilakukan oleh negara dan bisnis merupakan ancaman besar terhadap hak privasi dan hak asasi manusia

lainnya.[142] *Surveilans* digunakan dalam konflik bersenjata yang berdampak parah terhadap warga dan objek sipil. *Surveilans* yang meluas berisiko disalahgunakan untuk penyasaran berbasis ras (*racial profiling*) serta mengidentifikasi dan melacak individu dengan tujuan diskriminatif, misalnya berdasarkan keyakinan politik mereka. Bahkan ketika melayani tujuan yang sah, mulai dari mengelola lingkungan perkotaan yang kompleks hingga memfasilitasi akses ke layanan publik, *Surveilans* seringkali gagal memenuhi persyaratan proporsionalitas. Hal ini menimbulkan tantangan serius terhadap hak atas privasi dan kebebasan yang menjadi inti dari masyarakat demokratis yang terbuka.[143] Secara konsisten, sistem HAM PBB telah menyuarakan kekhawatiran mengenai *Surveilans* oleh lembaga pemerintah, termasuk penyadapan komunikasi secara massal dan terarah, akses serta pengumpulan data komunikasi, hingga intrusi ke perangkat elektronik melalui peretasan. Hal ini juga mencakup peningkatan *Surveilans* di ruang publik, baik secara daring maupun

[142] Office of the United Nations High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/60/45 (29 Agustus 2025).
[143] OHCHR, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/60/45.

luring, yang diperkuat melalui penggunaan teknologi biometrik dan sistem berbasis kecerdasan buatan.[144]

Intrusi melalui perangkat *Surveilans* memengaruhi hak privasi individu. Kantor Komisioner Tinggi PBB untuk HAM (OHCHR) mengkualifikasi *Surveilans* sebagai campur tangan sewenang-wenang atau melanggar hukum terhadap privasi, keluarga, rumah, atau korespondensinya *(arbitrary or unlawful interference with his or her privacy, family, home or correspondence)*. *Surveilans* dapat melanggar hak individu atas kebebasan berserikat dan berekspresi. Berdasarkan hukum HAM internasional, terdapat tiga prinsip sangat penting untuk menilai legalitas tindakan *Surveilans*.[145]

> *Pertama,* apakah hukum domestik mengizinkan *Surveilans*. Dalam kaitan ini penerus Frank La Rue, David Kaye, mengeluarkan laporan pada 2019 yang menegaskan bahwa norma hukum harus dirumuskan dengan cukup tepat untuk

[144] Office of the United Nations High Commissioner for Human Rights (OHCHR), *Mapping report: human rights and new and emerging digital technologies*, UN Doc. A/HRC/56/45 (20 Agustus 2024).
[145] Steve Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace*, 17 September 2019, https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance.

memungkinkan individu mengatur perilakunya sesuai dengan norma hukum tersebut dan harus dapat diakses oleh publik. Persyaratan norma hukum tidak boleh kabur atau terlalu luas *(vague or overbroad)* yang akan memungkinkan diskresi tanpa batas kepada pejabat pemerintah. Kerangka hukum itu sendiri harus dapat diakses publik, jelas, tepat, komprehensif, dan tidak diskriminatif.

Kedua, apakah tindakan *Surveilans* memenuhi standar hukum internasional sesuai prinsip kebutuhan dan proporsionalitas (*necessity and proportionality*) yang akan membatasi *Surveilans* pada situasi yang benar-benar dan terbukti diperlukan untuk mencapai tujuan yang sah (*strictly and demonstrably necessary to achieve a legitimate aim*).

Ketiga, apakah kepentingan yang membenarkan tindakan *Surveilans* itu sah. Banyak perbedaan pendapat dalam menentukan apa yang merupakan *Surveilans* yang sah dan apa yang merupakan penyalahgunaan kekuasaan. Meskipun pemerintah umumnya membenarkan

Surveilans atas dasar keamanan nasional atau ketertiban umum, Kantor Komisioner Tinggi PBB untuk HAM (OHCHR) memperingatkan bahwa pembatasan tersebut dapat secara tidak adil atau sewenang-wenang membatasi hak warga negara atas kebebasan berpendapat dan berekspresi. David Kaye berpendapat bahwa *Surveilans* yang sah mengharuskan negara untuk menunjukkan risiko yang ditimbulkan oleh ekspresi tertentu terhadap kepentingan tertentu dalam keamanan nasional atau ketertiban umum. Selain itu, diperlukan sistem pengawasan yang kuat dan independen yang mempercayakan lembaga peradilan untuk mengesahkan langkah-langkah *Surveilans* yang relevan dan memberikan pemulihan dalam kasus-kasus penyalahgunaan *Surveilans*. Selanjutnya David Kaye menambahkan bahwa *Surveilans* yang sah hanya boleh diterapkan ketika kepentingan seluruh bangsa dipertaruhkan dan harus mengecualikan *Surveilans* yang dilakukan semata-mata untuk kepentingan Pemerintah, rezim, atau kelompok kekuasaan.

Berbagai mekanisme regional menekankan perlunya pengaturan yang ketat, pembentukan mekanisme pengawasan, serta penerapan langkah-langkah akuntabilitas guna mencegah penyalahgunaan *Pegasus* dan perangkat *Spyware* serupa oleh pemerintah. Hal ini didasari oleh mendesaknya kebutuhan untuk melindungi hak asasi manusia, demokrasi, dan supremasi hukum dari ancaman teknologi *Surveilans* yang kian canggih:[146]

1) Laporan Majelis Parlemen Dewan Eropa (*Council of Europe's Parliamentary Assembly*) pada 2023 menyoroti penjualan Pegasus setidaknya kepada 14 negara Uni Eropa, termasuk Belgia, Jerman, Hongaria, Luksemburg, Belanda, Polandia, dan Spanyol. Laporan tersebut menyerukan moratorium atas penjualan dan penggunaan perangkat *Spyware* tersebut sampai kerangka hukum dan pelindungan yang memadai diberlakukan;

2) Komite Penyelidikan Parlemen Eropa (*European Parliament's Committee of*

[146] Cardillo, Fischer, dan Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

Inquiry/PEGA Comittee) yang bertugas menyelidiki penggunaan Pegasus dan perangkat *Spyware* serupa menemukan bukti penyalahgunaan di Polandia, Hongaria, dan Yunani. Rancangan rekomendasi Komite tersebut mengecam penggunaan *Spyware* yang tidak sah oleh pemerintah negara anggota dan menyerukan standar umum Uni Eropa untuk mengatur penggunaan perangkat *Surveilans* tersebut;

3) Badan Uni Eropa untuk Hak-Hak Fundamental (*European Union Agency for Fundamental Rights*) menekankan bahwa penggunaan Pegasus menimbulkan ancaman terhadap hak-hak fundamental yang dijamin dalam Piagam Uni Eropa, seperti kebebasan berekspresi, kebebasan pers, dan kebebasan berasosiasi. Badan Uni Eropa ini juga mengangkat isu tentang efektivitas kontrol ekspor Uni Eropa dan pelindungan HAM dalam pengadaan perangkat *Spyware* dari negara ketiga.

PEGA Committee mendesak pemerintah untuk membatasi pengadaan dan penggunaan *Spyware*

untuk tujuan keamanan nasional melalui langkah-langkah akuntabilitas, seperti pengawasan pengadilan independen atau audit untuk mencegah penyalahgunaan sekunder. PEGA Committee selanjutnya mendesak peningkatan transparansi dengan menerbitkan statistik tingkat tinggi setiap tahun yang mencakup (1) jumlah target *Spyware,* termasuk tujuan umum, kewarganegaraan, dan variabel demografis lainnya; (2) persentase target *Spyware* yang menghasilkan tuntutan pidana; (3) identitas pihak ketiga mana pun yang menerima akses ke teknologi *Spyware;* dan (4) deskripsi prosedur untuk melindungi HAM sepanjang siklus *Surveilans*. Pemerintah juga harus memberitahukan target setelah *Surveilans* berakhir dan jalur bagi individu tersebut untuk mencari keadilan jika terjadi pelanggaran HAM.[147]

Perangkat *Spyware* memiliki kemampuan untuk melakukan intrusi menyeluruh terhadap perangkat yang terinfeksi. Akibatnya, semua data di ponsel dapat diekstrak atau dipantau. Perangkat tersebut dapat digunakan untuk mengumpulkan data lebih lanjut dari lingkungan luar dan mengganggu konten

[147] Chin-Rothmann, "Cyber Mercenaries: Limiting Government Use of Commercial Spyware."

perangkat serta pesan yang dikirim. Dalam konteks ini, Pegasus sulit dideteksi dan dilacak. Meski demikian, perangkat yang telah disusupi *Spyware* memiliki beberapa gejala, misalnya, peningkatan penggunaan data, pengurasan baterai secara tiba-tiba, dan kinerja perangkat yang buruk atau lambat. Gejala seperti ini yang menjadi motivasi mengapa Pegasus atau perangkat *Spyware* lainnya, misalnya Predator dari Cytrox atau Candiru sangat menggoda untuk digunakan terhadap orang selain teroris dan pelaku tindak pidana sehingga dapat membahayakan HAM mereka, terutama hak privasi dan pelindungan data, serta kebebasan berbicara, berasosiasi, dan berkumpul. *Surveilans*, baik yang bersifat massal maupun terarah, dapat menciptakan efek gentar (*chilling effect*) terhadap berbagai aktivitas masyarakat, termasuk dalam ranah privat seperti kesehatan dan keagamaan. Hal ini pada akhirnya memicu sensor diri yang meluas. *Surveilans* telah meruntuhkan rasa aman dan memicu ketidakpercayaan publik secara masif, yang secara fundamental menjadi ancaman nyata bagi keberlangsungan demokrasi.[148]

[148] Megiddo, "Spyware Exports: Recognizing the Limits of Human Rights Law."

Spyware biasanya digunakan bersamaan dengan perangkat penindasan digital lainnya. Selain itu juga terdapat faktor-faktor sosial-ekonomi dan struktural lain yang berperan dalam situasi setiap orang yang tidak dapat dimitigasi oleh pengguna yang ditargetkan (diprofilkan). Sebagian besar individu yang menjadi target *Spyware* mengalami efek gentar (*chilling effect*), seperti melakukan sensor diri dan lebih berhati-hati dalam memilih kata guna menghindari tindakan represif pemerintah, mulai dari pencemaran nama baik dan kehilangan pekerjaan hingga kriminalisasi. Individu-individu yang ditargetkan kemudian menjadi ragu untuk bersosialisasi dan menjalin hubungan dengan individu lain, merasa lebih sulit untuk menjalani hidup secara otentik karena merasa berada dalam bayang-bayang *Surveilans*. Dalam beberapa contoh yang paling ekstrem, *Spyware* menyebabkan perampasan nyawa secara sewenang-wenang atau pemenjaraan berkepanjangan dalam kondisi yang mengerikan.[149]

Kasus pembunuhan Jamal Khashoggi merupakan bukti nyata betapa perangkat *Spyware* menjadi ancaman mematikan bagi demokrasi dan

[149] Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa."

HAM. Pegasus Project mengidentifikasi bahwa kasus pembunuhan Jamal Khashoggi tidak dapat dipisahkan dari intrusi komunikasi pribadi yang dikaitkan penggunaan teknologi *Spyware.* Dalam kasus ini bahkan hak-hak lain Jamal Khashoggi terlanggar, termasuk hak untuk hidup, hak bebas dari penyiksaan dan kekerasan fisik, hak kebebasan berekspresi, dan hak atas privasi.[150] Dalam kasus ini, klien NSO menggunakan perangkat Pegasus yang dapat mengubah telepon menjadi perangkat *Surveilans* yang tertanam pada mikrofon dan kamera yang diaktifkan tanpa sepengetahuan pengguna.[151]

Tidak dapat dipungkiri bahwa saat ini kita telah hidup di dunia *Surveilans* massal akibat maraknya penggunaan teknologi pengenalan wajah hingga pelacakan daring, baik oleh pemerintah maupun perusahaan teknologi. Namun, *Surveilans* yang ditargetkan (*targeted surveillance*) memiliki sifat yang sedikit berbeda. Ia merupakan penggunaan teknologi untuk memata-matai individu secara spesifik.

---

[150] Megiddo, "Spyware Exports: Recognizing the Limits of Human Rights Law."

[151] Stephanie Kirchgaessner, "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian*, 18 Juli J 2021, https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus. Diakses pada 6 Januari 2026.

Kebanyakan orang-orang yang menjadi target adalah jurnalis, blogger, dan aktivis yang menyuarakan kebenaran, mengungkap kesepakatan korupsi, menuntut reformasi pemilu, atau mempromosikan hak atas privasi. Dalam banyak kasus, pemerintah menggunakan berbagai perangkat siber canggih untuk memata-matai secara ilegal, seperti melalui panggilan tak terjawab yang tampaknya tidak berbahaya, pesan teks yang dipersonalisasi, atau pengalihan tanpa sadar ke situs web berbahaya.[152] Pada tahun 2020, Amnesty International merilis laporan mengenai penggunaan *Spyware* untuk mengintai para pembela HAM. Laporan tersebut mengungkap bahwa tokoh-tokoh seperti Ahmed Mansoor (Uni Emirat Arab), Maati Monjib (Maroko), dan Yahya Assiri (Arab Saudi) telah menjadi sasaran operasi *Surveilans*.[153]

Pegasus juga menyasar jurnalis asal Meksiko, yaitu Javier Valdez Cárdenas. Javier Valdez Cárdenas merupakan jurnalis senior pendiri surat kabar Río Doce. Ia dikenal karena menyelidiki kartel narkoba dan kekerasan di Meksiko. Pada Mei 2017, jurnalis ini tewas ditembak di dekat kantornya. Dua rekannya, Andrés

[152] Amnesty International, "When Is Targeted Surveillance Wrong?"
[153] Amnesty International, "When Is Targeted Surveillance Wrong?"

Villarreal dan Ismael Bojórquez, menerima pesan teks berisi tautan berbahaya yang dirancang untuk menginfeksi ponsel mereka. Laporan Citizen Lab mencatat bahwa sedikitnya 24 orang di Meksiko menjadi target serangan serupa, meskipun tidak terkait dengan aktivitas kriminal atau terorisme.[154] Kemudian, menyusul investigasi bersama tentang penggunaan *Spyware* Pegasus terhadap Galina Timchenko, salah satu pendiri, CEO, dan penerbit Meduza, Access Now, Citizen Lab, dan pakar keamanan digital independen Nikolai Kvantiliani telah mengungkap bagaimana setidaknya tujuh jurnalis dan aktivis Rusia, Belarusia, Latvia, dan Israel lainnya telah menjadi target *Spyware* Pegasus milik NSO Group di Uni Eropa.[155]

Penggunaan *Spyware,* khususnya Pegasus yang menyasar gerakan pro-demokrasi terlihat jejaknya di Thailand dan Yordania. Di Thailand, dari Oktober 2020

---

[154] Abdul Razzak, Masashi Crete-Nishihata, dan Ron Deibert, "Reckless VI: Mexican Journalists Investigating Cartels Targeted With NSO Spyware Following Assassination of Colleague," *The Citizen Lab*, 27 November 2018, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/#:~:text=Key%20Findings,to%20prevent%20the%20continuing%20abuse.Diakses pada November 2025

[155] "Exiled, Then Spied on: Civil Society in Latvia, Lithuania, and Poland Targeted With Pegasus Spyware - Access Now," *Access Now*, 30 Mei 2024, https://www.accessnow.org/publication/civil-society-in-exile-pegasus/. Diakses pada 16 Januari 2026.

hingga November 2021, sekitar 30 aktivis, akademisi, pengacara, dan pekerja LSM menjadi sasaran pada saat periode protes pro-demokrasi yang meluas. Di Yordania para pembela HAM harus bekerja di tengah lingkungan yang penuh intimidasi. Belakangan terungkap bahwa beberapa di antaranya, termasuk pengacara dan jurnalis, telah dimata-matai menggunakan *Spyware* Pegasus dalam kurun waktu antara Agustus 2019 hingga Desember 2021. Pola lain dari penggunaan Pegasus atau *Spyware* dapat dikaitkan dengan kecenderungan pemerintahan otoriter dan pelanggaran HAM. Hal ini teramati di Togo dan El Salvador. Di El Salvador sendiri, pada 2021, ditemukan praktik pengintaian terhadap para jurnalis dan aktivis masyarakat sipil. Kasus ini menjadi dasar untuk memetakan pola pemerintahan yang gemar menyalahgunakan teknologi ini. Pola ini terbentuk dari berbagai faktor yang saling berkelindan, mulai dari kehadiran sosok presiden autokratis yang terobsesi pada teknologi digital, rekam jejak intimidasi terhadap media, hingga iklim ketidakamanan dan pelanggaran HAM yang kronis. Ekosistem ini juga mencakup gerak lembaga intelijen, kepolisian, dan sektor keamanan swasta yang beroperasi tanpa pengawasan hukum, yang semuanya berkelindan dengan sejarah panjang

korupsi, kekerasan negara, serta otoritarianisme.[156]

Dalam perkembangannya, pola penggunaan *Spyware* ini tidak hanya menyasar langsung pada perangkat individu, tetapi juga membajak infrastruktur perusahaan teknologi global demi menjangkau target-target mereka. Bahkan WhatsApp dan perusahaan induknya Facebook menggugat NSO Group karena menggunakan server WhatsApp untuk mengirimkan perangkat lunak mata-mata Pegasus ke perangkat 1.400 pengguna. Dalam gugatan yang diajukan di Pengadilan Distrik California Utara pada Oktober 2019, Meta menuduh NSO Group melanggar U.S. Computer Fraud and Abuse Act (CFAA), California Comprehensive Data Access and Fraud Act, serta hukum kontrak dan pelanggaran hak milik. The Citizen Lab mengungkapkan lebih dari 100 serangan ini menargetkan anggota masyarakat sipil, termasuk aktivis HAM, jurnalis, pembangkang, pengacara, dan bahkan pemimpin agama.[157] Dokumen pengadilan secara khusus mencantumkan negara-negara tempat para korban yang terinfeksi oleh Pegasus

[156] Bień-Kacała, "Pegasus contra democratic process: experience from Europe."

[157] Access Now, "Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts," 23 Desember 2020, https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/. Diakses pada 16 Januari 2026.

berada. Jumlah korban tertinggi berada di Meksiko (456 orang), India (100), Bahrain (82), Maroko (69), Pakistan (58), Indonesia (54), dan Israel (51). Selain itu, menurut tabel yang berjudul "*Number of victims by country*" yang diserahkan ke pengadilan oleh WhatsApp, korban juga diidentifikasi di negara-negara seperti Spanyol (21 korban), Belanda (11), Hongaria (8), Prancis (7), Inggris Raya (2), dan Amerika Serikat (1). Satu korban berada di Republik Ceko.[158]

Terlebih, bila merujuk pada Laporan berjudul dari Ekonomi Pendudukan ke Ekonomi Genosida (*From economy of occupation to economy of genocide*) pada 2 Juli 2025 yang disusun Pelapor Khusus PBB tentang situasi HAM di Wilayah Palestina, genosida di wilayah Gaza dimungkinkan dan menguntungkan aktor korporasi khususnya raksasa teknologi, termasuk perusahaan *Surveilans*. Kepentingan korporasi disinyalir mendukung logika ganda kolonial pemukim Israel melalui penggusuran *(displacement)* dan penggantian *(replacement)*.[159] Teknologi

[158] Barbora Šturmová, "Pegasus Spyware Targeted Over 1,400 WhatsApp Users, Including in Hungary and Czechia, Court Documents Show," *VSquare*, 20 November 2024, https://vsquare.org/pegasus-spyware-hacking-whatsapp-meta-hungary-czech-republic/. Diakses pada 16 Januari 2026.

[159] Francesca Albanese, *From economy of occupation to economy of genocide*, Laporan Special Rapporteur on the situation of human rights in

Surveilans dan penahanan, yang biasanya digunakan untuk menegakkan segregasi/apartheid, telah berevolusi menjadi perangkat untuk menargetkan penduduk Palestina. Represi terhadap rakyat Palestina semakin terotomatisasi, dengan perusahaan teknologi menyediakan infrastruktur dwiguna untuk mengintegrasikan pengumpulan data massal dan *Surveilans*. Klaim Israel tentang kebutuhan keamanan telah memicu perkembangan yang belum pernah terjadi sebelumnya dalam layanan pemenjaraan dan *Surveilans*, mulai dari jaringan *closed-circuit television* (*CCTV*), *Surveilans* biometrik, jaringan pos pemeriksaan teknologi canggih, "dinding pintar" dan *Surveilans* drone hingga komputasi awan, kecerdasan artifisial dan analitik data guna mendukung personel militer di lapangan.[160]

Secara lebih luas, *Surveilans* digital yang ditargetkan memiliki dampak unik dan tidak proporsional terhadap perempuan, khususnya perempuan pembela HAM yang juga dapat menjadi sasaran negara melalui cara represi fisik. Mengingat perangkat *Spyware* bayaran memungkinkan kendali

---

the Palestinian territories occupied since 1967, UN Doc. A/HRC/59/23 (2 Juli 2025).

[160] Albanese, *From economy of occupation to economy of genocide*, UN Doc. A/HRC/59/23.

penuh atas perangkat yang terinfeksi, termasuk akses ke kamera, mikrofon, foto/video yang tersimpan, pesan, dan log panggilan, terdapat risiko signifikan bagi perempuan yang menjadi sasaran. Informasi pribadi ini dapat digunakan untuk memfasilitasi berbagai tindakan kekerasan berbasis gender yang difasilitasi teknologi, seperti pemerasan atau doxxing, yang memiliki dampak serius dan tidak proporsional terhadap perempuan yang menjadi sasaran. Lebih jauh, penargetan anggota perempuan dari masyarakat sipil menyebabkan beberapa sasaran hidup dalam keadaan ketakutan yang terus-menerus dan menjadi semakin terisolasi dan terbatas dalam pekerjaan dan kehidupan sosial mereka.[161] Kemudian, dampak *Spyware* dapat meluas melampaui individu yang menjadi target dan dapat memengaruhi anggota masyarakat lainnya. Misalnya, *Surveilans* terarah dapat melemahkan kemampuan masyarakat sipil untuk menjalankan aktivitas demi kepentingan publik, termasuk melakukan investigasi, terlibat dalam aktivisme HAM dan politik, serta berinteraksi dengan jaringan profesional dan pribadi mereka.[162]

---

[161] Siena Anstis & Jillian Sprenger, Civil society and access to justice: challenges of seeking remedy in the global fight against spyware, The International Journal Of Human Rights, 2025

162 ibid

G. Pertarungan Daud *versus* Jalut (Goliath): Publik yang Nirkuasa melawan Kekuatan Gigantik Korporasi Teknologi dalam Bingkai Lanskap Norma Bisnis dan HAM

Pasar *Spyware* global diperkirakan bernilai $12 miliar, dengan pemerintah dan lembaga penegak hukum sebagai pelanggan utama. Perangkat ini memiliki kemampuan untuk mengeksploitasi kerentanan *zero-day*, yakni celah keamanan yang belum diketahui oleh pengembang sistem. Google mencatat bahwa lebih dari separuh eksploitasi *zero-day* yang menargetkan produk-produk mereka berkaitan erat dengan industri *Spyware* komersial.[163] Pasar *Spyware* global saat ini didominasi oleh perusahaan swasta, seperti NSO Group, yang mengomersialkan teknologi *Surveilans* kepada pemerintah dengan mekanisme pengawasan yang sangat minim. Meskipun NSO mengklaim produknya bertujuan untuk memberantas terorisme dan kejahatan, berbagai laporan justru membuktikan adanya penyalahgunaan yang luas terhadap

[163] Mailyn Fidler, "Sanctions for Spyware," Lawfare, 13 Juni 2024, https://www.lawfaremedia.org/article/sanctions-for-spyware. Diakses pada 25 Januari 2026.

masyarakat sipil. Kasus pembunuhan Jamal Khashoggi dan Javier Valdez Cárdenas menjadi bukti minimnya mekanisme kontrol terhadap perusahaan tersebut. Pengaturan global yang masih minimalis memperburuk masalah ini, dan memungkinkan ekspor *Spyware* ke rezim otoriter tanpa akuntabilitas yang jelas.[164]

Pasar *Spyware* berkembang pesat seiring dengan perkembangan digitalisasi yang terus meningkat. Namun, perkembangan tersebut tidak dibarengi dengan kerangka kebijakan yang memadai untuk mengatur transaksi antara negara, badan intelijen, dan sektor keamanan siber swasta. Kondisi tersebut didukung oleh kecenderungan lembaga negara serta perusahaan untuk membiarkan pasar tetap tidak teregulasi demi menjaga keuntungan dari minimnya transparansi dan pengawasan.[165] Hal ini memungkinkan lembaga intelijen dan militer membeli paket *Spyware* untuk menginfeksi serta memata-matai para pengkritik, aktivis HAM, pengacara, hingga jurnalis. Oleh karena itu, dalam sepuluh tahun terakhir

[164]Kyle Volpi Hiebert, "The Growing Global Spyware Industry Must Be Reined In," *CIGI*, 27 Maret 2023, https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/. Diakses pada Oktober 2025.

[165] Cardillo, Fischer, dan Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

ini, pasar *Spyware* terus meningkat secara signifikan.[166]

Produsen perangkat *Spyware* dan perangkat *Surveilans* siber lainnya secara garis besar dapat dibagi dalam dua kelompok, yaitu (1) produsen yang memproduksi perangkat yang terkait dengan proses *local intelligence* dan penyimpanan data; dan (2) produsen yang memproduksi perangkat yang terkait dengan metode peretasan perangkat. Perusahaan-perusahaan dalam industri ini memiliki skala operasional yang bervariasi, begitu pula dengan tingkat kesadaran mereka terhadap mekanisme kontrol ekspor, sanksi internasional, dan kewajiban hukum yang menyertainya. Secara geografis, produksi perangkat *Spyware* serta teknologi *Surveilans* siber lainnya terkonsentrasi di kawasan Eropa. Berdasarkan pemetaan SIPRI (*Stockholm International Peace Research Institute*), tercatat sebanyak 188 perusahaan yang tersebar di 31 negara yang bergerak di industri ini. Dari total produsen tersebut, 51% berlokasi di 19 negara kawasan Eropa. 51% dari seluruh produsen tersebut berlokasi di 19 negara di kawasan Eropa, 22% berlokasi di tiga negara di kawasan Amerika, 13% di tiga negara di

[166] Cardillo, Fischer, dan Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

Kawasan Timur Tengah, dan 13% di lima negara di kawasan Asia dan Oseania. Penyebaran dan penyalahgunaan perangkat *Spyware* dan perangkat *Surveilans* siber lainnya menimbulkan ancaman serius terhadap HAM dan keamanan nasional. Berbagai laporan telah mendokumentasikan bagaimana sejumlah negara memanfaatkan *Spyware* untuk melakukan pelanggaran serius terhadap hukum HAM internasional. Selain itu, organisasi masyarakat sipil turut menyoroti penggunaan teknologi ini dalam konteks konflik bersenjata, yang berpotensi melanggar hukum humaniter internasional.[167]

Dilihat dari pola pelaksanaannya, operasi *Spyware* dapat dibagi ke dalam dua kategori utama. *Pertama*, operasi internal nasional serta aktivitas kelompok *Advanced Persistent Threat* (APT); yakni operasi yang dijalankan oleh aktor-aktor negara dengan kapasitas untuk melakukan serangan intrusi secara mandiri dan berkelanjutan. *Kedua*, operasi yang difasilitasi oleh vendor *Spyware* komersial, di mana negara membeli kemampuan teknis dari pihak swasta. Operasi dalam kategori pertama sering dilakukan oleh negara-negara yang sangat

[167] Mark Bromley dan Giovanna Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint*, SIPRI Report (Stockholm: SIPRI, September 2025), http://doi.org/10.55163/GVXO6716.

mumpuni, seperti kelompok operasi akses khusus yang dilakukan oleh National Security Agency, Unit 8200 Israel, dan aktor-aktor serupa dari Tiongkok atau Rusia yang mendapat dukungan dari pemerintah, baik langsung atau tidak langsung. Operasi kategori kedua dilakukan dengan menggunakan teknologi peretasan siap pakai yang dibeli dari perusahaan keamanan swasta. Produk-produk ini tidak mengharuskan aktor negara memiliki kapasitas internal untuk mengembangkan atau melakukan serangan atau pengawasan siber. Sebaliknya, pemerintah membeli kemampuan ini langsung dari perusahaan, yang menyediakan dukungan purna jual, seperti peningkatan teknis, pembaruan produk, pelatihan, dan layanan pelanggan. Kemunculan sektor *Spyware* komersial telah memberikan akses bagi berbagai negara untuk memperoleh perangkat *Surveilans* canggih yang sulit didapatkan melalui jalur mandiri.[168]

Kehadiran *Spyware* komersial memunculkan ancaman unik akibat karakteristik operasional dan tujuan penggunaannya. Teknologi ini dipasarkan sebagai solusi sah bagi penegak hukum untuk memberantas kejahatan dengan memberikan akses

[168] Feldstein dan Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

ke data sensitif, seperti pesan instan, panggilan, foto, surat elektronik, hingga riwayat penelusuran. Telepon seluler menjadi target utama karena perangkat ini bersifat personal dan berfungsi sebagai pusat komunikasi harian pengguna. Namun, terdapat pula varian yang menargetkan perangkat desktop, seperti Candiru, yang juga dikenal sebagai Karkadann, yang terdeteksi aktif setidaknya sejak 2020.

Meskipun negara-negara demokratis umumnya telah mengatur penggunaan *Spyware* melalui kerangka hukum untuk melindungi hak warga negara dan mencegah *Surveilans* massal, perlindungan ini sering kali terbatas pada yurisdiksi domestik serta rentan didegradasi oleh pergeseran rezim menuju otoritarianisme. Sementara itu, di banyak negara lain, ketiadaan mekanisme perlindungan hukum membuat penduduk sangat rentan terhadap praktik *Surveilans* tanpa kendali. Meskipun sejumlah negara demokratis sering mengatur penggunaan perangkat *Spyware* melalui kerangka hukum yang dirancang untuk melindungi hak-hak warga negara dan mencegah *Surveilans* massal, pelindungan ini sering kali terbatas pada yurisdiksi domestik serta rentan dirusak oleh pergeseran rezim menuju otoritarianisme. Sementara itu, di banyak negara lain, ketiadaan mekanisme perlindungan hukum membuat penduduk sangat

rentan terhadap praktik *Surveilans* tanpa kendali.[169]

Namun demikian, menurut Gail Horak, penelitian khusus tentang *Spyware* komersial masih terbatas karena beberapa alasan. *Pertama, Spyware* komersial biasanya dijual dan dibeli melalui perjanjian kerahasiaan. *Kedua, Spyware* digunakan secara diam-diam oleh operator pemerintah yang ingin tetap tidak terdeteksi di perangkat komputer target selama mungkin. *Ketiga*, teknologi ini juga relatif baru. *Spyware* komersial baru dikembangkan dalam satu dekade terakhir dan baru terungkap melalui kebocoran, peretasan, pelaporan investigatif, dan analisis forensik digital dalam beberapa tahun terakhir. Keberadaan *Spyware* internal yang dibuat oleh pemerintah, yang juga dikenal sebagai ancaman persisten tingkat lanjut, juga baru terungkap secara tidak langsung.[170]

Dalam konteks komersialisasi, Elaine Korzak mendefinisikan teknologi *Spyware* komersial secara luas sebagai kesatuan perangkat keras, perangkat lunak, dan keahlian teknis yang digunakan untuk

---

[169] Maxime Arquillière dkk., *Predators for Hire: A Global Overview of Commercial Surveillance Vendors*, Sekoia, 2025, https://blog.sekoia.io/predators-for-hire-a-global-overview-of-commercial-surveillance-vendors/.

[170] Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa."

memantau, mengeksploitasi, atau menganalisis data secara rahasia. Definisi ini mencakup seluruh spektrum aktivitas data, baik yang sedang disimpan, diproses, maupun ditransfer melalui infrastruktur teknologi informasi dan komunikasi. Dalam kaitan ini teknologi komunikasi dan informasi dapat mencakup perangkat, seperti komputer dan telepon seluler, atau jaringan telekomunikasi secara keseluruhan.[171]

Komersialisasi perangkat spionase dan *Surveilans*, yang semula merupakan ranah eksklusif negara namun kini bergeser menjadi komoditas komersial, telah menjadi perhatian utama Pelapor Khusus PBB tentang promosi dan perlindungan HAM serta kebebasan fundamental dalam pemberantasan terorisme. Dalam laporannya Pelapor Khusus menyatakan:[172]

> *"Sementara di era sebelumnya teknologi spionase dan Surveilans cenderung menjadi hak eksklusif lembaga pemerintah dan pakar teknis internal, di era modern sebagian besar perangkat Surveilans yang digunakan oleh*

[171] Korzak, "Managing Commercial Spyware Through Export Controls: Lesson Learned from the Wassenaar Experience."

[172] Fionnuala Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, UN Doc. A/HRC/52/39 (1 Maret 2023).

lembaga negara diperoleh dari sektor swasta. Perusahaan keamanan siber swasta yang bertanggung jawab atas alat-alat dengan kemampuan tersebut termasuk NSO, Quadream, dan Candiru/Saito Tech yang berbasis di Israel; Gamma International yang berbasis di Inggris; Vilicius Holding dan Trovicor yang berbasis di Jerman; Qosmos dan Amesys yang berbasis di Prancis; Area SpA dan Hacking Team/Memento Labs yang berbasis di Italia; perusahaan Cytrox, yang memiliki divisi di Hongaria, Israel, dan Makedonia Utara; perusahaan Amerika Serikat CyberPoint, Narus (anak perusahaan Boeing), Blue Coat Systems, dan Cisco Systems; dan perusahaan Uni Emirat Arab DarkMatter."

Oleh karena itu, Pelapor Khusus mendesak agar aktivitas bisnis dan perusahaan multinasional ini diatur, sejalan dengan kewajiban negara terkait pengaturan sektor bisnis, untuk mencegah pelanggaran HAM.[173] Hal senada dinyatakan oleh Komisaris Tinggi PBB untuk HAM bahwa diperlukan sistem yang lebih baik dan berbasis HAM untuk mengatur perdagangan perangkat *Spyware,*

[173] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*.

termasuk mekanisme untuk menetapkan akuntabilitas atas pelanggaran HAM pada produsen perangkat *Spyware* swasta dengan mewajibkan secara hukum agar perusahaan-perusahaan yang terlibat memenuhi: (1) tanggung jawab terhadap HAM; (2) jauh lebih transparan terkait dengan desain dan penggunaan produk; dan (3) menerapkan langkah-langkah akuntabilitas yang lebih efektif. Komisaris Tinggi juga menyerukan penangguhan perdagangan teknologi *Surveilans* yang memungkinkan Negara-negara untuk memperkuat rezim ekspor dan kontrol, serta untuk meningkatkan kerangka hukum yang menjamin privasi.[174] Seruan serupa dinyatakan oleh Pelapor Khusus PBB tentang promosi dan perlindungan hak atas kebebasan berekspresi, Pelapor Khusus PBB tentang situasi pembela HAM, Pelapor Khusus PBB tentang hak atas kebebasan berkumpul secara damai dan berasosiasi, dan anggota Kelompok Kerja PBB tentang Bisnis dan Hak Asasi Manusia. Para pemegang mandat Prosedur Khusus tersebut menyatakan: (1) menyuarakan kekhawatiran tentang bahaya yang ditimbulkan oleh teknologi *Surveilans* terhadap HAM; (2) mendesak komunitas internasional untuk mengembangkan

[174] Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*.

kerangka peraturan yang kuat untuk mencegah, mengurangi, dan memulihkan dampak negatif teknologi *Surveilans* terhadap HAM; dan (3) menerapkan moratorium atas penjualan dan transfer teknologi tersebut.[175]

Keprihatinan dan desakan moratorium dari PBB tersebut merupakan respons langsung terhadap transformasi industri *Surveilans* yang semakin tidak terkendali. Ekosistem vendor *Surveilans* komersial terbentuk dan memperkuat proses industrialisasi yang signifikan dalam rentang 2016 dan 2021. Vendor *Surveilans* komersial adalah perusahaan swasta atau kelompok perusahaan yang mengembangkan, memelihara, dan menjual *Spyware* kepada klien, biasanya lembaga pemerintah. Aktivitas vendor ini mencakup penelitian atau akuisisi kerentanan, pengembangan eksploitasi, forensik digital, infrastruktur komando dan kontrol, atau pelatihan klien, yang semuanya biasanya termasuk atau ditawarkan sebagai tambahan dalam paket lengkap. Evolusi ini terlihat dalam penawaran vendor, yang bergeser dari komponen teknis yang terisolasi ke solusi yang sepenuhnya terintegrasi. Pada awalnya vendor berfokus pada penyediaan alat tunggal,

---

[175] Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*.

seperti *implant Spyware* atau modul intersepsi lalu lintas. Seiring evolusi tersebut, aktor baru, seperti NSO telah menjual solusi siap pakai untuk lembaga pemerintah. Solusi ini mencakup rantai infeksi lengkap, seperti vektor intrusi, infrastruktur komando dan kontrol, eksfiltrasi data dengan antarmuka yang ramah pengguna yang menampilkan dasbor, dukungan multibahasa, dan kemampuan geolokasi. Perkembangan vendor ini kian nyata dengan terbentuknya departemen penjualan internasional yang terstruktur serta partisipasi aktif mereka dalam berbagai pameran profesional khusus di tingkat global.[176]

Pegasus membuktikan bagaimana pasar *Spyware* yang tidak teregulasi memfasilitasi pelanggaran HAM secara massal. Fenomena ini kemudian mencapai titik yang lebih mengkhawatirkan pada sistem penargetan berbasis AI seperti *Lavender* dan *The Gospel*, yang memperluas skala penindasan melalui kendali algoritmik. Upaya untuk mengatasi tantangan ini memerlukan pengawasan internasional, akuntabilitas perusahaan, dan perlindungan hukum yang lebih kokoh demi mencegah proliferasi *Spyware* yang tidak terkendali

[176] Arquillière dkk., *Predators for Hire: A Global Overview of Commercial Surveillance Vendors*.

serta perannya dalam membentuk ulang struktur keamanan dan kekuasaan global.[177]

David Lyon menawarkan penilaian menyeluruh terhadap *Surveilans* sebagai fenomena sosial. Semula, *Surveilans* dipahami sebagai alat kekuasaan negara, namun kini ia telah mengalami transformasi dan transfigurasi menjadi instrumen komersial yang kompleks. Menurut Lyon, *Surveilans* merupakan "Perhatian yang terfokus, sistematis, dan rutin terhadap detail pribadi untuk tujuan mempengaruhi, mengelola, melindungi, atau mengarahkan."[178] Melalui pemikirannya, Lyon menunjukkan bahwa kekuatan utama *Surveilans* terletak pada dinamika kekuasaan di dalamnya, yang memungkinkannya beroperasi sebagai sarana kontrol sosial sekaligus instrumen kekuasaan negara.

Studi kasus mengenai pemanfaatan Pegasus mengilustrasikan konvergensi antara privatisasi, transnasionalisasi, dan digitalisasi dalam *Surveilans*

---

[177] Afrose, "Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine."

[178] Dikutip dari Cecile Lourens, "Surveillance at the Intersection of Technology, Business and Politics: A Case Study of Pegasus Spyware," *Diggit Magazine*, 20 Mei 2022, https://www.diggitmagazine.com/articles/surveillance-intersection-technology-business-and-politics-case-study-pegasus-spyware. Diakses pada 12 Januari 2026

modern. Fenomena ini mengungkap adanya keterkaitan antara teknologi dan praktik pemantauan di berbagai sektor, yang melibatkan badan intelijen pemerintah, perusahaan swasta, hingga rezim otoriter. Integrasi tersebut menunjukkan bahwa *Surveilans* kini tidak lagi beroperasi dalam sekat-sekat yang terpisah, melainkan melalui ekosistem global yang melampaui batas kedaulatan negara.[179] Situasi ini menegaskan urgensi pembentukan kerangka kebijakan yang meregulasi penjualan dan ekspor teknologi *Spyware* dengan mengintegrasikan pertimbangan HAM ke dalam tata kelola *Surveilans* siber. Pembaruan regulasi ini sangat krusial untuk menjamin perlindungan warga sipil dari konsekuensi destruktif penyalahgunaan teknologi tersebut, baik oleh aktor negara maupun sektor swasta.[180] Lebih jauh, Pelapor Khusus PBB tentang Kebebasan Berpendapat dan Berekspresi menegaskan bahwa kerangka pengendalian ekspor global, serta implementasi nasional di wilayah tempat NSO Group beroperasi, tidak memadai dalam meregulasi teknologi *Surveilans* maupun memitigasi dampaknya terhadap HAM. Kondisi ini menimbulkan risiko serius terjadinya

[179] Lourens, "Surveillance at the Intersection of Technology, Business and Politics: A Case Study of Pegasus Spyware."
[180] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

pelanggaran hak-hak fundamental, terutama di yurisdiksi dengan kerangka hukum yang minimal atau bahkan tanpa aturan sama sekali terkait penggunaan perangkat *Spyware* tersebut.[181]

Kesenjangan antara regulasi ekspor dan praktik di lapangan ini tercermin secara nyata dalam kasus Azerbaijan. Meskipun negara tersebut tidak tercantum dalam daftar resmi penerima lisensi NSO Group, indikasi kuat kehadirannya di sana menjadi alarm yang mengkhawatirkan. Jika NSO Group terbukti menjual lisensi *Surveilans* siber kepada lembaga pemerintah di Azerbaijan, sebuah negara dengan rekam jejak pelanggaran kebebasan sipil, penindasan politik, dan penyiksaan, maka hal ini mengungkap fakta bahwa tidak ada yang dapat memastikan seberapa jauh jangkauan *Pegasus* dalam memfasilitasi represi di wilayah-wilayah yang tidak terpantau.[182]

Dalam beberapa dekade terakhir, kebutuhan untuk mengatur dan memantau pengembangan dan distribusi teknologi *Surveilans* siber telah diterima di

[181] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."
[182] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

seluruh dunia. Teknologi ini dalam perspektif hukum internasional dikategorikan sebagai teknologi dwiguna (*dual-use technology*) karena dapat digunakan untuk tujuan sipil maupun pertahanan. Ekspor teknologi penggunaan ganda diatur di banyak negara melalui Kesepakatan Wassenaar tentang Pengendalian Ekspor Senjata Konvensional dan Barang dan Teknologi Penggunaan Ganda (*Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*). Kesepakatan ini dirancang untuk mempromosikan transparansi dan tanggung jawab dalam transfer senjata dan teknologi sensitif internasional. Rezim pengendalian ekspor multilateral Wassenaar memfasilitasi pertukaran informasi di antara negara-negara peserta dan bertujuan untuk meningkatkan pengawasan ekspor senjata dan penggunaan ganda. Instrumen utama yang digunakan Kesepakatan Wassenaar untuk mencapai tujuan ini mencakup daftar barang-barang yang harus dikenakan pengendalian ekspor oleh negara-negara peserta.[183]

[183] Meskipun Perjanjian Wassenaar tidak mengikat secara hukum, pemerintah yang mengadopsi daftar kontrol Kesepakatan Wassenaar umumnya memasukkannya ke dalam undang-undang domestik dan mewajibkan mereka yang mengekspor barang-barang yang tercantum dalam perjanjian tersebut untuk memperoleh izin ekspor sebelum melakukan ekspor dengan mempertimbangkan faktor-faktor seperti

Kesepakatan Wassenaar merupakan bagian penting dari sistem pengendalian ekspor multilateral yang berisi peraturan terpisah untuk senjata pemusnah massal dan sistem pengirimannya. Fokus kesepakatan ini ada pada upaya multilateral untuk mengendalikan penyebaran senjata konvensional dan barang dwiguna dengan menyelaraskan dan mengoordinasikan kebijakan pengendalian ekspor setiap negara. Kesepakatan ini hanya menargetkan transfer barang-barang tertentu, dan bukan pengembangan, produksi, kepemilikan, atau penggunaannya. Kesepakatan ini memiliki dua daftar kontrol, yakni Daftar Amunisi (*Munitions List*) yang mencakup persenjataan konvensional, dan Daftar Barang dan Teknologi Dwiguna (*List of Dual-Use Goods and Technologies*). Daftar kontrol tersebut ditinjau dan diperbarui secara berkala, dan setiap keputusan mengenai barang-barang yang terdaftar dibuat berdasarkan konsensus.[184] Dengan demikian, kontrol yang telah diadopsi oleh Kesepakatan Wassenaar dapat memainkan peran kunci dalam

kebijakan dan tingkat keamanan di negara tujuan. Lihat, Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

[184] Elaine Korzak, "Regulating Commercial Spyware Through Export Controls," *Lawfare*, 10 Desember 2025, https://www.lawfaremedia.org/article/regulating-commercial-spyware-through-export-controls. Diakses pada 20 Januari 2026

meningkatkan pengawasan, transparansi, dan pembatasan dalam perdagangan *Spyware* dan perangkat *Surveilans* siber lainnya.[185] Setelah anggota memutuskan untuk memasukkan barang tertentu ke dalam salah satu daftar kontrolnya, implementasinya diserahkan kepada negara-negara peserta. Perubahan harus diimplementasikan dan diterapkan pada tingkat nasional agar efektif dan banyak keleluasaan diberikan kepada masing-masing negara.[186] Praktik penerapan kesepakatan Wassenaar dapat dilihat pada tabel berikut ini.[187]

Kawasan/negara	**Deskripsi**
Uni Eropa 	Uni Eropa menerapkan rezim otorisasi dan persetujuan yang mengatur ekspor barang-barang dwiguna tertentu melalui-

[185] Bromley dan Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint*.

[186] Per tahun 2025, keanggotaan Wassenaar mencakup 42 negara, terutama negara-negara anggota Organisasi untuk Kerja Sama Ekonomi dan Pembangunan (OECD), serta Ukraina, Federasi Rusia, dan India. Meskipun ini mencakup sebagian besar negara industri utama dan pemimpin dalam inovasi teknologi, pengaturan ini saat ini mengecualikan sejumlah negara penting, seperti Israel dan Tiongkok. Lihat,Bromley dan Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint*.

[187] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

	Peraturan Eropa untuk Ekspor Produk Dwiguna (*European Regulations for the Export of Dual-Use Products*). • Peraturan tersebut mencakup kontrol ekspor perangkat lunak intrusi dan sistem pengawasan komunikasi. Menurut Peraturan tersebut, ketika otoritas negara anggota Uni Eropa mempertimbangkan apakah akan menyetujui atau menolak permohonan ekspor, mereka harus mempertimbangkan, antara lain, kewajiban negara anggota berdasarkan sanksi yang dikenakan oleh Dewan Eropa atau oleh Dewan Keamanan PBB, dan pertimbangan yang berkaitan dengan penggunaan akhir barang yang diekspor.

	• Selain itu, Peraturan Kontrol Ekspor (*Export Control Regulations*) yang ditingkatkan yang mulai berlaku di Uni Eropa pada bulan September tahun lalu secara eksplisit mensyaratkan semua ekspor menghormati, dan mematuhi, HAM, dan hukum humaniter.
Amerika Serikat 	• Biro Industri dan Keamanan *(Bureau of Industry and Security/BIS)* bagian dari Departemen Perdagangan Amerika Serikat) bertanggung jawab untuk mengatur ekspor barang-barang dwiguna di Amerika Serikat. Badan ini mengoperasikan: (1) sistem perizinan untuk ekspor barang-barang yang dikendalikan; (2) menentukan kebijakan ekspor barang-barang yang

	dikendalikan; dan (3) menerapkan kebijakan penegakan hukum dan melaksanakan penegakan hukum ekstrateritorial. • Pada Desember 2021, pemerintahan Joe Biden mengakui ancaman berkelanjutan yang ditimbulkan oleh teknologi *Surveilans* siber dan mengumumkan Amerika Serikat akan memerangi penggunaan teknologi spionase dan *Surveilans* siber untuk memata-matai para pembangkang dan aktivis HAM di seluruh dunia dan menempatkan HAM sebagai pusat kebijakan luar negeri Amerika Serikat; • Sebagai bagian dari upaya ini, Komite Peninjau Pengguna Akhir *(End-User Review Committee)* dari (*Bureau of Industry and Security)* BIS memutuskan untuk menambahkan

	empat entitas asing, di antaranya dua perusahaan Israel, NSO Group dan Candiru, dalam Daftar Entitas (Entity List). Kemudian, *U.S. Export Administration Regulations* (Peraturan Administrasi Ekspor AS/EAR) memberlakukan persyaratan lisensi tambahan untuk ekspor ke entitas yang terdaftar, dan membatasi pengecualian untuk ekspor, re-ekspor, dan transfer ke entitas tersebut.[188]

Penerapan Kesepakatan Wassenaar dalam konteks

[188] Namun, tidak jelas apakah penambahan perusahaan ke Daftar Entitas telah mencegah penjualan *spyware*, dan mungkin ada kebutuhan untuk pengawasan yang lebih ketat terhadap industri surveilans siber, yang pengguna akhir dan penggunaan akhirnya sangat sulit dilacak dan penyalahgunaannya sulit untuk dilawan. Pertimbangan ini menyebabkan BIS pada Mei tahun lalu menerbitkan peraturan ekspor yang direvisi yang memberlakukan kontrol baru pada barang-barang keamanan siber yang dapat digunakan untuk spionase atau tindakan lain yang mengganggu jaringan atau perangkat tempat barang-barang tersebut berada. Lihat, Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

dua yurisdiksi utama, yakni Uni Eropa dan Amerika Serikat, terdapat beberapa refleksi yang bisa dipetik sebagai pembelajaran:[189]

> *Pertama,* keputusan kontrol ekspor telah diperumit oleh kebutuhan untuk menyeimbangkan kepentingan baru dan tambahan. Selain kepentingan ekonomi dan kekhawatiran keamanan nasional, negara-negara perlu mempertimbangkan HAM serta pertimbangan keamanan siber dalam konteks kontrol ekspor. Banyaknya pertimbangan ini mengharuskan setiap negara untuk berkontestasi dengan prioritas mereka sendiri agar dapat secara efektif terlibat dan membentuk kontrol ekspor, serta upaya pengaturan internasional lainnya.
>
> *Kedua,* kontrol ekspor Wassenaar bersifat kontroversial yang berdampak jangka panjang pada Kesepakatan Wassenaar dan anggotanya. Kegunaan kontrol ekspor, menghambat kemajuan internasional dalam masalah ini. Alih-alih berfokus pada satu mekanisme pengaturan, para pemangku kepentingan harus mengejar serangkaian

[189] Korzak, "Regulating Commercial Spyware Through Export Controls."

langkah nasional dan internasional untuk mengatasi *Spyware* komersial.

Ketiga, terdapat keterbatasan inheren pada kontrol Wassenaar dan pada kontrol ekspor secara umum yang perlu diidentifikasi dan diakui. Sementara, kontrol Wassenaar hanya menargetkan sebagian kecil teknologi *Spyware* komersial. Hal ini akan berimplikasi pada efektivitas kontrol ekspor akan terbatas.

Berdasarkan refleksi tersebut, keleluasaan yang luas negara peserta dalam mengimplementasikan kesepakatan. Wassenaar Menjadi titik kritis dan kesenjangan efektivitas pembatasan ekspor perangkat *Spyware* komersial.[190] Pada titik yang lain, Israel yang dominan dalam pasar *Spyware* global semakin tidak bertanggung jawab atas ekspor perangkat *Spyware* karena Israel bukan penandatangan Kesepakatan Wassenaar. Israel mengklaim menggunakan daftar kontrol dan memberlakukan kesepakatan ini melalui undang-undang nasional, khususnya Undang-

[190] Doron Hindin, "Can Export Controls Tame Cyber Technology?: An Israeli Approach," *Lawfare*, 12 Februari 2016, https://www.lawfaremedia.org/article/can-export-controls-tame-cyber-technology-israeli-approach. Diakses pada 25 Januari 2026.

> Undang Pengendalian Ekspor Pertahanan Israel (*Israeli Defense Export Control Law*) 2007. Undang-undang ini menunjukkan kepatuhan Israel terhadap ketentuan Perjanjian Wassenaar yang memungkinkan penghapusan hambatan perdagangan barang-barang dwiguna. Undang-Undang tersebut mengatur ekspor peralatan, jasa, dan pengetahuan pertahanan dan dwiguna, mencakup persyaratan untuk memperoleh izin ekspor dari otoritas yang berwenang, dan menetapkan kewajiban pemegang izin, seperti inspeksi, pencatatan, dan tanggung jawab pelaporan.[191]

Meskipun Israel mengawasi secara ketat ekspor teknologi pertahanan dan dwiguna seperti *Spyware,* kontrolnya terutama didasarkan pada pertimbangan pertahanan, keamanan nasional, dan hubungan luar negeri. Pertimbangan ini mengabaikan implikasi teknologi ini terhadap HAM. Bahkan jika HAM dipertimbangkan oleh regulator, kemungkinan besar promosi kebijakan keamanan nasional Israel akan lebih diutamakan daripada pelindungan terhadap HAM. Keputusan pemerintah dalam menentukan

[191] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

lisensi ekspor pertahanan tidak tunduk pada peninjauan yudisial (*judicial review*). Hal ini dikukuhkan oleh putusan preseden Mahkamah Agung Israel pada tahun 2022 yang menetapkan bahwa kebijakan ekspor teknologi siber ofensif ke negara asing berada di luar yurisdiksi pengadilan. Pengaturan teknologi tersebut dianggap sebagai hak prerogatif pemerintah, dengan pertimbangan keamanan nasional sebagai prioritas utama. Putusan ini secara efektif menutup jalur hukum bagi warga sipil maupun organisasi kemanusiaan untuk menggugat ekspor pertahanan ke wilayah kediktatoran atau rezim yang represif.[192]

Sejalan dengan hal tersebut, Anna W. Chan menekankan pentingnya penerapan **r**ezim tanggung jawab bersama (*shared responsibility*) dalam mekanisme penjualan perangkat *Spyware* oleh perusahaan multinasional. Dengan berpijak pada Kesepakatan Wassenaar sebagai instrumen internasional utama dalam kontrol transfer senjata dan teknologi *Surveilans*, rezim ini menuntut peran aktif negara untuk memantau korporasi secara ketat. Hal ini tidak hanya bertujuan untuk mencegah

[192] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

pelanggaran HAM sejak tahap awal, tetapi juga untuk membuka akses yang lebih luas bagi para korban dalam memperjuangkan keadilan dan akuntabilitas hukum. Terlebih lagi, sistem hukum internasional telah memungkinkan berbagai konseptualisasi mengenai tanggung jawab bersama (*shared responsibility*)[193] antara negara dan perusahaan multinasional yang beroperasi secara paralel untuk menutup kesenjangan akuntabilitas terkait dengan perilaku perusahaan multinasional. Hal ini dilandasi prinsip bahwa jika suatu korporasi bertindak atas instruksi atau di bawah arahan atau kendali negara, maka perilakunya dapat dikaitkan dengan negara. Selain itu, tanggung jawab bersama yang melibatkan aktor non-negara ini dapat muncul dalam situasi khusus melalui pengaturan institusional, di mana negara menjalin kontrak dengan korporasi untuk

[193] Rezim tanggung jawab bersama ini akan dibangun berdasarkan rezim multi-pemangku kepentingan berdasarkan Code of Conduct for Private Security Service Providers (ICoC). Pelaksanaan kode etik ini diawasi oleh International Code of Conduct Association (ICoCA) yang berperan sebagai komite pengawasan. Komite ini terdiri dari perwakilan dari perusahaan , kelompok masyarakat sipil, dan negara. Melalui kolaborasi, rezim tanggung jawab bersama akan memberikan praktik pemantauan, pelaporan, dan sertifikasi yang lebih baik bagi entitas korporasi. Lihat, Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

melaksanakan aktivitas *Surveilans* tertentu.[194]

Penerapan tanggung jawab bersama ini dapat merujuk pada Rancangan Pasal-Pasal tentang Tanggung Jawab Negara atas Perbuatan Salah secara Internasional (*Draft Articles on Responsibility of States for Internationally Wrongful Acts*) yang disusun oleh Komisi Hukum Internasional (*International Law Commission*). Rancangan pasal ini hanya berlaku untuk entitas korporasi swasta jika perilakunya dikaitkan dengan negara melalui hubungan yang diperlukan antara korporasi dan negara. Rancangan Pasal-Pasal tersebut bertujuan mengodifikasi aturan dasar hukum internasional mengenai tanggung jawab negara dengan menetapkan syarat-syarat yuridis untuk menentukan kapan suatu negara dianggap bertanggung jawab atas perbuatan salah secara internasional (*internationally wrongful acts*), baik yang berupa tindakan aktif maupun kelalaian (*omission*), serta menetapkan konsekuensi hukum yang timbul darinya. Aturan umum dikonstruksikan melalui keterkaitan perilaku dengan suatu negara di tingkat internasional dengan perilaku organ

[194] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

pemerintahannya, atau pihak lain yang telah bertindak di bawah arahan, hasutan, atau kendali organ-organ tersebut.[195]

Konstruksi norma yang sejalan dapat ditemukan dalam Prinsip-Prinsip Panduan PBB tentang Bisnis dan HAM (*United Nations Guiding Principles on Business and Human Rights*). Prinsip ke-4 secara spesifik menegaskan bahwa:

> *"Negara harus mengambil langkah tambahan untuk melindungi dari pelanggaran HAM oleh perusahaan bisnis yang dimiliki atau dikendalikan oleh negara, atau yang menerima dukungan dan layanan substansial dari lembaga negara."*

Prinsip ke-5 menetapkan bahwa negara tidak melepaskan kewajibannya ketika mereka memprivatisasi penyediaan layanan kepada bisnis yang dapat berdampak pada HAM. Di sisi lain, Prinsip ke-11 menetapkan perusahaan harusmenghindari pelanggaran HAM orang lain dan mengatasi dampak HAM yang merugikan, termasuk mengambil langkah-langkah yang memadai untuk pencegahan, mitigasi

[195] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

dan bila perlu, memberikan pemulihan. Beberapa mekanisme operasional uji tuntas yang diusulkan oleh Prinsip-Prinsip Panduan PBB, termasuk mengadopsi pernyataan komitmen terhadap HAM, mengadaptasi sistem manajemen risiko untuk mengurangi dampak aktual, dan melacak implementasi kebijakan HAM.[196]

Dalam perkembangannya kemudian, terdapat negara dan sebagian sektor swasta mengembangkan berbagai inisiatif untuk mengatasi proliferasi dan penyalahgunaan *Spyware* dan perangkat *Surveilans* siber lainnya. Inisiatif ini bertujuan untuk menetapkan norma dan standar baru, mendorong implementasi hukum HAM internasional yang lebih efektif, dan mencari kompensasi finansial dari produsen *Spyware*. Kontrol ekspor dan sanksi merupakan komponen penting dari upaya yang lebih luas untuk mengatur produksi, perdagangan, dan penggunaan *Spyware* serta perangkat *Surveilans* siber lainnya. Sejak 2012, lima kategori *Spyware* dan perangkat *Surveilans* siber lainnya telah ditambahkan ke daftar kontrol perangkat dwiguna yang dikelola oleh Kesepakatan

[196] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

Wassenaar dan Uni Eropa. Selain itu, Uni Eropa mengadopsi versi baru peraturan perangkat dwiguna Uni Eropa pada 2021, yang bertujuan untuk memperkuat kontrol terhadap ekspor *Spyware* dan perangkat *Surveilans* siber lainnya. Rezim sanksi Uni Eropa mencakup larangan ekspor teknologi *Surveilans* terhadap penerima tertentu, sementara sanksi Amerika Serikat secara spesifik menargetkan para produsen *Spyware*. Sejalan dengan itu, sebanyak 43 negara telah berkomitmen untuk menerapkan kontrol ekspor guna mencegah transfer *Spyware* serta perangkat *Surveilans* siber lainnya yang berisiko memfasilitasi pelanggaran HAM dan hukum humaniter internasional. Komitmen ini menjadi sangat signifikan karena negara-negara tersebut merupakan basis operasi bagi 68 persen perusahaan yang memproduksi *Spyware* dan teknologi siber di dunia.[197]

Secara umum, terdapat tiga cara untuk mengatasi penyebaran dan penyalahgunaan teknologi *Spyware* oleh rezim pemerintah di seluruh dunia. *Pertama*, berfokus pada penguatan rezim kontrol ekspor nasional yang diintegrasikan dengan standar HAM. Pendekatan ini dapat diwujudkan

[197] Bromley dan Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint*.

melalui pembentukan perjanjian internasional baru yang mengikat secara hukum, termasuk penerapan sanksi tegas atas penyalahgunaan teknologi tersebut. *Kedua***,** menitikberatkan pada tanggung jawab korporasi *Surveilans* siber untuk melaksanakan uji tuntas (*due diligence*) dan mengawasi penggunaan teknologi mereka secara mandiri. Keberhasilan mekanisme ini sangat bergantung pada risiko kerugian bisnis atau dampak reputasi negatif yang timbul apabila teknologi mereka terus-menerus dikaitkan dengan pelanggaran HAM.

Solusi *ketiga*, melibatkan mekanisme regulasi oleh perusahaan swasta (*regulation by private companies*) yang dirugikan secara langsung akibat penyalahgunaan teknologi *Spyware*. Dalam pendekatan ini, perusahaan teknologi besar yang ekosistem digitalnya disusupi mengambil langkah mandiri untuk membatasi ruang gerak produsen *Spyware*, misalnya melalui gugatan hukum, pemblokiran akses teknis, hingga penguatan sistem keamanan secara proaktif guna melindungi pengguna mereka.[198]

Mekanisme pengaturan swasta ini terus

[198] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

berkembang sebagai respons atas kemunculan kemampuan siber ofensif yang mengeksploitasi kerentanan dalam produk-produk raksasa teknologi. Eksploitasi tersebut dilakukan untuk membobol dan mengambil alih perangkat pengguna di seluruh dunia, yang secara langsung merusak integritas sistem mereka. Fenomena ini mendorong perusahaan teknologi besar seperti Meta, Amazon, dan Apple untuk mengambil inisiatif dalam mengisi kekosongan regulasi (*regulatory vacuum*) yang ditinggalkan oleh rezim kontrol ekspor. Melalui pengaturan swasta ini, mereka menerapkan tindakan tegas guna menghalangi ruang gerak perusahaan-perusahaan yang mengomersialkan kemampuan peretasan tersebut.[199]

Implementasi dari mekanisme ini terlihat dalam serangkaian tindakan tegas yang diambil oleh para raksasa teknologi. Pada 2019, Facebook (kini Meta) menggugat NSO Group atas eksploitasi celah keamanan pada aplikasi WhatsApp guna menginstal *malware*. Langkah serupa diikuti oleh Apple yang menuntut NSO Group untuk melarang mereka menggunakan produk serta layanan Apple

[199] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

selamanya, menyusul temuan peretasan terhadap pengguna iPhone secara global. Selain melalui jalur litigasi, tindakan preventif juga dilakukan secara teknis. Pada akhir 2021, Meta menutup ratusan akun yang terafiliasi dengan perusahaan intelijen siber Israel setelah terdeteksi memata-matai aktivis, politisi, dan jurnalis di berbagai negara. Amazon pun mengambil langkah serupa dengan memutus akses layanan *cloud* miliknya yang disalahgunakan oleh NSO Group untuk menyebarkan *malware*. Kasus-kasus tersebut mengonfirmasi bahwa perusahaan teknologi besar mampu bertindak sebagai aktor penegak hukum privat dengan memutus akses ke ekosistem produk mereka. Tindakan ini merupakan bagian dari *soft transnational enforcement mechanism*, sebuah mekanisme penegakan transnasional yang bekerja melampaui batas kedaulatan negara. Melalui jaringan global ini, perusahaan swasta secara tidak langsung turut menegakkan standar internasional serta melindungi keamanan siber serta hak asasi manusia di tingkat global.[200]

Pada titik yang lain, doktrin *state-centric* hukum

[200] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

HAM internasional yang berpusat pada negara telah menciptakan sejumlah masalah bagi pengacara yang mencoba meminta akuntabilitas perusahaan atas pelanggaran HAM. Berdasarkan doktrin *state-centric*, perusahaan bukanlah subjek kewajiban perjanjian, dan juga bukan aktor utama di bawah hukum internasional. Doktrin ini mengakibatkan korban perusahaan yang mencari ganti rugi di sistem peradilan negara asal mereka menghadapi banyak hambatan.[201]

[201] Kasus gugatan pelanggaran HAM melalui Alien Tort Statute pada awalnya seringkali digambarkan sebagai mesin utama untuk litigasi HAM transnasional di di Amerika Serikat. Namun, dalam perkembangannya kemudian dengan putusan Mahkamah Agung Amerika Serikat dalam kasus Kiobel v. Royal Dutch Petroleum Co. mengurangi kegunaan litigasi dengan memanfaatkan gugatan Alien Tort Statute. Mahkamah Agung dalam kasus Kiobel secara bulat memutuskan bahwa klaim para pemohon berada di luar yurisdiksi Alien Tort Statute karena Alien Tort Statute tidak berlaku secara ekstrateritorial jika klaim tersebut tidak menyentuh dan menyangkut Amerika Serikat dengan kekuatan yang cukup" Dengan demikian, gugatan ini tidak dapat lagi digunakan untuk meminta tanggung jawab hukum perusahaan multinasional atas pelanggaran HAM. Bahkan ketika suatu tindakan hukum tersedia dalam sistem hukum nasional, sejumlah masalah lain dapat membuat pencarian ganti rugi dalam sistem hukum nasional menjadi kurang menarik; Misalnya, prinsip bahwa korporasi mempertahankan kepribadian hukum yang terpisah dapat mempersulit tanggung jawab hukum perusahaan induk atas tindakan anak perusahaannya karena masing-masing merupakan entitas hukum yang terpisah. Selain itu, sistem hukum seperti Amerika Serikat, di mana doktrin forum non conveniens berlaku, dapat mencegah suatu kasus untuk dilanjutkan ketika yurisdiksi lain lebih cocok atau tepat, seperti lokasi tempat terjadinya dugaan perbuatan melawan hukum yang mengakibatkan pelanggaran HAM tersebut. Lihat, Ruth Cowley, "Kiobel's Impact on

Munculnya berbagai model pengaturan di luar tatanan negara kini mulai mengikis doktrin tradisional hukum internasional. Jika sebelumnya negara dianggap sebagai satu-satunya penanggung jawab utama (*primary duty bearer*) dalam menegakkan standar HAM dan kontrol ekspor teknologi *Surveilans*, kini peran tersebut mulai bergeser.[202]

Namun, mengandalkan pengaturan swasta yang diinisiasi raksasa teknologi bukanlah solusi yang ideal. Masalah fundamentalnya terletak pada benturan kepentingan. Motivasi yang mendorong perusahaan-perusahaan ini untuk bertindak seringkali berbeda dari motivasi negara, serta motivasi para korban utama sistem *Surveilans* siber. Perusahaan teknologi tidak memikirkan kepentingan publik atau nasional ketika mengejar pengaturan swasta. Sebaliknya, perusahan tersebut memilih untuk bersuara dan bertindak hanya ketika mengalami kerugian secara finansial, atau ketika menarik perhatian pada cara menangani

---

Disputes in International Law," *Norton Rose Fulbright*, Mei 2013, https://www.nortonrosefulbright.com/en/knowledge/publications/94bc936c/kiobels-impact-on-disputes-in-international-law. Diakses pada 25 Januari 2026. Lihat juga, Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

[202] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

penyalahgunaan produk mereka dengan cara yang menguntungkan secara finansial. Dengan cara yang sama, kerangka pengaturan swasta seharusnya tidak hanya membebankan tanggung jawab kepatuhan kepada perusahaan swasta, tetapi juga tidak boleh bergantung pada badan-badan swasta, yang memiliki tujuan utama untuk meningkatkan keuntungan mereka bukan untuk penegakan hukum dan HAM.[203]

David Kaye dan Sarah McKune menyatakan penggunaan perangkat *Spyware* merupakan isu kompleks karena menyerang privasi individu, proses hukum yang adil, dan kebebasan berekspresi dan berasosiasi. Oleh karena itu, kerangka hukum yang tepat harus diletakkan pada hukum HAM internasional, yang mensyaratkan: (1) kepentingan yang sah dalam setiap gangguan terhadap hak fundamental dan demonstrasi yang damai; (2) legalitas; dan (3) kebutuhan dan proporsionalitas. Apabila berpijak pada prinsip ini, maka negara-negara yang menggunakan perangkat *Surveilans* harus dilandasi kepentingan yang sah dalam keamanan nasional atau ketertiban umum. Meskipun demikian, keberadaan kepentingan tersebut

[203]Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

hanyalah satu aspek dari penyelidikan hukum. Persyaratan legalitas berarti penggunaan *Spyware* harus diatur oleh hukum secara spesifik dan disertai dengan pengamanan ketat untuk menghilangkan risiko campur tangan sewenang-wenang. Kebutuhan dan proporsionalitas mensyaratkan campur tangan tersebut harus merupakan instrumen yang paling tidak mengganggu di antara instrumen-instrumen yang mungkin mencapai tujuan yang sah dan proporsional dengan tujuan yang hendak dicapai.[204]

Dalam dimensi uji legalitas, penggunaan *Spyware* harus mampu menetapkan batasan HAM yang jelas, mengingat teknologi ini memungkinkan akses jarak jauh tanpa hambatan terhadap seluruh isi perangkat serta kontrol *real-time* atas fungsi audio, video, dan lokasi. Namun, hingga kini, pihak industri maupun penggunanya belum mampu merumuskan standar hukum atau praktik yang dapat menjawab tantangan besar ini. Mengingat rekam jejak pelanggaran HAM yang meluas, sulit untuk tidak berasumsi bahwa batasan hukum yang benar-benar tegas hanya akan menghancurkan model bisnis

[204] David Kaye dan Sarah McKune, "The Scourge of Commercial Spyware—and How to Stop It," *Lawfare*, 25 Agustus 2023, https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it. Diakses pada 23 Februari 2026

industri yang sangat menguntungkan ini. Maka tidak mengherankan jika industri *Spyware* enggan mengusulkan aturan yang serius.[205]

Pada saat yang sama, beban pembuktian atas uji kebutuhan dan proporsionalitas semestinya berada di pundak industri dan negara pengguna. Mereka harus mampu membuktikan bahwa tidak ada instrumen penegakan hukum lain yang tersedia, termasuk praktik *Surveilans* konvensional yang tidak memerlukan penetrasi jarak jauh ke perangkat pribadi. Namun, prinsip ini sulit ditegakkan karena minimnya transparansi pemerintah mengenai kepentingan strategis yang dipertaruhkan. Sejauh ini, banyak bukti justru menunjukkan hal sebaliknya; penggunaan *Spyware* jarang berkaitan dengan pencegahan kejahatan serius, melainkan lebih banyak mengungkap pelanggaran HAM sebagaimana didokumentasikan oleh Citizen Lab, Amnesty International, dan Access Now. Ketidakmampuan pembuktian ini juga berkaitan erat dengan masalah jurisdiksi ekstrateritorial. Seringkali, negara menggunakan *Spyware* untuk meretas target di luar perbatasan mereka tanpa izin. Padahal, secara

[205] Kaye dan McKune, "The Scourge of Commercial Spyware—and How to Stop It."

hukum, kebutuhan akan data lintas negara seharusnya memicu penggunaan perjanjian bantuan hukum timbal balik (*Mutual Legal Assistance Treaties*). Penggunaan MLAT memastikan adanya pengawasan yudisial dan pemenuhan hak atas proses hukum yang adil (*due process*), hal yang justru sengaja dihindari melalui penggunaan *Spyware*. Sejalan dengan itu, Fionnuala Ní Aoláin, Pelapor Khusus PBB untuk kontra-terorisme dan HAM, menegaskan bahwa karena teknologi ini secara inheren tidak memiliki fitur audit dan transparansi, ia pada dasarnya tidak akan pernah bisa memenuhi standar hak asasi manusia, seketat apa pun regulasi yang diterapkan.[206]

Makalah Posisi Pelapor Khusus PBB tentang Kontra-Terorisme dan HAM menetapkan sejumlah syarat teknis minimum yang wajib dipenuhi agar perangkat *Spyware* sejalan dengan standar HAM. Syarat-syarat itu meliputi:[207]

1) Memungkinkan pengguna untuk secara spesifik menargetkan data dan metadata tertentu, daripada secara otomatis

[206] Kaye dan McKune, "The Scourge of Commercial Spyware—and How to Stop It."
[207] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*.

memantau dan merekam semua data dan metadata;

2) Menghindari akses otomatis ke data yang berkaitan dengan kontak individu yang ditargetkan, kecuali pengguna secara khusus memerlukan informasi tambahan tersebut untuk tujuan investigasi;

3) Merancang mekanisme untuk mencegah penggunaan yang berbahaya, seperti sistem penandaan dan 'saklar pemutus' dalam kasus penyalahgunaan yang nyata; dan, dalam hal apa pun;

4) Membuat catatan audit yang tidak dapat dihapus, permanen, dan tidak dapat diedit tentang tindakan apa yang telah dilakukan oleh pengguna perangkat *Spyware,*termasuk setiap gangguan/modifikasi data/metadata, kapan hal itu terjadi, dan oleh siapa hal itu dilakukan sehingga penggunaan alat tersebut dapat diverifikasi, dan kepatuhannya terhadap Hak Asasi Manusia dinilai setelah kejadian oleh otoritas peradilan. Bagian dari catatan

> yang tidak dapat dihapus dan tidak dapat diedit tersebut harus berupa beberapa bentuk pengidentifikasi atau *watermark* sehingga otoritas peradilan yang mengawasi pengaduan dapat memverifikasi produsen perangkat *Spyware* yang diduga telah digunakan terhadap korban dan pelanggan tempat perangkat *Spyware* tersebut awalnya dipasok dan, dari sumber tersebut, dapat memaksa pengungkapan catatan audit sehingga legalitas setiap penggunaan yang dikeluhkan dapat ditinjau secara memadai.

David Kaye dan Sarah McKune menegaskan bahwa penerapan moratorium tetap menjadi langkah penting sebagai tindakan sementara di tengah masifnya penyalahgunaan *Spyware* dan intimidasi global. Selain moratorium, upaya strategis lainnya mencakup pelaporan investigatif oleh organisasi HAM dan jurnalis, keterlibatan aktif para ahli PBB, serta gugatan hukum yang diajukan oleh para korban maupun aktor korporasi seperti WhatsApp dan Apple. Investigasi oleh badan legislatif, penerapan daftar hitam (*blacklist*) oleh pemerintah, serta dialog

multilateral juga menjadi instrumen penting dalam membangun rezim akuntabilitas global guna memastikan penanaman standar HAM yang dipatuhi oleh setiap negara. Lebih lanjut, transparansi, pengawasan, dan akuntabilitas pemerintah, serta jalur efektif untuk pemulihan harus menjadi bagian dari ekosistem pengaturan, baik di ranah nasional maupun internasional. Pada saat bersamaan, keterlibatan sektor swasta dalam perdagangan teknologi *Surveilans* harus diakhiri atau setidaknya dibatasi seketat mungkin juga harus dipertimbangkan.[208]

H. Tantangan dalam Penyelesaian Kasus bagi Korban *Spyware*: Keterbatasan Pelindungan HAM yang Ada untuk Memberikan Pelindungan atas Kelahiran Hak-Hak Digital

Upaya hukum yang ditempuh oleh para korban *Spyware* komersial menghadapi berbagai hambatan struktural yang serius, baik dalam dimensi yurisdiksi, pembuktian, maupun keselamatan fisik para penggugat itu sendiri. Salah satu ilustrasi paling

[208] Kaye dan McKune, "The Scourge of Commercial Spyware—and How to Stop It."

dramatis dari hambatan nonlitigasi adalah kasus Ahmed Mansoor, seorang aktivis hak asasi manusia asal Uni Emirat Arab yang diakui secara internasional dan merupakan penerima penghargaan Martin Ennals Award. Pada Agustus 2016, Mansoor menerima pesan SMS di iPhone-nya yang menjanjikan "rahasia baru" mengenai tahanan yang disiksa di penjara-penjara UAE, dan ketika ia meneruskan pesan tersebut kepada para peneliti Citizen Lab, tautan tersebut diidentifikasi sebagai bagian dari infrastruktur eksploitasi yang terhubung dengan NSO Group dan *Spyware* Pegasus-nya.[209]

Pada Maret 2017, Mansoor ditangkap di rumahnya oleh dua belas anggota aparat keamanan negara UAE, dan setelah menjalani masa penahanan yang sebagian besar berlangsung dalam isolasi penuh dengan akses sangat terbatas terhadap keluarga maupun penasihat hukum, ia dijatuhi hukuman sepuluh tahun penjara pada Mei 2018 atas tuduhan menggunakan media sosial untuk menyebarkan "informasi palsu dan rumor yang merusak persatuan nasional." Kasus Mansoor

[209] Bill Marczak dan John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against A UAE Human Rights Defender," *The Citizen Lab*, 24 Agustus 2016, https://citizenlab.ca/research/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

memperlihatkan betapa seorang korban pengawasan digital yang berpotensi menjadi penggugat justru terlebih dahulu disingkirkan melalui aparatus hukum negara yang sama yang diduga melancarkan pengawasan tersebut, sehingga sama sekali tidak memiliki akses terhadap mekanisme peradilan.

Pada tataran litigasi formal, hambatan yurisdiksi terbukti menjadi rintangan yang kerap kali tidak dapat diatasi. Dalam gugatan yang diajukan oleh Hanan Elatr Khashoggi, istri jurnalis Jamal Khashoggi yang dibunuh, terhadap NSO Group di hadapan Pengadilan Distrik Amerika Serikat untuk Distrik Timur Virginia, pengadilan mengabulkan permohonan NSO Group untuk menolak gugatan atas dasar ketiadaan yurisdiksi personal. Pengadilan menyimpulkan bahwa pihak penggugat tidak cukup membuktikan adanya keterlibatan langsung NSO Group yang diarahkan secara spesifik kepada wilayah negara bagian Virginia, mengingat pengawasan yang disengketakan dilaksanakan oleh aktor-aktor pihak ketiga, yakni pemerintah Arab Saudi dan Uni Emirat Arab. Putusan ini kemudian dikuatkan oleh Pengadilan Banding Sirkuit Keempat, yang menegaskan bahwa NSO Group tidak secara sengaja memanfaatkan hak-hak

istimewa dalam melakukan aktivitas di Virginia. Pola yurisprudensi ini menegaskan bahwa doktrin "purposeful availment" dalam hukum yurisdiksi personal Amerika Serikat secara struktural merugikan korban ketika pengembang *Spyware* beroperasi secara tidak langsung melalui klien pemerintah.[210]

Di tingkat regional Asia Tenggara, kasus Jatupat Boonpattararaksa di Thailand menggambarkan hambatan berbeda yang bersifat evidentiary. Aktivis hak asasi manusia ini menggugat NSO Group setelah perangkatnya terinfeksi Pegasus sebanyak tiga kali antara Juni dan Juli 2021, menuntut ganti rugi senilai 2.500.000 Baht Thailand (setara 72.129 dolar AS), penghentian penggunaan *Spyware* terhadap perangkatnya, serta akses dan penghapusan data yang telah diekstraksi. Namun, pengadilan menolak gugatan tersebut dengan alasan bahwa bukti yang dihadirkan tidak memadai, khususnya terkait ketidakcukupan penjabaran mengenai proses dan hasil investigasi forensik yang menjadi dasar kesimpulan bahwa perangkat penggugat telah diinfeksi *Spyware*. Putusan ini menuai kritik dari

[210] *Hanan Elatr Khashoggi v. NSO Group Technologies Limited, dkk.*, No. 23-2234 (Pengadilan Banding Amerika Serikat untuk Sirkuit Keempat, 21 Mei 2025), https://law.justia.com/cases/federal/appellate-courts/ca4/23-2234/23-2234-2025-05-21.html.

Amnesty International, yang menyatakan bahwa kegagalan pengadilan dalam mengakui peran NSO Group dalam memfasilitasi pelanggaran HAM merupakan hal yang sangat mengkhawatirkan.

Secara teknis, Amnesty International dan Security Lab telah melakukan analisis forensik mendalam terhadap sejumlah perangkat milik para pembela HAM di Thailand dan menemukan bukti infeksi Pegasus, namun standar pembuktian yang diterapkan pengadilan ternyata melampaui kapasitas yang dapat dipenuhi oleh penggugat secara mandiri di persidangan. Hambatan pembuktian ini diperparah oleh posisi konsisten NSO Group yang menyatakan bahwa perusahaan hanyalah pengembang perangkat lunak tanpa kendali atas cara penggunaannya, dan bahwa produk-produknya secara eksklusif dijual kepada lembaga pemerintah untuk keperluan penegakan hukum dan penanggulangan terorisme suatu klaim yang bertentangan dengan temuan riset masyarakat sipil yang mendokumentasikan penyalahgunaan sistematis terhadap jurnalis dan aktivis di berbagai belahan dunia. Secara keseluruhan, ketiga dimensi hambatan ini, penangkapan pra-gugatan, ketiadaan yurisdiksi, dan standar pembuktian forensik yang

tinggi, membentuk sebuah struktur impunitas berlapis yang secara efektif memutus akses keadilan bagi para korban *Spyware* komersial.[211]

Sementara itu, klaim hak-hak digital sedang dalam proses menjadi HAM dan tidak lepas dari kontroversi karena setiap negara dan lembaga peradilan dapat memaknainya secara berbeda.[212] Perbedaan ini juga diperlihatkan melalui fakta bahwa dimensi fundamentalitas pelindungan data pribadi masih terus diperdebatkan, khususnya di kawasan Uni Eropa. Permasalahan fundamentalitas perlindungan data menjadi penting karena telah dipisahkan dari hak atas privasi dalam legislasi Uni Eropa dan telah disebut sebagai hak fundamental. Piagam Hak Fundamental Uni Eropa *(Charter of Fundamental Rights of the European Union)* mengartikulasikan hak privasi kepada warga negara dalam Pasal 7 dan hak atas perlindungan data dalam Pasal 8. Pasal 7 Piagam menetapkan ketentuan tentang

---

[211] Amnesty International, "Thailand: Dismissal of Landmark Case a Critical and Alarming Setback in Fight Against Unlawful Use of Spyware," 21 November 2024, https://www.amnesty.org/en/latest/news/2024/11/thailand-dismissal-of-landmark-case-a-critical-and-alarming-setback-in-fight-against-unlawful-use-of-spyware/.

[212] Yuval Shany, From digital rights to international human rights: The emerging right to a human decision maker, diakses pada 4 Mei 2026

penghormatan terhadap kehidupan pribadi dan keluarga yang mencakup berbagai macam isu, mulai dari kehidupan pribadi dan kehidupan keluarga hingga kekebalan rumah dan kerahasiaan komunikasi. Ketentuan ini didedikasikan sebagai pasal khusus untuk pelindungan data pribadi agar dapat diperlakukan dengan tepat. Sedangkan Pasal 8 Piagam mengakui hak atas perlindungan data pribadi sebagai hak fundamental baru yang berbeda dari hak atas penghormatan terhadap kehidupan pribadi dan keluarga, rumah, dan komunikasi yang tercantum dalam Pasal 7 Piagam. Pasal 8 Piagam terinspirasi dan didasarkan pada berbagai instrumen hukum meskipun perlindungan data pribadi tidak diakui sebagai hak khusus dalam kerangka instrumen internasional yang ada tentang pelindungan HAM. Pasal 8 Konvensi Eropa tentang HAM (European Convention on Human Rights), termasuk yurisprudensi Mahkamah HAM Eropa, tentang perlindungan privasi dan kehidupan pribadi menginspirasi fundamentalitas pelindungan data pribadi, meskipun perlindungan data pribadi tidak secara eksplisit disebutkan dalam Konvensi Eropa tentang HAM. [213]

[213] Bart van der SlootLegal Fundamentalism: Is Data Protection Really a Fundamental Right? Dalam Ronald Leenes, et.al., Data Protection and

Di satu sisi, terdapat aturan dan kasus pelindungan data yang memenuhi syarat sebagai fundamental. Misalnya ketentuan dalam Peraturan Pelindungan Data Umum (General Data Protection Regulation) tentang pengolahan data pribadi sensitif, seperti yang mengungkapkan orientasi seksual atau politik seseorang, kondisi medis, atau ras (etnis), memenuhi syarat sebagai hak fundamental dan penting dalam masyarakat demokratis. Selain itu, kasus-kasus tertentu dalam yurisprudensi Mahkamah Uni Eropa *(Court of Justice of the European Union)* mengartikulasikan hal-hal yang sangat penting untuk mendapatkan pelindungan terhadap HAM. Misalnya, kasus Digital Rights Ireland menyangkut legalitas *Data Retention Directive* yang mewajibkan negara untuk memantau dan menyimpan data lalu lintas internet jutaan warga negara yang tidak bersalah. Mahkamah Uni Eropa menetapkan Data Retention Directive tidak menetapkan aturan yang jelas dan tepat yang mengatur sejauh mana campur tangan terhadap hak-hak fundamental yang diabadikan dalam ketentuan Pasal 7 dan 8 Piagam HAM Eropa. Terdapat juga faktor-faktor lain yang tampaknya menunjukkan pelindungan data tampaknya melindungi nilai yang

Privacy: (In)visibilities and Infrastructures, (Cham: Springer International Publishing AG, 2017)

sangat berbeda dari nilai-nilai yang dilindungi oleh HAM konvensional. Berdasarkan Direktif dan Regulasi Uni Eropa, aturan pelindungan data bertujuan untuk melindungi dua nilai yang sangat berlawanan, yaitu kepentingan individu untuk melindungi data pribadi mereka dan kepentingan pengendali data *(data controllers)* untuk memproses data mereka di pasar internal Uni Eropa di sisi lain.[214]

Pertanyaan normatif dapat ini merujuk pada karakter peraturan pelindungan data dan kasus-kasus oleh Mahkamah HAM Eropa. HAM secara konvensional hanya melindungi sejumlah nilai yang sangat terbatas yang dianggap penting bagi kebebasan pribadi. Yurisprudensi Mahkamah HAM Eropa (*European Court of Human Rights),* misalnya, didasarkan pada konsep-konsep seperti *ratione personae, ratione materiae* dan *de minimis rule.* Berdasarkan pijakan ini kepentingan-kepentingan yang memiliki dampak serius pada kehidupan penggugat dan kepentingan pribadinya yang dilindungi dalam lingkup Konvensi. Akibatnya, pemrosesan data pribadi tidak akan dilindungi dalam lingkup Pasal 8 Konvensi HAM Eropa (European Convention on Human Rights), jika menyangkut

[214] ibid

pemrosesan data sepele, seperti nama dan alamat atau ketika aktivitas pemrosesan data harus dianggap sebagai aktivitas sehari-hari yang biasa. Pasal 8 Konvensi Hak Asasi Manusia Eropa menetapkan tentang pelindungan privasi dan kehidupan pribadi, meskipun pelindungan data pribadi tidak secara eksplisit masuk dalam cakupan pelindungan. Oleh karena itu, terdapat ambang batas bagi kasus-kasus untuk masuk dalam lingkup pelindungan ranah HAM. Sedangkan, instrumen pelindungan data tidak bertujuan untuk melindungi sejumlah nilai pribadi minimum yang penting. Sebaliknya, lingkup data pribadi telah diperluas secara signifikan dari waktu ke waktu. Sepanjang data tersebut dapat digunakan untuk mengidentifikasi seseorang, maka masuk dalam lingkup pelindungan data pribadi. [215]

Hal ini memperlihatkan terdapat perbedaan mendasar dalam sifat HAM dan aturan pelindungan data pribadi. Ketentuan HAM didasarkan pada larangan absolut dan bersyarat. Negara tidak boleh membatasi hak atas privasi dan kebebasan

[215] ibid

berekspresi, kecuali jika hal ini diperlukan dalam masyarakat demokratis dan diatur oleh hukum. Hak atas privasi melindungi hak individu terhadap campur tangan pemerintah, sementara aturan perlindungan data sudah mewujudkan kompromi antara hak dan kepentingan subjek data dan pengontrol data. Aturan pelindungan data itu sendiri sudah merupakan kompromi antara arus informasi yang bebas dan pelindungan data pribadi. Sebagian besar, aturan pelindungan data menyangkut aspek prosedural dan kualitas dari pemroses data pribadi. Misalnya ketika data pribadi diproses, pengontrol data harus memastikan data tersebut benar dan mutakhir, data tersebut diproses dengan cara yang aman dan rahasia, dan pemrosesan berlangsung secara transparan. Pasal 8 Piagam tidak hanya menetapkan data pribadi individu harus dilindungi, tetapi juga menentukan kapan dan bagaimana data pribadi dapat diproses secara sah. Lebih jauh, tidak hanya klausul pembatasan umum yang berlaku untuk Pasal 8 Piagam, hak mendasar atas perlindungan data itu sendiri sudah merupakan kompromi antara berbagai kepentingan yang sah. Dengan demikian, sementara hak atas privasi melindungi kepentingan individu dan dapat dibatasi dalam kondisi tertentu, misalnya jika kepentingan orang lain atau masyarakat luas lebih

besar daripada kepentingan individu, hak atas perlindungan data itu sendiri sudah merupakan kompromi antara berbagai kepentingan, termasuk kepentingan bisnis dan negara untuk memproses data. Dalam hal ini, pelindungan data tampaknya berbeda secara mendasar dari HAM. Asumsi penting yang mendasari hak atas pelindungan data adalah pemrosesan data itu sendiri sah dan bahkan perlu oleh bisnis dan negara, dan bahkan juga warga negara juga perlu memproses data pribadi mereka.[216] Sementara itu, terdapat asumsi yang menyatakan pemrosesan data pribadi sensitif dan data lain yang memiliki dampak signifikan pada kepentingan individu saat ini sudah dilindungi di bawah kerangka HAM, yaitu di bawah hak atas privasi. Hal yang sama dapat dikatakan tentang pengawasan massal, penyimpanan data, dan penyadapan skala besar; Tindakan tersebut biasanya merupakan pelanggaran terhadap kerahasiaan komunikasi dan hak atas kehidupan pribadi warga negara. Oleh karena itu, menghilangkan hak atas pelindungan data dari kerangka hak fundamental tidak akan membuat kepentingan-kepentingan ini tidak terlindungi.[217]

---

[216] ibid
[217] ibid

Pemaknaan yang berbeda antara hak atas pelindungan data pribadi yang masuk dalam lingkup hak digital dan HAM konvensional tersebut tidak terlepas dari perbedaan perspektif teori dan praktik hukum HAM internasional bermuara pada tiga ciri spesifik HAM, yakni universalitas, tidak dapat dicabut, dan kewajiban negara. Hak yang diakui berdasarkan hukum HAM internasional melekat pada setiap manusia, dan ketersediaan hak tersebut tidak bergantung pada status atau perilaku dan akibatnya, tidak dapat dicabut. Meskipun HAM pada prinsipnya bersifat non-absolut dan dapat dibatasi untuk melindungi hak orang lain atau kepentingan publik yang penting. Lebih lanjut, HAM menimbulkan kewajiban bagi negara yang menjalankan yurisdiksi atas pemegang hak individu yang relevan. Dalam konteks HAM digital, ini menyiratkan kewajiban untuk melindungi individu dari pelanggaran hak mereka oleh individu atau perusahaan lain, termasuk perusahaan teknologi. Lebih jauh, menurut Yuval Shany peralihan dari hak digital menuju HAM cenderung didasarkan pada pola pembenaran tertentu, yang terdiri dari klaim dan pertimbangan moral yang mendukung universalitas hak tersebut, ketidakberalihannya, dan pengenaan kewajiban korelatif, analisis masalah yang melibatkan analisis

biaya-manfaat yang mendukung pengenalan hak tersebut, dan identifikasi dukungan politik yang luas untuk mengakui hak yang dimaksud sebagai HAM yang baru (*(new human rights).* [218]

Pada saat yang sama, dampak disruptif dari sistem kecerdasan artifisal dapat memberikan tekanan yang cukup besar pada HAM yang ada. Terlebih lagi, karakteristik *black box* dari sistem kecerdasan artifisial dan kurangnya transparansi yang dihasilkan seputar proses pengambilan keputusan algoritmik mengundang pertimbangan tentang apakah norma HAM yang ada harus direvisi. Revisi terhadap HAM yang ada ini dibutuhkan agar HAM yang ada saat ini dapat menangkap kebutuhan dan kepentingan manusia baru yang ditimbulkan oleh teknologi baru ini. Sejauh mana hukum HAM yang ada memadai untuk menghadapi tantangan yang ditimbulkan oleh meningkatnya penggunaan sistem kecerdasan artifisial dan sejauh mana hukum tersebut perlu direvisi agar dapat secara efektif menanggapi tantangan baru yang ditimbulkan oleh peningkatan penerapan sistem kecerdasan artifisial ini ?[219]

[218] Yuval Shany, op.cit

Kemajuan dalam penerapan teknologi kecerdasan artifisial telah membuka jalan bagi aplikasi inovatif di bidang ilmu saraf, khususnya di bidang pemrosesan sinyal saraf dan neuroteknologi. Teknologi kecerdasan artifisial, termasuk machine learning, deep learning, dan analitik data, telah merevolusi pemrosesan sinyal saraf dengan meningkatkan akurasi, kecepatan, dan efisiensi analisis data. Integrasi kecerdasan artifisial dengan neuroteknologi juga telah membuka pintu baru untuk pengembangan teknologi bantu *(assistive technologies) brain-computer interfaces,* teknik *neuromodulation*, dan *neuroprosthetic*. Algoritma kecerdasan artifisial dapat meningkatkan kinerja dan kemampuan adaptasi perangkat ini, memungkinkan kontrol, interpretasi, dan penerjemahan sinyal saraf secara tepat menjadi perintah atau umpan balik yang dapat ditindaklanjuti.[220]

---

[219] Yuval Shany, The Need for and Feasibility of an International AI Bill of Human Rights, Accelerator Fellowship Programme, Institute for Ethics in AI, University of Oxford November, White Paper, 2025

[220] Siamak Pedrammehr , et.al., (eds.), Artificial Intelligence Advancements in Neural Signal Processing and Neurotechnology, https://www.frontiersin.org/research-topics/61562/artificial-intelligence-advancements-in-neural-signal-processing-and-neurotechnology, diakses pada 4 Mei 2026

Pada perkembangan teknologi yang lain berbasis kecerdasan artifisial, seperti neuroteknologi tetap membutuhkan data dalam jumlah besar sebagai bahan operasinya. Pada saat yang sama, hampir seluruh data internet yang tersedia untuk umum telah dianalisis oleh perusahaan-perusahaan kecerdasan artifisial gigantik. Perusahaan gigantik kini membutuhkan data baru demi terus menyempurnakan model-model inovasi baru yang tengah dirancang. Dalam konteks ini, neuroteknologi menghadirkan peluang yang menarik bagi perusahaan-perusahaan tersebut, karena teknologi ini memungkinkan mereka untuk mengumpulkan data otak dalam jumlah masif. Data yang bersumber dari otak ini yang sangat kaya akan informasi. Banyak perusahaan akan memanfaatkan peluang ini. Konsekuensi lebih jauh, *Surveilans* pikirin *(mind surveillance)* akan menjadi semakin meluas dan bersifat invasif. Situasi ini memunculkan beragam risiko karena sensor-sensor saraf tersebut juga mampu memodifikasi aktivitas otak. [221] Neuroteknologi akan secara bertahap disematkan ke dalam banyak perangkat konsumen, dan dengan

[221] Arnaud Mittempergher , Artificial intelligence can read our thoughts, 2025, lihat https://www.artificialreality.ch/p/ai-can-read-our-thoughts, diakses pada 30 April 2026

demikian akan berdampak pada kehidupan banyak orang. Arnaud Mittempergher mengidentifikasi risiko pemanfaatan neuroteknologi:[222]

1) Surveilan massal oleh pemerintah dan pihak swasta;
2) Hilangnya privasi;
3) *Surveilans* mental di tempat kerja;
4) *Surveilans* terhadap para disiden politik;
5) Manipulasi pemikiran demi tujuan politik;
6) Polisi pemikiran (*Thought police);*
7) Interogasi paksa;
8) Manipulasi proses otak yang bisa memengaruhi niat, emosi, dan pengambilan keputusan seseorang;
9) Manipulasi persepsi dan ingatan;
10) Penyisipan citra buatan ke dalam benak seseorang;
11) Risiko terhadap integritas mental, martabat

[222] Arnaud Mittempergher, Neurorights against mental surveillance, 2025, lihat https://www.artificialreality.ch/p/neurorights-against-mental-surveillance, diakses pada 1 Mei 2026

manusia, identitas pribadi, kebebasan berpikir, dan otonomi;

12) Serangan siber terhadap implan otak, yang dapat menimbulkan berbagai konsekuensi seperti pencurian, modifikasi, atau penghapusan ingatan. Serangan ini juga dapat memengaruhi otonomi fisik seseorang atau menimbulkan dampak psikologis yang signifikan, seperti kecemasan, depresi, atau masalah kesehatan mental lainnya ;

13) Diskriminasi oleh perusahaan asuransi;

14) Manipulasi konsumen oleh perusahaan komersial;

15) Pembuatan senjata yang dirancang untuk melumpuhkan dan mendisorientasi otak manusia;

16) Penjualan data otak kepada pihak ketiga.

Dalam konteks ini, PBB pada 2024 melontarkan kekhawatiran pemanfaatan neuroteknologi dengan memanfaatan ketiadaan atau kelemahan instrumen

hukum yang berdampak pada HAM:[223]

> Kemungkinan dalam beberapa tahun mendatang, produk-produk neuroteknologi yang memiliki langkah-langkah keselamatan tidak memadai serta risiko HAM akan dikomersialkan secara luas.. Produk-produk tersebut akan meresap ke seluruh aspek kehidupan sehari-hari, terlepas dari kenyataan di sebagian besar negara, instrumen hukum yang berlaku masih belum jelas, lemah, atau bahkan tidak ada sama sekali. Celah-celah yang ada dalam instrumen hukum, kurangnya keahlian dan kapasitas teknis, serta ketiadaan badan pengawas yang memadai merupakan faktor-faktor yang pastinya akan dimanfaatkan oleh perusahaan-perusahaan besar yang mengejar keuntungan. Risikonya adalah, tanpa adanya rambu-rambu pengaman yang diperlukan, industri ini akan terus tumbuh tanpa kendali ke arah yang sama: memprioritaskan profitabilitas dan kemudahan di atas pertimbangan etika dan HAM.

[223] ibid

Marcello Ienca dan Roberto Andorno menilai bahwa hak-hak yang ada saat ini tidak lgi memadai untuk merespons risiko-risiko yang berkaitan dengan neuroteknologi. Oleh karena itu, perlu segera melakukan rekonseptualisasi HAM tertentu, atau bahkan penciptaan hak-hak baru. Marcello Ienca dan Roberto Andorno kemudian memunculkan istilah *neurorights* untuk mengatasi tidak memadainya HAM yang ada saat ini mengatasi penerapan neuroteknologi yang berisiko terhadap HAM.[224] Marcello Ienca dan Roberto Andorno menegaskan situasi *terra incognita* hukum HAM internasional untuk mengatasi penerapan neuroteknologi yang mengancam ragam HAM. Oleh karena itu, hukum HAM harus segera berbenah dan adaptif atas risiko yang muncul akibat penerapan teknologi ini:[225]

> Meskipun neuroteknologi berpotensi berdampak pada HAM, seperti privasi, kebebasan berpikir, hak atas integritas

[224] ibid

[225] Marcello Ienca and Roberto Andorno, Towards new human rights in the age of neuroscience and neurotechnology, Life Sciences, Society and Policy, 13:5 (2017)

mental, kebebasan dari diskriminasi, hak atas peradilan yang adil, atau prinsip larangan inkriminasi diri *(self-incrimination),* namun hukum HAM internasional belum memuat rujukan eksplisit apapun mengenai ilmu saraf. Berbeda dengan perkembangan biomedis lainnya yang telah menjadi subjek upaya penetapan standar, baik di tingkat domestik maupun internasional, neuroteknologi sebagian besar masih menjadi *terra incognita* bagi hukum HAM. Kendati demikian, implikasi yang ditimbulkan oleh ilmu saraf dan neuroteknologi terhadap karakteristik inheren manusia menuntut adanya respons yang cepat dan adaptif dari hukum HAM.

Penggunaan teknologi *Surveilans* berpotensi mengancam HAM baru yang lahir di ranah daring. Kelahiran HAM baru dipicu pemanfaatan perangkat teknologi-teknologi baru. Kelahiran HAM baru mensyaratkan pelindungan baru untuk menyesuaikan dengan manifestasi pelanggaran HAM baru tersebut. Pengakuan atas ketidakmampuan

HAM yang sudah mapan untuk memberikan pelindungan yang memadai *(inadequacy of protection)* bagi kelompok-kelompok tertentu dibandingkan dengan kelompok lainnya menjustifikasi urgensi pelindungan HAM baru. Argumentasi lainnya kondisi kontemporer yang baru menantang kemampuan suatu HAM yang sudah mapan untuk memberikan pelindungan yang memadai bagi suatu nilai sosial yang penting. Artikulasi HAM baru tersebut tidak terlepas dari kontestasi antarHAM, antara HAM konvensional dengan HAM baru. Kontestasi ini memunculkan kondisi ketidakmampuan pelindungan HAM yang ada. Dalam konteks ini muncul permasalahan kesetaraan perlindungan HAM di ranah daring dengan perlindungan HAM di ranah luring. Pada titik yang sama mengemuka permasalahan konsepsi pelindungan yang sepenuhnya berakar dan berasal dari ranah luring atau penerapan upaya pemulihan hak yang berlaku di ranah luring untuk diterapkan secara efektif di ranah daring.[226]

Kelahiran HAM baru telah memengaruhi model tata kelola HAM vertikal yang konvensional kehilangan

[226] Mart Susi, The Non-coherence Theory of Digital Human Rights, (Cambridge: Cambridge University Press, 2024)

setidaknya sebagian efektivitasnya mengatasi permasalahan interaksi HAM dengan perangkat teknologi digital. Ketidaksesuaian antara kerangka kerja dan model tata kelola HAM di ranah luring dengan realitas siber secara bertahap bertransformasi menjadi justifikasi diskursif bagi model-model tata kelola yang baru *(new governance model).* Model tata kelola horizontal diajukan sebagai model yang lebih tepat untuk diterapkan pada konteks interaksi HAM di ranah digital. Terdapat aspek spesifik dalam kontestasi yang menjadi ciri khas model tata kelola HAM di ranah Internet. Klaim-klaim HAM baru cenderung berbenturan dengan kerangka kerja yang sudah mapan. Dalam konteks hak digital, kemajemukan kerangka diskursif serta narasi pengaturan terwujud melalui adanya koeksistensi antara model tata kelola pengaturan yang bersifat horizontal dan vertikal di ranah Internet. *Status quo* pengaturan dan ideologis yang ada tidak selaras dengan realitas-realitas baru yang muncul. Joanna Kulesza menawarkan pendekatan multi-stakeholderisme dalam tata kelola internet, sebagai model pembuatan kebijakan terdistribusi yang didasarkan pada kerja sama sukarela antar-aktor-aktor kunci yang biasanya diidentifikasi sebagai negara, sektor bisnis, dan masyarakat sipil yang

beroperasi sesuai dengan peran masing-masing melalui prinsip konsensus dan kode yang berjalan. [227]

Salah satu dampak teknologi terhadap HAM sehingga memunculkan klaim HAM baru merujuk pada perkembangan neuro-rights. *Neuro-rights* muncul sebagai respons terhadap pesatnya perkembangan neuroteknologi, yang berpotensi mengubah cara manusia memahami dan memperlakukan otak manusia. Akan tetapi, teknologi-teknologi ini juga menghadirkan tantangan etis dan sosial yang signifikan terkait dengan pelindungan hak-hak individu, privasi, dan otonomi mental.[228] Kelahiran *neuro-rights* ini tidak terlepas dari HAM yang ada saat ini tidak mampu memberikan pelindungan yang memadai terhadap ancaman dan risiko yang ditimbulkan oleh perkembangan-perkembangan ini. Perkembangan neuroteknologi memunculkan pertanyaan mengenai seberapa meyakinkankah klaim HAM saat ini mampu memberikan pelindungan yang memadai, serta risiko atau kerugian apa yang mungkin timbul dari

[227] ibid

[228] Yan Cornejo, Neurorights, Neurotechnologies and Personal Data: Review of the Challenges of Mental Autonomy, Journal of Digital Technologies and Law, 2(3), 2024

pengenalan HAM baru tersebut. Klaim HAM baru menghadapi tantangan bagaimana pendasaran yuridis klaim HAM baru tersebut. Sementara itu, HAM baru didefinisikan sebagai hak-hak yang pada saat pertama kali digagas belum diakui secara eksplisit dalam perjanjian HAM mana pun, dan juga belum diakui dengan cara lain apa pun sebagai hak dalam pengertian hukum.[229] Inisiatif mengusulkan HAM baru bagi ranah digital merupakan respons terhadap tantangan-tantangan baru terhadap HAM di dunia yang kian terdigitalisasi. Perkembangan mutakhir dalam upaya memperkuat tata kelola kecerdasan artifisial turut berkontribusi dalam perdebatan ini. Namun, apakah benar-benar terdapat kebutuhan untuk mengakui HAM digital yang benar-benar baru, ataukah sudah cukup memadai untuk sekadar menyesuaikan atau memperluas hak-hak yang sudah ada melalui interpretasi guna menghadapi ancaman-ancaman baru yang muncul dari dunia maya? Inisiatif HAM baru merupakan suatu proses yang bermula dari identifikasi kebutuhan pelindungan baru dilanjutkan dengan perumusannya dalam bentuk hak, dan akhirnya pengakuan serta

[229] Nora Hertz, Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought, Neuroethics 16:5 (2023)

implementasi pelindungannya.[230]

Menurut Yuval Shany dalam beberapa kasus, kesenjangan normatif antara HAM luring dengan kebutuhan serta kepentingan para pengguna daring mencapai tingkat yang meresahkan. Situasi ini mengisyaratkan bahwa adaptasi terhadap hak yang sudah ada tidak lagi layak dilakukan, atau justru akan menghasilkan luaran yang sangat tidak memadai. Dalam keadaan-keadaan seperti ini, pengembangan HAM baru, seperti hak untuk tidak dijadikan subjek keputusan algoritmik *(right not to be subject to algorithmic decisions)* atau hak untuk dilupakan *(right to be forgotten*) mungkin menjadi langkah yang patut diambil.[231]

Keterbatasan hukum HAM internasional menurut Yuval Shany menempatkan pengguna hak-hak digital dalam ketidakpastian risiko kepastian mendapatkan pelindungan HAM:[232]

> Menavigasi di antara norma-norma lama dan baru melibatkan dilema kebijakan

[230] Wolfgang Benedek, Is There a Need for New Digital Human Rights in AI Governance? Tiina Pajuste, (ed.), Human Rights in the Digital Domain: Core Questions, (Cambridge: Cambridge University Press & Assessment, 2026)
[231] Yuval Shany, Digital Rights and the Outer Limits of International Human Rights Law , German Law Journal 24, (2023),
[232] ibid

hukum yang pelik. Pembentukan norma-norma baru dalam Hukum HAM Internasional tidak serta-merta mengharuskan pengenalan kerangka kerja hukum HAM internasional yang baru, melainkan justru menyoroti kekurangan-kekurangan pada kerangka kerja yang sudah ada. Namun, mengakui ketidaksesuaian hak-hak yang berlaku di ranah luring tanpa adanya seperangkat HAM baru yang siap sedia untuk memberikan pelindungan bagi para pengguna daring menciptakan risiko individu-individu akan terombang-ambing tanpa kepastian yakni, menghadapi kesenjangan perlindungan. Pada saat yang sama, berpegang teguh pada norma-norma hukum HAM internasional yang ada saat ini, meskipun norma-norma tersebut kian dipandang tidak lagi relevan juga berakibat pada kurangnya pelindungan terhadap kebutuhan dan kepentingan di ranah daring.

Pada level nasional perlindungan menyeluruh

terhadap HAM fundamental di era digital juga terbatas karena hak-hak digital belum tertanam sebagai hak konstitusional. Menurut Juliane Müller penanganan pelindungan hak di tingkat konstitusional menawarkan kerangka kerja yang lebih kuat dan langgeng untuk menghadapi ancaman digital yang kian bermunculan, dibandingkan hanya mengandalkan undang-undang biasa semata. Seiring dengan semakin besarnya pengaruh teknologi digital terhadap pelaksanaan hak-hak sipil dan politik, serta kebebasan-kebebasan fundamental lainnya, jaminan konstitusional yang kokoh menjadi sangat esensial untuk menjawab tantangan-tantangan baru mulai dari *Surveilans* dan penyensoran yang tidak sah hingga tata kelola berbasis algoritma dan monopoli data.[233] Oleh karena itu, mengabadikan hak-hak digital di dalam konstitusi menawarkan kerangka kerja yang unik, tangguh, dan langgeng untuk melindungi hak-hak fundamental dari berbagai tantangan baru di era digital. Pelindungan hak-hak digital akan semakin kuat mengingat konstitusional lebih sulit untuk diubah dan memiliki kedudukan yang lebih tinggi dibandingkan undang-undang.

[233] Juliane Müller , Rights in the Digital Age, https://www.idea.int/publications/catalogue/html/rights-digital-age, diakses pada 1 Mei 2026

Konstitusionalitas hak digital berperan sebagai landasan yang kokoh bagi pelindungan hak dan kebebasan fundamental di tengah konteks teknologi yang terus berkembang. Dengan menanamkan hak-hak digital ke dalam konstitusi negara-negara dapat memastikan adanya pelindungan yang konsisten. Pada saat yang sama, langkah ini juga menyediakan mekanisme pengawasan yang lebih kuat untuk mencegah penyalahgunaan kekuasaan oleh pemerintah, seperti *Surveilans* atau penyensoran yang tidak sah maupun potensi tindakan melampaui batas oleh aktor-aktor swasta, termasuk perusahaan teknologi raksasa atau entitas yang memonopoli data. Pengakuan konstitusional menetapkan standar yang jelas bagi perilaku korporasi yang etis dan akuntabel, serta mengirimkan sinyal yang kuat, baik di tingkat domestik maupun internasional bahwa hak-hak digital diperlakukan secara serius dan dilindungi pada tingkatan hukum tertinggi.[234]

Dalam konteks ini, HAM telah ditetapkan dan dilindungi oleh hukum, baik melalui perjanjian internasional, konstitusi nasional, maupun berbagai undang-undang, upaya memastikan hukum-hukum tersebut ditegakkan, termasuk dengan membawa

[234] ibid

kasus-kasus tertentu ke pengadilan belum membawa keadilan bagi korban. Pengadilan tidak selalu menjadi wadah yang ramah terhadap penegakan HAM. Penundaan yang memakan biaya besar, aturan prosedur yang menghambat, manuver hukum dengan memanfaatkan celah hukum yang ada, serta hakim yang kurang berempati, baik secara terpisah maupun secara gabungan dari faktor-faktor tersebut dapat menyebabkan kasus-kasus ketidakadilan akhirnya ditolak. Risiko kegagalan bahkan jauh lebih tinggi di negara-negara yang independensi dan imparsialitas peradilannya masih diragukan. Para hakim mungkin merasa enggan untuk menegakkan HAM, ketika undang-undang yang represif dan/atau diskriminatif justru memperoleh dukungan luas dan didukung penuh oleh para politisi. [235]

Pada saat yang sama, seiring kemajuan teknologi digital, kini media digital dan media sosial menawarkan perangkat baru yang penting bagi gerakan sosial, aktivis, dan kritikus negara. Pada titik yang sama, perangkat ini juga secara substansial untuk memperluas *Surveilans* negara dan penindasan terhadap aktor-aktor tersebut.

---

[235] **Defending Human Rights in Court, https://www.openglobalrights.org/courts/, diakses pada 1 Mei 2026**

Penggunaan *Surveilans* digital oleh negara-negara sudah berlangsung lama. *Surveilans* ini dapat mengambil banyak bentuk dan memungkinkan pemerintah untuk mengumpulkan intelijen yang dapat digunakan untuk menargetkan individu atau kolektif tertentu. Misalnya, teknologi dwiguna, seperti inspeksi paket mendalam, memungkinkan operator untuk memantau lalu lintas dan konten Internet. Demikian pula, media sosial dapat dipantau dengan cara yang serupa. Sementara *Surveilans* konvensional sering dilakukan pada target tertentu atau kelompok target yang lebih kecil. Represi digital memungkinkan *Surveilans* terjadi dalam skala besar ketika dilakukan dengan melibatkan Penyedia Layanan Internet. [236]

Praktik yang berlangsung memperlihatkan, *Surveilans* terselubung dapat dilakukan oleh berbagai aktor swasta. Pertama, individu dan kelompok dapat terlibat dalam *Surveilans* daring. Kedua, korporasi juga berperan penting di bidang ini, baik secara mandiri maupun melalui kemitraan mereka dengan pemerintah. Pemerintah dan korporasi dapat melakukan kontrak langsung dengan

[236] Jennifer Earl, Thomas V. Maher , Jennifer Pan, The digital repression of social movements, protest, and activism: A synthetic review, Earl et al., Sci. Adv. 8, (2022)

kelompok peretas atau bekerja sama dengan mereka secara tidak langsung melalui perantara. Kemudian munculnya fenomena *Surveilans* kapitalisme yang memungkinkan *Surveilans* dalam skala besar dan mikro yang ditargetkan secara simultan terhadap tindakan dan minat pengguna oleh korporasi. Selain itu, beberapa kebijakan yang ada justru menguntungkan perusahaan media sosial dan menjadi keuntungan bagi pemerintah yang berniat untuk menekan aktivisme daring. Perusahaan telah memperoleh keuntungan dengan menjual data pribadi pengguna kepada penegak hukum, menjual teknologi yang dibutuhkan untuk melakukan *Surveilans* berbasis jaringan kepada pemerintah; menjual *Spyware* yang memanfaatkan eksploitasi *zero-day* untuk mengubah ponsel menjadi perangkat *Surveilans* seluler; dan menjual perangkat kecerdasan artifisial yang digunakan untuk *Surveilans* massal dan dapat dengan mudah digunakan kembali untuk tujuan represif. Perusahaan-perusahaan, seperti NSO Group, Gamma Group, dan Hacking Team menyediakan akses negara terhadap layanan eksploitasi, peretasan, dan *Surveilans*. [237]

Penggunaan perangkat *Spyware* Sebagian

[237] ibid

besar dilakukan secara rahasia dan dengan pengawasan terbatas, pemerintah menggunakan perangkat *Spyware* untuk menargetkan dan mengumpulkan informasi tentang masyarakat sipil. Hal ini telah menyebabkan banyak pelanggaran HAM terhadap masyarakat sipil, yang secara langsung dilakukan oleh negara-negara represif dan dimungkinkan oleh perusahaan perangkat *Spyware.* Penargetan *Spyware* masyarakat sipil yang rentan, seperti jurnalis dan pembela HAM, akan menghadapi hal yang komplek untuk mengakses terhadap keadilan. Setiap individu mungkin memiliki konsepsi yang berbeda tentang seperti apa keadilan seharusnya dalam konteks memulihkan kerugian yang mereka alami. Selain itu, setiap individu mungkin menghadapi hambatan unik tergantung pada konteks tempat mereka berada.[238] Serangan *Spyware* yang ditargetkan dapat memberikan penyerang akses waktu nyata ke data lokasi dan komunikasi dan sekaligus dapat menimbulkan ancaman fisik yang nyata bagi target. Dalam kaitan ini, serangan *Spyware* seringkali diikuti penahanan sewenang-wenang, penyiksaan, dan pembunuhan di luar hukum. Kasus Loujain Al-Hathloul, seorang pembela HAM

[238] Siena Anstis & Jillian Sprenger, op.cit

perempuan Arab Saudi memperlihatkan keterkaitan tersebut. Dalam proses hukum di Amerika Serikat, Al-Hathloul mengklaim penggunaan perangkat *Spyware* untuk memata-matai komunikasi dan pergerakannya menyebabkan penangkapan sewenang-wenang oleh Uni Emirat Arab dan pemindahannya ke Arab Saudi. Sesampainya di Arab Saudi, Al-Hathloul kemudian ditahan, dipenjara, dan disiksa.[239]

Meskipun PBB telah menegaskan komitmennya terhadap HAM universal secara daring, seperti halnya di dunia nyata. Prinsip ini hanya benar-benar bermakna ketika para pelanggar menghadapi konsekuensi, dan jika dunia nyata menjadi indikatornya. Banyak kasus memperlihatkan data pribadi digunakan untuk merusak demokrasi, serangan siber dilancarkan untuk melumpuhkan infrastruktur penting, atau celah keamanan *zero-day* disebarkan untuk menginfeksi perangkat dengan *ransomware*, namun para pelaku hampir tidak pernah menghadapi keadilan.[240]

Perkembangan teknologi berbasis data

[239] ibid

[240] Marietje Schaake, Internet governance needs tough love, 2019, lihat, https://www.gwi-boell.de/en/2019/11/18/internet-governance-needs-tough-love, diakses pada 5 Mei 2026

bermuara pada ketidakadilan baru dan menjadi sumber kerugian bagi individu dan komunitas yang semakin meningkat. Sementara itu, mengakses jalur keadilan dan ganti rugi pada era masyarakat digital saat ini sulit dan hampir mustahil dalam beberapa kasus. Terdapat kesenjangan akuntabilitas terkait dengan meningkatnya kerugian digital, Pada titik yang lain respons kebijakan terhadap perilaku yang mengakibatkan kerugian digital tersebut tidak memadai. Situasi ini menyebabkan masalah sekunder, yakni korban kerugian digital tidak memiliki jalur yang jelas menuju keadilan.[241] Kerugian yang disebabkan oleh teknologi dapat terjadi secara daring, tetapi kerugian yang ditimbulkan tetap ada terlepas dari batas digital dan fisik. Apa yang terjadi di dunia digital meluas ke dunia fisik, dan apa yang sering tampak seperti pelanggaran privasi sebenarnya merupakan pelanggaran penentuan nasib sendiri dan kepribadian. Upaya melindungi hak penentuan nasib sendiri dan kepribadian melibatkan pengakuan bahwa hak digital merujuk pada penerapan semua HAM dan tidak boleh dibatasi hanya pada sejumlah hak sipil dan politik karena,

[241] World Economic Forum Global Future Council on Data Policy, AI for Humanity and Media, Entertainment and Sport, Pathways to Digital Justice, White Paper, World Economic Forum, 2022

penggunaan teknologi digital memiliki dampak yang semakin besar pada semua HAM. Algoritma yang digunakan dengan tujuan memprediksi dan memengaruhi perilaku masyarakat memengaruhi kebebasan berpikir. Sistem otomatis lainnya memperkuat bias rasial (etnis) atau sosial yang ada sehingga melembagakan diskriminasi dan kerugian lainnya. Oleh karena itu, melindungi hak digital harus mencakup semua bentuk penentuan nasib sendiri dan kepribadian yang diarahkan pada keadilan digital *(digital justice)*.[242]

Secara umum, keadilan digital dalam pengertian korektif berkaitan dengan perbaikan kesalahan masa lalu, yakni kerugian yang telah dilakukan terhadap individu atau kelompok. Seringkali, upaya koreksi tersebut dilakukan dengan mengenakan tanggung jawab korelatif pada pelaku kesalahan yang bertanggung jawab. Namun demikian, dapat terjadi ketidakadilan korektif, misalnya, ketika besarnya kerugian diremehkan atau sama sekali tidak diperhatikan, ketika tidak ada akuntabilitas atau ketika tidak ada jalur yang efektif untuk memulihkan kerugian terhadap individu atau kelompok yang dirugikan hak digitalnya. Namun,

[242] ibid

mengingat kesenjangan pengetahuan yang kritis dan tingkat ketidakpastian seputar kurangnya akuntabilitas yang terlibat, perlu diakui bahwa bahkan upaya terbaik untuk mengatasi kerugian ini mungkin tidak cukup. Salah satu tantangan berkaitan dengan karakterisasi potensi jenis kerugian baru yang mungkin disebabkan oleh teknologi berbasis data. Misalnya, sistem kecerdasan artifisial mereduksi identitas gender individu menjadi biner dan memiliki konsekuensi yang nyata. Ketika seorang individu dan komunitasnya tidak terwakili, maka akan kehilangan kemampuan untuk memperjuangkan HAM dan kebebasan mendasar mereka secara efektif. [243]

Tantangan lain muncul dari fakta bahwa sebagian besar kerangka kerja moral dan hukum bergantung pada identifikasi yang jelas terhadap pelaku kesalahan yang bertanggung jawab yang berkewajiban memulihkan martabat dan reputasi korban dengan cara tertentu atau memberikan restitusi atau kompensasi kepada korban atas kerugian yang diderita. Namun, dalam banyak kasus yang melibatkan analitik berbasis data dan prediktif, alokasi tanggung jawab tersebut diperumit oleh anonimitas daring, banyaknya aktor yang terlibat

[243] ibid

dalam proses tersebut, dan apa yang disebut *problem of many hands.* Lebih lanjut, bahkan ketika ada entitas yang jelas yang dapat dijadikan sasaran tanggung jawab dan kesalahan, menetapkan fakta dan tingkat kerugian dapat menjadi tantangan. Kesulitan yang paling menonjol dalam kasus-kasus ketidakjelasan algoritma yaitu, kasus-kasus ketika dasar-dasar yang digunakan algoritma prediktif untuk membuat atau merekomendasikan suatu keputusan tetap tidak dapat dipahami oleh manusia, termasuk pengguna dan pengembang algoritma tersebut. [244] Selanjutnya, kurangnya transparansi menimbulkan tantangan dalam identifikasi potensi kerugian. Situasi ini diperparah oleh kenyataan bahwa banyak pendekatan teknis yang digunakan untuk membuat algoritma tersebut dapat diinterpretasikan masih rapuh dan tidak dapat diandalkan atau tidak cukup didasarkan pada tujuan tertentu yang menjadi dasar interpretasi tersebut. Tantangan selanjutnya, bahkan ketika memiliki sarana teknis untuk mengidentifikasi kerugian, hambatan praktis yang ada untuk mendapatkan ganti rugi perlu dipertimbangkan. Hambatan tersebut mungkin termasuk membebankan beban yang tidak

[244] ibid

semestinya kepada korban dalam memberikan bukti kerugian. Pembuktian akan semakin menyulitkan korban ketika lembaga yang dituduh melakukan kerugian adalah penjaga gerbang terhadap bukti ini sehingga memperkuat ketidakadilan dan ketidakseimbangan kekuasaan yang ada.[245]

Tantangan-tantangan tersebut secara umum berkaitan dengan akses terhadap keadilan yang mengacu pada hak untuk mewujudkan keadilan. Hal ini dapat mencakup akses ke sistem peradilan formal serta jaminan proses hukum yang adil, hak untuk diadili secara adil, dan pelaksanaan putusan. Prinsip-Prinsip Panduan tentang Bisnis dan Hak Asasi Manusia memberikan aksentuasi akses terhadap keadilan dalam hukum HAM internasional juga membutuhkan akses terhadap pemulihan, di antaranya dapat berupa permintaan maaf, restitusi, kompensasi, sanksi hukuman, atau penerapan mekanisme untuk mencegah kerugian di masa mendatang. Keadilan dan upaya pemulihannya, dapat diupayakan di tingkat domestik atau internasional dan dapat melibatkan mekanisme penyelesaian sengketa dan penegakan hukum formal atau alternatif. Akses terhadap keadilan tentu saja melibatkan konteks

[245] ibid

sosial yang menjadi latar dari sistem peradilan tersebut beroperasi. Seringkali hambatan sosial atau lainnya yang dihadapi oleh beberapa individu dalam upaya mengakses mekanisme pemulihan.[246]

Sampai saat ini, cara utama akses keadilan yang diinisiasi oleh masyarakat sipil meliputi litigasi perdata serta advokasi untuk reformasi legislatif domestik dan tindakan pemerintah lainnya untuk mengendalikan industri perangkat *Spyware*.[247] Langkah litigasi ini akan menghadapi beragam upaya vendor *Spyware* untuk menghambat jalan menuju akuntabilitas, seperti perubahan identitas, struktur perusahaan yang tidak transparan, dan perpindahan antar yurisdiksi. Korban individu dari *Spyware,* terutama ketika menjadi sasaran negara-negara yang kuat dan memiliki sumber daya yang memadai, menghadapi biaya yang tinggi dalam menempuh jalur hukum terhadap vendor *Spyware* dan tantangan prosedural dalam menunjukkan sebab akibat dan kesalahan. Selain biaya litigasi, individu dapat menderita pembalasan fisik, finansial, atau lainnya terhadap diri mereka sendiri atau afiliasi mereka, termasuk keluarga, teman, kolega, dan penyedia

[246] Siena Anstis & Jillian Sprenger, op.cit
[247] ibid

layanan kesehatan.[248] Dalam konteks ini, menurut Sara Ann Brackett dan Jen Roberts, tantangan dalam menempuh jalur untuk menagih akuntabilitas penggunaan *Spyware* berbasis litigasi, meliputi: [249]

1) Kesadaran individu yang menjadi target *Spyware* masih kurang

   Kesadaran individu akan penggunaan *Spyware* merupakan prasyarat penting untuk menagih akuntabilitas. *Spyware* dirancang agar tidak terdeteksi oleh korban dan seringkali hanya dapat dideteksi dengan analisis forensik tingkat lanjut. Tanpa pengetahuan atau kecurigaan terhadap penggunaan *Spyware*, individu yang perangkatnya diretas mungkin tidak dapat menuntut keadilan atau mengambil tindakan pencegahan untuk melindungi diri mereka sendiri, kontak mereka, atau komunikasi mereka. Kesadaran akan dampak dan bahaya *Spyware* telah meningkat dalam beberapa tahun terakhir karena tindakan

[248] Sara Ann Brackett and Jen Roberts, 404 Accountability not found: Spyware accountability through software liability, Atlantic Council, 2025
[249] ibid

penting dari kerja investigasi masyarakat sipil. Dalam kasus-kasus penting seperti serangan terhadap aktivis HAM, jurnalis, dan pengacara di Meksiko, para korban dan anggota keluarga mereka yang terdampak telah berkolaborasi dengan kelompok peneliti dan advokasi, termasuk Citizen Lab, Amnesty International, dan Access Now, untuk mengaitkan pesan teks yang mencurigakan dengan upaya untuk menginstal Pegasus milik NSO Group di perangkat mereka. Dalam kasus-kasus baru-baru ini, termasuk penggunaan Graphite milik Paragon terhadap jurnalis Eropa dan perangkat milik NSO Group atau Candiru terhadap anggota masyarakat sipil terkemuka di Catalonia, pemberitahuan ancaman dari Apple dan WhatsApp telah mendorong investigasi forensik dari Citizen Lab, yang mengkonfirmasi keberadaan *Spyware.* Tanpa kecurigaan dan konfirmasi selanjutnya tentang penggunaan *Spyware,* individu tidak dapat melakukan tindakan hukum terhadap vendor *Spyware;*

2) Ketidakjelasan vendor perangkat *Spyware*

Hambatan lain terhadap akuntabilitas vendor *Spyware* adalah ketidakjelasan pasar *Spyware.* Laporan Mythical Beasts dari Atlantic Council telah memetakan ekosistem *Spyware* menguraikan taktik yang digunakan oleh vendor *Spyware* untuk mengaburkan identitas mereka. Vendor *Spyware* sering mengubah nama, dalam beberapa kasus berkali-kali, untuk menyembunyikan identitas mereka dan berpotensi untuk mengurangi dampak bisnis dari pelaporan negatif. Sebagai contoh, Vendor Candiru Ltd mengubah namanya empat kali berturut-turut dari tahun 2016 hingga 2020 dan sekarang beroperasi sebagai Saito Tech Ltd. Berbagai entitas di pasar *Spyware* yang telah mengubah nama. Tanpa konvensi penamaan yang konsisten dan catatan hukum, organisasi masyarakat sipil, individu yang menjadi target, dan perusahaan seringkali tidak dapat menentukan entitas dan individu yang bertanggung jawab, yang memungkinkan

vendor *Spyware* untuk bertindak tanpa hukuman. Vendor *Spyware* juga terlibat dalam restrukturisasi perusahaan, termasuk membuka cabang, mengembangkan anak perusahaan, menciptakan kemitraan strategis, atau membangun hubungan pemasok, yang dapat mempersulit untuk mengaitkan insiden *Spyware* dengan entitas tertentu. Tanpa adanya atribusi infeksi *Spyware* kepada vendor tertentu, litigasi tidak dapat menghasilkan akuntabilitas dari vendor tertentu atas kerugian spesifik yang diderita.

3) Kesulitan dalam menetapkan yurisdiksi

Gugatan terhadap vendor *Spyware* juga menghadapi hambatan untuk menentukan tempat persidangan yang tepat. Dalam gugatan terhadap vendor *Spyware,* lokasi fisik yang relevan dapat bervariasi dan sulit ditentukan. Penentuan yurisdiksi menjadi tantangan besar karena berkaitan dengan upaya memverifikasi kewarganegaraan perusahaan atau negara tempat aktivitas

vendor *Spyware*, lokasi perangkat yang menjadi sasaran, kewarganegaraan dan tempat tinggal individu yang menjadi sasaran, lokasi perusahaan dan infrastruktur komputasi yang menyediakan produk teknologi yang menjadi sasaran *Spyware*, dan status hukum pembeli perangkat lunak *Spyware* tersebut. Sifat kerugian yang tersebar dan terdesentralisasi dalam kasus-kasus ini dapat mempersulit penentuan pengadilan mana yang merupakan jalur yang tepat untuk klaim terhadap vendor *Spyware* dan, oleh karena itu, memiliki yurisdiksi untuk mengadili suatu kasus;

4) Risiko terungkapnya informasi teknis

Hambatan lain untuk keberhasilan litigasi terhadap vendor *Spyware* berkaitan dengan risiko terungkapnya metode deteksi dan sumber penelitian kepada vendor *Spyware.* Upaya mengidentifikasi *Spyware* berdasarkan jejak teknis atau pola perilaku vendor *Spyware,* yang memungkinkan atribusi infeksi *Spyware* ke vendor atau perangkat *Spyware t*ertentu.

Namun, pengungkapan informasi tersebut kepada publik dapat berisiko memberi tahu vendor *Spyware* tentang detail yang diandalkan peneliti untuk mendeteksi infeksi dan infrastruktur *Spyware*, memungkinkan adopsi taktik baru. Pengungkapan ini memungkinkan vendor untuk menjaga perangkat mereka selangkah lebih maju dari individu yang ditargetkan. Pada September 2024, Apple membatalkan gugatan yang sedang berlangsung terhadap NSO Group, dengan alasan lebih memilih untuk menghindari risiko terungkapnya intelijen ancaman dan kemampuan deteksi selama litigasi. Hal ini menggambarkan pertukaran antara manfaat pengungkapan indikator kepada publik dan risiko memberi tahu vendor *Spyware* tentang teknik yang terdeteksi. Peneliti dan perusahaan teknologi dapat memilih untuk mengungkapkan detail untuk menginformasikan dan melindungi publik, mengekspos informasi seperti nama domain, alamat email, dan nama proses yang digunakan oleh vendor *Spyware.* Pengungkapan ini sering

mendorong vendor *Spyware* untuk beralih ke konfigurasi infrastruktur baru untuk menghindari deteksi dan atribusi. Upaya menjaga kerahasiaan indikator teknis tertentu dari infeksi *Spyware* juga dapat memungkinkan atribusi serangan di masa mendatang, seperti yang ditunjukkan oleh laporan Citizen Lab tentang FORCEDENTRY. Lebih jauh, vendor *Spyware t*elah membuktikan infrastruktur mereka dapat bangkit kembali dari paparan publik dan terus beroperasi, seperti yang terjadi pada Intellexa Consortium. Setidaknya dalam tiga kasus yang dimulai pada 2023, infrastruktur Intellexa Consortium berhasil diungkap oleh para peneliti masyarakat sipil dari Amnesty International, Insikt Group dari Recorded Future, dan Sekoia. Hasil penelitian masyarakat sipil tersebut mengakibatkan penonaktifan internal infrastruktur Intellexa Consortium yang berdampak pada kemampuan konsorsium untuk menyebarkan atau memelihara infeksi. Penonaktifan infrastruktur ini kemudian diperparah oleh sanksi Departemen Keuangan AS

terhadap anggota Intellexa Consortium pada 2024.

Pelanggaran HAM akibat proliferasi industri *Spyware* masih terjadi. Hal ini bersumber pada kurangnya kemauan politik untuk mengambil langkah-langkah yang diperlukan untuk mengendalikan industri *Spyware* dan melindungi HAM. Argumentasi yang dipergunakan untuk menjustifikasi penggunaan perangkat *Spyware* untuk tujuan penegakan hukum dan keamanan nasional. Banyak dari negara-negara, termasuk negara-negara demokrasi liberal terus menggunakan *Spyware* atau teknologi serupa, atau mengizinkan industri ini berkembang di dalam wilayah mereka. Secara keseluruhan, tanpa pengakuan pemerintah bahwa kerugian yang ditimbulkan oleh *Spyware* digital lebih besar daripada keuntungan finansial dan politiknya, kemungkinan besar akan selalu ada kurangnya kemauan politik untuk melakukan perubahan yang berarti.[250] Oleh karena itu, upaya untuk mencapai akuntabilitas *Spyware* melalui struktur perlindungan legislatif tetap signifikan. Langkah legislasi ini, apabila diimplementasikan, maka dapat membentuk kembali insentif bagi

[250] Siena Anstis & Jillian Sprenger, op.cit

perusahaan teknologi untuk membantu dalam upaya mencapai akuntabilitas *Spyware*. Dengan demikian, langkah legislatif menjadi modalitas untuk menagih akuntabilitas penggunaan *Spyware*. Langkah selanjutnya, litigasi dan tindakan akuntabilitas lainnya yang dilakukan oleh perusahaan teknologi seperti Apple (iMessage, iPhone), Google (Android), dan Meta (WhatsApp) meskipun akan menghadapi hambatan, perusahaan-perusahaan ini memiliki kemampuan unik untuk melawan risiko dan bahaya *Spyware* serta mengatasi hambatan tersebut. Litigasi dan tindakan pencegahan perusahaan teknologi tidak selalu melibatkan kompensasi langsung kepada korban atau keadilan atas kerugian sebelumnya, tetapi dapat bertindak sebagai langkah pencegahan penting untuk mencegah bahaya *Spyware* di masa mendatang, melengkapi pendekatan lain untuk menuntut akuntabilitas penggunaan *Spyware.*[251]

Keberhasilan gugatan yang dilayangkan korporasi melalui mekanisme litigasi di pengadilan di Amerika Serikat menunjukkan urgensi melibatkan peran korporasi untuk menuntut akuntabilitas penggunaan *Spyware.* Penggugat korporasi yang diduga menjadi korban NSO Group lebih berhasil

[251] Sara Ann Brackett and Jen Roberts, op.cit

mengatasi hambatan prosedural daripada penggugat individu. Dua kasus gugatan korporasi satu diajukan oleh Apple dan yang lainnya oleh WhatsApp milik Meta, berhasil melewati tantangan yurisdiksi NSO Group. NSO Group akhirnya menjalani akuntabilitasnya dalam kasus yang diajukan oleh WhatsApp, sebagian besar karena penolakannya untuk memberikan informasi kepada pengacara pihak lawan selama proses pengumpulan bukti. Pada akhirnya, pada 6 Mei 2025 juri memberikan ganti rugi sebesar $167 juta kepada WhatsApp. NSO Group telah meminta pengadilan untuk mengurangi jumlah ganti rugi tersebut secara drastis atau memerintahkan persidangan ulang.[252] Meskipun pada September 2024, Apple memutuskan untuk mencabut gugatannya, sebagian karena Apple akan dipaksa untuk mengungkapkan informasi tentang praktik keamanan Apple yang telah dicari oleh perusahaan *Spyware* predator selama bertahun-tahun. Menurut Apple penarikan gugatan tu dilandasi pertimbangan pelindungan penggunanya:[253]

> Apple saat ini menggunakan *threat-intelligence information* untuk melindungi

[252] Nadine Farid Johnson, Unlocking Justice: A Policy Roadmap for Victims of Spyware, 2025, https://knightcolumbia.org/blog/unlocking-justice-a-policy-roadmap-for-victims-of-spyware, diakses pada 6 Mei 2026
[253] ibid

> setiap penggunanya di dunia, pengungkapan apa pun, bahkan di bawah kontrol yang paling ketat, akan membahayakan informasi ini.

Pada sisi yang lain, gugatan individu mengalami kegagalan karena hambatan prosedural. Setidaknya tiga gugatan telah diajukan di pengadilan federal Amerika Serikat terhadap NSO Group atas nama korban individu yang menuduh pelanggaran berbagai undang-undang federal dan negara bagian setelah menghadapi serangan perangkat *Spyware* Pegasus. Berbagai tantangan prosedural di pengadilan memperlambat atau bahkan mencegah kasus-kasus tersebut mencapai pokok perkara, membuat para korban berada dalam ketidakpastian tanpa jalan keluar. Para penggugat ini menghadapi hambatan yurisdiksi yang signifikan, terkadang kasus mereka ditolak berdasarkan alasan pendahuluan ini setelah pertempuran berbulan-bulan di pengadilan. Hakim telah menolak upaya untuk meminta akuntabilitas NSO Group atas pelanggaran undang-undang negara bagian dan federal yang melarang peretasan dan pengambilan data tanpa izin dengan alasan bahwa perusahaan tersebut tidak memiliki ikatan yang memadai dengan Amerika Serikat atau negara bagian tertentu. [254]

[254] ibid

Para hakim juga telah menolak kasus-kasus dengan alasan bahwa Amerika Serikat bukanlah forum yang tepat untuk kasus-kasus ini, sehingga gugatan seharusnya diajukan di yurisdiksi lain di luar Amerika Serikat. Misalnya, Pengadilan Sirkuit Keempat baru-baru ini menguatkan putusan pengadilan distrik federal di Virginia yang menolak gugatan terhadap NSO Group yang diajukan oleh janda jurnalis yang dibunuh, Jamal Khashoggi, karena kurangnya yurisdiksi personal. Tantangan prosedural ini mencegah para hakim untuk membahas pokok perkara terhadap NSO Group, sehingga korban invasi *Spyware* berada dalam ketidakpastian dan tanpa jalan keluar di pengadilan Amerika Serikat, meskipun mereka menderita pelanggaran privasi, keamanan, dan kebebasan berekspresi akibat teknologi perusahaan tersebut.[255]

Penggunaan *forum non conveniens* menjadi perhatian khusus dalam kasus-kasus yang menyangkut HAM dimana pengadilan Amerika Serikat mungkin menjadi satu-satunya tempat yang masuk akal untuk melanjutkan kasus-kasus tersebut. Meskipun pengadilan distrik Amerika Serikat mungkin

[255] ibid

cenderung mengarahkan para pihak dalam kasus *Spyware* untuk berlitigasi di negara tempat tergugat didirikan atau negara tempat dugaan serangan terjadi, kenyataannya membawa kasus semacam itu ke pengadilan di yurisdiksi tersebut tidak mungkin terjadi. Misalnya, NSO Group didirikan di Israel, sementara pemerintah Israel mengambil langkah-langkah luar biasa untuk melemahkan litigasi WhatsApp, seperti yang dilaporkan The Guardian. Dan pengadilan di negara-negara seperti Arab Saudi, Uni Emirat Arab, atau El Salvador di mana penargetan terhadap para pembangkang HAM dan jurnalis adalah hal yang umum, namun bukanlah tempat yang tepat untuk menegakkan keadilan. Sebagaimana ditunjukkan oleh banyaknya litigasi *Spyware* yang baru muncul, para calon penggugat menghadapi tantangan prosedural dalam mengajukan kasus di pengadilan Amerika Serikat maupun di pengadilan lain di seluruh dunia, yang mengancam situasi di mana tidak ada pengadilan yang akan terbuka untuk mendengarkan kasus para korban ini berdasarkan substansinya.[256]

Jalur untuk mendapatkan ganti rugi melalui litigasi sangat penting bagi para korban *Spyware.* Pilihan bagi para calon penggugat ini tidak konsisten

[256] ibid

dan tidak jelas, namun kerugian dan ancaman keamanan yang terkait dengan *Spyware* terus berlanjut dan meningkat tanpa henti. Para pembuat kebijakan harus mengatasi ketidakseimbangan mendasar ini dan menciptakan kondisi yang setara bagi para korban *Spyware,* sehingga memungkinkan jalur untuk mendapatkan ganti rugi.[257]

I. Urgensi Pengembangan Ekosistem Akuntabilitas Penggunaan *Spyware* di Indonesia Berbasis Hak Asasi Manusia

I.1. Kekosongan Hukum Penggunaan *Spyware* Komersial dan Pengadaan *Spyware* Komersial

Laporan Amnesty International menunjukkan pelindungan HAM yang ekstensif sekalipun tidak akan melindungi masyarakat sipil dari *Spyware* yang sangat invasif.[258] Di Indonesia, meskipun Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) telah diratifikasi melalui Undang-Undang Nomor 12 Tahun

[257] ibid

[258] Amnesty International, *The Predator Files: Caught in the Net*, Index: ACT 10/7245/2023, 9 Oktober 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/. Diakses pada Agustus 2025.

2005, substansi kovenan tersebut belum sepenuhnya ditransformasikan ke dalam hukum domestik yang operasional. Ratifikasi ICCPR merupakan komitmen awal Indonesia dalam mengakui katalog hak fundamental warga negara, seperti hak atas kebebasan berekspresi, berkumpul, keamanan pribadi, serta perlindungan dari penahanan sewenang-wenang. Sayangnya, komitmen ini belum mewujud dalam regulasi spesifik yang mengatur penggunaan *Spyware* dan *Surveilans* secara sah. Hingga saat ini, Indonesia masih belum memiliki aturan khusus yang secara eksplisit dan komprehensif menempatkan penggunaan serta pengadaan *Spyware* sebagai objek norma tersendiri. Kekosongan hukum ini dapat melanggengkan praktik *Surveilans* tanpa akuntabilitas yang mengancam hak-hak fundamental, mengganggu stabilitas demokrasi, dan membahaya kan keamanan nasional.

Kekosongan regulasi di tingkat nasional tersebut tidak dapat dilepaskan dari kompleksitas perumusan kebijakan terkait teknologi *Surveilans* di tingkat global. Pengaturan menjadi sulit karena *Spyware* merupakan bagian dari kapabilitas siber ofensif yang tidak memiliki wujud konkret, sehingga sifat teknisnya sulit dipahami. Kesulitan ini diperparah oleh ketiadaan kerangka kerja

yang jelas untuk mendefinisikan skala operasi serta mengukur dampak perangkat tersebut secara pasti. Dampak teknologi ini terhadap tatanan keseimbangan kekuatan internasional masih terus diperdebatkan. Ketika negara maupun aktor non-negara memperoleh akses dan menggunakan kapabilitas siber ofensif, instabilitas di ruang siber pun meningkat. Persoalan ini menjadi semakin mendesak seiring dengan bertambahnya jumlah aktor siber yang disponsori negara serta meningkatnya tingkat keparahan serangan siber. Oleh karena itu, pengembangan kebijakan tidak seharusnya terjebak pada upaya sia-sia untuk memblokir proliferasi *Spyware* secara absolut, melainkan harus fokus pada strategi mereduksi utilitas teknologi tersebut serta memengaruhi struktur insentif bagi para aktor yang terlibat dalam penyebarannya.[259]

Meski demikian, upaya memengaruhi struktur insentif tersebut sering kali berbenturan dengan realitas pasar *Spyware* komersial yang masih minim regulasi. Kontrol terhadap transaksi pasar sendiri merupakan langkah krusial, tapi perdagangan komersial bukanlah satu-satunya sumber ancaman

[259] Cardillo, Fischer, dan Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

keamanan, mengingat banyak kapabilitas serupa dikembangkan secara internal oleh institusi negara. Hingga saat ini, kebijakan internasional masih terjebak dalam perdebatan mengenai parameter penggunaan *Spyware* sah. Ketidakjelasan standar inilah yang menyebabkan volume penjualan komersial tidak dapat dijadikan indikator bagi tingkat penggunaan teknologi yang bertanggung jawab. Sebuah transaksi mungkin saja sah secara prosedural, namun tetap berujung pada penyalahgunaan yang destruktif. Sejarah menunjukkan bahwa pasar komersial hanyalah salah satu bagian dari tantangan proliferasi yang lebih luas. Faktanya, pelanggaran HAM sistematis justru kerap terjadi melalui penggunaan *Spyware* secara vertikal terhadap warga negara sendiri, maupun secara diagonal terhadap warga negara asing dan kelompok diaspora dengan dalih kepentingan keamanan negara.[260]

Ketidakjelasan parameter tersebut sering kali berakar pada terminologi yang inkonsisten, yang selama ini menjadi kendala utama dalam perumusan kebijakan. Jean Robert dkk. menekankan bahwa

[260] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

efektivitas regulasi sangat bergantung pada presisi definisi *Spyware* yang membedakannya secara tegas dari teknologi *Surveilans* lainnya. Dalam kerangka ini, *Spyware* didefinisikan sebagai sebuah teknologi atau alat yang beroperasi sepenuhnya tanpa persetujuan maupun pengetahuan target, atau individu lain yang memiliki akses sah terhadap perangkat sasaran (seperti ponsel atau komputer) tersebut. Definisi ini mengecualikan:[261]

1. Teknologi tanpa akses ke perangkat sasaran: Mencakup perangkat lunak yang sama sekali tidak masuk ke dalam sistem perangkat milik target. Alat ini hanya bekerja di luar, yakni mengumpulkan data yang sedang berpindah di jalur komunikasi (seperti penyadapan paket data atau *sniffing* melalui kabel/Wi-Fi).

2. Alat dengan akses fisik: Mencakup produk yang membutuhkan sentuhan fisik langsung pada perangkat sasaran (seperti *stalkerware*) atau harus berada dalam jarak dekat dengan posisi perangkat

[261] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

tersebut (seperti alat forensik dan penyadap seluler).

Pembatasan tersebut dilakukan secara sengaja untuk mencegah pencampuran berbagai instrumen *Surveilans* lain ke dalam kategori *Spyware*.[262]

Berdasarkan definisi tersebut, teridentifikasi 435 entitas yang beroperasi di pasar *Spyware* antara tahun 1992 hingga 2023. Identifikasi ini mencakup vendor beserta anak perusahaannya, pejabat senior, hingga investor. Pemetaan ini bertujuan untuk menciptakan transparansi pada rantai pasok yang sering kali sengaja disamarkan, sehingga pembuat kebijakan dapat melacak aliran modal dan teknologi yang memfasilitasi pelanggaran HAM. Berikut adalah tabel yang merinci istilah-istilah aktor kunci tersebut:[263]

[262] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."
[263] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

Elemen Rantai Pasok	Deskripsi/Peran
Vendor *Spyware*	Entitas komersial yang mengembangkan, mendukung, dan menjual *Spyware* kepada pengguna akhir. Pengembangan dan dukungan ini dapat mencakup riset kerentanan dan pengembangan eksploitasi, pengembangan muatan *malware,* perintah dan kontrol teknis, manajemen operasional, serta pelatihan dan dukungan, tetapi tidak harus mencakup semuanya
Individu	Orang yang terlibat langsung dengan vendor atau pemasok, atau entitas yang terkait langsung dengan vendor atau pemasok. Individu dapat berupa pendiri perusahaan, pejabat manajemen senior, atau investor.

Pemasok	Pemasok menjual komponen atau layanan yang digunakan untuk mengembangkan produk *Spyware* tetapi tidak secara langsung mengembangkan atau mengoperasikan *Spyware* atau layanan serupa. Pemasok dapat menjual kerentanan atau layanan berlangganan eksploitasi kepada vendor yang kemudian mengembangkan perangkat lunak sebenarnya. Pemasok merupakan bagian penting namun sering diabaikan dalam pasar ini.
Mitra	Mitra adalah perusahaan yang terhubung dengan vendor *Spyware*, meskipun sifat hubungan tersebut dapat mengambil beberapa bentuk yang berbeda. *Pertama,* mitra dapat tidak terkait dengan pengembangan *Spyware* itu sendiri tetapi penting untuk operasi lain dari vendor (misalnya, layanan pemasaran atau penjualan). *Kedua,* mitra dapat menyediakan produk *Surveilans* pelengkap, seperti

	perangkat penyadap telekomunikasi atau cara untuk memproses data yang dikumpulkan dari *Spyware*, seperti alat pemetaan data lokasi
Perusahaan *holding*	Perusahaan *holding* adalah jenis badan usaha yang memiliki saham beredar dari perusahaan lain. Tujuan utamanya adalah untuk mengendalikan dan mengelola satu atau lebih perusahaan yang dimilikinya, daripada memproduksi barang atau jasa sendiri. Perusahaan *holding* dapat memiliki berbagai aset, termasuk saham perusahaan lain, real estate, paten, merek dagang, dan banyak lagi. Dengan memegang kendali atas perusahaan lain, perusahaan *holding* dapat memengaruhi atau mengarahkan kebijakan dan keputusan manajemennya. Struktur ini dapat memberikan manfaat seperti manajemen risiko, keuntungan pajak, dan kontrol yang disederhanakan atas beberapa bisnis.

Anak Perusahaan	Perusahaan yang lebih dari lima puluh persen sahamnya dimiliki oleh perusahaan induk atau perusahaan *holding*. Anak perusahaan terpisah dan secara hukum berbeda dari perusahaan induk atau perusahaan holdingnya, yang biasanya tercermin dalam independensi tata kelola, keuangan, pajak, dan kewajibannya. Namun, perusahaan induk seringkali memiliki pengaruh yang cukup besar terhadap anak perusahaannya.

Kemudian berdasarkan operasional pasar *Spyware* terdapat enam kecenderungan berbeda, yaitu:

1) Mayoritas entitas yang teridentifikasi berdomisili di Israel, India, dan Italia;
2) Pengusaha serial/berpindah *(serial entrepreneurs)* sangat banyak;
3) Kemitraan yang kuat antara vendor *Spyware* dan perangkat keras *Surveilans*;
4) Upaya yang disengaja dan berulang oleh perusahaan untuk mengubah identitas dan bahkan struktur perusahaan mereka;

5) Pergerakan struktur perusahaan tersebut melintasi batas yurisdiksi strategis;
6) Mobilitas lintas batas modal yang signifikan yang mendukung pengembangan dan penjualan *Spyware.*

Keenam kecenderungan tersebut perlu mendapat aksentuasi dalam pengembangan kebijakan pengaturan akuntabilitas penggunaan *Spyware*. Fokus kebijakan tidak boleh hanya menyasar entitas hukum, tetapi juga harus mempertimbangkan dinamika industrinya sebagai berikut:[264]

1) Pengusaha serial/berpindah

Terdapat pola berulang di mana karyawan, termasuk para pendiri, meninggalkan perusahaan pertama mereka untuk mendirikan dan bekerja di perusahaan lain. Hal ini tidak berbeda dengan budaya *startup* lainnya di mana kewirausahaan serial semacam ini umum terjadi. Namun, dalam konteks pasar ini, terdapat risiko yang jauh lebih besar mengingat adanya kesamaan mendasar pada fungsi teknis produk *Spyware* serta kuatnya hubungan

[264] Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

personal antara pelanggan (pemerintah) dengan para pendiri maupun karyawan senior. Dalam kumpulan data yang dianalisis, terlihat bahwa para pendiri vendor dan pemasok sering kali tetap terlibat dalam industri ini dengan berpindah dari satu entitas ke entitas lainnya.[265]

Oleh karena itu, pengawasan seharusnya tidak lagi terbatas pada entitas korporasi, melainkan harus menyasar pada mobilitas talenta individu yang berpindah antarperusahaan. Untuk menghambat perpindahan talenta antar vendor, badan perizinan ekspor dapat meminta informasi yang lebih rinci tentang personel kunci dan pekerjaan mereka sebelumnya untuk membantu mengidentifikasi individu yang dikategorikan sebagai pelanggar

[265] NSO Group, yang bisa dibilang vendor *spyware* paling terkenal, adalah contoh utama dari fenomena ini. Perusahaan ini didirikan pada tahun 2010 di Israel yang merupakan pengembang *spyware* Pegasus. Meskipun ada investigasi dari Uni Eropa dan tindakan pengaturan dari Amerika Serikat perusahaan tersebut terus mengoperasikan cabang di Amerika Serikat dan Luksemburg bersama dengan anak perusahaan di Bulgaria dan Siprus. Contoh lain, Vendor Quadream Inc., yang dikenal dengan *spyware* Reign, didirikan pada 2016 di Israel oleh mantan karyawan NSO Group, serta mantan pejabat militer dan dikenal dengan nama Kvader Ltd. di Israel. Seperti Quadream Inc., Interionet Systems Ltd. (Interionet) adalah vendor Israel yang didirikan pada tahun 2015 oleh mantan karyawan NSO Group. Pengusaha Israel salah satu pemegang saham dan anggota dewan NSO, juga duduk di dewan Interionet. Lihat, Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

berulang terhadap hukum dan kebijakan yurisdiksi lain. Para pembuat kebijakan juga harus mempertimbangkan untuk fokus pada individu ketika mencoba membatasi aktivitas berbahaya oleh vendor, daripada hanya vendor sebagai entitas bisnis, mengingat fluiditas talenta antarperusahaan.

2) Kemitraan dengan *Surveilans* Perangkat Keras

Vendor *Spyware* terkadang bermitra dengan perusahaan *Surveilans* berbasis perangkat keras yang produknya mungkin melengkapi fungsionalitas perangkat *Spyware* mereka. Terdapat sembilan vendor atau pemasok yang memiliki setidaknya satu mitra resmi, di mana lima di antaranya beraliansi khusus dengan perusahaan perangkat keras.[266]

[266] Contoh paling aktif dari kemitraan ini adalah Konsorsium Intellexa, yang mencakup hubungan antara tujuh perusahaan perangkat keras yang berbeda. Dibentuk di sekitar pendiri pada 2018, Grup Intellexa terdiri dari beberapa perusahaan termasuk Cytrox AD, WS WiSpear Systems Limited (juga didirikan oleh pendiri yang sama), dan Senpai Technologies Ltd. Pada tahun 2020, Grup Intellexa berkembang untuk memasukkan Intellexa S.A., yang sebelumnya dikenal sebagai Intellexa Single Member. Cytrox AD dibentuk pada 2017 di Makedonia Utara dan mengembangkan spyware yang dikenal sebagai Predator. WS WiSpear Systems Limited mengkhususkan diri dalam mencegat sinyal Wi-Fi yang ditargetkan dan mengekstrak kata sandi serta komunikasi dari jarak jauh, dan Senpai Technologies Ltd. adalah perusahaan intelijen sumber terbuka yang mengkhususkan diri dalam menganalisis data dari ponsel yang terinfeksi spyware. Lihat, Roberts dkk., "Mythical Beasts and Where to Find Them:

Meskipun kolaborasi antarproduk pelengkap adalah hal lumrah dalam bisnis, sinergi dalam pasar *Spyware* ini menuntut perhatian khusus. Fenomena ini menegaskan bahwa kebijakan harus menyasar ekosistem pasar secara menyeluruh melalui kolaborasi lintas negara, mengingat regulasi yang hanya berfokus pada satu vendor atau yurisdiksi tertentu akan memiliki efektivitas yang terbatas. Untuk memperkuat pengawasan, regulasi terhadap jenis dukungan bagi vendor yang melayani lembaga pemerintah perlu diperketat. Langkah ini mencakup perluasan transparansi melalui prinsip *Know Your Vendor* (Kenali Vendor Anda) untuk menjangkau seluruh rantai kemitraan di luar transaksi awal. Rekomendasi ini menjadi sangat mendesak mengingat identitas vendor yang terus berubah, sekaligus menyingkap kompleksitas hubungan antara pasar *Spyware* dengan industri *Surveilans* elektronik lainnya.

3) Pergeseran identitas vendor

Vendor *Spyware* kerap mengganti nama resmi hingga merombak seluruh struktur perusahaan mereka secara berkala. Strategi ini bukan tanpa alasan; perubahan identitas tersebut sengaja

---

Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

dilakukan untuk menyamarkan jejak operasional sekaligus meminimalisir dampak dari pemberitaan negatif atau skandal yang menimpa mereka. Meskipun nama resmi perusahaan sering berganti, laporan publik biasanya tetap merujuk pada entitas tersebut dengan nama mereka yang paling populer. Hal ini menciptakan celah yang berbahaya karena dapat menyamarkan aktivitas operasional vendor yang masih berlangsung, sekaligus menghambat upaya peneliti, pembuat kebijakan, hingga investor dalam melakukan uji tuntas (*due diligence*). Data menunjukkan bahwa rata-rata entitas di pasar ini mengganti nama lebih dari satu kali, dengan masa penggunaan satu nama hanya bertahan rata-rata 4,5 tahun. Fenomena 'pergantian kulit' yang cepat ini mempersulit pelacakan rekam jejak jangka panjang dan memungkinkan vendor bermasalah untuk terus mendapatkan pendanaan atau kontrak baru dengan identitas yang seolah-olah bersih.[267]

[267] Untuk memberikan perspektif pergeseran terjadi pada perusahaan Holding memiliki persentase perubahan nama tertinggi sebesar 34,4 persen, diikuti oleh Vendor (14,3 persen), Mitra (20,8 persen), Pemasok (lima persen), dan Investor (2,1 persen).Identitas yang paling sering berubah adalah perusahaan yang awalnya dikenal sebagai Candiru Ltd, yang mengubah namanya empat kali selama sembilan tahun berikutnya, dan pada saat penulisan ini dikenal sebagai Saito Tech Ltd. Vendor yang awalnya dikenal sebagai Candiru Ltd didirikan pada tahun 2014 di Israel. Candiru Ltd telah menjual produk ke Hongaria, Spanyol, dan Uni Emirat Arab, yang

Berbagai contoh ini menunjukkan mengapa sulit bagi para pembuat kebijakan dan peneliti untuk melacak vendor. Pergeseran identitas vendor menciptakan ilusi bahwa vendor telah berhenti beroperasi padahal mereka beroperasi dengan nama yang berbeda. Citra ini menjadi lebih rumit dengan anak perusahaan dan cabang karena mereka juga dapat dengan cepat berganti nama. Kompleksitas ini kian diperparah oleh jaringan anak perusahaan dan kantor cabang yang juga kerap berganti nama dalam waktu singkat. Guna mengatasi taktik penyamaran ini, solusi kebijakan harus berfokus pada pelacakan hubungan antar-individu dan investor di balik entitas tersebut. Langkah konkret yang dapat diambil adalah memperketat prosedur pengadaan *Spyware* melalui kewajiban prinsip *Know Your Vendor*, yang mengharuskan pengungkapan hubungan pemasok hingga tingkat pertama dan kedua. Selain itu, peningkatan transparansi dan konsistensi pada

semuanya menggunakan *spyware* untuk penindasan politik terhadap oposisi dan masyarakat sipil. Perubahan nama tahunan grup antara tahun 2016 dan 2020 tidak disertai dengan perubahan struktur perusahaan. Pada 2021, Candiru Ltd dan nama-nama terkaitnya ditambahkan ke Daftar Entitas Amerika Serikat bersama dengan NSO Group. Dalam wacana umum, vendor tersebut sering disebut Candiru Ltd, laporan ini merujuk pada semua vendor dengan nama hukum mereka saat ini, yang untuk Candiru Ltd adalah Saito Tech Ltd. Lihat, Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

registrasi perusahaan sangat diperlukan untuk memetakan keterhubungan antar-identitas ini, bahkan ketika mereka beroperasi melintasi berbagai yurisdiksi.

4) Perpindahan Yurisdiksi Strategis

Beberapa vendor membangun jaringan anak perusahaan, kantor cabang, hingga kemitraan yang melintasi berbagai batas yurisdiksi strategis. Relokasi ini dapat menawarkan berbagai manfaat spesifik lokasi, mulai dari memfasilitasi penjualan ke pasar Uni Eropa dengan perusahaan yang berdomisili di Uni Eropa hingga menempatkan cabang di negara-negara dengan hukum yang lebih longgar.[268]

Struktur hukum nasional yang berbasis pada batas kedaulatan sering kali gagal menjangkau vendor *Spyware* yang sengaja merancang jaringan anak perusahaan lintas negara untuk menghindari kontrol ekspor. Praktik arbitrase yurisdiksi ini menciptakan ketidakjelasan operasional dan rantai pasok yang

[268] Pada 2017, vendor Israel Quadream Inc. mendirikan pemasok, InReach Technologies Limited, di Siprus. Menurut Quadream Inc. dalam pengajuan pengadilan untuk tujuan tunggal mempromosikan produk Quadream Inc. di Uni Eropa. Struktur keuangan InReach Technologies Limited juga mencakup A.I.L Nominal Services Ltd. (A.I.L), yang juga didirikan di Siprus pada tahun 2010 sebagai perusahaan induk, dengan seorang individu yang memiliki hubungan dengan Kementerian Pertahanan. Lihat, Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

signifikan, terutama ketika vendor berpindah ke wilayah dengan regulasi yang lebih longgar guna menumpulkan efektivitas kebijakan internasional. Kompleksitas ini kian diperparah oleh aliran modal lintas batas yang sangat dinamis, sehingga upaya untuk menagih akuntabilitas perusahaan menjadi semakin sulit dilakukan tanpa adanya langkah-langkah yang secara tegas membatasi celah pelarian hukum tersebut.

5) Mobilitas Modal Global

Investor di vendor *Spyware* sering kali melintasi perbatasan dengan modal mereka. Seperti pasar konvensional lainnya, vendor dan pemasok *Spyware* memiliki basis investor yang berdomisili di berbagai yurisdiksi. Terdapat empat yurisdiksi yang paling sering mewakili asal investor, yaitu Italia, Israel, Amerika Serikat, dan Inggris mencakup 46,3 persen dari semua investor. Karakter investasi *Spyware* bervariasi dari modal ventura, ekuitas swasta, dan pinjaman pemerintah hingga akuisisi langsung dan kepemilikan ekuitas langsung. Secara statistik, setiap vendor dan pemasok dalam kumpulan data ini rata-rata memiliki 4,75 persen investor yang teridentifikasi. Hal ini menunjukkan bahwa operasional mereka didukung oleh jaringan pendanaan yang cukup luas. Sebagai

contoh, teridentifikasi 14 entitas asal Amerika Serikat yang berinvestasi di pasar ini, di mana 12 di antaranya menyuntikkan modal ke vendor yang berbasis di Israel.[269]

Dinamika arus modal lintas batas ini menuntut kerja sama internasional yang erat, di mana Amerika Serikat dan Uni Eropa memegang peran sentral dalam menerapkan pengawasan ketat terhadap hubungan investor di pasar *Spyware*. Penguatan transparansi, seperti kewajiban pelaporan pemilik manfaat (*beneficial ownership*), menjadi langkah krusial untuk mendukung uji tuntas (*due diligence*) dan peninjauan transaksi yang lebih mendalam. Bagi vendor di luar AS, usulan perluasan peninjauan keamanan terhadap investasi keluar (*outbound investment*) memberikan dasar hukum untuk mengatalogkan, atau bahkan

[269] Contoh spesifik dari tren ini adalah Paragon Solutions. Paragon didirikan pada tahun 2019 di Israel. Beberapa tahun kemudian pada 2022, perusahaan tersebut mendirikan Paragon Solutions US, anak perusahaan yang berdomisili di Amerika Serikat. Sejak didirikan, Paragon telah melakukan upaya yang disengaja untuk menembus pasar Amerika Serikat. Paragon Solutions juga memiliki dua investor yang berbasis di Amerika Serikat. Battery Ventures, yang dianggap sebagai salah satu perusahaan modal ventura terkemuka di dunia dan berkantor pusat di Boston, merupakan investor di Paragon Solutions pada saat penulisan ini. Perusahaan ini juga didukung oleh Blumberg Capital, perusahaan modal ventura besar Amerika Serikat lainnya. Lihat, Roberts dkk., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

memblokir, aliran modal ke entitas berisiko. Selain itu, penggunaan sanksi yang ditargetkan, baik terhadap vendor maupun investor itu sendiri, menjadi instrumen penting untuk membatasi ruang gerak pasar. Meski penggunaan sanksi sepihak masih menjadi perdebatan hangat, instrumen ini tetap menjadi opsi strategis dalam lanskap kebijakan keamanan nasional untuk menekan proliferasi teknologi *Surveilans* berbahaya.

Dengan berpijak pada hasil identifikasi ruang lingkup permasalahan tersebut, Jen Roberts dkk mengusulkan rekomendasi kebijakan dengan tujuan untuk mendorong transparansi yang lebih besar di seluruh pasar, membatasi arbitrase yurisdiksi, dan lebih efektif mengawasi hubungan pemasok dan investor. Lebih jauh, tujuan kebijakan ini akan mengatasi peluang signifikan untuk membatasi risiko dan kerugian yang timbul dari proliferasi *Spyware.* Rekomendasi yang dapat menjadi pertimbangan dalam mengembankan kebijakan penggunaan *Spyware* juga mencakup dimensi perilaku vendor, rezim uji tuntas investor yang kuat, penilaian risiko pemerintah yang kaya informasi sebelum pengadaan, dan dukungan hukum yang kredibel untuk transparansi jangka panjang yang lebih besar di pasar. Berdasarkan

ruang lingkup rekomendasi tersebut secara garis besar pengaturan akuntabilitas penggunaan *Spyware*, difokuskan pada beberapa dimensi:

1) Mandatkan persyaratan "Kenali Vendor Anda"

Karakteristik utama akuisisi *Spyware* seharusnya secara teori harus didasari pelaksanaan uji tuntas, maka kesenjangan yang ada dalam kebijakan saat ini adalah kemampuan untuk melaksanakan uji tuntas berkaitan dengan identitas vendor dan rantai pasokan yang berubah. Dalam konteks ini, maka penting untuk menerapkan persyaratan Kenali Vendor yang mengharuskan vendor *Spyware* untuk mengungkapkan hubungan pemasok dan investor. Ini adalah langkah kredibel menuju informasi yang lebih baik tentang segmen pasar *Spyware* yang mungkin dijalin oleh pemerintah. Kenali Vendor akan menciptakan lingkungan pelaporan yang lebih konsisten tentang pasar *Spyware*, memberikan kemampuan untuk memeriksa di mana rantai pasokan prospektif mereka mungkin mencakup perusahaan yang ada dalam daftar entitas yang dibatasi sebelum memberikan kontrak. Kenali Vendor juga akan memungkinkan upaya jangka panjang untuk mengurangi anggaran pemerintah yang mengalir ke

pemasok atau vendor berisiko tinggi. Versi yang lebih efektif dari persyaratan ini dapat mewajibkan pengungkapan perusahaan lebih jauh di rantai pasokan, termasuk pemasok ke pemasok vendor;

2) Meningkatkan registrasi perusahaan yang dikelola pemerintah

Senada dengan Kenali Vendor, registrasi perusahaan yang dikelola pemerintah merupakan sumber daya untuk uji tuntas dan akuntabilitas. Registrasi ini akan memainkan peran penting dalam rezim kebijakan yang lebih tegas yang menangani pergerakan lintas batas, atau investasi pada vendor *Spyware.* Registrasi ini juga akan menjadi sumber informasi penting untuk uji tuntas oleh calon investor serta memberikan visibilitas yang lebih baik ke dalam entitas bisnis yang beroperasi di yurisdiksi masing-masing. Oleh karena itu, agar registrasi perusahaan menjadi sumber kebenaran tentang struktur bisnis dan keuangan serta sejarah vendor, registrasi tersebut harus komprehensif, dapat diakses secara terbuka oleh publik, dan memiliki informasi yang terverifikasi. Beberapa hal penting yang relevan untuk meningkatkan registrasi ini adalah:

a. Perluas cakupan minimum data yang dicatat dalam registrasi.

identifikasi kepemilikan manfaat mewajibkan persyaratan tentang kategori dan detail terkait yang ada dalam registrasi perusahaan. Persyaratan tersebut harus mencakup informasi dasar perusahaan, seperti: (1) nama, nomor registrasi, ID pembayaran, alamat, detail kontak, dan tanggal registrasi; (2) detail kepemilikan, mencakup eksekutif senior, dewan manajemen, dan pemilik manfaat sebenarnya; (3) jumlah karyawan, informasi keuangan, antara lain neraca, arus kas, laporan laba rugi, dan investor; (4) riwayat perubahan nama, dan status hukum aktivitas, misalnya likuidasi, aktif, atau pailit. Informasi ini berfungsi sebagai persyaratan minimum, tetapi dapat diperluas untuk mencakup riwayat merger dan akuisisi, tindakan hukum terhadap perusahaan, dan lisensi ekspor aktif.

b. Perluasan Identifikasi Kepemilikan Manfaat *(beneficial ownership identification)*

Pengakuan yang lebih baik terhadap pemilik manfaat di balik vendor *Spyware* dan pemasok, akan memberikan penangkal yang kuat terhadap banyak kecenderungan perilaku perusahaan perangkat *Spyware* komersial. Perbaikan lebih lanjut mengenai

identifikasi kepemilikan manfaat mewajibkan perusahaan untuk melaporkan individu yang memiliki dua 25% atau lebih dari saham dan hak suara atau menjalankan kendali signifikan atas manajemen perusahaan. Transparansi kepemilikan manfaat didukung dan dipantau oleh beberapa organisasi internasional, seperti *Financial Action Task Force (FATF)* dan *OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes.*

c. Publikasi data registrasi perusahaan yang dikelola pemerintah

Peningkatan registrasi harus menyediakan akses publik ke data perusahaan *Spyware* komersial pada semua yurisdiksi. Kualitas catatan yang buruk akan menghambat upaya uji tuntas oleh banyak pihak. Misalnya, basis data perusahaan berkualitas tinggi dan dapat diakses publik akan menyediakan materi informasi untuk rezim uji tuntas investor yang jauh lebih baik di pasar *Spyware.* Ini juga akan membantu menyamakan kedudukan antara regulator di berbagai yurisdiksi. Hal ini akan memungkinkan kolaborasi lintas batas dalam mengatur perilaku vendor, pemasok, dan investor perangkat *Spyware*. Selain itu, juga akan memungkinkan entitas yang tunduk pada uji tuntas pelanggan, misalnya, bank, notaris, penyedia layanan

perusahaan, untuk meningkatkan proses verifikasi mereka dan melaporkan ketidaksesuaian.

3) Memperkaya, mengaudit, dan mempublikasikan izin ekspor

Persyaratan perizinan ekspor adalah mekanisme bagi pemerintah untuk membatasi penjualan dan penggunaan produk dan layanan tertentu di luar perbatasan mereka. Lisensi ekspor merupakan ranah yang kompleks yang ditandai dengan variabilitas antar negara yang signifikan dalam standar, barang yang dicakup, dan penerapan uji kepentingan publik yang lebih luas, seperti pertimbangan HAM. Bahkan, pihak berwenang dapat mengurangi prioritas risiko HAM dengan dalih pertimbangan yang berlawanan, seperti pertumbuhan industri atau pengaruh geopolitik yang dirasakan mendukung persetujuan lisensi. Oleh karena itu, penerapan kontrol ekspor terhadap teknologi *Spyware* harus tetap menjaga keseimbangan antara beragam kepentingan tersebut.

Beberapa vendor *Spyware*, seperti NSO Group, secara terbuka memanfaatkan fakta bahwa ekspor mereka dilisensikan oleh lembaga pemerintah sebagai indikasi legalitasnya. Pelapor Khusus PBB tentang Kebebasan Berpendapat dan Berekspresi, menyatakan

kerangka kontrol ekspor global dan implementasi nasionalnya di wilayah tempat NSO Group beroperasi tidak memadai untuk mengatur teknologi *Surveilans* atau memperhitungkan dampak HAM. Akibatnya, meskipun ekspor NSO Group memang dilisensikan, ekspor yang dilakukan NSO Group dan ekspor vendor lain masih dapat menimbulkan risiko serius terhadap HAM, terutama di yurisdiksi di mana kerangka hukum yang mengatur penggunaan produknya minimal atau bahkan tidak ada. Penguatan rezim perizinan ekspor dapat dilakukan melalui tiga cara. *Pertama,* lisensi kontrol ekspor untuk *Spyware* dan layanan terkait erat harus mencakup nama semua karyawan yang pekerjaannya memiliki dampak material pada pengembangan produk yang menjadi subjek lisensi ekspor. *Kedua,* untuk memastikan kontrol ekspor efektif di dalam negeri, pemerintah harus menerapkan audit wajib dan berkala pada praktik perizinan, serta memberikan sanksi bagi pelanggaran. *Ketiga,* laporan audit dan izin ekspor asli tersebut juga harus dapat diakses oleh publik melalui otoritas perizinan nasional.

4) Membatasi Arbitrase Yurisdiksi oleh Vendor

Menerapkan kebijakan di luar yurisdiksi suatu negara merupakan tantangan dan menghadirkan peluang bagi vendor perangkat *Spyware* dan pihak lain

yang berupaya menghindari kontrol kebijakan ekstrateritorialitas ini sering dieksploitasi oleh vendor perangkat *Spyware* untuk melakukan arbitrase yurisdiksi dan mengambil keuntungan dari inkonsistensi antarpemerintah. Rekomendasi mengusulkan membatasi langkah arbitrase dengan fokus pada peningkatan hambatan bagi vendor yang terkait dengan lisensi ekspor untuk teknologi *Surveilans* elektronik, termasuk perangkat *Spyware* untuk meninggalkan satu yurisdiksi dan mewajibkan pelaporan cabang dan anak perusahaan baru. Arbitrase yurisdiksi oleh vendor *Spyware* merusak supremasi hukum, efisiensi pengawasan kebijakan, integritas pasar, dan dapat memicu persaingan kebijakan di antara yurisdiksi yang berbeda di mana negara akan mengadopsi persyaratan kebijakan yang berstandar rendah untuk menarik bisnis dan investasi.

Oleh karena itu, pengembangan kebijakan harus difokuskan beberapa strategi utama. *Pertama,* harus mempersulit dan mempermahal biaya bagi vendor yang memiliki lisensi ekspor untuk keluar dari suatu yurisdiksi. Hal ini harus mencakup kewajiban pengungkapan publik atas setiap pembukaan atau penutupan anak perusahaan atau cabang oleh vendor yang telah diberikan lisensi untuk mengekspor

Spyware.

Kedua, para pembuat kebijakan dengan wewenang yang ada untuk mengatur investasi masuk harus secara otomatis meninjau transaksi yang berdampak pada struktur kepemilikan vendor *Spyware* domestik dengan cara apa pun. Vendor yang gagal menandai transaksi tersebut, termasuk jika informasi tersebut terungkap melalui mekanisme pengungkapan Kenali Vendor (*Know Your Vendor*) yang diwajibkan, harus dilarang berpartisipasi dalam pengadaan pemerintah dan/atau lisensi ekspor mereka ditangguhkan untuk jangka waktu tertentu. Dalam konteks pasar *Spyware,* persyaratan pemberitahuan akan meningkatkan transparansi pasar dan membantu menempatkan regulator di berbagai yurisdiksi pada posisi yang lebih setara. Hal ini juga akan memungkinkan pemangku kepentingan utama, termasuk organisasi masyarakat sipil, untuk memiliki visibilitas terhadap operasi vendor *Spyware* dan kepatuhan mereka terhadap persyaratan peraturan. *Ketiga*, harmonisasi persyaratan pengungkapan ini harus menjadi bagian dari mekanisme kolaboratif dan kerja sama antarpemerintah. Hambatan efektif terhadap keluarnya vendor *Spyware* ini dari pasar akan membantu meningkatkan potensi pengaruh kebijakan domestik.

5) Memberikan perlindungan yang lebih besar terhadap Gugatan Strategis Terhadap Partisipasi Publik *(Strategic Lawsuits Against Public Participation/SLAPP)*

Salah satu kecenderungan yang lebih luas untuk menuntut akuntabilitas penggunaan perangkat *Spyware* adalah pentingnya pelaporan terbuka melalui jurnalisme dan penelitian. Kecenderungan yang mengkhawatir kan baru-baru ini mengancam untuk merusak pelaporan ini karena sejumlah vendor *Spyware* menggunakan Gugatan Strategis Terhadap Partisipasi Publik (SLAPP). Pada titik ini, menjadi strategis bagi negara-negara yang menjadi pilihan yurisdiksi/tuan rumah gugatan (*states hosting parties*) bagi korban gugatan SLAP mengangkat isu ini melalui saluran diplomatik untuk melindungi korban dan menagih akuntabilitas penggunaan *Spyware* komersial.

Selain dimensi-dimensi tersebut di atas, berkaitan dengan pengembangan kebijakan, maka perlu belajar dari pengalaman Jerman, di mana penguatan keamanan siber dilakukan melalui kerangka hukum yang komprehensif dan melampaui

sekadar penanganan spionase siber. Pengaturan hukum Jerman juga mencakup kejahatan digital seperti akses tidak sah ke sistem elektronik, pencurian data, serta produksi dan distribusi alat penyusupan.[270] Pengaturan tersebut tertuang dalam *Strafgesetzbuch (StGB)* atau Kitab Undang-Undang Hukum Pidana Jerman. Secara lebih spesifik, pengaturan keamanan siber Jerman dirancang untuk melindungi sektor-sektor yang dikategorikan sebagai infrastruktur kritis antara lain energi, air, telekomunikasi, transportasi, dan layanan kesehatan. Operator di sektor-sektor tersebut diwajibkan menerapkan standar dan langkah-langkah keamanan siber yang memadai guna melindungi sistem mereka dari berbagai ancaman siber, termasuk spionase dan sabotase digital. Dalam kerangka kelembagaan, Kantor Federal untuk Keamanan Informasi *Bundesamt für Sicherheit in der Informationstechnik (BSI)* berperan sebagai otoritas pusat dalam pengelolaan keamanan siber nasional. BSI bertanggung jawab untuk mendorong penerapan praktik keamanan siber, menyediakan panduan teknis bagi entitas publik dan swasta, serta

[270] Mohamad Djafar Sodiq dkk., "Kebijakan dan Regulasi Spionase Siber di Indonesia," *IDEAS: Jurnal Pendidikan, Sosial, dan Budaya* 10, no. 4 (November 2024), https://jurnal.ideaspublishing.co.id/index.php/ideas/article/view/1909/799.

mengoordinasikan respons terhadap insiden siber. Kerangka hukum Jerman yang kuat dan jelas berperan sebagai benteng pertahanan terhadap ancaman siber. Ditambah dengan kerangka hukum yang transparan sehingga dapat memastikan kejelasan dan efisiensi dalam menangani ancaman siber.[271]

Dalam konteks Indonesia, penggunaan *Spyware* diatur secara tidak langsung melalui berbagai peraturan perundang-undangan yang berkaitan dengan keamanan siber, pelindungan data pribadi, penyadapan, dan kejahatan siber. Kekosongan aturan khusus untuk pengadaan teknologi sensitif berpotensi menyebabkan ambiguitas dalam prosedur dan pengawasan. Hal ini juga dapat disalahgunakan, terutama karena karakteristik paradoksal perangkat *Spyware* yang dapat digunakan untuk tujuan keamanan nasional, tetapi juga berpotensi disalahgunakan untuk pelanggaran privasi dan kebebasan berpendapat. Tabel peraturan perundang-undangan yang berkaitan dengan *Spyware* di Indonesia secara ringkas tersaji di bawah ini.[272]

[271] Lihat Lampiran 2
[272] Sumber data diolah FITRA

Peraturan Perundang-Undangan	Keterangan
UU Nomor 19 Tahun 2016 perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE);	Pasal 31: Mengatur larangan penyadapan informasi elektronik tanpa izin dan Pasal 32: Melarang perubahan, penghapusan, atau penyadapan data elektronik tanpa hak.
UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur pelindungan data pribadi di Indonesia, termasuk data yang dikumpulkan secara tidak sah melalui *Spyware*	Pasal 16: Pengendali data wajib mencegah akses tanpa izin terhadap data pribadi dan Pasal 65 sampai dengan pasal 66: Mengatur sanksi administratif dan pidana bagi pelaku yang mengumpulkan, menggunakan, atau menyebarkan data pribadi secara tidak sah.
PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Dimana dalam PP ini mengatur keamanan sistem elektronik, termasuk pelindungan terhadap ancaman seperti *malware* dan *Spyware*.	Penyelenggara sistem elektronik diwajibkan menerapkan standar keamanan siber untuk mencegah penyalahgunaan data.

Undang-Undang No. 35 Tahun 2009 tentang Narkotika (UU Narkotika).	Undang-Undang ini mengatur mengenai perluasan teknik penyidikan penyadapan (wiretapping). Dalam pasal Pasal 78 ayat (1) Dalam keadaan mendesak dan Penyidik harus melakukan penyadapan, penyadapan dapat dilakukan tanpa izin tertulis dari ketua pengadilan negeri lebih dahulu. Dan ayat (2) Dalam waktu paling lama 1 x 24 (satu kali dua puluh empat) jam Penyidik wajib meminta izin tertulis kepada ketua pengadilan negeri mengenai penyadapan sebagaimana dimaksud pada ayat (1).

Mekanisme keamanan siber di Indonesia dibangun melalui kerangka hukum dan kelembagaan yang menempatkan keamanan digital sebagai bagian dari kepentingan nasional. Badan Siber dan Sandi Negara (BSSN) berperan sebagai otoritas utama dalam perumusan kebijakan teknis, pengamanan sistem elektronik pemerintah, serta koordinasi deteksi dan respons insiden siber lintas sektor. Kerangka peraturan perundang-undangan keamanan siber bertumpu pada UU ITE, UU Pelindungan Data Pribadi,

serta berbagai peraturan terkait penyelenggaraan sistem elektronik. Peraturan perundang-undangan ini mewajibkan penyelenggara sistem elektronik untuk melindungi data dan sistem dari akses tidak sah, kebocoran, dan penyalahgunaan, sekaligus memberikan dasar hukum bagi negara dalam pencegahan dan penanganan ancaman siber. Indonesia juga menetapkan pelindungan khusus bagi infrastruktur informasi vital dan objek vital nasional, seperti sektor energi, keuangan, telekomunikasi, dan layanan publik digital. Namun, tantangan masih muncul dalam bentuk fragmentasi kewenangan serta perlunya pengawasan yang lebih kuat agar kebijakan keamanan siber tetap sejalan dengan prinsip HAM dan pelindungan data pribadi.

Selama ini, kewenangan melakukan penyadapan berada di berbagai peraturan sektoral atau terpisah seperti UU ITE, UU Telekomunikasi, UU KPK dan lainnya. Tidak adanya undang-undang khusus yang menjadi payung hukum penyadapan mengakibatkan ketidakseragaman prosedur dan standar yang digunakan dan berpotensi disalahgunakan untuk tujuan di luar penegakan hukum.[273]

[273] "Apa Kabar RUU Penyadapan?," *Tempo.co*, 26 Juni 2021, https://www.tempo.co/hukum/apa-kabar-ruu-penyadapan-823459. Diakses pada November 2025

Keberadaan payung hukum terkait penyadapan penting untuk memberikan kepastian prosedural, menentukan kewenangan lembaga yang berwenang, serta menetapkan aturan tentang izin dari otoritas yang independen seperti pengadilan, sekaligus membedakan antara penyadapan untuk penegakan hukum (*pro justitia*) atas permintaan Kepolisian atau Kejaksaan dan penyadapan untuk tujuan intelijen atau keamanan negara seperti BIN dan BNN. Hal yang tidak penting adalah bagaimana memastikan adanya mekanisme *judicial oversight* (izin pengadilan) yang efektif, serta penegasan batasan dan pengawasan untuk mencegah penyadapan yang tidak sah atau akuntabilitas penggunaannya.

Di sisi lain, detail teknis terkait penggunaan dan pengadaan *Spyware* tidak tercantum secara terbuka dan komprehensif dalam hukum yang diketahui publik. Praktik yang sering ditemui biasanya diatur dalam peraturan internal lembaga dengan akses keterbukaan publik yang tidak transparan. Namun, secara hukum larangan hukum penyadapan dan intersepsi komunikasi telah diatur melalui legislasi. Misalnya, dalam Pasal 31 UU ITE (UU No.11/2008 jo. perubahan) yang melarang intersepsi tanpa hak dan memasang

batasan legal atas praktik penyadapan. Putusan Mahkamah Konstitusi (MK) Nomor 5/PUU-VIII/2010 menyatakan bahwa penyadapan adalah hal yang sangat sensitif karena membatasi HAM dan harus diatur dalam undang-undang khusus. Tindak lanjut dari putusan tersebut hanya diatur dengan Peraturan Pemerintah (PP), hal ini kemudian menimbulkan polemik karena dipandang tidak dapat memenuhi syarat legalitas, keterbukaan, dan harus diatur oleh Undang-Undang.[274] Oleh karena itu, kekosongan pengaturan ini dapat menjadi masukan bagi pemerintah maupun legislasi untuk membuat pengaturan yang lebih komprehensif tentang penyadapan dan *Spyware* sebagai objek norma tersendiri.

[274] Nur Alam, "Konstitusionalitas Penyadapan (Interception) Dengan Peraturan Pemerintah Dari Sudut Pandang Perlindungan Hak Asasi Manusia," *Jatiswara* 27, no. 3 (November 2012).

Bukti resmi bahwa Indonesia membeli Pegasus memang belum ditemukan hingga saat ini. Namun, laporan dari Citizen Lab dan Amnesty Tech dalam rentang tahun 2019–2021 mengonfirmasi adanya jejak infeksi *Spyware* tersebut pada perangkat milik sejumlah aktivis dan jurnalis di Indonesia. Jika memang ada pengadaan, kemungkinan melibatkan BIN atau Densus88, dilakukan secara *off-budget* (di luar APBN formal), menggunakan belanja rahasia dan tidak melalui mekanisme Pengadaan Barang Jasa (PBJ) biasa seperti Layanan Pengadaan Secara Elektronik (LPSE) dengan mekanisme tender. Terdapat bukti impor dan penggunaan teknologi pengawasan melalui perantara dan jalur komersial non-publik. Laporan investigasi dan liputan media mencatat jejak produk seperti Pegasus dan *Spyware* lainnya yang masuk ke Indonesia, dan ada temuan mengenai akuisisi melalui pihak ketiga atau perantara.[275] Meskipun pengadaan perangkat *Spyware* bermanfaat untuk mengatasi

[275] M. Faiz Zaki, "Amnesty International Ungkap Polri Impor Alat Sadap, Ini Kata Pakar Kepolisian Soal SOP Penyadapan," *Tempo.co*, 20 Juni 2024, https://www.tempo.co/hukum/amnesty-international-ungkap-polri-impor-alat-sadap-ini-kata-pakar-kepolisian-soal-sop-penyadapan-61122. Diakses pada Agustus 2025.

kriminalitas, penggunaannya sangat rentan disalahgunakan bahkan *Spyware* sendiri telah menjadi masalah HAM dan keamanan secara global.

Jejak penggunaan perangkat *Spyware* di Indonesia terungkap dalam investigasi kolaboratif antara Amnesty International dan Tempo. Investigasi tersebut mengungkap bahwa sejak tahun 2017 hingga 2023, sejumlah lembaga negara dan perusahaan di Indonesia diduga telah mengimpor serta menggunakan teknologi *Spyware*. Laporan tersebut juga mengidentifikasi bahwa perangkat-perangkat *Surveilans* ini tidak disuplai secara langsung, melainkan melalui jaringan perantara dan broker yang kompleks. Pola distribusi ini menyebabkan transaksi serta penggunaan alat-alat tersebut berlangsung secara tertutup dan tidak transparan. Terdapat empat vendor yang teridentifikasi termasuk Q Cyber Technologies SARL yang berbasis di Luksemburg (terkait dengan NSO Group), konsorsium Intellexa, Wintego Systems Ltd dan Saito Tech yang berbasis di Israel (dikenal sebagai Candiru), dan Raedarius M8 Sdn Bhd yang berbasis di Malaysia (terkait dengan FinFisher). Perangkat *Spyware* yang masuk ke Indonesia diduga telah dibeli dan digunakan oleh institusi seperti Kepolisian RI dan Badan Siber dan Sandi Negara (BSSN). Hal tersebut

menimbulkan kekhawatiran atas potensi pelanggaran privasi dan menyusutnya ruang sipil, terutama di tengah belum adanya aturan yang mengatur secara tegas penggunaan teknologi pengawasan *Spyware* di Indonesia.[276] Selanjutnya, laporan Amnesty International menunjukkan adanya dugaan kuat keterlibatan jaringan perusahaan domestik dan internasional dalam pengadaan teknologi *Surveilans* canggih bagi sejumlah lembaga negara di Indonesia.[277]

Dalam lanskap digital Indonesia yang terus berkembang, bayangan gelap penggunaan teknologi *Spyware* harus menjadi perhatian serius karena berkaitan dengan kerentanan privasi dan keamanan siber nasional. Pengadaan *Spyware* di Indonesia melibatkan aktor negara dan non-negara, seperti perusahaan swasta dan lain lain. Perangkat *Spyware* yang semakin canggih kini digunakan untuk menyasar target yang luas, mulai dari aktivis hingga tokoh politik. Meskipun pengadaan dan penggunaannya sering kali

[276] Han Revanda Putra, "Investigasi Tempo Ungkap Perusahaan Israel Diduga Pasok Spyware ke Indonesia Sejak 2017," *Tempo.co*, 20 Juni 2024, https://www.tempo.co/arsip/investigasi-tempo-ungkap-perusahaan-israel-diduga-pasok-spyware-ke-indonesia-sejak-2017-62228. Diakses pada Desember 2025.

[277] Putra, "Investigasi Tempo Ungkap Perusahaan Israel Diduga Pasok Spyware ke Indonesia Sejak 2017."

berlindung di balik dalih keamanan nasional serta penegakan hukum, praktik ini tetap menuntut pengawasan yang ketat.

I.2. Kesenjangan Transparansi dalam Pengadaan Barang dan Jasa Teknologi Intelijen dan *Surveilans*

Dugaan bahwa lembaga negara di Indonesia menggunakan *Spyware* sebenarnya bukan hal baru. Jejaknya sudah terlihat sejak tahun 2013 melalui pernyataan resmi Kementerian Pertahanan mengenai pengadaan perangkat *Surveilans*. Kementerian Pertahanan menyatakan bahwa mereka telah bekerja sama dengan perusahaan bernama Gamma TSE Ltd. UK untuk pengadaan alat antisadap yang nantinya akan digunakan oleh Badan Intelijen Negara (BIN). Selain itu, pada 2018 publik dikejutkan juga dengan penggunaan *Spyware* Pegasus oleh Kepolisian RI dan BIN. Terlebih lagi pada tahun ini, Kejaksaan telah menandatangani perjanjian kerja sama dengan operator telekomunikasi seperti XL, Telkomsel dan operator lainnya, yang memberikan Kejaksaan kewenangan yang sangat luas untuk memasang dan

mengoperasikan perangkat penyadap untuk mendapatkan informasi dengan alasan penegakan hukum.[278]

Selain itu, dari segi anggaran negara dalam konteks pertahanan dan keamanan terdapat kenaikan yang cukup signifikan pada era pemerintahan Prabowo Subianto. Pada tahun 2025 anggaran pertahanan dan keamanan mengalami kenaikan sekitar Rp 25 triliun dibandingkan tahun 2024, yakni dari Rp 139 triliun pada 2024 menjadi Rp 165 triliun pada 2025. Penambahan terutama dilakukan untuk meningkatkan kesejahteraan prajurit TNI serta modernisasi alat utama sistem persenjataan (*alutsista*).[279] Selanjutnya, estimasi alokasi biaya untuk pembelian *Spyware* Pegasus antara 2016 - 2022, dapat dilihat melalui tabel berikut:[280]

---

[278] Lihat, Fahmi Ramadhan, "Teken Nota Kesepakatan dengan Provider, Kejagung Bisa Pasang Alat Sadap untuk Kumpulkan Data," *Tribunnews.com*, 26 Juni 2025, https://www.tribunnews.com/nasional/2025/06/26/teken-nota-kesepakatan-dengan-provider-kejagung-bisa-pasang-alat-sadap-untuk-kumpulkan-data.

[279] Kurnia Yunita Rahayu dan Hidayat Salam, "Sejalan dengan Visi Prabowo, Anggaran Pertahanan Naik Jadi Rp 165 Triliun," *Kompas.id*, 16 Agustus 2024, https://www.kompas.id/artikel/sejalan-dengan-visi-prabowo-anggaran-pertahanan-naik-jadi-rp-165-triliun. Diakses pada 15 Januari 2026.

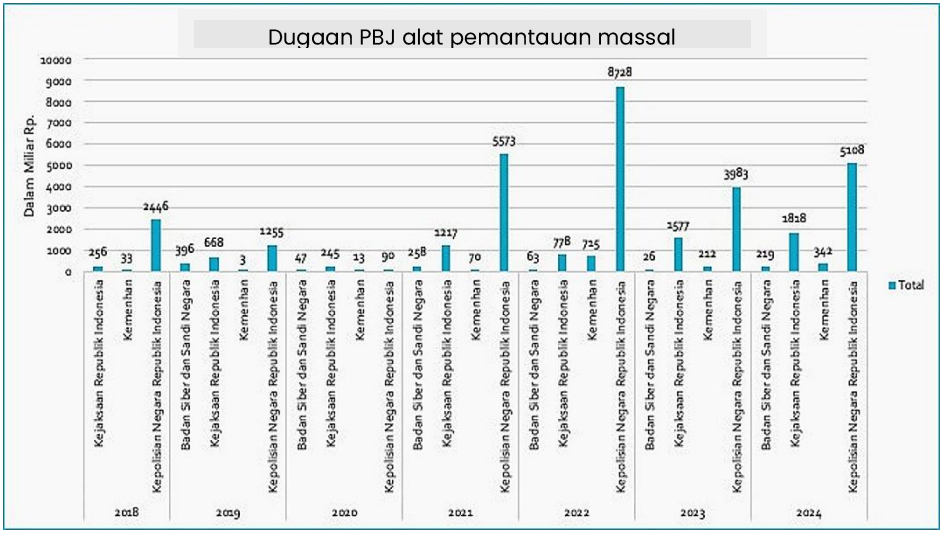
[280] Laporan Amnesty International diolah FITRA

Komponen	Estimasi Biaya
Biaya lisensi awal (setup)	USD 8-10 juta
Paket per target (per device)	USD 500 ribu – 1 juta per 10-50 target
Dukungan teknis & pemeliharaan tahunan	USD 1-2 juta per tahun
Total kontrak (selama 2–3 tahun)	USD 15-25 juta (Rp250-400 miliar)

Lebih jauh, belanja publik untuk alokasi intelijen, sistem dan teknologi *Surveilans* merupakan bagian penting dari fungsi penegakan hukum, keamanan dan pertahanan negara. Anggaran semacam ini tidak hanya mencakup biaya operasional personil dan logistik, tetapi juga pengadaan perangkat dan sistem teknologi yang mendukung fungsi intelijen dan *Surveilans*. Misalnya, dalam periode 2018–2024,

Kemenhan (BIN) tercatat mengeluarkan Rp1,3 triliun untuk sembilan paket pengadaan terkait aktivitas digital, termasuk sistem komando dan kontrol serta *intelligence target surveillance,* yang menunjukkan adanya investasi pada teknologi pemantauan dan *Surveilans*.

Menurut data Sekretariat Nasional Forum Indonesia Untuk Transparansi Anggaran (Seknas FITRA) dan Lembaga Studi dan Advokasi Masyarakat (ELSAM) APBN sebesar 36,1 triliun digunakan oleh lima lembaga negara, yaitu TNI, Kepolisian RI, BIN serta Kejaksaan untuk pengadaan teknologi *Surveilans* massal (*mass surveillance*). Alokasi anggaran perangkat intelijen dan *Surveilans* pada keempat lembaga negara sepanjang 2018-2024 dapat dilihat melalui diagram di bawah ini.[281]



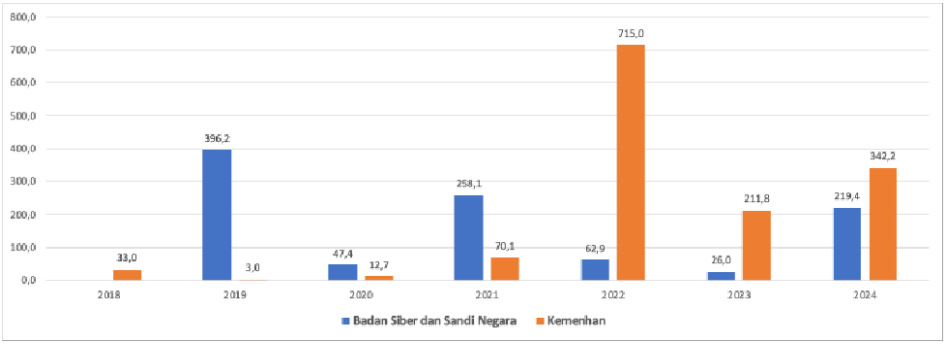
[281] Data hasil olahan FITRA

Analisis tersebut diperkuat melalui Laporan terbaru GlobalData, *Indonesia Defense Market Size, Trends, Budget Allocation, Regulations, Acquisitions, Competitive Landscape and Forecast to 2030*. Laporan tersebut mengungkapkan, pengeluaran pertahanan kumulatif Indonesia diperkirakan mencapai $46,6 miliar dalam periode 2024–2028. Dari total tersebut, porsi untuk anggaran akuisisi diprediksi sebesar 28,4% atau setara dengan $13,3 miliar. Pengeluaran pengadaan pertahanan diperkirakan akan mencatat tingkat pertumbuhan tahunan majemuk (CAGR) sebesar 1,5% selama periode 2024-2028 dan mencapai $2,7 miliar pada 2028. Menurut Abhijit Apsingikar, Aerospace & Defense Analyst at GlobalData, anggaran pertahanan Indonesia sebagian besar didorong oleh kebutuhan untuk mengurangi dampak bencana alam dan melakukan inisiatif modernisasi militer. Indonesia berupaya memperluas postur pertahanannya serta meningkatkan kompleks industri manufaktur pertahanan dalam negeri melalui inisiatif modernisasi militer. Lebih lanjut, meningkatnya fundamentalisme ditambah dengan radikalisme daring (*online radicalism*) telah memperburuk ancaman terorisme, yang, telah memaksa Indonesia untuk berinvestasi besar-besaran dalam keamanan siber dan aparat kontra-terorisme.[282]

Data anggaran internal institusi penegak hukum dan lembaga pemerintah lain juga menunjukkan alokasi dana signifikan untuk peralatan intelijen dan perangkat *Surveilans*. Dalam dokumen anggaran Kejaksaan Agung, tercatat pagu anggaran Rp 6,5 triliun untuk pengadaan peralatan intelijen, laboratorium forensik digital, bahkan perangkat monitoring taktis, yang semuanya berkaitan dengan penguatan fungsi investigasi dan *Surveilans*. Sementara itu, Badan Siber dan Sandi Negara (BSSN) sebagai otoritas keamanan siber nasional pada tahun 2018-2024 memperoleh pagu indikatif sekitar Rp 1 triliun. Tidak ada anggaran yang dialokasikan untuk perluasan cakupan *Surveilans* melalui National Security Operation Center (NSOC), meskipun ini merupakan program prioritas untuk meningkatkan kemampuan deteksi dan respons ancaman siber. Keterbatasan anggaran ini dikhawatirkan berimplikasi pada efektivitas pengamanan ruang siber nasional. Di tingkat legislatif, anggota DPR juga menekankan pentingnya investasi teknologi intelijen modern guna meningkatkan kapasitas Badan Intelijen Negara (BIN) dalam

[282] "Indonesia Defense Expenditure to Reach $9.7 Billion by 2028," *Asia Pacific Defence Reporter*, 31 Agustus 2023, https://asiapacificdefencereporter.com/indonesia-defense-expenditure-to-reach-9-7-billion-by-2028/. Diakses pada 15 Januari 2025.

teknologi intelijen modern guna meningkatkan kapasitas Badan Intelijen Negara (BIN) dalam menghadapi tantangan keamanan yang semakin kompleks di era digital. Menurut anggota Komisi III, Bambang Soesatyo, kebutuhan akan perangkat intelijen terkini adalah bagian dari upaya menjaga kedaulatan dan keamanan bangsa.[283] Alokasi anggaran alat intelijen dan *Surveilans* di Kemenhan dapat dilihat melalui tabel di bawah ini.[284]



[283] Bagus Ahmad Rizaldi, "Anggota DPR Sebut BIN Perlu Investasi Teknologi Intelijen Terkini," *Antaranews.com*, 21 Mei 2025, https://www.antaranews.com/berita/4820745/anggota-dpr-sebut-bin-perlu-investasi-teknologi-intelijen-terkini.. Diakses pada Desember 2025.
[284] Data hasil olahan FITRA

Isu transparansi dan akuntabilitas anggaran pengadaan teknologi *Surveilans* sering kali menjadi sorotan publik dan organisasi masyarakat sipil. Kekhawatiran muncul terutama ketika anggaran besar dialokasikan untuk sistem yang bersifat sensitif seperti pengawasan digital dan kemampuan *Surveilans* tanpa penjelasan rinci kepada publik tentang tujuan, mekanisme pengawasan, dan jaminan pelindungan hak asasi manusia. Anggaran besar untuk alat penyadap sering tidak disertai bukti efektivitas dan mekanisme kontrol yang kuat, sehingga potensi penyalahgunaan tidak bisa diabaikan.[285] Dalam perspektif kebijakan anggaran publik, pengeluaran untuk intelijen dan *Surveilans* memang menjadi kebutuhan strategis dalam menjaga keamanan nasional. Namun, alokasi untuk intelijen dan *Surveilans* juga menuntut sistem pengawasan internal yang ketat, transparansi penggunaan anggaran, dan kerangka hukum yang jelas agar fungsi tersebut tidak berujung pada pelanggaran hak privasi maupun hak kebebasan sipil fundamental, baik sipil di ruang digital maupun fisik.

[285]Aliansi Jurnalis Independen, "Jelang Pemilu 2024, Perlu Regulasi Penggunaan Alat Sadap seperti Pegasus," *Aji.or.id*, 23 Juni 2023, https://www.aji.or.id/informasi/jelang-pemilu-2024-perlu-regulasi-penggunaan-alat-sadap-seperti-pegasus. Diakses pada Desember 2025.

Apabila ditelisik lebih jauh terdapat sepuluh besar pengadaan barang dan jasa perangkat intelijen dan *Surveilans* sepanjang 2018-2024, seperti terlihat pada tabel di bawah ini.[286]

[286] Data hasil olahan FITRA

Tahun	Alat Intelijen dan *Surveilans*	Kementerian	Anggaran	Metode Pemilihan
2021	Pengadaan Peralatan Sistem Pengawasan Teknologi Informasi (Aktive)	Kejaksaan RI	488.469.587.460	Penunjukan Langsung
2023	Peralatan Sistem Pencari Target Mobile (Dynamic Active Target Monitoring System) Pertempuran	Kepolisian RI	418.849.966.000	Penunjukan Langsung
2022	Pengadaan Hybrid Surveillance Car With Compact Portable Active Intelligent Intercept TA 2022	Kepolisian RI	412.644.600.000	Tender
2023	Pengadaan Surveillance Car	Kepolisian RI	399.716.120.000	Tender

	With Active Intercept Monitoring Intelligence System			
2019	Pengadaan Peralatan Counter Surveillance Tahap III	Kejaksaan RI	379.782.040.000	Penunjukan Langsung
2022	Pengadaan Hybrid Surveillance Car With Compact Portable Active Intelligent Interceptta. 2022	Kepolisian RI	359.805.343.000	Tender
2022	Pengadaan Disclosure Mobile Surveillance And Communication Devices Detector Ta. 2022	Kepolisian RI	352.484.407.000	Tender
2022	Pengadaan Disclosure Mobile	Kepolisian RI	352.484.407.000	Tender

	Surveillance And Communication Devices Detector Ta. 2022			
2023	Pengadaan Hybrid Surveillance Car With Compact Portable Active Intelligent Intercept	Kepolisian RI	350.138.916.000	Tender
2024	Pengadaan Peralatan Intelijen Kartu TIK Digital dengan Basis Biometrik untuk Data Kriminal Kejaksaan RI	Kejaksaan RI	350.000.000.000	Penunjukan Langsung

Selanjutnya, alokasi pengadaan barang dan jasa sepuluh besar di Kementerian Pertahanan sepanjang 2018-2024 dapat dilihat melalui tabel berikut ini.[287]

[287] Data hasil olahan FITRA

Tahun	Alat Intelijen dan *Surveilans*	Satker	Anggaran	Metode Pemilihan
2022	Sistem Komando Siber Intelijen	Mabes TNI AD	199.995.537.000	Penunjukan Langsung
2024	Pengadaan Sistem Monitoring Threat Intelligence and Target Intelligence (Dispamsanal)	MABES TNI AL TNI AL	100.000.000.000	Penunjukan Langsung
2022	Portable Wireless Intelligence Monitoring System	Mabes TNI AD	97.348.807.000	Penunjukan Langsung
2022	Stealth Intelligence Military Task	Mabes TNI AD	97.155.441.000	Penunjukan Langsung
2022	Baseline Electronic Aggregation Cyber Center	Mabes TNI AD	96.218.126.000	Penunjukan Langsung

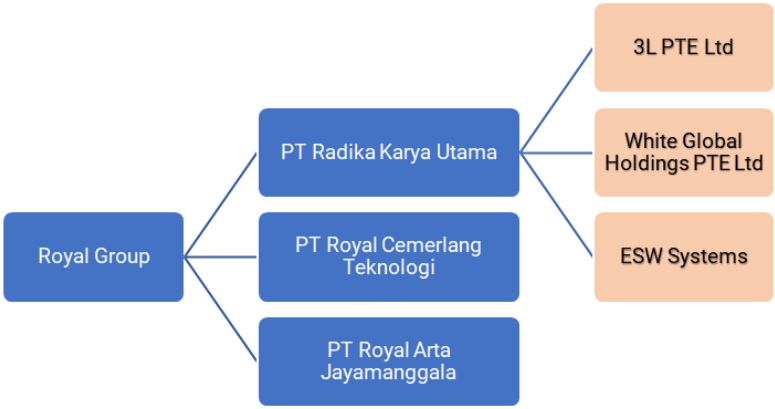
2022	Locator Intelligance Information Control of Dissemination Area	Mabes TNI AD	95.020.118.000	Penunjukan Langsung
2024	Pengadaan System Cyber Troops (Multiyears Tahap II)	Mabes TNI AD	69.993.498.000	Penunjukan Langsung
2024	Pengadaan Integrated Wireless Intelligence Secure Data (Multiyears Tahap II)	Mabes TNI AD	67.846.877.000	Penunjukan Langsung
2024	Pengadaan Tap Wire Silent Intelligence (Multiyears Tahap-2)		59.311.174.000	Penunjukan Langsung

2023	Tactical Intelligence Monitoring Surveillance Tahap I	Mabes TNI AD	43.500.000.000	Penunjukan Langsung

Berdasarkan data di atas, anggaran pengadaan barang dan jasa untuk kebutuhan intelijen, *Surveilans*, dan teknologi *Spyware* di Indonesia kerap dilakukan melalui mekanisme penunjukan langsung. Penggunaan mekanisme ini seringkali dilandasi pertimbangan kerahasiaan, urgensi keamanan, sifat strategis kegiatan dan bahkan keterbatasan vendor. Secara regulatif, skema ini memang dimungkinkan dalam aturan pengadaan barang dan jasa pemerintah. Namun, dalam praktiknya, penunjukan langsung sering digunakan pada pengadaan teknologi pengawasan bernilai besar dan berisiko tinggi tanpa proses kompetitif yang memadai.

Kondisi tersebut diperkuat melalui laporan Amnesty International yang menunjukkan jaringan perusahaan domestik dan internasional dalam pengadaan teknologi pengawasan canggih untuk lembaga negara di Indonesia. Salah satu aktor utama

pengadaan perangkat *Spyware* di Indonesia adalah PT. Radika Karya Utama, perusahaan berbasis di Indonesia yang tercatat memiliki riwayat pengadaan teknologi *Surveilans* atas nama institusi pemerintah, di samping aktivitas komersial lain yang tidak berkaitan langsung dengan sistem pengawasan. PT. Radika Karya Utama juga beroperasi melalui sejumlah entitas korporasi lain, seperti PT. Royal Cemerlang Teknologi dan PT. Royal Arta Jaya Manggala, yang kerap dikaitkan dalam satu payung usaha yang dikenal sebagai Royal Group. Jaringan struktur organisasi Royal Group dalam pengadaan perangkat *Spyware* di Indonesia dapat diilustrasikan melalui gambar berikut ini:[288]



[288] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia." https://www.amnesty.org/en/documents/asa21/7974/2024/en/ diakses pada Desember 2025.

Berdasarkan dokumen tender publik, diketahui bahwa PT. Radika Karya Utama pernah memenangkan pengadaan sistem intrusi tanpa klik (*zero-click intrusion*) dan memiliki sistem *Surveilans* telekomunikasi serta geolokasi yang berasal dari Circles, perusahaan afiliasi NSO Group asal Israel. Sistem tersebut dilaporkan diterapkan pada jaringan IP 203.142.69.82 – 84 dan 117.102.125.50–52 yang terdaftar atas nama perusahaan-perusahaan tersebut. Dokumen tender P.T. Radika Karya Utama mengindikasikan keterlibatan langsung dalam implementasi teknologi *Surveilans* tingkat lanjut.[289]

Skor	Judul	Penyedia	LPSE	Tanggal Pengumuman	Nilai Kontrak
60	PERALATAN DAN MATERIIL KHUSUS DIT INTELKAM (ZERO CLICK INSTRUKSION SYSTEM) POLDA METRO JAYA BERIKUT PENGIRIMAN	PT. RADIKA KARYA UTAMA	LPSE Kepolisian Republik Indonesia	22 September 2017	Rp 98.912.000.000,00
57	PENGADAAN ALMATSUS PENGEMBANGAN ZERO CLICK INSTRUSION SYSTEM (IOS) APBN TA. 2018	PT. RADIKA KARYA UTAMA	LPSE Kepolisian Republik Indonesia	14 February 2018	Rp 149.831.000.000,00

Di tingkat internasional, Amnesty International juga mengidentifikasi peran White Global Holdings PTE Ltd, 3L PTE Ltd, dan ESW Systems. Ketiga perusahaan

[289] Lihat *OpenTender.net*

yang berbasis di Singapura ini menggambarkan diri mereka sebagai entitas yang saling terkait dan aktif dalam perdagangan teknologi *Surveilans* serta perlengkapan militer dan kepolisian bagi pasar global, termasuk Indonesia. Struktur kepemilikan ketiga perusahaan ini dinilai tidak transparan. Catatan korporasi mengungkap bahwa sejumlah warga negara Indonesia pernah tercatat sebagai pemegang saham dan pengurus, termasuk individu yang juga memiliki keterkaitan dengan perusahaan-perusahaan di Indonesia. Catatan perdagangan menunjukkan bahwa pada Maret 2019, White Global Holdings mengirimkan produk yang dideskripsikan sebagai "modul instalasi satu klik Android (*Android one click installation module*)" kepada Badan Siber dan Sandi Negara (BSSN). Deskripsi ini mengindikasikan penjualan solusi *Spyware* yang mampu menginfeksi perangkat Android target secara langsung. Selain itu, pada Juli 2021, ESW Systems tercatat mengekspor berbagai lisensi sistem pengawasan bernilai lebih dari USD 11 juta kepada Kepolisian RI, termasuk lisensi deteksi grafis berbasis daftar pantauan dan sistem pelacakan geolokasi waktu nyata *(realtime)*. Produk-produk tersebut diduga berkaitan dengan analisis lalu lintas jaringan seluler

dan sistem pelacakan berbasis *Surveilans*. Catatan perdagangan lainnya juga menunjukkan pengiriman produk bertajuk "WINT SYSTEM" dari ESW Systems kepada Kepolisian RI, yang diyakini berkaitan dengan teknologi *Surveilans* milik Wintego Systems, perusahaan yang dikenal memasarkan perangkat *Spyware* dan intersepsi jaringan taktis. Seluruh produk tersebut termasuk dalam kategori teknologi dwiguna yang memiliki potensi digunakan sebagai instrumentasi penyalahgunaan terhadap HAM.

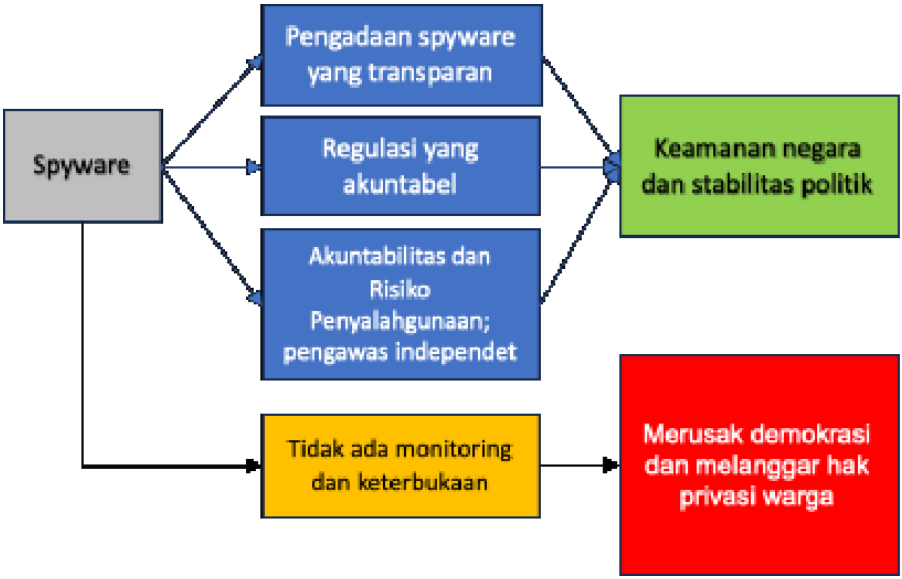
Amnesty International telah menghubungi seluruh perusahaan yang disebutkan termasuk Radika, White Global Holdings, 3L, ESW Systems, serta entitas Royal Group; untuk meminta klarifikasi terkait pengadaan *Spyware,* hubungan antarperusahaan, dan pemenuhan komitmen penghormatan terhadap HAM sesuai Prinsip-Prinsip Panduan PBB tentang Bisnis dan HAM. Namun, tidak satu pun memberikan tanggapan sebelum laporan dipublikasikan. Permintaan klarifikasi juga diajukan kepada Kepolisian RI dan Badan Siber dan Sandi Negara (BSSN), tetapi tidak memperoleh respons substantif. Kepolisian RI menolak menanggapi tuduhan yang disampaikan. Selain itu, Amnesty International juga mengungkap keterlibatan HEHA, perusahaan berbasis di Singapura, yang tercatat

mengekspor perangkat keras bertajuk "Sistem Infiltrasi Intelijensi Siber; Eksfiltrasi (Cyber Intelligence Infiltration; Exfiltration System)" ke KepolisianRI pada 2020–2021 dengan nilai total sekitar USD 33 juta. Seperti perusahaan lain yang disorot, HEHA juga tidak memberikan klarifikasi atas pertanyaan terkait produsen teknologi, mekanisme pengadaan, maupun penilaian dampak HAM. Temuan-temuan ini menegaskan lemahnya transparansi dan akuntabilitas dalam pengadaan teknologi *Surveilans* di Indonesia, sekaligus potensi penyalahgunaan *Spyware* di tengah belum adanya kerangka hukum yang komprehensif untuk mengatur praktik penyadapan dan *Surveilans* digital.

Perdagangan *Spyware* yang tidak transparan dan minim akuntabilitas ke Indonesia telah menambah jajaran instrumen berbahaya yang berpotensi digunakan untuk intimidasi. Investigasi Laboratorium Keamanan Amnesty International (*Amnesty International Security Lab*) mengungkap bukti penjualan serta penyebaran *Spyware* invasif ke sejumlah lembaga negara, termasuk Polri dan BSSN, sepanjang periode 2017–2023. Transaksi ini terjadi melalui jejaring vendor dan broker yang beroperasi dengan struktur kepemilikan rumit dan minim

transparansi, di antaranya Q Cyber Technologies (NSO Group), Intellexa, Wintego, Candiru, serta Raedarius M8 (FinFisher). Investigasi tersebut juga mengidentifikasi infrastruktur digital berbahaya yang terkait dengan *Spyware* Candiru dan Predator dari Intellexa. Infrastruktur ini mencakup penggunaan domain palsu yang dirancang untuk mengelabui jurnalis, organisasi masyarakat sipil, hingga partai oposisi agar mengklik tautan berbahaya yang berpotensi menginfeksi perangkat mereka. Meskipun sulit ditemukan bukti infeksi langsung pada individu tertentu karena sifat *Spyware* yang sangat rahasia, keberadaan infrastruktur ini mengonfirmasi adanya upaya penargetan yang sistematis.[290] Dampak penggunaan perangkat *Spyware*, apabila tidak dilakukan pengaturan untuk menuntut akuntabilitas berdasarkan HAM, supremasi hukum, dan keadilan dapat dilihat melalui ilustrasi gambar di bawah ini.[291]

[290] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia."
[291] Gambar hasil olahan peneliti



Kondisi tersebut menunjukkan adanya pola penunjukan langsung secara berulang yang melibatkan penyedia yang sama dalam pengadaan sistem intrusi, pelacakan geolokasi, dan perangkat pemantauan digital. Minimnya keterbukaan informasi publik mengenai spesifikasi teknis, nilai kontrak, hingga dasar pemilihan penyedia ini menimbulkan kekhawatiran serius terhadap potensi konflik kepentingan, inefisiensi anggaran, serta penyalahgunaan teknologi *Surveilans*. Kondisi ini memperlihatkan adanya ruang abu-abu antara kebutuhan keamanan negara dan prinsip akuntabilitas

anggaran publik. Tanpa pengawasan yang ketat, uji tuntas HAM, serta mekanisme kontrol independen, praktik penunjukan langsung dalam pengadaan teknologi *Surveilans* berisiko melemahkan transparansi pengelolaan anggaran dan memperbesar ancaman terhadap hak privasi serta kebebasan sipil fundamental warga negara. Pada saat bersamaan, pengadaan barang/jasa terkait *Spyware* di Indonesia menghadapi tantangan serius dalam hal akuntabilitas, terutama karena sifat sensitif teknologi ini dan potensi penyalahgunaannya. Oleh karena itu, diperlukan pengendalian ekspor teknologi spionase dan peningkatan transparansi serta akuntabilitas dalam penggunaannya untuk melindungi hak dan kebebasan fundamental setiap warga negara.

I.3. Jejak-Jejak Penggunaan Perangkat *Spyware* di Indonesia dan Ancamannya Terhadap HAM: Refleksi dari Kasus *Pengembang Inti dan Jaringan Pendukung*

Dalam laporan yang dipublikasikan oleh Amnesty International bertemakan *Global: A Web of Surveillance – Unravelling a murky network of Spyware exports to*

Indonesia" tahun 2024 lalu, setidaknya ada lima perusahaan *Spyware* yang menjual teknologinya kepada Indonesia yaitu FinFisher, Wintego Systems Ltd, Intellexa Consorsium, Candiru dan NSO Group. Produk perangkat *Spyware* ini diduga digunakan di berbagai macam lembaga seperti BIN, BSSN, Kepolisian RI dan TNI. Berikut rincian kelima perusahaan tersebut:

1) Finfisher

Finfisher merupakan perangkat yang dikembangkan oleh Gamma International GmBH asal Munich, Jerman yang berfungsi sebagai alat intrusi serta pemantauan jarak jauh. Kemudian alat tersebut dipasarkan dan dijual oleh Gamma Group basis UK kepada aparat penegak hukum dan badan intelijen negara.[292] Dalam brosur pemasaran FinSpy dijelaskan bahwa teknologi ini bekerja dengan cara menembus 40 sistem antivirus yang telah diuji secara berkala, melakukan komunikasi dengan kantor induk, serta mampu memantau aktivitas Skype (panggilan, pesan, transfer berkas, video, dan

[292]Morgan Marquis-Boire dkk., "You Only Click Twice: FinFisher's Global Proliferation," *Citizen Lab*, 13 Maret 2013, https://citizenlab.ca/research/you-only-click-twice-finfishers-global-proliferation-2/#1.

daftar kontak). Selain itu, teknologi ini dapat merekam berbagai bentuk komunikasi umum seperti email, pesan instan, *Voice-Over-IP,* melakukan pemantauan langsung melalui webcam dan mikrofon, melacak lokasi negara asal target, mengekstraksi file secara diam-diam dari hard disk, merekam *keylogger* untuk mempercepat analisis, melakukan forensik jarak jauh secara langsung pada sistem target serta menerapkan filter untuk informasi yang dianggap penting. Teknologi ini dapat bekerja di berbagai perangkat Windows, Mac OS X dan Linux. Setelah alat ini terpasang, perangkat yang terinfeksi dapat diakses dan dikendalikan dari jarak jauh begitu sistemnya terhubung ke jaringan internet, tanpa memandang lokasi geografis di mana target berada.[293]

Pada 2012 silam, Citizen Lab melakukan pemantauan terhadap server FinSpy selama satu tahun dan menemukan adanya 36 server FinSpy yang tersebar di 25 negara, beberapa di antaranya adalah Indonesia, Australia, Bahrain, Bangladesh, Brunei, Canada, Republik Ceko,

[293] https://wikileaks.org/spyfiles/docs/gamma/289_remote-monitoring-and-infection-solutions-finspy.html

Estonia, Ethiopia, Jerman, India dan lain sebagainya. Di Indonesia sendiri teknologi ini telah beroperasi sejak tahun 2012 dan telah ditemukan ada tiga operator telekomunikasi yang menggunakan teknologi dari Gamma International GmBH tersebut, yaitu P.T. Telkom, P.T. Matrixnet Global dan Biznet ISP. Alamat Protokol Internet (IP *Address*) sengaja tidak dipublikasikan secara menyeluruh untuk mencegah operator menonaktifkan atau memindahkan infrastruktur server mereka selama proses pemantauan berlangsung. Meski demikian, tabel di bawah ini merangkum sejumlah alamat IP yang telah teridentifikasi kuat menggunakan teknologi FinSpy di Indonesia.

Alamat IP	**Operator**	**Negara**
118.97.xxx.xxx	PT Telkom	Indonesia
118.97.xxx.xxx	PT Telkom	Indonesia
103.28.xxx.xxx	PT Matrixnet Global	Indonesia
112.78.143.34	Biznet ISP	Indonesia
112.78.143.26	Biznet ISP	Indonesia

Selain digunakan oleh operator telekomunikasi, teknologi FinSpy juga diduga digunakan oleh lembaga negara, yaitu Badan Siber dan Sandi Negara (BSSN). Indikasi ini pertama kali muncul ketika seorang anggota Hacking Team berada di Indonesia untuk melakukan uji coba teknologi bagi BSSN. Alamat IP yang terkait dengan FinSpy yaitu "/28" seperti yang ditemukan di berbagai negara seperti Mongolia, Belgia dan Serbia ditemukan juga pada header sebuah email yang dikirim oleh karyawan Hacking Team tersebut saat ia berada di lingkungan BSSN.[294] Email itu dikirim pada pukul 12.39 WIB, 6 Februari 2013, dan pada hari yang sama terdapat rapat yang telah dijadwalkan pukul 10.00 WIB sebelumnya di lembaga tersebut. Berdasarkan temuan tersebut, besar kemungkinan email itu dikirim dari dalam gedung BSSN, dan kedua server FinFisher yang berada dalam blok alamat IP yang sama kemungkinan juga dimiliki atau dioperasikan oleh organisasi tersebut.

Dalam konteks ekspor impor, Gamma

[294] Bill Marczak dkk., "Mapping FinFisher's Continuing Proliferation," *Citizen Lab*, 15 Oktober 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#51.

International GMBH tidak secara langsung menjual produk FinSpy ke Indonesia, melainkan melalui entitas bisnis bernama Raedarius M8 yang berlokasi di Malaysia dan Jerman lalu dijual ke Indonesia dalam bentuk hardware components seperti Fanless Computer Accessories, Plastic Case, Power Supply for Single Board Computer dan lain sebagainya kepada PT. Digital Solusi Prima yang merupakan perusahaan di Indonesia tentunya dengan harga yang sangat fantastis. Tetapi tidak ada temuan lebih jauh kepada siapa produk-produk ini dijual.[295] Perlu diketahui bahwa *Spyware* tidak selalu dijual sebagai satu produk lengkap. Dalam banyak kasus, teknologi ini ditawarkan dalam bentuk komponen terpisah yang kemudian dirakit, disesuaikan, atau diintegrasikan oleh pihak pembeli di Indonesia.

2) Wintego Systems Ltd

Wintego Systems Ltd merupakan perusahaan yang menjual perangkat lunak mata-mata asal Israel, perusahaan tersebut memperjualbelikan produknya kepada Kepolisian Republik Indonesia

[295] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia."

melalui perusahaan retail di Singapura bernama Ataka Enterprises PTE Ltd dan ESW Systems PTE Ltd.

Produk yang ditawarkan antara lain adalah Helios, Catch App yang beroperasi di bawah merek WINT yang digunakan untuk menembus enkripsi WhatsApp dan mengumpulkan semua data seperti pesan, rekaman suara, dokumen, foto dan lainnya yang bisa dikirim atau diterima oleh sesama pengguna WhatsApp. Selain WhatsApp, pada tahun 2022, ditemukan bahwa perangkat lunak tersebut dapat mengintrusi telepon genggam android dengan menggunakan Chrome browser dan Samsung browser dari jarak jauh.

Selain itu, *Spyware one-click intrusion system* ini beroperasi dengan cara meniru portal berita atau situs web yang sah. Berdasarkan analisis jaringan yang dilakukan oleh Amnesty International pada tahun 2018 terhadap situs tribunnews.org, diketahui bahwa *Spyware* tersebut meniru portal berita resmi TribunNews.com. Situs lainnya yang pernah ditiru adalah galaxyupdate(.)network yang merupakan domain dari telepon genggam Samsung. Setelah situs tersebut diakses oleh korban, perangkat lunak mata-mata ini secara

otomatis akan menginfeksi perangkat korban.

Setelah dilakukannya analisa database perdagangan komersial, diketahui bahwa produk Wintego dijual ke Indonesia pada 9 September 2019 melalui perusahaan bernama ESW Systems yang berlokasi di Singapura langsung pada Kepolisian Republik Indonesia.

3) Intellexa Consortium

Intellexa Group merupakan sebuah perusahaan yang dibentuk pada tahun 2018 oleh anggota militer Israel bernama Tal Dilian bersama dengan rekan kerja lainnya. Produk yang ditawarkan adalah produk *tactical and zero click network injection*. Kemudian perusahaan ini berkembang menjadi sebuah konsorsium atau perkumpulan perusahaan. Pemegang saham (*shareholders*) dalam Intellexa Consortium di antaranya adalah Wispear (Siprus), Cytrox (Makedonia Utara), Cytrox Holdings Zrt (Hungaria), serta Intellexa S.A. dan Thalestris Ltd (Irlandia).[296] Mayoritas perusahaan tersebut memiliki spesialisasi dalam

[296] Amnesty International Security Lab, "Technical Deep Dive into Intellexa Alliance Surveillance Products," *Amnesty International*, 9 Oktober 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

Open Source Intelligence (OSINT) dan pembuatan avatar virtual.

Perangkat lunak mata-mata buatan Intellexa Alliance, yang dikenal dengan nama Predator merupakan salah satu teknologi *Spyware* yang sangat intrusif. Perangkat ini mampu mengakses sepenuhnya seluruh data yang tersimpan maupun yang ditransmisikan dari perangkat korban, serta dirancang agar tidak meninggalkan jejak apa pun pada perangkat tersebut, sehingga mustahil untuk membuktikan bahwa ada potensi dan/atau penyalahgunaan perangkat mata-mata tersebut secara nyata.

Setelah dilakukannya penelusuran IP Address dari situs palsu yang menyerupai situs resmi Suara Oposisi, Gelora News (website milik Partai Gelora) dan Suara Papua oleh Amnesty International beberapa waktu lalu, ternyata teknologi *Spyware* bernama Predator sudah digunakan di Indonesia sejak tahun 2021 dan digunakan setidaknya selama dua tahun sampai Desember 2023. [297]

Selain Predator, Intellexa Group juga memiliki

[297] Amnesty International, "Technical Deep Dive into Intellexa Alliance Surveillance Products."

berbagai teknologi dan komponen pendukung yang digunakan untuk merakit dan mengoperasikan ekosistem *Spyware*. Teknologi tersebut mencakup Helios, Green Arrow, Red Arrow, CyOP, AAA, SpearHead, Alpha-Max, Epsilon, PDS, Nebula, IS, Nova, Triton, Mars, Jupiter, Orion, Cerebro, Jasmine, IOTA, Eagle, GLINT, dan SMINT, yang masing-masing memiliki fungsi berbeda.[298]

Komponen-komponen ini dirancang untuk mendukung berbagai kebutuhan pengawasan, mulai dari *Spyware* yang mampu mengintrusi perangkat digital target, komponen pendukung utama Predator, alat analisis hasil intersepsi, sistem avatar atau bot untuk mengelola "avatar", yakni akun palsu di media sosial dan aplikasi pesanan, yang digunakan untuk melakukan rekayasa sosial terhadap target agar membuka tautan satu-klik (1-click link), hingga pemantauan lalu lintas internet (*Internet Traffic Monitoring*). Pendekatan ini memungkinkan Intellexa membangun sistem pengawasan yang fleksibel, dapat disesuaikan dengan kebutuhan operator/pengguna, serta diintegrasikan dalam

[298] Amnesty International, "Technical Deep Dive into Intellexa Alliance Surveillance Products."

satu ekosistem pengintaian yang kompleks dan terkoordinasi.

4) Candiru/ Saito Tech

Candiru, yang biasa dikenal dengan nama Saito Tech merupakan perusahaan *Surveilans* yang mengembangkan dan menjual produk *cyber infiltration system* bernama Cyrus yang digunakan untuk menginfiltrasi perangkat seperti Windows PC, Android dan IOS. Perusahaan ini didirikan pada tahun 2014 oleh Ya'acov Weitzman dan Eran Shorer, keduanya memiliki sejarah sebagai angggota IDF Military Intelligence Unit 8200 serta pernah bekerja di perusahaan NSO Group yang dikenal luas dengan produk *Spyware*nya, Pegasus.[299]

Temuan Amnesty International dan Citizen Lab menyebutkan bahwa produk tersebut masuk ke Indonesia melalui sebuah perusahaan berbasis di Singapura, yaitu Heha PTE Ltd, untuk digunakan oleh Kepolisian Republik Indonesia. Perangkat ini

[299] Sophie in 't Veld (Rapporteur), *Draft 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))*, European Parliament Committee of Inquiry (PEGA), 8 November 2022.

diketahui telah digunakan sejak tahun 2020. Produk yang diekspor ke Indonesia dikirim dalam bentuk beberapa komponen *hardware* terpisah, yang mencakup *management server*, *visualization server*, *central storage*, *backup server*, switch, UPS, firewall, KVM beserta layar, serta server rack. Pengiriman dilakukan dalam dua tahap, yakni pada Mei 2020 dengan nilai USD 79.303, dan pada Juli 2020 dengan nilai USD 75.815.[300] Di tahun berikutnya yaitu 2021, ditemukan bahwa ada pengadaan terpisah pada tanggal 27 Januari 2021 yang berkaitan dengan komponen *software* dan lisensi senilai 33.089.849 USD.

Sama halnya dengan alat Wintego Systems Ltd, cara kerja produk dari Candiru/ Saito Tech adalah dengan meniru website resmi dari TribunNews, Tirto, MediaIndonesia, ANTARA News, Indoprogess dan Partai Gelora. Tidak hanya di Indonesia, teknologi ini juga beroperasi di Saudi Arabia, Israel, UAE dan Hungaria.

5) NSO Group

NSO Group merupakan singkatan dari nama para

[300] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia."

pendirinya, yaitu Niv Carmi, Shalev Hulio, dan Omri Lavie. Perusahaan ini adalah perusahaan *Spyware* asal Israel yang mengembangkan perangkat lunak pengawasan siber yang mampu menginfiltrasi perangkat pribadi dengan sistem operasi seperti iOS dan Android. Selain beroperasi sebagai entitas utama, perusahaan ini juga memiliki beberapa anak perusahaan termasuk Circles dan Q Cyber Technologies.

Laporan forensik yang dikeluarkan oleh Amnesty International, Citizen Lab, serta beberapa organisasi lainnya, menyebutkan bahwa setidaknya terdapat 12 negara yang menggunakan atau melakukan pengadaan teknologi *Spyware* dari NSO Group. Beberapa di antaranya adalah Jerman, Inggris, Swiss, Prancis, Amerika Serikat dan juga Indonesia.[301] Terdapat temuan pengiriman dari Q Cyber Technologies kepada salah satu perusahaan di Indonesia. Pada tahun 2023, Tempo yang tergabung dalam jaringan Indonesian Leaks mengungkap bahwa

[301] Amnesty International Security Lab, "Forensic Methodology Report: How to Catch NSO Group's Pegasus," *Amnesty International*, 18 Juli 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

teknologi Pegasus diduga telah digunakan oleh Kepolisian Republik Indonesia serta Badan Intelijen Negara (BIN).

Berdasarkan data dalam Layanan Pengadaan Secara Elektronik (LPSE) Kepolisian RI, tender tersebut dimenangkan oleh perusahaan Indonesia bernama PT Radika Karya Utama. Teknologi yang dimaksud tercatat dengan nama "Peralatan Materiil Khusus DIT INTELKAM (Zero Click Intrusion System)" dan tercantum dalam dua pengadaan, yaitu pada September 2017 dan Februari 2018, dengan total nilai mencapai sekitar Rp 247,7 miliar.

Keterlibatan lima vendor utama di atas hanyalah satu bagian dari ekosistem *Surveilans* yang lebih kompleks di Indonesia. Selain para penyedia perangkat lunak intrusi tersebut, investigasi lebih lanjut mengungkap adanya jaringan entitas pendukung dan perantara yang berperan dalam menyediakan infrastruktur operasional serta teknologi pelengkap. Penelusuran afiliasi korporat yang dilakukan oleh FIND per November 2025 memperluas peta ini dengan mengidentifikasi tiga entitas tambahan yang memiliki keterkaitan erat dalam rantai pasok teknologi *Surveilans* di tanah air. Entitas-entitas ini adalah Polus

Group, Therian Lab dan Pallabotta Technologies Ltd.

Polus Group, yang juga dikenal dengan nama Polus Tech, merupakan sebuah perusahaan teknologi *Surveilans* yang berkedudukan di Swiss. Perusahaan ini didirikan oleh Niv Karmi, tokoh yang dikenal luas di industri teknologi pengawasan global, mengingat ia juga merupakan salah satu pendiri dari NSO Group, perusahaan *Spyware* kontroversial yang telah menjadi sorotan komunitas internasional.

Polus Group sendiri berfokus pada pengembangan dan distribusi teknologi *Surveilans*, khususnya teknologi yang memiliki kemampuan intersepsi dan pemantauan komunikasi melalui perangkat telepon genggam, salah satunya adalah teknologi yang dikenal sebagai IMSI Catcher.

IMSI Catcher merupakan perangkat teknologi yang dirancang untuk memantau dan mengidentifikasi perangkat ponsel melalui jaringan telekomunikasi seluler. Cara kerjanya adalah dengan meniru sinyal stasiun pemancar ponsel (*Base Transceiver Station*/BTS), sehingga perangkat ponsel di sekitarnya secara otomatis terhubung ke perangkat tersebut. Melalui mekanisme ini, IMSI Catcher mampu menangkap seluruh nomor identifikasi unik

(*International Mobile Subscriber Identity*/IMSI) dari setiap ponsel yang berada dalam jangkauannya tanpa sepengetahuan pemilik perangkat.[302]

Melalui penelusuran afiliasi korporat terhadap individu-individu yang terhubung dengan Polus Group per 18 November 2025, FIND berhasil mengidentifikasi sejumlah entitas yang berdomisili di Singapura, Siprus, dan Uni Emirat Arab. Entitas-entitas tersebut, dalam kurun waktu antara tahun 2023 hingga 2025, telah menyalurkan teknologi *Surveilans* melalui beberapa skema, yakni (1) kepada perusahaan-perusahaan di Indonesia yang sebelumnya telah menerima produk serupa secara langsung dari Polus Group, (2) kepada kontraktor-kontraktor pemerintah lain yang telah teridentifikasi di Indonesia; atau (3) secara langsung kepada badan penegak hukum negara di Indonesia.

Keterkaitan jaringan bisnis Niv Karmi tidak berhenti pada Polus Group semata. Ia juga tercatat sebagai anggota dewan (*board member*) dari Therian Labs Technologies AG, sebuah entitas terpisah namun bergerak dalam ekosistem industri yang serupa, yakni pengembangan dan distribusi produk intelijen sinyal

[302] Tim Privacy International dan ELSAM, *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi*, (Jakarta: ELSAM, 2015), hlm. 45-46.

militer (*military signal intelligence products*) untuk kepentingan keamanan publik dan pertahanan dalam negeri (*homeland security*). Therian Labs sendiri memiliki board member sekaligus pemegang saham tunggal bernama Itiel Elata, hal ini dibuktikan dengan adanya alamat surel resmi yang berdomain Polus Group yaitu itiel.elata@polustech.com dan diketahui masih aktif digunakan hingga 19 September 2025. Selain itu, ia diketahui pernah hadir dalam Indo Defence Expo and Forum di Jakarta, Indonesia pada bulan Juni 2025 dengan kapasitasnya sebagai Executive dari Polus Tech (Switzerland) Ltd.

Perusahaan ini memperoleh lisensi ekspor teknologi *Surveilans* ke Indonesia pada tahun 2022, dengan nilai mencapai CHF 4,84 juta atau setara dengan Rp75,3 miliar (berdasarkan kurs rata-rata 2022). Meskipun demikian, hingga saat ini tidak ditemukan data agregasi perdagangan internasional yang secara eksplisit mencantumkan Therian Labs sebagai pihak pengirim (*shipper*) maupun penerima (*consignee*) dalam transaksi pengiriman barang apapun.

Kompleksitas jaringan bisnis Itiel Elata semakin terlihat ketika diketahui bahwa ia juga menjabat sebagai Direktur Pallabotta Technologies Ltd sejak Juli

2021. Keberadaan perusahaan ini menambah lapisan baru dalam peta afiliasi bisnis Elata yang telah mencakup Therian Labs. Sebagai catatan, Pallabotta Technologies Ltd memiliki afiliasi yang beroperasi di Dubai, yaitu Pallabotta Technologies FZCO (selanjutnya disebut Pallabotta UAE). Kehadiran entitas ini memperluas jangkauan operasional jaringan bisnis tersebut hingga ke kawasan Timur Tengah.

Dalam agregasi data perdagangan, ditemukan bahwa Pallabotta UAE sempat melakukan pengiriman sebanyak 174 ke Indonesia dari bulai Mei 2023 hingga Juni 2025. Berikut rinciannya:

a. Pada Mei 2023, ada sebanyak 18 pengiriman yang ditujukan kepada PT. Radika Karya Utama, produk yang dikirimkan berupa komponen, lisensi, dan program berkaitan dengan target location tracking system senilai USD 11,106,110. Kemudian pada bulan Juni 2025, ada sebanyak 2 pengiriman lagi bernama “Digital Forensic Toolkit” dan “Portable Active Monitoring System” senilai USD 2.5juta.

b. Beberapa bulan setelahnya yaitu pada November 2023, ada sebanyak 28

pengiriman untuk produk yang sama dan ditujukan kepada Kejaksaan Agung senilai USD 11,723,920.

c. Selain itu, dari bulan Februari 2024 - Mei 2025 ada sebanyak 126 pengiriman yang ditujukan kepada PT Terra Lentera Asia, produk yang didistribusikan oleh perusahaan tersebut dideskripsikan dengan berbagai label, antara lain sebagai 'analitik data' (*data analytics*), 'alat investigasi analisis strategis dan identifikasi target' (*strategic analysis investigation tools and target identification*), hingga 'peralatan intelijen' (*intelligence equipment*). Senilai USD 62, 245,180.

Fakta lainnya, Terra Lentera Asia berhasil memenangkan sebuah tender tertutup yang diselenggarakan oleh Kejaksaan Agung Republik Indonesia pada 28 Desember 2023 dengan nilai kontrak mencapai USD 12 juta atau setara dengan Rp 189,6 Miliar. Tender tersebut mencakup pengadaan kapabilitas *Surveilans* yang deskripsinya hampir identik kata per kata dengan spesifikasi produk yang

kemudian dikirimkan oleh Pallabotta UAE kepada Terra Lentera Asia pada bulan Februari 2024 lalu.

Kesesuaian deskripsi yang demikian presisi antara dokumen tender dan spesifikasi pengiriman ini sulit untuk dianggap sebagai kebetulan semata, dan justru memperkuat dugaan adanya keterkaitan langsung antara jaringan distribusi Pallabotta UAE dengan kontrak pengadaan teknologi *Surveilans* yang diperoleh Terra Lentera Asia dari institusi penegak hukum negara.

Temuan tersebut semakin mengkhawatirkan apabila disandingkan dengan dengan perkembangan kebijakan yang terjadi beberapa waktu berselang. Pada 25 Juni 2025, Kejaksaan Agung Republik Indonesia secara resmi menandatangani Perjanjian Kerja Sama (PKS) dengan empat operator telekomunikasi nasional, yakni PT Telekomunikasi Indonesia Tbk, PT Telekomunikasi Selular, PT Indosat Tbk, dan PT XLSmart Telecom Sejahtera Tbk. Perjanjian tersebut secara resmi dilandasi oleh kepentingan untuk mengoptimalkan fungsi intelijen kejaksaan, khususnya dalam rangka pelacakan buronan dan penanganan Daftar Pencarian Orang (DPO).[303]

[303] ELSAM (Lembaga Studi dan Advokasi Masyarakat), "Kejaksaan Agung Teken MoU Penyadapan dengan Operator Telekomunikasi, Privasi Warga

Perusahaan Broker/ Middleman Teknologi Spyware di Indonesia

Struktur jaringan ini semakin berlapis dengan keterlibatan sejumlah perusahaan perantara lokal yang mengelola aspek administratif dan distribusi. Entitas seperti Radika Karya Utama, Terra Lentera Asia, dan Maracipta Utama muncul sebagai aktor kunci dalam rantai distribusi ini. Peran mereka sebagai perantara tidak hanya mempermudah akses bagi vendor asing, tetapi juga memperlebar celah akuntabilitas dalam pengadaan barang dan jasa teknologi intelijen di tanah air.

PT. Radika Karya Utama (RKU) merupakan salah satu perusahaan Indonesia yang berdiri pada tahun 2007, nama perusahaan ini kerap disebut dalam berbagai laporan terkait dugaan pengadaan teknologi *Surveilans* dengan tingkat intrusi yang sangat tinggi berupa *Spyware* Pegasus yang diproduksi oleh NSO Group (Israel). Nama perusahaan ini pertama kali mencuat dalam temuan Amnesty International, yang mengindikasikan adanya keterkaitan antara entitas di

---

Dikorbankan atas Nama Penegakan Hukum," Siaran Pers, 26 Juni 2025, diakses pada 28 Maret 2026, https://www.elsam.or.id/siaran-pers/kejaksaan-agung-teken-mou-penyadapan-dengan-operator-telekomunikasi--privasi-warga-dikorbankan-atas-nama-penegakan-hukum.

Indonesia dengan distribusi atau rantai pasok teknologi pengawasan kepada Kepolisian Republik Indonesia dengan nilai pengadaan yang dilaporkan mencapai Rp 247,7 Miliar pada tahun 2017-2018.

Selain produk NSO Group, berdasarkan analisis agregasi data perdagangan internasional yang kami peroleh dari FIND NGO,[304] ditemukan adanya pengiriman produk teknologi *Surveilans* dari Polus Group (Swiss) kepada RKU pada Maret 2021. Dalam dokumen pengiriman tersebut, produk yang dikirimkan disamarkan dengan label "*Pelican Cases*" dan "*Textile Rucksack*", dengan nilai total yang tercatat sebesar USD 950.

Beberapa tahun sebelumnya yaitu pada tahun 2020, Polus Group telah memperoleh izin ekspor peralatan *Surveilans* senilai CHF 2,23 juta (*Confoederatio Helvetica Franc*/Franc Swiss) atau setara dengan Rp 48 miliar. Pada tahun berikutnya, yakni 2021, adanya izin ekspor tambahan senilai CHF 1,7 juta atau setara dengan Rp36,6 miliar turut diberikan kepada perusahaan tersebut.

Lebih lanjut, pada tahun 2022, Polus Group

[304] FIND sebuah lembaga investigasi nirlaba yang berfokus pada pelacakan jaringan bisnis dan aliran dana di balik penyebaran teknologi surveilans. https://find.ngo/about

kembali memperoleh perizinan ekspor peralatan *Surveilans* dengan nominal CHF 22,86 juta atau setara dengan Rp 355,6 miliar (berdasarkan kurs rata-rata tahun 2022 sebesar Rp 15.557/CHF). Meskipun demikian, pasca periode tersebut tidak ditemukan bukti adanya pengiriman langsung dari Polus Group ke Indonesia. Pengiriman selanjutnya dilakukan melalui perantara (*middleman*), yakni perusahaan yang diidentifikasi sebagai Radika Karya Utama.

IndonesiaLeaks menemukan bahwa RKU diduga telah melakukan pengadaan berbagai teknologi pengawasan termasuk sistem intrusi zero click atas nama Kepolisian Republik Indonesia setidaknya sejak September 2017. Laporan Amnesty Tech juga mengindikasikan bahwa RKU kemungkinan berperan sebagai perantara (intermediary seller) bagi NSO Group dan anak perusahaannya yaitu Circles. Indikasi ini didasarkan pada temuan infrastruktur teknis di mana sistem pengawasan yang diduga digunakan di Indonesia terdeteksi beroperasi pada IP Address yang terdaftar atas nama "RADIKA KARTA UTAMA", yang sangat mungkin merupakan salah eja sebagian dari nama perusahaan tersebut.

Selain itu, ada tiga perusahaan lain asal Singapura bernama ESW Systems Pte Ltd, White Global

Holdings and 3L Pte Ltd yang mengirimkan peralatan *Surveilans* pada November 2020 dan Juni 2021 kepada RKU dalam waktu yang bersamaan dengan pengiriman yang dilakukan oleh Polus Group. Hingga saat ini, belum dapat diidentifikasi apakah ada keterkaitan maupun koneksi antara pengiriman yang dilakukan oleh ketiga perusahaan asal Singapura tersebut dengan Polus Group. Dalam temuan singkat FIND, pada bulan Desember 2020, adanya pengiriman beberapa barang dengan nama 'Nemesis Tactical Backpack', 'Nemesis Enigma GSM Interception System', dan 'Nemesis Vehicular Mobile Targeting Surveillance System' seharga 4 juta USD kepada RKU. Namun tidak diketahui kepada siapa nantinya barang tersebut akan dijual.

Tepat sepuluh bulan kemudian, Polus Group tercatat melakukan pengiriman produk bernama 'Nemesis B-Unit' kepada perusahaan Indonesia, Maracipta Utama. Yang menarik perhatian adalah adanya kemiripan signifikan antara produk yang dikirimkan oleh perusahaan asal Singapura, 3L Pte Ltd, dengan produk yang dikirimkan oleh Polus Group. Kemiripan tersebut menimbulkan dugaan bahwa 3L Pte Ltd kemungkinan merupakan anak perusahaan (*subsidiary*) dari Polus Group, atau setidaknya memiliki

hubungan kerja sama (*partnership*) dengan perusahaan tersebut.

Keterlibatan Politisi dalam Pengadaan Spyware di Indonesia

Temuan yang lebih mengejutkan terungkap melalui dokumen pemberitahuan perubahan data perseroan Administrasi Hukum Umum (AHU) tertanggal 29 November 2023 milik PT Radika Karya Utama, yang diperoleh ELSAM dari Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham) kementerian yang kini telah mengalami perubahan nomenklatur menjadi Kementerian Hukum pasca pemisahan urusan hak asasi manusia di bawah pemerintahan Presiden Prabowo Subianto. Dokumen tersebut secara eksplisit mencantumkan susunan pengurus dan pemegang saham perusahaan, dan yang paling mencengangkan salah satu komisaris utamanya adalah seorang politisi yang pernah menjabat sebagai anggota DPR RI periode 2014–2019.[305]

Fakta ini bukan sekadar anomali administratif. Kehadiran figur berlatar belakang politik di dalam struktur inti perusahaan yang terindikasi terlibat dalam

[305] Kementerian Hukum dan HAM RI, Profil Perusahaan PT. Radika Karya Utama, tahun 2020. Halaman.17, diakses pada 20 Oktober 2025.

distribusi teknologi *Spyware* berisiko tinggi menimbulkan pertanyaan serius yang tidak dapat diabaikan: sejauh mana terjadi persilangan antara kepentingan bisnis, jaringan kekuasaan politik, dan kewenangan negara dalam ekosistem pengawasan digital di Indonesia?

Lebih jauh, dalam berbagai konteks global, teknologi sejenis telah berulang kali didokumentasikan sebagai instrumen pelanggaran hak asasi manusia digunakan untuk memata-matai jurnalis, aktivis, pembela HAM, hingga kelompok-kelompok rentan lainnya. Apabila pola serupa terjadi di Indonesia, maka keberadaan aktor politik dalam rantai bisnis *Spyware* ini berpotensi menciptakan konflik kepentingan yang sistemik dan berbahaya bagi demokrasi.

Indonesia Sebagai "Legal Grey Area" Untuk Penjualan Spyware

Berdasarkan laporan investigasi yang diterbitkan oleh Lighthouse Reports pada Oktober 2025, Indonesia tidak hanya tercatat sebagai pengguna teknologi *Spyware* yang bersifat sangat intrusif, tetapi juga diduga berperan sebagai perantara (*middleman*) dalam ekosistem distribusi dan penggunaan

perangkat lunak pengawasan tersebut. [306]

Sampai dengan saat ini Indonesia belum memiliki kerangka hukum yang secara komprehensif dan eksplisit mengatur perdagangan, akuisisi maupun penggunaan teknologi *Spyware*. Kekosongan regulasi ini menyebabkan Indonesia dikategorisasikan sebagai negara dengan legal grey area yang secara tidak langsung membuka celah bagi masuknya teknologi *Surveilans* berisiko tinggi dari berbagai perusahaan yang memiliki *track record* pelanggaran HAM tanpa pengawasan yang memadai.

Kondisi ini diperparah oleh fragmentasi regulasi yang ada. Ketentuan mengenai penyadapan dan pengawasan komunikasi hingga saat ini masih tersebar dalam berbagai instrumen hukum yang bersifat sektoral, yakni UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), UU Tindak Pidana Terorisme, dan UU Komisi Pemberantasan Korupsi (UU KPK) yang masing-masing hanya mengatur penyadapan dalam konteks kasus-kasus tertentu dengan pengawasan yudisial (*judicial oversight*) yang sangat terbatas.

---

[306]Gabriel Geiger dkk., "Surveillance Secrets," *Lighthouse Reports*, 23 Mei 2024, diakses 1 April 2026, https://www.lighthousereports.com/investigation/surveillance-secrets/.

Yang lebih mengkhawatirkan, fragmentasi regulasi tersebut justru menciptakan ruang kompetisi kelembagaan yang tidak sehat. Sejumlah institusi negara termasuk Tentara Nasional Indonesia (TNI), Kejaksaan Agung, dan Kepolisian Republik Indonesia (Polri) tampak berlomba-lomba untuk mengakuisisi dan memperluas kewenangan penyadapan, tanpa dilandasi oleh mekanisme pengawasan yudisial yang memadai maupun justifikasi hukum yang transparan. Klaim "demi kepentingan penegakan hukum" atau "pencegahan kejahatan" yang kerap dijadikan tameng legitimasi oleh institusi-institusi tersebut perlu dikritisi secara serius.

Beberapa temuan menunjukkan bahwa teknologi *Surveilans* yang diperoleh atas nama penegakan hukum, dalam praktiknya, terdapat indikasi digunakan jauh melampaui batas-batas yang seharusnya memasuki ranah pengawasan politik, pembungkaman kebebasan sipil, dan penargetan kelompok-kelompok yang tidak memiliki keterkaitan dengan aktivitas kriminal apapun. Legitimasi terhadap penggunaan *Spyware* yang tengah berkembang justru mengancam fondasi hukum hak asasi manusia internasional, khususnya prinsip *necessity* dan *proportionality*. Dalam penanganan kejahatan berat sekalipun, penggunaan

alat ini sulit dipertanggungjawabkan secara hukum selama masih ada metode pengawasan alternatif yang lebih proporsional. Pada hakikatnya, kapasitas pengawasan yang dimiliki *Spyware* tidak dapat diselaraskan dengan hak privasi individu, asas praduga tak bersalah, maupun nilai-nilai yang menopang tatanan masyarakat demokratis.[307]

Sementara itu, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang baru disahkan belum secara spesifik menyentuh dimensi penggunaan *Spyware* oleh negara sebagai aktor. Tidak adanya undang-undang tunggal yang mengatur penyadapan secara menyeluruh menciptakan vakum hukum yang justru dimanfaatkan sebagai celah oleh berbagai pihak baik aktor negara maupun non-negara.

Dalam konteks perdagangan internasional, ketiadaan regulasi ekspor-impor teknologi *dual-use* yang ketat di Indonesia menjadikan negara ini sebagai pasar tujuan yang strategis bagi perusahaan-perusahaan penyedia *Spyware* global. Teknologi yang secara internasional diklasifikasikan sebagai dual-use yakni teknologi yang dapat digunakan baik untuk

[307] Bojan Perkov dkk., *A Privacy Nightmare: Understanding Spyware*, (Share Foundation, 2025), hlm. 57.

kepentingan sipil maupun militer semestinya tunduk pada mekanisme kontrol ekspor yang ketat sebagaimana diatur dalam kerangka *Wassenaar Arrangement*, sebuah rezim pengendalian ekspor multilateral yang mengatur transfer teknologi konvensional dan dual-use. Namun, lemahnya implementasi mekanisme serupa di sisi Indonesia sebagai negara penerima (*recipient country*) menciptakan asimetri regulasi yang berbahaya.

Lebih jauh, pola yang teridentifikasi dalam penelitian ini di mana produk *Spyware* disamarkan dalam dokumen pengiriman sebagai barang-barang komersial biasa seperti USB, CPUs, Monitor, *Pelican Cases* dan *Textile Rucksack* mengindikasikan bahwa para aktor dalam rantai distribusi teknologi pengawasan secara sadar mengeksploitasi kelemahan sistem klasifikasi bea cukai Indonesia. Ketiadaan kapasitas teknis yang memadai di tingkat bea cukai dan lembaga pengawas ekspor-impor untuk mengidentifikasi teknologi *dual-use* yang tersamar menjadikan Indonesia rentan terhadap penyelundupan teknologi *Surveilans* yang terlindungi oleh fasad legalitas administratif.

Situasi ini pada akhirnya menciptakan paradoks yang berbahaya bahwa negara hadir sebagai pembeli

utama teknologi *Spyware*, sekaligus absen sebagai regulator yang efektif. Tanpa kerangka hukum yang komprehensif, mekanisme pengawasan yang independen, dan transparansi dalam pengadaan teknologi *Surveilans*, Indonesia tidak hanya menjadi legal grey area dalam peta perdagangan *Spyware* global tetapi juga berpotensi menjadi laboratorium impunitas bagi praktik pengawasan digital yang melanggar hak asasi manusia.

J. Penutup

J.1. Kesimpulan

Penggunaan teknologi *Surveilans* yang masif telah menempatkan hak asasi manusia pada titik nadir. Instrumen yang awalnya dirancang untuk keamanan nasional kini sering diselewengkan untuk menyasar para pembela HAM. Industri *Surveilans* swasta yang minim regulasi telah menciptakan pasar bagi penyalahgunaan kekuasaan yang mengancam hak-hak fundamental warga negara. Di sisi lain, upaya untuk mengatur industri *Surveilans* di tingkat global juga menemui sejumlah tantangan besar akibat karakter industri *Spyware* yang tertutup dan kompleks.

Karakter ini juga tampak dalam pengadaan dan penggunaan *Spyware* di Indonesia. Berdasarkan penelusuran terhadap dokumen pengadaan barang dan jasa pemerintah serta dokumen korporat terkait, riset ini menemukan bahwa akuisisi perangkat *Surveilans* tidak hanya melibatkan vendor utama global, tetapi juga ditopang oleh jaringan entitas pendukung yang menyediakan infrastruktur operasional dan teknologi pelacakan geolokasi. Kehadiran jaringan penyedia spesialis ini memungkinkan aktivitas *Surveilans* berjalan efektif di bawah radar pengawasan publik.

Kompleksitas dalam melacak rantai pasok dan pembelian teknologi ini berakar pada minimnya akuntabilitas dan kultur ketertutupan dalam pengadaan alat intelijen. Pemanfaatan entitas perantara lokal dalam sistem pengadaan negara sering kali menjadi lapisan administratif yang secara efektif memisahkan identitas penyedia teknologi asli dari dokumen yang dapat diakses publik. Struktur berlapis ini, ditambah dengan berkelindannya kepentingan ekonomi-politik dalam jalur distribusi, mempertegas betapa sulitnya melakukan kontrol terhadap penguasaan alat intelijen yang beroperasi dalam ruang hampa pengawasan.

Dalam konteks regulasi, Indonesia berada dalam *"legal grey area"* atau zona abu-abu regulasi. Ketiadaan mekanisme pengawasan independen dan kontrol peradilan yang ketat terhadap pengadaan alat sadap menjadikan Indonesia pasar yang terbuka bagi penyebaran *Spyware*. Tanpa reformasi kebijakan yang progresif, kesenjangan antara masifnya kapasitas pemantauan negara dengan perlindungan hak warga akan terus melebar, mengancam supremasi hukum dan masa depan keadilan digital.

J. 2. Rekomendasi

Untuk memastikan akuntabilitas penggunaan *Spyware,* maka diperlukan penguatan kebijakan, baik melalui legislasi, regulasi, bahkan penggunaan anggaran publik, termasuk pengadaan barang dan jasa berbasis HAM. Optimalisasi *e-procurement* dan pengawasan ketat juga menjadi *conditio sine qua non* untuk memperkuat transparansi pengadaan barang dan jasa perangkat tersebut. Pemerintah harus mencegah korupsi, melindungi hak asasi manusia dari penyalahgunaan *Spyware*, dan meningkatkan kepercayaan publik terhadap proses penggunaan teknologi keamanan siber. Oleh karena itu, riset ini merekomendasikan:

1) Menyusun regulasi khusus tentang pengadaan dan penggunaan *Spyware,* termasuk klasifikasi perangkat, kriteria lembaga pengguna, serta standar perlindungan hak asasi manusia.

2) Mewajibkan mekanisme pengadaan yang transparan melalui sistem e-procurement pemerintah, dengan kategori khusus untuk teknologi pengawasan yang memerlukan izin lintas lembaga.

3) Menguatkan pengawasan independen oleh Dewan Perwakilan Rakyat (DPR), Badang Pengawasan Keuangan (BPK), Ombudsman Republik Indonesia (ORI), Komnas HAM, Komisi Kejaksaan dan Komisi Kepolisian Nasional (Kompolnas) atas setiap kontrak pengadaan *Spyware* untuk memastikan kepatuhan hukum dan HAM. Selain itu, peran Lembaga Perlindungan Saksi dan Korban (LPSK) juga dibutuhkan dalam hal terdapat korban dari penggunaan teknologi *Spyware.*

4) Mewajibkan platform teknologi seperti Apple, Meta, dan Google secara hukum

melalui pengadilan untuk membuka akses data forensik perangkat kepada korban yang terverifikasi dan lembaga investigasi independen apabila terdapat bukti permulaan yang cukup mengenai infeksi *Spyware*, guna mengatasi ketimpangan struktural dalam pembuktian yang selama ini menjadi hambatan utama bagi korban dalam memperoleh keadilan.

5) Menerapkan prinsip kebutuhan dan proporsionalitas, di mana *Spyware* hanya boleh digunakan untuk penegakan hukum yang sah, terbatas waktunya, serta mendapat persetujuan pengadilan.

6) Membangun mekanisme audit berkala atas efektivitas, biaya, dan dampak HAM dari penggunaan *Spyware*, serta kewajiban pelaporan publik dalam bentuk ringkasan non-teknis.

Daftar Pustaka

Access Now. "Exiled, Then Spied on: Civil Society in Latvia, Lithuania, and Poland Targeted With Pegasus Spyware - Access Now," Mei 30, 2024. https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

———."Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts." Desember 23, 2020. https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/.

Afrose, Samia. "Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine." Bachelor's thesis, Harvard University, 2025.

Alam, Nur. "Konstitusionalitas Penyadapan (Interception) Dengan Peraturan Pemerintah Dari Sudut Pandang Perlindungan Hak Asasi Manusia." *Jatiswara* 27, no. 3 (November 2012).

Albanese, Francesca. *From economy of occupation to economy of genocide*. Laporan Special Rapporteur on the situation of human rights in the

Palestinian territories occupied since 1967. UN Doc. A/HRC/59/23. Juli 2, 2025.

Alfarizi, M. Khory. "Fakta-Fakta Pegasus, Spyware Canggih Yang Disebut Masuk Indonesia." *Tempo*, Juni 20, 2023. https://www.tempo.co/politik/fakta-fakta-pegasus-spyware-canggih-yang-disebut-masuk-indonesia-175195.

Aliansi Jurnalis Independen. "Jelang Pemilu 2024, Perlu Regulasi Penggunaan Alat Sadap seperti Pegasus." *Aji.or.id.* Juni 23, 2023. https://www.aji.or.id/informasi/jelang-pemilu-2024-perlu-regulasi-penggunaan-alat-sadap-seperti-pegasus.

Allsop, Jon. "Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press." Columbia Journalism Review, Februari 14, 2023. https://www.cjr.org/the_media_today/pegasus_spyware_court_cases.php.

Amnesty International. "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia," 2024.

———. "When Is Targeted Surveillance Wrong?," Agustus 10, 2023.

https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/.

———. *A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia*. Index: ASA 21/7974/2024. Mei 20, 2024. https://www.amnesty.org/en/documents/asa21/7974/2024/en/.

———. *The Predator Files: Caught in the Net*. Index: ACT 10/7245/2023, Oktober 9, 2023. https://www.amnesty.org/en/documents/act10/7245/2023/en/.

———. "Thailand: Dismissal of Landmark Case a Critical and Alarming Setback in Fight Against Unlawful Use of Spyware." November 21, 2024. https://www.amnesty.org/en/latest/news/2024/11/thailand-dismissal-of-landmark-case-a-critical-and-alarming-setback-in-fight-against-unlawful-use-of-spyware/.

Amnesty International Security Lab. "Forensic Methodology Report: How to Catch NSO Group's Pegasus." *Amnesty International*. Juli 18, 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

———. “Technical Deep Dive into Intellexa Alliance Surveillance Products.” *Amnesty International*. Oktober 9, 2023. https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO). “Operating From the Shadows: Inside NSO Group’s Corporate Structure.” Amnesty International Ltd, 2021.

Amnesty International UK. “Evidence of Global Opposition to US Mass Surveillance,” Januari 16, 2026. https://www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq.

Anderson, Stuart Joseph. “Comparing Section 889’s Huawei Ban and the Cybersecurity Maturity Model Certificate: The Challenge of Pursuing Cybersecurity Through Friend-Shoring.” *Public Contract Law Journal* 54, no. 2 (2025).

Angiolillo, Fabio, Ana Good God, and Staffan I. Lindberg. “DEMOCRACY REPORT 2025: 25 Years of Autocratization – Democracy Trumped?” V-Dem Institute, Maret 2025.

Anugrahanto, Nino Citra, and Kurnia Yunita. "Satu Dekade Tren Indeks Demokrasi Indonesia Menurun." *Kompas.id*, Maret 5, 2025. https://www.kompas.id/artikel/satu-dekade-tren-indeks-demokrasi-indonesia-menurun.

Arquillière, Maxime, dkk. *Predators for Hire: A Global Overview of Commercial Surveillance Vendors*. Sekoia, 2025. https://blog.sekoia.io/predators-for-hire-a-global-overview-of-commercial-surveillance-vendors/.

Article19. "Slovakia: Use of Pegasus a Threat to Democracy and Human Rights," September 9, 2024. https://www.article19.org/resources/slovakia-use-of-pegasus-a-threat-to-democracy-and-human-rights/#:~:text=The%20European%20Union%20Agency%20for,use%20of%20Pegasus%20in%20Slovakia.

Asia Pacific Defence Reporter. "Indonesia Defense Expenditure to Reach $9.7 Billion by 2028." *Asia Pacific Defence Reporter*. Agustus 31, 2023. https://asiapacificdefencereporter.com/indonesia-defense-expenditure-to-reach-9-7-billion-by-2028/

BBC. "Pegasus: Who Are the Alleged Victims of Spyware Targeting?," Juli 22, 2021. https://www.bbc.com/news/world-57891506.

———. “Pegasus: Spyware Sold to Governments 'Targeted Activists'.” Juli 19, 2021. https://www.bbc.com/news/world-57891506.

BDS Movement. “The Dangerous Rise of Military-Grade Spyware – a Global Day of Action,” June 18, 2025. Diakses Desember 31, 2025. https://bdsmovement.net/Global-Day-Action-Against-Spyware.

Bień-Kacała, Agnieszka. “Pegasus contra democratic process: experience from Europe.” Dalam *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World*, disunting oleh Michał Balcerzak dan Julia Kapelańska-Pręgowska. Cheltenham: Edward Elgar Publishing Limited, 2024.

Bloch, Julie, Sukti Dhital, Rashmika Nedungadi, and Nikki Reisch. “CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent.” Just Security, Mei 15, 2019. https://www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/.

Bromley, Mark, dan Giovanna Maletta. *Export Controls and Spyware: Enhancing Oversight,*

Transparency and Restraint. SIPRI Report. Stockholm: SIPRI, September 2025. http://doi.org/10.55163/GVXO6716.

Cardillo, Maira, Sina Fischer, dan Aditi Kekre. *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*. Geneva Graduate Institute dan CyberPeace Institute, 2023.

Carpenter, Chris. "Symposium on Forensic and Counter-Forensic Approaches to International Law: Digital Evidence and the Gaze – a Conceptual Framework for Analyzing Digital Evidence Through a Foucauldian Lens." Opinio Juris, Maret 16, 2026. https://opiniojuris.org/2025/12/10/symposium-on-forensic-and-counter-forensic-approaches-to-international-law-digital-evidence-and-the-gaze-a-conceptual-framework-for-analyzing-digital-evidence-through-a-foucauldian-lens/.

Cecco, Leyland. "Spyware Is Huge Threat to Global Human Rights and Democracy, Expert Warns." *The Guardian*, Agustus 10, 2022. https://www.theguardian.com/world/2022/aug/09/spyware-canada-threat-democracy-human-rights.

Chan, Anna W. "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware." *The Brooklyn Journal of International Law* 44, no. 2 (2019). https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/7/.

Chin-Rothmann, Caitlin. "Cyber Mercenaries: Limiting Government Use of Commercial Spyware." Georgetown Journal of International Affairs, September 4, 2024. https://gjia.georgetown.edu/2024/09/04/cyber-mercenaries-limiting-government-use-of-commercial-spyware/.

Cowley, Ruth. "Kiobel's Impact on Disputes in International Law." *Norton Rose Fulbright*, Mei 2013. https://www.nortonrosefulbright.com/en/knowledge/publications/94bc936c/kiobels-impact-on-disputes-in-international-law.

Dragonfly Intelligence. "Risks to organisations from spyware," Juni 27, 2024. https://dragonflyintelligence.com/news/global-risks-to-organisations-from-spyware/.

Deibert, Ronald J. *Chasing Shadows: Cyber Espionage, Subversion, and the Global Fight for Democracy*. Toronto: Simon & Schuster, 2025.

Dumbrava, Costica. *Impact of the Use of Spyware on Fundamental Rights*. Brussels: European Parliamentary Research Service, 2023. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf,

Feldstein, Steven. "Spyware Exports: Recognizing the Limits of Human Rights Law." SSRN, Desember 23, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123661.

———. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, September 17, 2019. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance.

Feldstein, Steven, and Brian Kot. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace, Maret 2023.

———. “Mapping the Shadowy World of Spyware and Digital Forensics Sales.” Carnegie Endowment for International Peace, Februari 27, 2023. https://carnegieendowment.org/features/commercial-spyware?lang=en.

Fidler, Mailyn. “Sanctions for Spyware.” Lawfare, Juni 13, 2024. https://www.lawfaremedia.org/article/sanctions-for-spyware.

Ní Aoláin, Fionnuala, dan Adriana Edmeades Jones. “Spyware Out of the Shadows: The Need for a New International Regulatory Approach.” *Just Security*. 15 Mei 2023. https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/.

Fortinet. “What Is Spyware? Definition, Types and Protection | Fortinet,” n.d. https://www.fortinet.com/resources/cyberglossary/spyware.

Gamma Group. “Remote Monitoring and Infection Solutions: FinSpy.” *WikiLeaks Spyfiles*. Desember 1, 2011. https://wikileaks.org/spyfiles/docs/gamma/289_remote-monitoring-and-infection-solutions-finspy.html.

Geiger, Gabriel, dkk. “Surveillance Secrets.” *Lighthouse Reports*. Mei 23, 2024. https://www.lighthousereports.com/investigation/surveillance-secrets/.

Global Justice Clinic. “Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights,” Maret 1, 2019.

Guterl, Fred. “Special Report: When Spyware Turns Phones Into Weapons.” Committee to Protect Journalists, Oktober 13, 2022. https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/.

Hanan Elatr Khashoggi v. NSO Group Technologies Limited, dkk. No. 23-2234. Pengadilan Banding Amerika Serikat untuk Sirkuit Keempat, Mei 21, 2025. https://law.justia.com/cases/federal/appellate-courts/ca4/23-2234/23-2234-2025-05-21.html.

Hever, Alexandra. “The Price of Inequality: Why Tax Is a Human Rights Issue.” *HRRC* (blog), Juni 27, 2025. https://www.humanrightsresearch.org/post/the-price-of-inequality-why-tax-is-a-human-rights-issue.

Hidayat, Bagja. "Indonesia 2026: Makin Riuh Makin Represif." *Tempo*, Januari 4, 2026. https://www.tempo.co/prelude/sampul-tempo-edisi-khusus-indonesia-2026-2104222.

Hiebert, Kyle Volpi. "The Growing Global Spyware Industry Must Be Reined In." *CIGI*, Maret 27, 2023. https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/.

Hindin, Doron. "Can Export Controls Tame Cyber Technology?: An Israeli Approach." *Lawfare*, Februari 12, 2016. https://www.lawfaremedia.org/article/can-export-controls-tame-cyber-technology-israeli-approac

Horak, Steven. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023.

Hrle, Vladimir. "Corporate Responsibility in the Age of Surveillance and Transnational Repression: Legal Obligations and Human Rights Due Diligence." International Bar Association, Agustus 21, 2025. https://www.ibanet.org/corporate-responsibility-in-

age-of-surveillance-and-transnational-repression-legal-obligations-human-rights-due-diligence.

International Commission of Jurists. "Digital Technologies and Human Rights: a Legal Framework." International Commission of Jurists, Mei 2022.

In 't Veld, Sophie (Rapporteur). *Draft 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))*. European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA). November 8, 2022.

———. "Spyware Regulation: Will the New European Commission Step Up?." *Digital Frontlines*. Januari 31, 2025. https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/,

Kaye, David. "David Kaye: Here's What World Leaders Must Do About Spyware." Committee to Protect Journalists, Oktober 13, 2022. https://cpj.org/2022/10/david-kaye-what-world-leaders-must-do-about-spyware/.

Kaye, David, dan Sarah McKune. "The Scourge of Commercial Spyware—and How to Stop It." *Lawfare*, Agustus 25, 2023. https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it.

Kotliar, Dan M., and Elinor Carmi. "Keeping Pegasus on the Wing: Legitimizing Cyber Espionage." *Information, Communication & Society* 27, no. 8 (2024): 1499–1529. https://doi.org/10.1080/1369118X.2023.2245873

Kirchgaessner, Stephanie. "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests." *The Guardian*, Juli 18, 2021. https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, Michael Safi, and Luke Hoyland. "Revealed: Leak Uncovers Global Abuse of Cyber-surveillance Weapon." *The Guardian*, Juli 18, 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

Korzak, Elaine. “Managing Commercial Spyware Through Export Controls: Lesson Learned from the Wassenaar Experience.” Center for Long-Term Cybersecurity (CLTC) UC Berkeley, Maret 2025.

———.“Regulating Commercial Spyware Through Export Controls.” *Lawfare*, Desember 10, 2025. https://www.lawfaremedia.org/article/regulating-commercial-spyware-through-export-controls.

Lighthouse Reports. “Surveillance Secrets.” *Lighthouse Reports*. Mei 23, 2024. https://www.lighthousereports.com/investigation/surveillance-secrets/.

Loewenstein, Antony. “How Palestine Became Israel’s Spyware Test-bed.” New Internationalist, Oktober 19, 2023. https://newint.org/features/2023/10/02/spy-games.

Lourens, Cecile. “Surveillance at the Intersection of Technology, Business and Politics: A Case Study of Pegasus Spyware.” *Diggit Magazine*, Mei 20, 2022. https://www.diggitmagazine.com/articles/surveillance-intersection-technology-business-and-politics-case-study-pegasus-spyware.

Marczak, Bill, dkk. "Mapping FinFisher's Continuing Proliferation." *Citizen Lab*. Oktober 15, 2015. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#51.

Marquis-Boire, Morgan, dkk. "You Only Click Twice: FinFisher's Global Proliferation." *Citizen Lab*. Maret 13, 2013. https://citizenlab.ca/research/you-only-click-twice-finfishers-global-proliferation-2/#1.

Marczak, Bill, dan John Scott-Railton. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against A UAE Human Rights Defender." *The Citizen Lab*, Agustus 24, 2016. https://citizenlab.ca/research/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marzocchi, Ottavio, and Martina Mazzini. *Pegasus and Surveillance Spyware*. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, 2022.

Megiddo, Tamar. "Spyware Exports: Recognizing the Limits of Human Rights Law." SSRN, Desember 23, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123661.

Monahan, Torin, dan David Murakami Wood. "Introduction: Surveillance Studies as a Transdisciplinary Endeavor." Dalam *Surveillance Studies: A Reader*, diedit oleh Torin Monahan dan David Murakami Wood. Oxford: Oxford University Press, 2018.

Morris, Daniel, and Cathrine Bloch Veiberg. "Public Procurement as a Tool to Address Human Rights Risk in the Use of Digital Technology to Deliver Essential Public Services." Copenhagen K: The Danish Institute for Human Rights, February 2024.

Ní Aoláin, Fionnuala. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. UN Human Rights Special Procedures. April 2023.

———.*Global Study on the Impact of Counter-Terrorism Measures on Civil Society and Civic Space*. Laporan Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. UN Doc. A/HRC/52/39. Maret 1, 2023.

———. *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and*

preventing violent extremism. UN Doc. A/HRC/52/39. Maret 1, 2023.

Office of the United Nations High Commissioner for Human Rights (OHCHR). *Mapping report: human rights and new and emerging digital technologies*. UN Doc. A/HRC/56/45. Agustus 20, 2024.

———. *The Right to Privacy in the Digital Age*. UN Doc. A/HRC/60/45. Agustus 29, 2025.

Papaprodromou, Lazaros G. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023.

Papademetriou, George T. "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry." *Harvard Human Rights Journal* 36 (2023).

Perkov, Bojan, dkk. *A Privacy Nightmare: Understanding Spyware*. Share Foundation, 2025.

Prashad, Vijay, and Ubai Al-aboudi. "How the World Enriches from the Blood of the Palestinians." Progressive International, November 17, 2025. https://progressive.international/wire/2025-11-17-how-

the-world-enriches-from-the-blood-of-the-palestinians/en/.

Putra, Han Revanda. "Investigasi Tempo Ungkap Perusahaan Israel Diduga Pasok Spyware ke Indonesia Sejak 2017." *Tempo.co*. Juni 20, 2024. https://www.tempo.co/arsip/investigasi-tempo-ungkap-perusahaan-israel-diduga-pasok-spyware-ke-indonesia-sejak-2017-62228.

Qandeel, Mais, and Özgün Erdener Topak. "Genocidal Surveillant Assemblage in Palestine: A Socio-Legal Analysis." *Journal of Genocide Research*, October 2025. https://doi.org/10.1080/14623528.2025.2567372.

Rahayu, Kurnia Yunita dan Hidayat Salam. "Sejalan dengan Visi Prabowo, Anggaran Pertahanan Naik Jadi Rp 165 Triliun." *Kompas.id*. Agustus 16, 2024. https://www.kompas.id/artikel/sejalan-dengan-visi-prabowo-anggaran-pertahanan-naik-jadi-rp-165-triliun.

Ramadhan, Fahmi. "Teken Nota Kesepakatan dengan Provider, Kejagung Bisa Pasang Alat Sadap untuk Kumpulkan Data." *Tribunnews.com*. Juni 26, 2025. https://www.tribunnews.com/nasional/2025/06/26/tek

en-nota-kesepakatan-dengan-provider-kejagung-bisa-pasang-alat-sadap-untuk-kumpulkan-data.

Razzak, Abdul, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VI: Mexican Journalists Investigating Cartels Targeted With NSO Spyware Following Assassination of Colleague." The Citizen Lab, November 27, 2018. https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/#:~:text=Key%20Findings,to%20prevent%20the%20continuing%20abuse.

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review* 126 (1934).

Richard, Laurent, dan Sandrine Rigaud. *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy*. New York: Henry Holt and Co., 2023.

Rizaldi, Bagus Ahmad. "Anggota DPR Sebut BIN Perlu Investasi Teknologi Intelijen Terkini." *Antaranews.com*. Mei 21, 2025. https://www.antaranews.com/berita/4820745/anggota-dpr-sebut-bin-perlu-investasi-teknologi-intelijen-terkini.

Roberts, Jen, Trey Herr, Nitansha Bansal, Nancy Messieh, Emma Taylor, Jean Le Roux, Sopo Gelava, and Atlantic Council. "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights." Atlantic Council, September 4, 2024. https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

Rueckert, Phineas. "Pegasus: The New Global Weapon for Silencing Journalists." Forbidden Stories, Juli 18, 2021. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

Santos, Edmarverson A. "Human Rights and the Global Digital Surveillance Infrastructure." *Diplomacy and Law* (blog), Juli 3, 2025. https://www.diplomacyandlaw.com/post/human-rights-and-the-global-digital-surveillance-infrastructure.

Sartor, Giovanni, and Andrea Loreggia. "The Impact of Pegasus on Fundamental Rights and Democratic Processes." European Union, 2022.

Scott-Railton, John, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, and Ron Deibert. "GeckoSpy: Pegasus Spyware Used Against Thailand's Pro-Democracy Movement - the Citizen Lab." The Citizen Lab, Juli 7, 2022. https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/.

Sexton, Mike. "What Is Spyware and Why Should Policymakers Care?" Third Way, Maret 9, 2023. https://www.thirdway.org/memo/what-is-spyware-and-why-should-policymakers-care.

Silberman, Michael. "Policing Pegasus: The Promise of U.S. Litigation for Commercial Spyware Accountability." *Georgetown Law Technology Review* 8, no. 1 (2024).

Sodiq, Mohamad Djafar, dkk. "Kebijakan dan Regulasi Spionase Siber di Indonesia." *IDEAS: Jurnal Pendidikan, Sosial, dan Budaya* 10, no. 4. November, 2024. https://jurnal.ideaspublishing.co.id/index.php/ideas/article/view/1909/799.

Sooknanan, Isabella S. S. "Digital Authoritarianism and the Expansion of the Global Surveillance State."

Senior thesis, Fordham University, 2023. https://research.library.fordham.edu/cgi/viewcontent.cgi?article=1138&context=international_senior.

Šturmová, Barbora. "Pegasus Spyware Targeted Over 1,400 WhatsApp Users, Including in Hungary and Czechia, Court Documents Show." *VSquare*, 20 November 2024. https://vsquare.org/pegasus-spyware-hacking-whatsapp-meta-hungary-czech-republic/.

Tax Justice Network. "Inequalities and Democracy and Human Rights," November 13, 2020. https://taxjustice.net/topics/inequalities-and-democracy-and-human-rights/.

Tempo. "Apa Kabar RUU Penyadapan?." Juni 26, 2021. https://www.tempo.co/hukum/apa-kabar-ruu-penyadapan-823459.

The Initiative for Human Rights Principles in Fiscal Policy. *Principles for Human Rights in Fiscal Policy*.

Tim Privacy International dan ELSAM. *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi*. Jakarta: ELSAM, 2015.

UN General Assembly. *The Right to Privacy in the Digital Age*. UN Doc. A/RES/73/179. 17 Desember 2018.

UN Human Rights Council. *The Rights to Freedom of Peaceful Assembly and of Association*. Resolusi A/HRC/50/L.16. Juni 30, 2022.

———. *The Rights to Freedom of Peaceful Assembly and of Association*. Resolusi A/HRC/50/L.20. Juli 4, 2022.

———. *Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi*. A/HRC/41/CRP.1. Juni 19, 2019.

UN Interregional Crime and Justice Research Institute (UNICRI) dan UN Office of Counter-Terrorism (UNOCT). *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks*. 2024.

Uren, Tom. "Amnesty Flags Possible Spyware Abuse in Indonesia." Lawfare, Mei 17, 2024. https://www.lawfaremedia.org/article/amnesty-flags-possible-spyware-abuse-in-indonesia

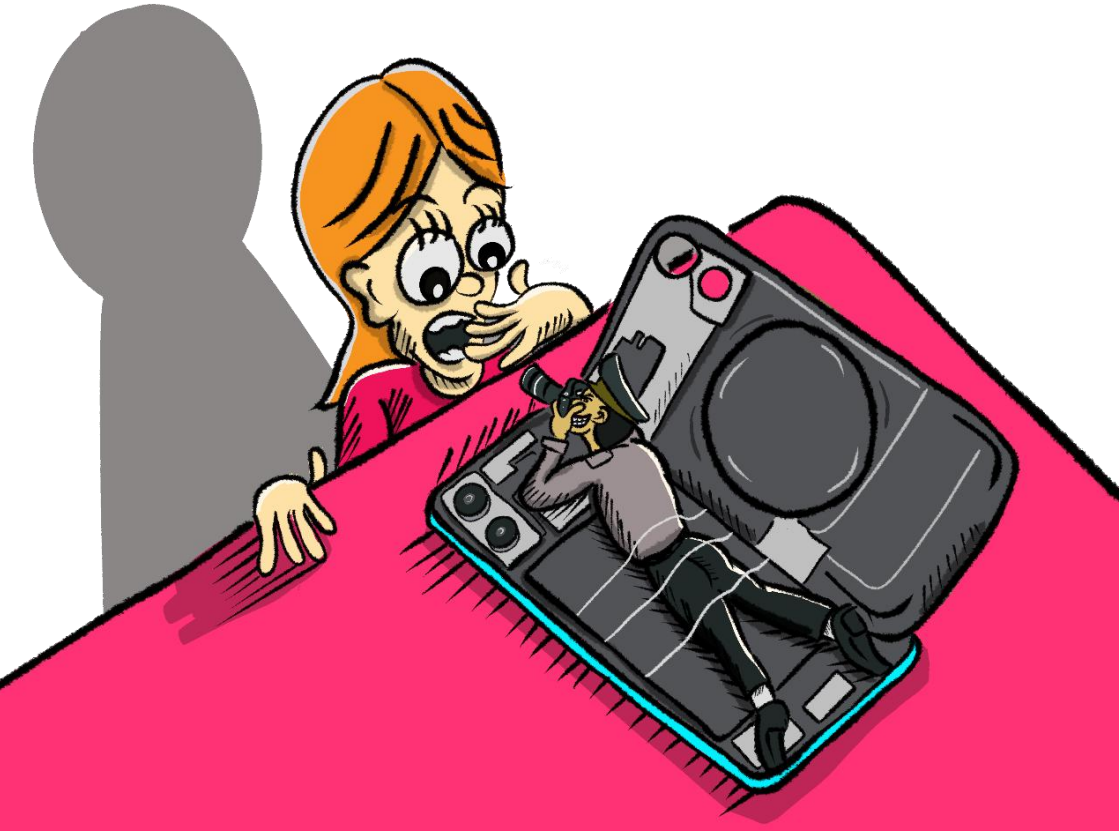
Veld, Sophie in 't. "An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?" Digital Front Lines, n.d. https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/.

Vijayan, Suchitra. "Technologies of Genocide: How Big Tech Profits From Mass Annihilation." The Polis Project, Agustus 20, 2025. https://thepolisproject.com/listen/technologies-of-genocide-how-big-tech-profits-from-mass-annihilation/.

Yepes, Rodrigo Uprimny, and Mariana Matamoros. "A Human Rights-based Approach to Tax Systems." *Dejusticia*, Oktober 2024. https://www.dejusticia.org/en/a-human-rights-based-approach-to-tax-systems/.

Zaki, M. Faiz. "Amnesty International Ungkap Polri Impor Alat Sadap, Ini Kata Pakar Kepolisian Soal SOP Penyadapan." *Tempo.co*. Juni 20, 2024. https://www.tempo.co/hukum/amnesty-international-ungkap-polri-impor-alat-sadap-ini-kata-pakar-kepolisian-soal-sop-penyadapan-61122.

Zvi, Ronnie Rosen. "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading." Georgetown Law, Januari 30, 2023. https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading/.



NEW FEATURE INSTALLED: 24/7 SURVEILLANCE

Profil

Sejarah ELSAM

Lembaga Studi dan Advokasi Masyarakat (ELSAM) dibentuk pada 14 Agustus 1993 oleh sejumlah aktivis organisasi masyarakat sipil yang mewakili berbagai unsur, isu, dan kelompok kepentingan. Mereka adalah Abdul Hakim Garuda Nusantara (Direktur YLBHI), Asmara Nababan (JKLPK), Hadimulyo (LSAF), Sandra Moniaga (Walhi), dan Agustinus Rumansara (Sekretaris INFID). Pembentukan ELSAM tak bisa dilepaskan dari situasi sosial politik saat itu, masa ketika Orde Baru sedang giat-giatnya melakukan pembangunan tanpa menghiraukan hak-hak masyarakat terdampak.

Dalam perkembangannya, ELSAM bergerak melakukan berbagai kajian, dan produksi pengetahuan, yang keseluruhannya digunakan sebagai basis advokasi, baik di jalur kebijakan, maupun pengadilan. Dalam perjalanannya, kondisi politik telah

membawa ELSAM untuk melakukan pengembangan sejumlah varian strategi kegiatan. Mulai dari advokasi garda depan, berhadapan langsung dengan negara, hingga menjalankan fungsi kemanusiaan, mendampingi para korban—khususnya korban pelanggaran HAM yang berat di masa lalu. Pada saat yang bersamaan ELSAM juga menjadi inisiator sekaligus pendorong lahirnya berbagai legislasi untuk memperkuat sistem perlindungan HAM. Hampir seluruh kebijakan yang lahir di kala transisi, ELSAM turut terlibat dalam meramunya.

Mulai dari Pengesahan Konvensi Anti-Penyiksaan, UU Hak Asasi Manusia, UU Pengadilan Hak Asasi Manusia, UU Komisi Kebenaran dan Rekonsiliasi, sampai UU Perlindungan Saksi dan Korban, sekaligus pembentukan Lembaga Perlindungan Saksi dan Korban (LPSK).

Lebih jauh, perubahan struktur politik dan kekuasaan telah memberikan warna pada model pengorganisasian dan kerja-kerja advokasi HAM yang dilakukan dari masa ke masa. Transformasi secara periodik ini memungkinkan untuk turut menjajaki sejauh mana posisi ELSAM dalam gerakan HAM berikut kontribusi kritisnya dalam mengembangkan diskursus HAM di Indonesia. Berbagai pendekatan dan strategi

advokasi yang digunakan, setidaknya telah memberikan ruang bagi lembaga untuk mengembangkan berbagai metode keterlibatan dalam mendorong perubahan kebijakan: mulai dari produksi pengetahuan, rangkaian proses advokasi kebijakan, litigasi strategis di pengadilan, multiplikasi jaringan dan kelembagaan masyarakat sipil, hingga kemitraan yang strategis dengan berbagai pemangku kepentingan, termasuk pendidikan untuk peningkatan kapasitas jaringan.

Pada perkembangan aktualnya, isu penting yang menandai perubahan cara advokasi dan studi yang dilakukan ELSAM ini misalnya terlihat dalam isu-isu teknologi dan HAM, bisnis dan HAM, serta keadilan transisional.

Advokasi kebijakan yang terkait dengan pemanfaatan teknologi digital, sebagai salah satu contoh, merupakan wajah baru ELSAM dalam rangka memastikan memperbaiki situasi kebebasan berekspresi sekaligus perlindungan hak atas privasi di Indonesia. ELSAM juga mulai menyadari pentingnya keterlibatan aktor-aktor non-negara, khususnya korporasi dalam ekosistem penegakkan HAM. Oleh karenanya, dalam perkembangannya ELSAM bahkan melibatkan sektor bisnis dalam menyusun sebuah

komitmen HAM bagi korporasi. Ini merupakan pijakan penting dalam upaya mengaplikasikan berbagai prinsip HAM dalam operasi korporasi, yang dimasa mendatang diharapkan dapat menjadi instrumen yang mengikat bagi kerja-kerja mereka—korporasi.

Secara kelembagaan, untuk pertama kalinya ELSAM berdiri sebagai sebuah Yayasan, dengan Hadimulyo sebagai ketua, Asmara Nababan menjabat sekretaris, serta Agustinus Rumansara, Abdul Hakim Garuda Nusantara, dan Sandra Moniaga sebagai anggotanya. Selanjutnya pada awal tahun 2000-an terjadi perubahan bentuk kelembagaan ELSAM dari semula Yayasan menjadi Perkumpulan terbatas, sampai dengan saat ini. Badan Pelaksana ELSAM untuk pertama kalinya dipimpin oleh Abdul Hakim Garuda Nusantara (1993-2002), kemudian Ifdhal Kasim (2002-2005), Agung Putri Astrid Kartika (2006-2010), Indriaswati D. Saptaningrum (2010-2015), Wahyu Wagiman (2016-2020), Wahyudi Djafar (2020-2025) dan Desiana Samosir (2025-sekarang)

Tentang ELSAM

Sejak berdiri pada 14 Agustus 1993, Lembaga Studi dan Advokasi Masyarakat (ELSAM) telah

mengembangkan strategi untuk menggabungkan metode kerja organisasi think tank dan gerakan hak asasi manusia (HAM), dalam operasionalnya. Karakter inilah yang membuat ELSAM unik, sebagai think tank berbasis gerakan, dengan dua fokus utama: studi menggunakan pendekatan berbasis hak, dan melakukan advokasi kebijakan. ELSAM berupaya untuk terus mendorong hadirnya kebijakan berbasis bukti untuk memperkuat penghormatan, pemenuhan, dan perlindungan HAM.

Pembentukan ELSAM dimaksudkan untuk mencapai tujuan mewujudkan tatanan masyarakat yang berpegang pada nilai-nilai hak asasi manusia, keadilan dan demokrasi. Dalam mencapai tujuan tersebut, ELSAM mengembangkan setidaknya empat kegiatan utama: (1) studi dan produksi pengetahuan HAM untuk mendukung advokasi kebijakan; (2) pengarusutamaan HAM dalam pembentukan kebijakan; (3) advokasi hukum untuk mendorong perubahan kebijakan, termasuk melalui sarana litigasi strategis; dan (4) penyelenggaraan berbagai pendidikan HAM, dengan variasi topik dan target audiensi yang beragam.

Berbagai kegiatan utama di atas terutama diaplikasikan dalam sejumlah area topik strategis

merespons kecepatan inovasi teknologi digital. Kontribusi ELSAM untuk menghadirkan kebijakan digital yang menekankan pendekatan berpusat pada manusia (human centric approach), diakui publik dengan keluarnya ELSAM sebagai pemenang Good ID Award 2020, untuk kategori keamanan. Sebuah penghargaan global untuk individu dan organisasi masyarakat sipil, yang berkontribusi penting dalam mendorong hadirnya kebijakan digital yang baik.

ELSAM juga terlibat aktif dalam penguatan kelembagaan HAM di Indonesia, seperti Komisi Nasional HAM, Lembaga Perlindungan Saksi dan Korban, serta upaya memastikan konsistensi pelaksanaan HAM melalui dukungan dalam optimalisasi kebijakan Rencana Aksi Nasional (RAN) HAM. ELSAM juga secara terus-menerus melakukan penguatan kapasitas berbagai pemangku kepentingan dalam HAM, baik negara maupun masyarakat sipil. ELSAM menyelenggarakan kursus HAM berbagai topik untuk pembela HAM, pengacara publik, pengambil kebijakan, aparat penegak hukum, juga korporasi.

Menuju 2045, ELSAM memiliki tujuan akhir perubahan: "Masyarakat Indonesia yang berdaya, inklusif, setara, dan cakap teknologi dalam tatanan

HAM dan demokrasi untuk keadilan sosial dan ekologis". Diterjemahkan dalam Rencana Strategis 2025-2030 yang terbagi ke dalam 5 (lima) Sasaran Jangka Menengah (*Intermediate Outcome*), sebagaimana berikut ini:

1. Terbangunnya fondasi bagi aliansi politik dengan para reformis dalam institusi negara.

1) Menguatnya cara pandang kritis masyarakat sipil terhadap kebijakan dalam konteks semesta digital.

2) Tersedianya infrastruktur pengetahuan untuk menumbuhkan aktivisme HAM dalam semesta digital.

3) Berkembangnya konstituensi baru yang berperspektif HAM sebagai warga dalam semesta digital.

4) Terbangunnya narasi baru yang mendukung agenda HAM dan hak-hak korban dalam semesta digital.

Alamat:
Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA
Phone: (+62 21) 797 2662 Email: office@elsam.or.id
Website: www.elsam.or.id
Media Sosial: X: @elsamnews Instagram: @elsamnews
Facebook: @elsamjkt Youtube: @perkumpulanelsam