

Policy Brief

Bayang-Bayang Panopticon Digital: Membangun Kerangka Akuntabilitas Berbasis Hak Asasi Manusia dalam Tata Kelola *Spyware* di Indonesia



Policy Brief

Bayang-Bayang *Panopticon* Digital: Membangun Kerangka Akuntabilitas Berbasis Hak Asasi Manusia dalam Tata Kelola *Spyware* di Indonesia

Penulis:

Tim ELSAM



***Policy Brief Bayang-Bayang Panopticon Digital:
Membangun Kerangka Akuntabilitas Berbasis Hak Asasi
Manusia dalam Tata Kelola Spyware di Indonesia***

Penulis:

Tim ELSAM

Editor:

Sungeb

Design & Layout:

Dodi Sanjaya

Samuel Johanes

Pertama kali dipublikasikan dalam Bahasa Indonesia oleh Lembaga Studi dan Advokasi Masyarakat (ELSAM) 2026

April 2026



Daftar Isi

Daftar Isi	i
A. Latar Belakang	1
B. Penyalahgunaan Spyware dan Dampaknya terhadap Hak Asasi Manusia	3
C. Tanggung Jawab Negara dalam Menjamin Akuntabilitas Spyware	9
D. Penggunaan Spyware dalam Perspektif Bisnis dan Hak Asasi Manusia	20
E. Mekanisme Pemulihan	23
F. Rekomendasi	27
Daftar Pustaka	29

A. Latar Belakang

Nilai industri *spyware* komersial global diperkirakan mencapai sekitar USD 12 miliar per tahun.¹ Angka tersebut mencerminkan tingginya permintaan, terutama dari pemerintah, terhadap teknologi yang berpotensi digunakan untuk melanggar hak privasi dan hak asasi manusia (HAM) ini. Berbagai penelitian mengungkapkan bahwa penggunaan *spyware* komersial oleh negara berlangsung secara tertutup dan sulit diawasi publik. Antara tahun 2011 hingga 2023, setidaknya terdapat 74 pemerintah di seluruh dunia yang menjalin kontrak dengan perusahaan *spyware* swasta untuk memperoleh akses terhadap perangkat pengawasan tersebut.²

Tingginya permintaan terhadap *spyware* komersial mendorong terbentuknya ekosistem industri yang luas dan kompleks. Penelitian Atlantic Council yang mencakup periode 1992 hingga 2023 mengungkapkan sedikitnya 49 vendor utama, 36 anak perusahaan, 24 perusahaan mitra, serta 20 pemasok teknologi dan komponen. Industri ini juga didukung oleh jejaring finansial yang mencakup 32 perusahaan induk, 95 investor, dan 179 individu.³ Penelitian tersebut juga menemukan sejumlah pola dalam industri *spyware*, termasuk perubahan identitas vendor secara berkala, perpindahan yurisdiksi untuk menghindari pembatasan hukum, dan aliran modal lintas negara. Pola-pola tersebut membuat industri *spyware* sulit diawasi.

Israel merupakan salah satu aktor utama dalam ekspor *spyware* global. Dataset yang disusun oleh Carnegie Endowment for International Peace

¹ Kyle Volpi Hiebert, "The Growing Global Spyware Industry Must Be Reined In," *Centre for International Governance Innovation*, 27 Maret 2023, <https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/>, diakses 3 Mei 2026.

² Steve 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>, diakses 3 Mei 2026.

³ 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*, 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/>, diakses 3 Mei 2026.

menunjukkan bahwa dari 74 pemerintah yang teridentifikasi membeli spyware komersial dan teknologi forensik digital, 56 di antaranya berasal dari perusahaan yang berbasis di Israel atau berafiliasi dengan entitas Israel, termasuk NSO Group, Cellebrite, Cytrox, dan Candiru.⁴

Kondisi tersebut berkaitan dengan kebijakan kontrol ekspor di negara pengekspor yang bekerja melalui sistem perizinan, di mana setiap transaksi *spyware* ke negara tujuan harus memperoleh persetujuan pemerintah. Dalam praktiknya, penilaian perizinan ekspor lebih banyak didasarkan pada keamanan nasional dan kepentingan strategis dibandingkan pada pertimbangan HAM. Mekanisme tersebut memungkinkan banyak transaksi memperoleh persetujuan, sehingga berkontribusi pada luasnya distribusi teknologi *spyware* di pasar global.

Distribusi global tersebut memperluas ketersediaan *spyware* di berbagai negara, termasuk di negara-negara dengan kerangka hukum pengawasan yang belum memadai seperti Indonesia, sehingga membuka kemungkinan penggunaannya oleh aktor negara di tingkat domestik.

Di Indonesia, *spyware* diduga telah digunakan oleh aparat penegak hukum (APH) dan badan intelijen meskipun kerangka hukumnya belum komprehensif. RUU Penyesuaian telah mulai dibahas sejak 2018 dan sempat masuk dalam Program Legislasi Nasional DPR periode 2015–2019. RUU tersebut bertujuan untuk menetapkan standar penyesuaian oleh APH dan badan intelijen serta menciptakan mekanisme penyesuaian yang lebih ketat, transparan, dan akuntabel. Namun hingga saat ini, RUU Penyesuaian belum juga disahkan.

Berdasarkan gambaran situasi tersebut, tulisan ini bertujuan untuk mengidentifikasi berbagai tantangan dalam memastikan akuntabilitas *spyware* di Indonesia. Pertama-tama tulisan ini memberikan gambaran umum terkait lanskap dugaan penyalahgunaan *spyware* di Indonesia, termasuk jenis-jenis *spyware* dan cara kerjanya, aktor yang terlibat, serta korban yang terdampak.

⁴ Feldstein dan Kot, “Why Does the Global Spyware Industry Continue to Thrive?”

Tulisan ini menganalisis secara kritis akuntabilitas negara dan perusahaan terkait penggunaan *spyware*. Analisis akan dilakukan dengan mengelaborasi tantangan hukum, transparansi, pengawasan independen, dan mekanisme pemulihan bagi korban yang terdampak. Selain itu, tulisan ini juga merekomendasikan beberapa langkah yang perlu diimplementasikan oleh berbagai aktor guna mendorong akuntabilitas *spyware*.

B. Penyalahgunaan *Spyware* dan Dampaknya terhadap HAM

Penelitian ELSAM (2026) menunjukkan bahwa berbagai jenis *spyware* diduga digunakan oleh pemerintah Indonesia. Rincian temuan ini disajikan dalam Tabel 1 berikut.

Tabel 1: Jenis-jenis *Spyware* yang Diduga digunakan di Indonesia

Spyware	Deskripsi
Pegasus	Pegasus dapat bekerja melalui tautan eksploitasi yang dirancang khusus dan dikirimkan kepada target. Ketika tautan tersebut dibuka, sistem dapat menjalankan rangkaian eksploitasi zero-day untuk menembus fitur keamanan ponsel dan menginstal Pegasus tanpa sepengetahuan atau persetujuan pengguna. Setelah ponsel terinfeksi dan Pegasus terinstal, ponsel tersebut akan terhubung ke server perintah dan kontrol (<i>command and control/C&C</i>) milik operator untuk menerima dan mengeksekusi instruksi. Melalui koneksi ini, Pegasus kemudian mengekstraksi dan mengirimkan data pribadi target ke server C&C, termasuk kata sandi, daftar kontak, kalender, pesan teks, serta panggilan suara dari aplikasi pesan seluler populer. Selain itu, operator juga dapat mengaktifkan kamera dan mikrofon ponsel untuk merekam aktivitas di sekitar ponsel.

Predator	Predator mampu mengakses seluruh data yang tersimpan maupun yang ditransmisikan dari perangkat korban. <i>Spyware</i> ini juga dirancang untuk beroperasi secara tersembunyi tanpa meninggalkan jejak yang mudah terdeteksi. Karakteristik tersebut membuat keberadaan maupun potensi penyalahgunaan <i>spyware</i> jenis ini sulit untuk dibuktikan secara langsung.
FinFisher/F inSpy	FinSpy merupakan <i>spyware</i> yang dirancang untuk mengakses dan memantau aktivitas pada perangkat yang terinfeksi. Teknologi ini dapat merekam berbagai bentuk komunikasi, termasuk panggilan dan pesan Skype, email, pesan instan, serta komunikasi Voice-over-IP (VoIP). Selain itu, FinSpy juga mampu melakukan pemantauan melalui webcam dan mikrofon, melacak lokasi perangkat, serta mengekstraksi file dari sistem target secara diam-diam. FinSpy juga dilengkapi dengan fungsi <i>keylogger</i> untuk merekam aktivitas pengetikan dan mendukung analisis jarak jauh terhadap sistem yang terinfeksi. Perangkat yang terinfeksi dapat diakses dan dikendalikan dari jarak jauh selama terhubung ke internet, dan tersedia untuk berbagai sistem operasi seperti Windows, macOS, dan Linux.
Helios/ WINT	Helios merupakan <i>catch application</i> yang beroperasi di bawah merek WINT. <i>Spyware</i> ini dirancang untuk mengakses komunikasi pada aplikasi WhatsApp. Helios dapat mengekstraksi berbagai data dari aplikasi tersebut, termasuk pesan, rekaman suara, dokumen, foto, serta berkas lain yang dikirim atau diterima oleh pengguna. Helios juga mampu menginfeksi perangkat yang menjalankan sistem operasi Android, termasuk perangkat buatan Samsung, melalui eksploitasi jarak jauh pada peramban Chrome.

	Selain itu, spyware <i>one-click intrusion system</i> ini dapat beroperasi dengan meniru portal berita atau situs web yang sah. Setelah situs tersebut diakses oleh korban, perangkat lunak mata-mata ini dapat menginfeksi perangkat korban.
Altamides	Altamides (<i>Advanced Location Tracking and Deception System</i>) merupakan sistem pengawasan yang digunakan untuk melacak lokasi perangkat melalui jaringan telekomunikasi, termasuk lintas negara, berdasarkan nomor telepon target. Selain pelacakan lokasi, Altamides juga diklaim dapat mencegah pesan teks dan panggilan telepon, serta mengakses aplikasi perpesanan seperti WhatsApp. Sistem ini juga disebut mampu memanipulasi pesan yang dikirim atau diterima oleh pengguna.
Cyrus	Cyrus merupakan <i>spyware</i> yang dikembangkan oleh perusahaan Candiru. Cyrus mampu menginfeksi komputer, jaringan, serta perangkat seluler melalui berbagai metode eksploitasi dan penyebaran <i>malware</i>. Candiru menawarkan layanan tambahan opsional yang memungkinkan perluasan sistem untuk menargetkan individu yang berada di negara lain. Candiru menawarkan kapasitas <i>Agents Exfiltration Concurrency</i> sebanyak 10, yaitu jumlah infeksi simultan yang dapat aktif dalam satu waktu. Pelanggan juga dapat membeli kapasitas tambahan untuk memperluas jumlah target yang dapat diawasi secara bersamaan.
Circles	Circles merupakan perusahaan yang menjual sistem pengawasan berbasis Signaling System 7 (SS7), yaitu protokol yang digunakan operator telekomunikasi untuk mengatur komunikasi dalam jaringan seluler. Melalui eksploitasi terhadap sistem tersebut,

	Circles memungkinkan penggunanya untuk melacak lokasi target serta mencegah panggilan suara dan pesan teks SMS. Kemampuan ini juga dapat digunakan untuk mengintersepsi kode autentikasi dua faktor yang dikirim melalui SMS.
IMSI Catcher	IMSI Catcher merupakan alat pengawasan yang digunakan untuk memantau dan mengidentifikasi ponsel melalui jaringan telekomunikasi seluler. Alat ini bekerja dengan meniru sinyal stasiun pemancar seluler (<i>Base Transceiver Station</i> atau BTS), sehingga ponsel di sekitarnya secara otomatis terhubung ke perangkat tersebut. Melalui mekanisme ini, IMSI Catcher dapat menangkap nomor identitas pelanggan seluler (<i>International Mobile Subscriber Identity</i> atau IMSI) dari ponsel yang berada dalam jangkauannya tanpa sepengetahuan pengguna.

(sumber: ELSAM, 2026)

Spyware di Indonesia dilaporkan telah digunakan untuk mengawasi masyarakat sipil dan politisi. Investigasi kolaboratif Lighthouse Reports, Tempo, dan sejumlah media lainnya pada tahun 2025 menemukan bahwa teknologi pengawasan milik FirstWap ini digunakan untuk menargetkan Ali Nur Yasin, editor senior Tempo,⁵ dan Beathor Suryadi, politikus Partai Demokrasi Indonesia Perjuangan (PDIP).⁶

Penggunaan *spyware* terhadap jurnalis dan aktor politik berdampak tidak hanya pada hak atas privasi, tetapi juga pada kebebasan pers, kebebasan

⁵ Lighthouse Reports, "Surveillance Secrets," *Lighthouse Reports*, 2025, <https://www.lighthousereports.com/investigation/surveillance-secrets/>, diakses 23 Februari 2026.

⁶ Raymundus Rikang, "Investigasi: Jejak Pelacakan Nomor Telepon Aktivis dan Tokoh Publik", *Tempo* (Oktober 2025) <https://www.tempo.co/investigasi/lacak-nomor-ponsel-aktivis-tokoh-publik-2079647> diakses pada 3 Mei 2026.

berekspresi, dan ruang perbedaan pandangan politik. Praktik semacam ini pada akhirnya dapat melemahkan proses demokrasi. Hak atas privasi, kebebasan berekspresi, dan kebebasan pers merupakan hak yang dijamin dalam UUD NRI 1945⁷ dan Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR), yang telah diratifikasi Indonesia melalui Undang-Undang Nomor 12 Tahun 2005.⁸

Dalam konteks yang lebih luas, penelitian ELSAM (2026) memetakan berbagai aktor yang terlibat dalam rantai pengadaan spyware di Indonesia. Tabel 2 berikut menjelaskan para aktor tersebut.

Tabel 2: Aktor dalam Rantai Pasok Jual-Beli Spyware di Indonesia

Spyware	Vendor	Terduga Pemasok	Terduga Pengguna
Pegasus	NSO Group (Israel)	• Q Cyber Technologies SARL (Luksemburg) • PT Radika Karya Utama (Indonesia)	• Kepolisian RI dan Badan Intelijen Negara (BIN) • Kepolisian RI
Predator	Intellexa Consortium (Siprus)	<i>Tidak diketahui</i>	<i>Tidak diketahui</i>
FinFisher/ FinSpy	Gamma International GmbH (Jerman)	• Raedarius M8 (Malaysia dan Jerman) • PT Digital Solusi Prima (Indonesia)	Badan Siber dan Sandi Negara (BSSN)

⁷ Undang-Undang Dasar Negara Republik Indonesia 1945 art 28E ayat (3), 28F, 28G ayat (1).

⁸ Undang-Undang No. 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik).

Helios/ WINT	Wintego Systems (Israel)	• Ataka Enterprises PTE Ltd (Singapura) • EWS Systems PTE Ltd (Singapura) • PT Royal Cemerlang Teknologi (Indonesia, terafiliasi dengan PT Radika Karya Utama)	Kepolisian RI
Cyrus	Candiru/Saito Tech (Israel)	Heha PTE Ltd (Singapura)	Kepolisian RI
Altamides	PT FirstWap International (Indonesia, dikelola oleh warga negara Eropa)	<i>Tidak diketahui</i>	<i>Tidak diketahui</i>
Circles	Circles (Israel, terafiliasi dengan NSO Group)	PT Radika Karya Utama (Indonesia)	Kepolisian RI
IMSI Catcher	Polus Group (Swiss), Therian Lab dan Pallabotta Technologies Ltd (UAE)	PT Radika Karya Utama (Indonesia)	Kejaksaan Agung RI

(sumber: ELSAM, 2026)

Berdasarkan tabel di atas, penyediaan spyware di Indonesia melibatkan aktor dari berbagai negara, mulai dari Israel sebagai vendor dominan, negara-negara Uni Eropa seperti Swiss, Siprus, Jerman, dan Luksemburg, hingga Uni Emirat Arab serta sejumlah negara ASEAN seperti Malaysia dan Singapura. Kondisi ini menunjukkan bahwa perdagangan spyware beroperasi melalui jaringan lintas negara yang melibatkan vendor, pemasok, dan perantara di berbagai yurisdiksi.

Analisis terhadap aktor dan yurisdiksi dalam jaringan tersebut penting untuk memahami tantangan tata kelola dan akuntabilitas dalam perdagangan *spyware* lintas batas, termasuk mekanisme pertanggungjawaban dan akses pemulihan bagi korban. Isu ini akan dibahas pada bagian selanjutnya.

C. Tanggung Jawab Negara dalam Menjamin Akuntabilitas *Spyware*

Negara memiliki kewajiban untuk melindungi warga negara dari pelanggaran HAM yang timbul akibat penyalahgunaan *spyware*. Namun, hingga saat ini Indonesia belum memiliki kerangka hukum dan kebijakan yang memadai untuk memastikan akuntabilitas penggunaan *spyware*, baik dalam aspek perdagangan, pengadaan, maupun pengawasannya. Dalam kerangka *United Nations Guiding Principles on Business and Human Rights* (UNGPs), negara didorong untuk menerapkan langkah-langkah *smart mix* melalui kombinasi regulasi dan kebijakan, serta penguatan transparansi dan pengawasan, guna mencegah pelanggaran HAM yang berkaitan dengan aktivitas perusahaan teknologi.

Bagian ini membahas sejumlah tantangan dalam kerangka regulasi dan kebijakan di Indonesia terkait akuntabilitas *spyware*, khususnya dalam aspek: (a) kontrol ekspor-impor, serta (b) transparansi dan pengawasan independen.

Tantangan Kerangka Hukum Kontrol Ekspor-Impor Spyware

Penelitian ELSAM (2026) mengidentifikasi bahwa penyediaan *spyware* yang diduga digunakan oleh Pemerintah Indonesia melibatkan berbagai aktor lintas negara. Aktor-aktor tersebut memiliki peran yang beragam, mulai dari vendor,

pemasok, dan mitra perusahaan, hingga perusahaan induk dan anak perusahaan yang terlibat dalam perdagangan *spyware*. Kondisi ini menunjukkan bahwa perdagangan *spyware* beroperasi melalui jaringan lintas yurisdiksi yang kompleks.

Saat ini, terdapat setidaknya empat kerangka hukum relevan, baik yang bersifat *soft law* maupun *hard law*, yang mengatur kontrol ekspor-impor *spyware*. Dalam berbagai instrumen tersebut, *spyware* umumnya dikategorikan sebagai teknologi dwiguna (*dual-use technology*), yaitu teknologi yang dapat digunakan untuk kepentingan sipil maupun militer atau keamanan.

Tabel 3: Kerangka Hukum Ekspor-Impor *Spyware*

Kerangka Hukum	Keterangan
Kesepakatan <i>Wassenaar</i> tentang Kontrol Ekspor untuk Senjata Konvensional dan Barang dan Teknologi Dwiguna 1996 ⁹	Kesepakatan Wassenaar dibentuk untuk mendukung keamanan serta stabilitas regional dan internasional melalui peningkatan transparansi dan tanggung jawab dalam transfer senjata konvensional serta barang dan teknologi dwiguna (<i>dual-use technology</i>), guna mencegah akumulasi senjata dan teknologi yang berpotensi mengganggu stabilitas regional dan internasional. Negara-negara peserta berupaya, melalui kebijakan nasional mereka, untuk memastikan bahwa transfer barang-barang ini tidak berkontribusi pada pengembangan atau peningkatan kemampuan militer yang merusak tujuan-tujuan ini dan tidak dialihkan untuk mendukung kemampuan tersebut. Saat ini terdapat 42 negara yang tergabung dalam

⁹ The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies 1996.

	Kesepakatan <i>Wassenaar</i> . Kesepakatan <i>Wassenaar</i> bersifat sukarela (<i>voluntary</i>).
Proses <i>Pall Mall</i> dan Kode Praktik Negara dalam Menangani Proliferasi dan Penggunaan Kemampuan Intrusi Siber Komersial yang Tidak Bertanggung Jawab 2025 ¹⁰	Diinisiasi oleh Prancis dan Britania Raya, Proses <i>Pall Mall</i> merupakan inisiatif internasional multi-pemangku kepentingan yang bertujuan untuk mendorong komitmen politik dalam menanggulangi penyebaran dan penggunaan teknologi surveilans komersial yang tidak bertanggung jawab. Saat ini, terdapat setidaknya 25 negara yang tergabung dalam Proses <i>Pall Mall</i>, termasuk Britania Raya, Amerika Serikat, Jepang, Korea Selatan, Ghana, dan sejumlah negara Eropa lainnya. Proses <i>Pall Mall</i> bersifat sukarela (<i>voluntary</i>) sehingga tidak mengikat secara hukum.
Regulasi Uni Eropa 2021/821 ¹¹	Regulasi EU 2021/821 merupakan kerangka hukum yang mengikat (<i>legally binding</i>) yang berlaku bagi negara-negara Uni Eropa terkait kontrol ekspor, broker, asistensi teknis, transit, dan transfer barang-barang dwiguna (<i>dual-use items</i>).
Peraturan Menteri Perdagangan tentang Ekspor dan Impor	Terdapat setidaknya dua peraturan utama yang mengatur kontrol ekspor dan impor di Indonesia, yaitu Peraturan Menteri Perdagangan Nomor 23 Tahun 2023 tentang Kebijakan dan Pengaturan Ekspor sebagaimana telah diubah terakhir melalui Permendag Nomor 9 Tahun 2025

¹⁰ GOV.UK, "The *Pall Mall* Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities," GOV.UK, <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>, diakses 3 Mei 2026.

¹¹ Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast).

	(Permendag Ekspor), serta Peraturan Menteri Perdagangan Nomor 16 Tahun 2025 tentang Kebijakan dan Pengaturan Impor sebagaimana telah diubah terakhir melalui Permendag Nomor 37 Tahun 2025 (Permendag Impor).
--	---

(sumber: ELSAM, 2026)

Masing-masing dari keempat kerangka hukum tersebut memiliki sejumlah kelemahan dan tantangan, baik pada tingkat desain pengaturan maupun dalam implementasinya. Wassenaar Arrangement dan Proses Pall Mall bersifat tidak mengikat (*voluntary*), sehingga tidak menimbulkan kewajiban hukum yang dapat dipaksakan. Kondisi ini menyebabkan implementasi sangat bergantung pada komitmen politik negara-negara peserta, yang pada akhirnya menghasilkan variasi tingkat kepatuhan dan standar pengendalian antarnegara.

Sementara itu, implementasi Regulasi Uni Eropa 2021/821 menghadapi sejumlah tantangan. Penelitian Centre for Democracy and Technology (2025) mengidentifikasi setidaknya lima tantangan utama implementasi regulasi tersebut, meliputi:¹² (1) keterbatasan transparansi, yang ditandai dengan minimnya pengawasan publik terhadap sebagian besar keputusan perizinan ekspor. Laporan nasional yang tersedia juga bersifat sangat teragregasi dan tidak memberikan rincian yang memadai; (2) kewajiban uji tuntas (*due diligence*) yang masih lemah, karena eksportir menghadapi ketidakpastian dalam menilai risiko HAM, sementara standar yang jelas mengenai penilaian risiko yang memadai belum sepenuhnya tersedia; dan (3) tidak adanya mekanisme pemantauan penggunaan akhir yang sistematis. Setelah lisensi diberikan, umumnya tidak terdapat kewajiban yang mengikat untuk melacak penggunaan aktual *spyware* di negara tujuan, sehingga setelah produk

¹² Silvia Lorenzo Perez dkk., *How the EU's Dual-Use Regime Falls Short on Tackling Spyware* (Centre for Democracy & Technology Europe, 2025).

meninggalkan wilayah Uni Eropa, visibilitas terhadap penggunaannya menjadi sangat terbatas, baik bagi eksportir maupun otoritas pengawas.

Selain itu, (4) terdapat prosedur nasional yang tidak seragam, karena administrasi kontrol ekspor di negara-negara anggota bervariasi baik dari segi prosedur maupun kapasitas. Perbedaan ini dapat menciptakan ketidakpastian bagi industri serta membuka risiko pemilihan yurisdiksi yang dianggap memiliki standar pengawasan yang lebih longgar; dan (5) terdapat asimetri dalam pasar internal Uni Eropa, karena masih lemahnya kontrol terhadap transfer *spyware* intra-Uni Eropa. Kondisi ini menciptakan celah yang dapat dimanfaatkan oleh perusahaan untuk menghindari aturan kontrol ekspor ke luar Uni Eropa.

Selain tantangan tersebut, EU Regulation 2021/821 juga menghadapi keterbatasan dalam menjangkau praktik penghindaran regulasi melalui pendirian perusahaan di yurisdiksi di luar Uni Eropa. Skema ini memungkinkan pelaku usaha yang terkait dengan warga negara Uni Eropa untuk memindahkan aktivitasnya ke negara ketiga—misalnya Indonesia—guna menghindari kewajiban kontrol ekspor-impor yang berlaku di Uni Eropa.

Dalam konteks rezim nasional, pengaturan ekspor dan impor di Indonesia menunjukkan pendekatan yang cenderung menyederhanakan perizinan. Permendag Ekspor dan Permendag Impor merupakan peraturan turunan dari Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja yang ditujukan untuk mendorong percepatan pertumbuhan ekonomi melalui penyederhanaan perizinan berusaha.¹³ Salah satu implikasinya adalah penggunaan Nomor Induk Berusaha (NIB) sebagai izin dasar bagi perusahaan untuk melakukan kegiatan ekspor dan impor. Dalam praktiknya, skema tersebut menjadikan NIB sekaligus sebagai izin untuk kegiatan ekspor dan impor tanpa adanya diferensiasi khusus berdasarkan tingkat risiko barang atau teknologi yang diperdagangkan.

¹³ Ady Thea DA, "Sederhanakan Proses Ekspor-Impor, Pemerintah Pangkas Ratusan Regulasi," *Hukumonline*, 23 Juni 2022, <https://www.hukumonline.com/berita/a/sederhanakan-proses-ekspor-impor--pemerintah-pangkas-ratusan-regulasi-lt62b44803ca9f5/>, diakses 3 Mei 2026.

Dalam konteks kontrol ekspor-impor teknologi berisiko tinggi seperti *spyware* dan teknologi surveilans, pengaturan tersebut dinilai belum memadai. Oleh karena itu, diperlukan penguatan pengaturan melalui persyaratan tambahan bagi perusahaan yang terlibat dalam ekspor-impor *spyware*, berupa: (1) perizinan khusus dengan proses penilaian dampak HAM, (2) kewajiban transparansi bagi perusahaan pemegang izin ekspor-impor, dan (3) mekanisme pelaporan publik atas dugaan pelanggaran atau penyalahgunaan izin ekspor-impor.

Lebih lanjut, penelitian ELSAM (2026) menggarisbawahi keterlibatan negara-negara anggota ASEAN seperti Singapura dan Malaysia dalam pengadaan *spyware* ke Indonesia. Hingga saat ini, ASEAN belum memiliki kerangka hukum regional yang secara khusus mengatur kontrol ekspor-impor teknologi *spyware*. Dengan kecenderungan pendekatan ASEAN yang mengutamakan *soft law*, peluang pembentukan kerangka hukum yang mengikat di tingkat regional diperkirakan masih terbatas.

Ketiadaan kerangka regional tersebut memperkuat fragmentasi pengaturan yang ada, sehingga diperlukan pendekatan pada tingkat global untuk mengisi kekosongan norma. Dalam konteks ini, Perserikatan Bangsa-Bangsa (PBB) dapat dipandang sebagai aktor kunci dalam mendorong pembentukan kerangka hukum global terkait kontrol ekspor-impor teknologi *spyware*.

Secara historis, sejumlah rezim internasional dapat dijadikan rujukan normatif, termasuk Konvensi Basel tentang Pengendalian Pergerakan Lintas Batas Limbah Berbahaya dan Pembuangannya yang diadopsi pada tahun 1989 di bawah kerangka Perserikatan Bangsa-Bangsa (UNEP) dan telah diratifikasi oleh lebih dari 190 negara.¹⁴

Meskipun objek pengaturannya berbeda, mekanisme dalam Konvensi Basel terkait pengendalian pergerakan lintas batas dapat menjadi referensi dalam

¹⁴ The Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and their Disposal 1989.

perancangan kerangka pengaturan ekspor-impor *spyware*. Selain itu, pengalaman implementasi Konvensi Basel selama hampir empat dekade juga memberikan pelajaran penting terkait desain kelembagaan serta mekanisme kepatuhan dalam rezim pengaturan teknologi sensitif lintas negara.

Pentingnya Transparansi dan Pengawasan Independen (Independent Oversight)

Instrumen pengawasan terhadap *spyware* harus dilakukan sejak tahapan awal, yakni proses pengadaan barang dan jasa yang dilakukan pemerintah. Penelitian ELSAM (2026) menemukan bahwa isu transparansi anggaran pengadaan teknologi *spyware* sering kali menjadi sorotan publik dan organisasi masyarakat sipil. Penelusuran yang dilakukan Sekretariat Nasional Forum Indonesia untuk Transparansi Anggaran (Seknas FITRA) menemukan bahwa lima lembaga negara (TNI, Kepolisian RI, BIN, dan Kejaksaan RI) memiliki anggaran setidaknya 36,1 triliun APBN sepanjang 2018–2024 untuk pengadaan teknologi surveilans massal (*mass surveillance*). Kekhawatiran muncul terutama ketika anggaran besar dialokasikan untuk sistem yang bersifat sensitif seperti *spyware* dan pengawasan massal tanpa penjelasan rinci kepada publik tentang tujuan, mekanisme pengawasan, dan jaminan perlindungan HAM.

Oleh karena itu, tulisan ini merekomendasikan pengintegrasian kewajiban transparansi yang menyeluruh dengan penjelasan rinci dalam proses pengadaan barang dan jasa, yang saat ini diatur berdasarkan Peraturan Presiden No. 16 Tahun 2018 mengenai Pengadaan Barang/Jasa Pemerintah, yang telah diubah sebanyak dua kali pada 2021 dan 2025. Penguatan kewajiban transparansi ini salah satunya dapat dilakukan melalui publikasi Rencana Umum Pengadaan (RUP) oleh kementerian/lembaga. Keterbukaan informasi RUP menjadi salah satu instrumen pengawasan publik yang krusial.¹⁵

Lebih lanjut, setelah pengawasan dalam tahapan pengadaan barang dan jasa, diperlukan mekanisme pengawasan independen pada tahapan

¹⁵ Agus Sunaryanto, “Transparansi Pengadaan Pemerintah,” *Antikorupsi.org*, 15 Maret 2018, <https://antikorupsi.org/id/article/transparansi-pengadaan-pemerintah>, diakses 3 Mei 2026.

penggunaan teknologi *spyware* oleh pemerintah. Karena itu, dibutuhkan lembaga pengawas independen sebagai institusi yang dibentuk oleh negara dengan mandat hukum untuk melakukan pengawasan terhadap fungsi-fungsi tertentu dalam sektor publik, termasuk pemerintahan dan sektor keamanan.¹⁶ Penting untuk menggarisbawahi bahwa penggunaan *spyware* umumnya dilakukan oleh aparat penegak hukum (APH) dan lembaga intelijen di Indonesia, yang sering kali beroperasi dalam sistem yang tidak transparan atas dalih “keamanan nasional”. Kondisi ini menimbulkan kebutuhan yang kuat akan mekanisme *check and balance* yang efektif untuk memastikan bahwa kewenangan tersebut tidak disalahgunakan.

Pembelajaran dari berbagai negara menunjukkan bahwa sejumlah mekanisme pengawasan independen telah dikembangkan untuk memastikan akuntabilitas penggunaan *spyware*. Tabel berikut membandingkan mekanisme pengawasan di beberapa negara.

Tabel 4: Perbandingan Mekanisme Pengawasan di Berbagai Negara

Negara	Mekanisme Pengawasan	Catatan
Britania Raya (UK)	Pengawasan terhadap surveilans di UK dilakukan oleh Kantor Komisioner Kekuasaan Investigasi (<i>Investigatory Powers Commissioner's Office</i> /IPCO), yang memiliki tanggung jawab untuk meninjau penggunaan kewenangan investigasi oleh otoritas publik, seperti	IPCO bukan lembaga pengawas independen karena berada di bawah pengawasan Departemen Dalam Negeri (<i>Home Office</i>) UK. IPT, di sisi lain, merupakan lembaga yudisial yang didirikan secara independen.

¹⁶ DCAF, *Tip-Sheets for Reporting on Security Management and Oversight: Media and Security Sector Reform Toolkit* (2021), https://www.dcaf.ch/sites/default/files/imce/SSAD/Media%20Toolkit/MediaSSR_Toolkit_Tipsheet%2016.pdf, diakses 3 Mei 2026.

	badan intelijen dan penegak hukum.¹⁷ IPCO didirikan berdasarkan <i>Investigatory Powers Act 2016</i>. Selain itu, UK juga memiliki Investigatory Powers Tribunal (IPT),¹⁸ sebuah lembaga yudisial independen yang didirikan berdasarkan <i>Regulation of Investigatory Powers Act 2000</i> (RIPA) untuk menangani aduan terkait surveilans yang dilakukan secara melanggar hukum oleh badan publik, termasuk badan intelijen (MI5, MI6, GCHQ) dan polisi.	Namun, IPT dapat melakukan sidang secara rahasia, sehingga membatasi kemampuan publik untuk mengajukan keberatan hukum.¹⁹
Amerika Serikat (AS)	Pengawasan terhadap surveilans di AS terutama diatur oleh Undang-Undang Pengawasan Intelijen Asing (<i>Foreign Intelligence Surveillance Act 1978/FISA</i>) dan dipantau oleh Pengadilan Pengawasan Intelijen Asing (<i>Foreign Intelligence Surveillance Court/FISC</i>). Peran FISC adalah untuk memberikan pengawasan yudisial terhadap kegiatan lembaga intelijen AS dalam lingkungan yang	Sebagian besar perintah dan pengajuan FISC bersifat sangat rahasia, tetapi setelah <i>USA FREEDOM Act 2015</i>, setiap interpretasi hukum penting oleh pengadilan harus dipublikasikan. Pada 2025, Trump melemahkan PCLOB dengan memecat 3 anggota Dewan Demokratnya. Hal ini

¹⁷ GOV.UK, "Investigatory Powers Commissioner's Office," GOV.UK, 1 Juli 2025, <https://www.gov.uk/government/organisations/investigatory-powers-commissioners-office>, diakses 3 Mei 2026.

¹⁸ The Investigatory Powers Tribunal, "Home," *The Investigatory Powers Tribunal*, <https://investigatorypowertribunal.org.uk/>, diakses 3 Mei 2026.

¹⁹ Privacy International, "Our Challenge against UK's Secret TCN Powers," *Privacy International*, 13 Maret 2025, <http://privacyinternational.org/long-read/5547/our-challenge-against-uks-secret-tcn-powers>, diakses 3 Mei 2026.

	terklasifikasi. Selain FISC, AS juga memiliki <i>Privacy and Civil Liberties Oversight Board</i> (PCLOB),²⁰ sebuah lembaga independen yang berada di bawah Cabang Eksekutif dan bertanggung jawab untuk memastikan bahwa kegiatan kontra-terorisme pemerintah dilakukan sesuai dengan kebutuhan untuk melindungi privasi dan kebebasan sipil. PCLOB didirikan berdasarkan <i>Implementing Recommendations of the 9/11 Commission Act of 2007</i>. Selain itu, PCLOB merupakan bagian inti dari dasar hukum Kerangka Kerja Privasi Data EU-AS, mekanisme hukum yang menjadi dasar transfer data antara AS dan EU.	merupakan kemunduran bagi transparansi pemerintah AS dan mengancam privasi serta keamanan nasional tidak hanya warga negara AS, tetapi juga warga negara dan pemerintah asing.
Uni Eropa (EU)	Kerangka hukum penggunaan <i>spyware</i> di EU diatur oleh hukum masing-masing negara anggota, umumnya dapat ditemukan dalam ketentuan hukum pidana (<i>criminal code</i>) negara anggota. Pasca terungkapnya penyalahgunaan <i>spyware</i> di	Komite PEGA juga menegaskan bahwa mekanisme pengawasan independen terhadap penggunaan <i>spyware</i> di EU sangat lemah atau tidak efisien di beberapa negara anggota.

²⁰ Privacy and Civil Liberties Oversight Board, "US Privacy and Civil Liberties Oversight Board (PCLOB)," *Privacy and Civil Liberties Oversight Board*, <https://www.pclob.gov/>, diakses 3 Mei 2026.

	beberapa negara EU, Parlemen Eropa membentuk Komite PEGA (<i>The European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware</i>) pada Maret 2022 untuk melakukan penyelidikan lebih lanjut. Pada Mei 2023, Komite PEGA mempublikasikan hasil investigasi yang menyoroti penggunaan <i>spyware</i> terhadap jurnalis, pembela HAM dan politisi di negara-negara seperti Yunani, Polandia, Hungaria, dan Spanyol, sering kali tanpa pengawasan yang memadai atau upaya hukum bagi para korban.²¹ Komite PEGA mencatat bahwa masing-masing negara anggota memiliki mekanisme pengawasan <i>ex ante</i> (Kewajiban persetujuan berdasarkan Perintah Pengadilan, Putusan Dewan Independen Khusus) dan <i>ex post</i> (melalui Otoritas Pelindungan Data Pribadi, Komite Khusus Parlemen, Ombudsman).	
--	---	--

(sumber: ELSAM, 2026)

²¹ Quentin Liger dan Mirja Gutheil, “The Use of Pegasus and Equivalent Surveillance Spyware” (Parlemen Eropa, 2023), [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU\(2022\)740151_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf), diakses 3 Mei 2026.

Di Indonesia, pengaturan penggunaan *spyware* oleh aparat penegak hukum (APH) pada dasarnya berada dalam kerangka hukum penyadapan yang saat ini diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHP).²² KUHP mengatur bahwa penyadapan merupakan bagian dari upaya paksa (Pasal 89) yang dapat dilakukan oleh penyidik untuk kepentingan penyidikan (Pasal 136). Selain itu, dalam hal dilakukannya penyadapan, penyidik diwajibkan membuat berita acara penyadapan (Pasal 156).

Namun demikian, KUHP belum mengatur mekanisme pengawasan sebelum penyadapan dilakukan, baik melalui persetujuan pengadilan maupun bentuk pengawasan independen lainnya. Pengaturan tersebut juga terbatas pada penyadapan untuk kepentingan penegakan hukum oleh APH, sehingga penggunaan *spyware* oleh badan intelijen negara berada di luar cakupan ketentuan tersebut.

KUHP sebenarnya memandatkan pengaturan lebih lanjut mengenai penyadapan melalui Undang-Undang tentang Penyadapan (Pasal 136). Akan tetapi, hingga tulisan ini disusun, Rancangan Undang-Undang (RUU) Penyadapan belum juga disahkan. Kekosongan hukum ini membuka ruang yang luas bagi penyalahgunaan kewenangan penyadapan tanpa mekanisme pengawasan yang memadai. Oleh karena itu, pemerintah perlu segera menetapkan RUU Penyadapan sebagai prioritas dalam Program Legislasi Nasional (Prolegnas) dan memulai pembahasannya.

D. Penggunaan *Spyware* dalam Perspektif Bisnis dan HAM

Prinsip-Prinsip Panduan PBB tentang Bisnis dan HAM (*United Nations Guiding Principles on Business and Human Rights/UNGPs*)²³ menawarkan

²² KUHP mendefinisikan penyadapan sebagai kegiatan untuk memperoleh informasi pribadi yang dilakukan secara rahasia dalam penegakan hukum dengan cara mendengarkan, merekam, membelokkan, menghambat, mengubah, menyambungkan, memasang alat pada jaringan, memasang alat perekam secara tersembunyi, dan /atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik, dengan menggunakan jaringan kabel komunikasi, jaringan nirkabel, atau melalui jaringan sistem informasi elektronik internet, sesuai dengan perkembangan ilmu pengetahuan dan teknologi.

²³ United Nations Development Programme (UNDP) Indonesia, *Prinsip-Prinsip Panduan PBB tentang Bisnis dan Hak Asasi Manusia (UNGP) Bahasa Indonesia*,

kerangka kerja yang kuat untuk mencegah pelanggaran HAM dalam aktivitas bisnis serta memulihkan dampak yang ditimbulkan dari pelanggaran tersebut.

UNGPs berfokus pada HAM yang diakui secara internasional dan mendorong perusahaan beserta pemangku kepentingannya untuk memperhatikan risiko pelanggaran HAM yang paling serius akibat aktivitas bisnis mereka. Pemerintah Indonesia telah mengintegrasikan pendekatan UNGPs ke dalam kerangka hukum nasional melalui pengesahan Peraturan Presiden Nomor 63 Tahun 2023 tentang Strategi Nasional Bisnis dan Hak Asasi Manusia (Perpres BHAM).²⁴ Perpres tersebut menjadi pedoman bagi pemerintah dalam perencanaan, pelaksanaan, dan pemantauan kebijakan bisnis dan HAM, sekaligus mendorong perusahaan dan aktor non-negara lainnya untuk menghormati HAM dalam aktivitas bisnis mereka.

UNGPs memberikan pedoman bagi perusahaan untuk mengidentifikasi risiko pelanggaran HAM serta mengambil langkah-langkah untuk mencegah dan menangannya. Prinsip-prinsip tersebut berlaku bagi seluruh perusahaan, tanpa memandang sektor industri, ukuran, struktur, maupun konteks operasionalnya. Dalam konteks penggunaan teknologi *spyware*, prinsip-prinsip tersebut menjadi relevan bagi perusahaan yang mengembangkan, menjual, maupun menyediakan layanan teknologi surveilans tersebut. Pada dasarnya, perusahaan *spyware* perlu “mengetahui dan menunjukkan” bahwa mereka menghormati HAM dalam seluruh kegiatan dan hubungan bisnisnya.²⁵ Untuk itu, perusahaan *spyware* memiliki tanggung jawab untuk: (a) menerapkan

<https://www.undp.org/indonesia/publications/prinsip-prinsip-panduan-pbb-tentang-bisnis-dan-hak-asasi-manusia-ungp-bahasa-indonesia>, diakses 3 Mei 2026.

²⁴ Peraturan Presiden (Perpres) Nomor 60 Tahun 2023 tentang Strategi Nasional Bisnis dan Hak Asasi Manusia 2023.

²⁵ Office of the United Nations High Commissioner for Human Rights, *The UN Guiding Principles in the Age of Technology: A B-Tech Foundational Paper* (Geneva: OHCHR, 2020), <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>; Office of the United Nations High Commissioner for Human Rights, *Identifying and Assessing Human Rights Risks Related to End-Use: A B-Tech Foundational Paper* (Geneva: OHCHR, 2020), <https://www.ohchr.org/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>, diakses 3 Mei 2026.

komitmen kebijakan yang relevan; (b) melakukan uji tuntas HAM; dan (c) terlibat dalam upaya pemulihan atas kerugian yang dialami korban.

Penerapan uji tuntas HAM telah menjadi bagian penting dalam berbagai kerangka hukum dan kebijakan terkait teknologi *spyware*, salah satunya Regulasi Uni Eropa 2021/821. Dalam kerangka UNGPs, uji tuntas HAM mencakup beberapa tahapan utama, yaitu: (1) mengidentifikasi dan menilai risiko HAM untuk memahami sifat serta tingkat keparahan potensi pelanggaran yang dapat ditimbulkan oleh aktivitas bisnis; (2) mengambil langkah untuk mencegah dan mengurangi risiko tersebut, termasuk melalui integrasi ke dalam fungsi dan proses internal perusahaan; (3) melacak efektivitas langkah mitigasi yang telah dilakukan; dan (4) mengomunikasikan langkah penanganan HAM kepada pemangku kepentingan yang relevan.

Dalam hal mengidentifikasi dan menilai risiko HAM (langkah pertama dari uji tuntas HAM), UNGPs mendorong perusahaan untuk:²⁶

- Melihat Kemungkinan Dampak Secara Menyeluruh: Ini berarti perusahaan perlu mengidentifikasi risiko terhadap seluruh HAM yang berkaitan dengan seluruh rangkaian kegiatan dan hubungan bisnisnya. Hal ini mencakup penilaian atas apakah dan bagaimana desain, pengembangan, promosi, penjualan atau perizinan, kontrak, serta penggunaan produk dan layanan perusahaan dapat menimbulkan dampak buruk terhadap HAM.
- Fokus pada Kerugian yang Paling Serius: Ini berarti bahwa prioritas penanganan harus ditentukan berdasarkan aktivitas bisnis yang memiliki, atau berpotensi menimbulkan, dampak paling serius, luas, atau berkepanjangan terhadap individu dan kelompok terdampak. Dalam kerangka UNGPs, tingkat keparahan dampak dinilai berdasarkan skala (*scale*), cakupan (*scope*), serta kemungkinan untuk dipulihkan (*remediability*).

²⁶ OHCHR, *Identifying and Assessing Human Rights Risks Related to End-Use*.

- Komunikasi yang Bermakna dengan Pemangku Kepentingan: Ini berarti bahwa perusahaan perlu melibatkan pemangku kepentingan eksternal yang relevan untuk menyampaikan sekaligus menjelaskan proses penilaian dan prioritas risiko HAM yang dilakukan perusahaan.

Dalam konteks pengaturan perusahaan *spyware* di Indonesia, langkah-langkah uji tuntas HAM tersebut penting untuk diintegrasikan ke dalam kerangka hukum nasional. Integrasi tersebut dapat dilakukan melalui penerapan kewajiban uji tuntas HAM dalam pengaturan ekspor-impor serta pengadaan barang dan jasa di sektor keamanan dan pertahanan. Adapun aspek pemulihan bagi korban pelanggaran HAM akan dielaborasi pada bagian berikutnya.

E. Mekanisme Pemulihan

Salah satu permasalahan utama dalam kasus penyalahgunaan *spyware* adalah ketiadaan mekanisme pemulihan bagi korban. Baik aktor pemerintah maupun non-pemerintah, termasuk perusahaan yang terlibat dalam pengembangan, penjualan, maupun penggunaan *spyware*, memiliki tanggung jawab untuk menyediakan mekanisme pemulihan bagi korban yang hak asasinya dilanggar akibat penyalahgunaan teknologi tersebut. Hak atas pemulihan yang efektif bagi korban pelanggaran HAM sendiri dijamin dalam berbagai instrumen hukum HAM internasional, termasuk Kovenan Internasional tentang Hak-Hak Sipil dan Politik (*International Covenant on Civil and Political Rights/ICCPR*), yang telah diratifikasi Indonesia pada tahun 2005.

UNGPs menyediakan kerangka kerja untuk memberikan pemulihan bagi korban pelanggaran HAM yang timbul dari cara perusahaan maupun negara mengembangkan, menerapkan, dan menggunakan teknologi *spyware*. UNGPs menekankan bahwa pemulihan atas pelanggaran HAM yang terkait dengan aktivitas bisnis dapat dilakukan melalui berbagai bentuk dan mekanisme. Dalam hal ini, prinsip “efektivitas” menjadi tolok ukur utama untuk menilai apakah suatu mekanisme pemulihan benar-benar memberikan manfaat bagi individu dan

kelompok terdampak.²⁷ Prinsip 31 UNGPs lebih lanjut menetapkan delapan kriteria efektivitas yang dapat digunakan sebagai kerangka bagi perusahaan teknologi, pembuat kebijakan, regulator, serta aktor terkait lainnya untuk menilai efektivitas mekanisme pemulihan yang tersedia.

UNGPs membagi mekanisme remediasi pelanggaran HAM yang terkait dengan bisnis menjadi tiga jenis utama:

- **Mekanisme Peradilan:** yaitu pengadilan domestik, pengadilan regional, serta mekanisme HAM regional dan internasional.
- **Mekanisme Non-Peradilan Berbasis Negara:** yaitu berbagai mekanisme dalam struktur negara yang berpotensi memberikan pemulihan dalam berbagai bentuk, seperti regulator, ombudsman, inspektorat, badan penanganan pengaduan publik, Titik Kontak Nasional dalam Pedoman OECD untuk Perusahaan Multinasional, serta lembaga HAM nasional.
- **Mekanisme Pengaduan Non-Negara:** yaitu mekanisme remediasi yang dikembangkan dan dikelola oleh perusahaan, atau dalam beberapa kasus oleh asosiasi industri maupun kelompok multi-pemangku kepentingan. UNGPs juga menekankan bahwa negara dapat mendorong penguatan mekanisme ini, misalnya dengan menjadikannya sebagai prasyarat bagi perusahaan untuk berpartisipasi dalam pengadaan barang dan jasa pemerintah.

Berbagai jenis mekanisme pemulihan memiliki kontribusi yang berbeda dalam memulihkan pelanggaran HAM. Oleh karena itu, individu dan kelompok terdampak dapat memerlukan berbagai pendekatan, baik yudisial maupun non-yudisial, untuk memenuhi kebutuhan pemulihan mereka. Ekosistem pemulihan yang berfungsi dengan baik akan memperluas pilihan yang tersedia bagi pihak yang membutuhkan pemulihan, bukan justru membatasinya. Dengan

²⁷ Office of the United Nations High Commissioner for Human Rights (OHCHR), *Access to Remedy and the Technology Sector: Basic Concepts and Principles: A B-Tech Foundational Paper* (Geneva: OHCHR), <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>, diakses 3 Mei 2026.

demikian, negara perlu mengadopsi pendekatan yang holistik dan berbasis sistem dalam merancang serta mengevaluasi rezim hukum, lembaga, dan berbagai mekanisme pemulihan yang relevan.²⁸

Pemulihan bagi korban penyalahgunaan *spyware* dapat mencakup beberapa bentuk. *Pertama*, restitusi, yaitu pengembalian kondisi korban ke keadaan semula. *Kedua*, kompensasi, termasuk kompensasi finansial atas kerugian yang dialami. *Ketiga*, rehabilitasi, yang mencakup penyediaan layanan medis, psikologis, hukum, dan sosial. *Keempat*, kepuasan, yang dapat berupa pengakuan atas pelanggaran HAM, permintaan maaf, serta sanksi terhadap pelaku seperti denda atau hukuman pidana. *Kelima*, jaminan ketidakberulangan, yaitu langkah-langkah untuk mencegah terulangnya pelanggaran di masa depan, termasuk melalui putusan pengadilan dan perubahan kebijakan.

Dalam konteks mekanisme pemulihan yudisial, sejumlah praktik telah diterapkan di berbagai negara. Di Yunani, pada Maret 2026 pengadilan domestik menjatuhkan hukuman delapan tahun penjara kepada empat tersangka, termasuk dua warga Israel, dalam skandal *spyware* yang mengguncang pemerintah negara tersebut pada 2022. Di Israel, pada tahun 2023, seorang pengacara HAM bersama sejumlah aktivis dan warga Israel mengajukan permohonan pembukaan penyidikan pidana kepada Jaksa Agung Israel terhadap aktivitas perusahaan *spyware* Israel, Cognyte Software Ltd, serta para pejabat dari Kementerian Pertahanan dan Kementerian Luar Negeri Israel, atas dugaan keterlibatan dalam membantu dan bersekongkol dalam kejahatan terhadap kemanusiaan di Myanmar.²⁹

Selain mekanisme yudisial tersebut, mekanisme pemulihan non-yudisial juga telah digunakan dalam bentuk pengaduan kepada Titik Kontak Nasional

²⁸ OHCHR, *Access to Remedy and the Technology Sector*.

²⁹ Justice for Myanmar, "JFM Calls on Israel's Attorney General to Take Urgent Action Following Application for Criminal Investigation into Cognyte's Business in Myanmar," *Justice for Myanmar*, Januari 2023, <https://www.justiceformyanmar.org/press-releases/jfm-calls-on-israels-attorney-general-to-take-urgent-action-following-application-for-criminal-investigation-into-cognytes-business-in-myanmar>, diakses 3 Mei 2026.

(*National Contact Point/NCP*) OECD. Pada tahun 2013, Privacy International, Reporters Without Borders, Bahrain Watch, Business and Human Rights Centre, serta ECCHR mengajukan pengaduan terhadap perusahaan *spyware* Gamma dan Trovicor kepada Titik Kontak Nasional OECD di Inggris dan Jerman.³⁰ Pada tahun 2014, Titik Kontak Nasional Inggris menyatakan bahwa Gamma melanggar pedoman HAM OECD, sementara Titik Kontak Nasional Jerman menolak melakukan penyelidikan dan hanya melanjutkan proses ke tahap mediasi.

Di Indonesia, mekanisme pemulihan bagi korban penyalahgunaan *spyware* masih sangat terbatas. Kesiapan pemerintah dalam aspek kerangka hukum dan kelembagaan dalam kerangka UNGPs juga masih lemah. Kondisi ini berkontribusi pada belum tersedianya mekanisme pemulihan yang efektif bagi korban penyalahgunaan *spyware*. Temuan tersebut menunjukkan bahwa penguatan mekanisme pemulihan dalam tata kelola *spyware* merupakan bagian dari implementasi menyeluruh UNGPs, yang mencakup tiga pilar utama, yaitu kewajiban negara untuk melindungi, tanggung jawab perusahaan untuk menghormati, serta akses terhadap pemulihan yang efektif bagi korban.

³⁰ Privacy International, "OECD Complaint v. Gamma (Surveillance Technology Exports from UK to Bahrain)," *Privacy International*, <http://privacyinternational.org/legal-action/oecd-complaint-v-gamma-surveillance-technology-exports-uk-bahrain>, diakses 3 Mei 2026.

Rekomendasi

Sejalan dengan implementasi UNGPs, penguatan penguatan tata kelola *spyware* menjadi penting. Penguatan ini tidak hanya menekankan pencegahan melalui uji tuntas HAM, tetapi juga memastikan tersedianya mekanisme pemulihan yang efektif. Untuk itu, tulisan ini merekomendasikan sejumlah langkah berikut:

Internasional

- Mendorong pemerintah Uni Eropa untuk memperkuat implementasi Regulasi Uni Eropa 2021/821 dalam pengawasan ekspor teknologi pengawasan dan *spyware*.
- Mendorong Perserikatan Bangsa-Bangsa (PBB) untuk menginisiasi pembentukan kerangka hukum global terkait *spyware* guna memperkuat standar akuntabilitas internasional.
- Mendorong Pemerintah Indonesia untuk bergabung dalam Proses Pall Mall dan Kesepakatan Wassenaar sebagai sarana untuk berbagi praktik baik dan memperkuat kapasitas pengendalian teknologi sensitif, meskipun keduanya bersifat tidak mengikat.

Nasional

- Mendesak Pemerintah Indonesia untuk menetapkan Rancangan Undang-Undang Penyesuaian sebagai prioritas dalam Program Legislasi Nasional (Prolegnas) serta memastikan proses pembahasannya melibatkan organisasi masyarakat sipil, akademisi, dan masyarakat.
- Mendorong Pemerintah Indonesia untuk menerapkan kewajiban uji tuntas HAM dalam kerangka hukum terkait ekspor-impor serta pengadaan barang dan jasa di sektor keamanan dan pertahanan.
- Mendorong Pemerintah Indonesia untuk memperketat pengendalian ekspor-impor teknologi berisiko tinggi seperti *spyware* dan teknologi

surveilans dengan: (1) mewajibkan perizinan khusus yang disertai penilaian dampak HAM; (2) mewajibkan transparansi perusahaan pemegang izin; dan (3) menyediakan mekanisme pelaporan publik atas dugaan pelanggaran atau penyalahgunaan izin.

- Mendorong Pemerintah Indonesia untuk memperkuat tata kelola pengadaan barang dan jasa dengan: (1) mewajibkan transparansi Rencana Umum Pengadaan (RUP) oleh kementerian/lembaga; dan (2) mensyaratkan komitmen HAM bagi perusahaan yang berpartisipasi dalam pengadaan teknologi surveilans.
- Mendorong Pemerintah Indonesia untuk memastikan tersedianya mekanisme pemulihan yang efektif bagi korban penyalahgunaan *spyware* melalui pembentukan mekanisme pengaduan dan pemulihan yang independen, mudah diakses, dan mampu memberikan tindak lanjut yang efektif, baik melalui jalur yudisial maupun non-yudisial.

Daftar Pustaka

Perjanjian Internasional dan Peraturan Perundang-Undangan

Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, 1989.

International Covenant on Civil and Political Rights, 1966.

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast), 2021.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 1996.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

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

Peraturan Presiden Republik Indonesia Nomor 60 Tahun 2023 tentang Strategi Nasional Bisnis dan Hak Asasi Manusia.

Peraturan Menteri Perdagangan Republik Indonesia Nomor 23 Tahun 2023 tentang Kebijakan dan Pengaturan Ekspor.

Peraturan Menteri Perdagangan Republik Indonesia Nomor 9 Tahun 2025 tentang Perubahan Ketiga atas Permendag Nomor 23 Tahun 2023.

Peraturan Menteri Perdagangan Republik Indonesia Nomor 16 Tahun 2025 tentang Kebijakan dan Pengaturan Impor.

Peraturan Menteri Perdagangan Republik Indonesia Nomor 37 Tahun 2025 tentang Perubahan atas Permendag Nomor 16 Tahun 2025.

Laporan, Kebijakan, dan Dokumen Kelembagaan

Office of the United Nations High Commissioner for Human Rights (OHCHR). "Access to Remedy and the Technology Sector: Basic Concepts and Principles." B-Tech Foundational Paper.

<https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf>.

_____. "Identifying and Assessing Human Rights Risks Related to End-Use." B-Tech Foundational Paper.

<https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/identifying-human-rights-risks.pdf>.

_____. "The UN Guiding Principles in the Age of Technology." B-Tech Foundational Paper.

<https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf>.

United Nations Human Rights Council. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. Perserikatan Bangsa-Bangsa, 2011.

United Nations Development Programme (UNDP). "Prinsip-Prinsip Panduan PBB tentang Bisnis dan Hak Asasi Manusia (UNGP)."

<https://www.undp.org/indonesia/publications/prinsip-prinsip-panduan-pbb-tentang-bisnis-dan-hak-asasi-manusia-ungp-bahasa-indonesia>.

Organization for Economic Co-operation and Development (OECD). *OECD Guidelines for Multinational Enterprises*. Paris: OECD Publishing, 2011.

Liger, Quentin, dan Marc Gutheil. "The Use of Pegasus and Equivalent Surveillance Spyware." Parlemen Eropa, 2023.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU\(2022\)740151_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf).

Perez, Silvia Lorenzo, dkk. *How the EU's Dual-Use Regime Falls Short on Tackling Spyware*. Centre for Democracy & Technology Europe, 2025.

Roberts, Jen, dkk. "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights." Atlantic Council, 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/>.

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

Hiebert, Kyle Volpi. "The Growing Global Spyware Industry Must Be Reined In." Centre for International Governance Innovation, 2023. <https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/>.

Sunaryanto, Agus. "Transparansi Pengadaan Pemerintah." Indonesia Corruption Watch, 2018. <https://antikorupsi.org/id/article/transparansi-pengadaan-pemerintah>.

Berita dan Sumber Daring

Privacy International. "OECD Complaint v. Gamma (Surveillance Technology Exports from UK to Bahrain)." <https://privacyinternational.org/legal-action/oecd-complaint-v-gamma-surveillance-technology-exports-uk-bahrain>.

_____. "Our Challenge against UK's Secret TCN Powers."
<https://privacyinternational.org/long-read/5547/our-challenge-against-uks-secret-tcn-powers>.

Justice for Myanmar. "JFM Calls on Israel's Attorney General to Take Urgent Action Following Application for Criminal Investigation into Cognyte's Business in Myanmar." *Justice for Myanmar*. Januari 2023.
<https://www.justiceformyanmar.org/press-releases/jfm-calls-on-israels-attorney-general-to-take-urgent-action-following-application-for-criminal-investigation-into-cognytes-business-in-myanmar>.

Investigatory Powers Commissioner's Office. GOV.UK.
<https://www.gov.uk/government/organisations/investigatory-powers-commissioners-office>.

Investigatory Powers Tribunal. "Home."
<https://investigatorypowerstribunal.org.uk/>.

Lighthouse Reports. "Surveillance Secrets."
<https://www.lighthousereports.com/investigation/surveillance-secrets/>.

UK Government. "The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities."
<https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>.

Times of Israel. "Israeli Spyware Maker Sentenced to 8 Years in Greece's Predator Case." 26 Februari 2026.
<https://www.timesofisrael.com/israeli-spyware-maker-sentenced-to-8-years-in-greeces-predator-case/>.

Rikang, R. "Investigasi: Jejak Pelacakan Nomor Telepon Aktivis dan Tokoh Publik." *Tempo*, Oktober 2025.

<https://www.tempo.co/investigasi/lacak-nomor-ponsel-aktivis-tokoh-publik-2079647>.

Thea, D. A., dan Ady. "Sederhanakan Proses Ekspor-Impor, Pemerintah Pangkas Ratusan Regulasi." *Hukumonline*, 23 Juni 2022.

<https://www.hukumonline.com/berita/a/sederhanakan-proses-ekspor-impor--pemerintah-pangkas-ratusan-regulasi-lt62b44803ca9f5/>.

US Privacy and Civil Liberties Oversight Board (PCLOB).

<https://www.pclob.gov/>

