Madani: Jurnal Ilmiah Multidisiplin
Volume 3, Nomor 11, December 2025, P. 225-231
E-ISSN: 2986-6340

DOI: https://doi.org/10.5281/zenodo.17906007

Pengaturan Hukum Penggunaan Spyware oleh Kepolisian Siber Dalam Pengawasan Digital

Legal Regulation of Spyware Use by Cyber Police in Digital Surveillance

Akbar Tristanto Putra, Frans Simangusong
Universitas 17 Agustus 1945 Surabaya
Email : akbartristantoputra29@gmail.com

Abstrak

Perkembangan teknologi informasi pada era digital mendorong aparat penegak hukum, khususnya kepolisian siber, untuk mengadopsi perangkat pengawasan digital yang semakin canggih dalam mendeteksi, menganalisis, dan mencegah kejahatan siber yang bersifat kompleks dan cepat berubah. Salah satu instrumen yang kerap dikaitkan dengan fungsi intelijen penegakan hukum adalah penggunaan perangkat pengintai lunak berbahaya (spyware) yang mampu mengakses informasi secara diam-diam dan mengumpulkan data sensitif dari perangkat target. Meskipun secara operasional spyware memberikan efektivitas dalam kegiatan intelijen, penggunannya menimbulkan persoalan mendasar terkait legalitas, batas kewenangan, dan perlindungan hak privasi warga negara. Dalam konteks Indonesia, kewenangan kepolisian dalam melakukan pengawasan digital memang berlandaskan pada UU No. 2 Tahun 2002 tentang Kepolisian Negara RI dan UU No. 17 Tahun 2011 tentang Intelijen Negara, namun kedua regulasi tersebut belum mengatur secara spesifik mekanisme penggunaan spyware. Di sisi lain, UU ITE dan UU Perlindungan Data Pribadi memberikan batasan ketat terhadap akses ilegal, intersepsi, dan pemrosesan data pribadi tanpa dasar hukum yang sah. Oleh karena itu, penelitian ini menelaah urgensi pengaturan hukum yang komprehensif untuk penggunaan spyware oleh kepolisian siber guna memastikan keseimbangan antara efektivitas penegakan hukum dan perlindungan hak asasi manusia. Hasil kajian menunjukkan bahwa pengaturan khusus diperlukan untuk mencegah penyalahgunaan wewenang, menjamin akuntabilitas, serta memastikan bahwa pengawasan digital dilakukan berdasarkan prinsip legalitas, proporsionalitas, dan transparansi dalam kerangka negara hukum yang demokratis.
Kata kunci: *spyware, kepolisian siber, pengawasan digital*

Abstract

The development of information technology in the digital era has encouraged law enforcement officials, particularly cyber police, to adopt increasingly sophisticated digital surveillance tools to detect, analyze, and prevent complex and rapidly changing cybercrimes. One instrument often associated with law enforcement intelligence functions is the use of malicious software (spyware) capable of covertly accessing information and collecting sensitive data from target devices. Although spyware is operationally effective in intelligence activities, its use raises fundamental issues related to legality, limits of authority, and protection of citizens' privacy rights. In the Indonesian context, the police's authority to conduct digital surveillance is based on Law No. 2 of 2002 concerning the Indonesian National Police and Law No. 17 of 2011 concerning State Intelligence, but neither regulation specifically regulates the mechanisms for spyware use. On the other hand, the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law impose strict restrictions on illegal access, interception, and processing of personal data without a valid legal basis. Therefore, this study examines the urgency of comprehensive legal regulations for the use of spyware by cyber police to ensure a balance between effective law enforcement and human rights protection. The study's findings indicate that specific regulations are needed to prevent abuse of authority, ensure accountability, and ensure that digital surveillance is conducted based on the principles of legality, proportionality, and transparency within a democratic, rule-of-law framework.
Keywords: spyware, cyber policing, digital surveillance.

Article Info
Received date: 25 November 2025 Revised date: 30 November 2025 Accepted date: 05 December 2025

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang sangat pesat dalam beberapa dekade terakhir telah mengubah cara kita hidup, berinteraksi, dan berbisnis. Teknologi ini tidak hanya memengaruhi aspek sosial dan ekonomi, tetapi juga menciptakan tantangan baru dalam bidang

keamanan. Dengan semakin canggihnya perangkat keras dan lunak yang ada, ancaman terhadap privasi dan keamanan individu di dunia maya semakin meningkat, baik dalam bentuk kejahatan siber seperti peretasan data, penyebaran informasi palsu, hingga serangan yang lebih besar yang dapat merusak infrastruktur vital negara. Dalam konteks ini, negara-negara di seluruh dunia, termasuk Indonesia, terus berupaya untuk mengatasi tantangan tersebut dengan mengembangkan sistem pengawasan digital untuk menjaga ketertiban dan melindungi kepentingan nasional. Salah satu instrumen yang digunakan dalam pengawasan digital ini adalah perangkat lunak pengintai atau spyware. Spyware adalah jenis perangkat lunak yang dirancang untuk mengumpulkan informasi dari perangkat yang terinfeksi tanpa sepengetahuan penggunanya. Secara umum, spyware digunakan oleh individu atau kelompok dengan niat jahat untuk memata-matai aktivitas pengguna lain, mencuri data pribadi, atau melacak kebiasaan online tanpa izin. Meskipun demikian, dalam beberapa tahun terakhir, spyware juga digunakan oleh aparat penegak hukum sebagai alat dalam pengawasan digital guna mendeteksi dan mencegah kejahatan siber. Di negara-negara dengan infrastruktur digital yang berkembang pesat, penggunaan spyware oleh kepolisian siber untuk menyelidiki kejahatan seperti peretasan, perdagangan ilegal, dan ancaman terorisme siber menjadi hal yang umum[1].

Spyware dapat berfungsi sebagai alat yang efektif dalam mendeteksi dan mengatasi kejahatan siber, penggunaannya juga memunculkan perdebatan yang mendalam mengenai batas-batas hak privasi, kebebasan individu, dan keabsahan tindakan hukum yang dilakukan oleh aparat negara. Dalam konteks ini, Indonesia, sebagai negara dengan populasi terbesar di Asia Tenggara dan penggunaan internet yang sangat tinggi, menghadapi tantangan besar terkait pengaturan hukum mengenai penggunaan spyware oleh kepolisian siber dalam pengawasan digital. Meskipun Indonesia telah memiliki berbagai undang-undang yang mengatur mengenai tindak pidana di dunia maya, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), regulasi yang secara khusus mengatur penggunaan spyware oleh kepolisian siber dalam konteks penegakan hukum dan pengawasan digital masih sangat terbatas. Tanpa adanya regulasi yang jelas, penggunaan spyware oleh aparat penegak hukum berisiko menimbulkan masalah serius terkait pelanggaran hak privasi individu dan kebebasan pribadi yang dilindungi oleh konstitusi. Selain itu, ketidakjelasan regulasi ini juga berpotensi menimbulkan celah hukum yang dapat dimanfaatkan oleh pihak-pihak tertentu untuk menyalahgunakan perangkat ini dengan tujuan yang tidak sah, seperti penyalahgunaan kekuasaan atau peretasan ilegal yang merugikan masyarakat. Oleh karena itu, penting untuk menganalisis lebih dalam mengenai pengaturan hukum yang ada terkait penggunaan spyware oleh kepolisian siber dalam tindakan pengawasan digital. Aspek pertama yang perlu diperhatikan adalah kejelasan hukum terkait penggunaan spyware oleh kepolisian siber. Regulasi yang jelas dan tegas sangat penting untuk memastikan bahwa penggunaan spyware dilakukan dalam kerangka hukum yang sesuai, dan hanya digunakan untuk tujuan yang sah, seperti penanggulangan kejahatan siber, perlindungan data pribadi, dan pemberantasan tindakan terorisme[2].

Aturan hukum yang jelas juga diperlukan untuk menetapkan prosedur dan batasan dalam penggunaan spyware agar tidak melanggar hak privasi individu dan kebebasan berekspresi. Kejelasan hukum ini akan memberikan kepastian bagi masyarakat mengenai apa yang dapat dan tidak dapat dilakukan oleh kepolisian siber dalam konteks pengawasan digital. Aspek kedua yang perlu dicermati adalah masalah pengawasan terhadap penggunaan spyware oleh kepolisian siber. Sebagai negara yang menganut prinsip negara hukum, Indonesia harus memastikan bahwa segala tindakan yang diambil oleh aparat penegak hukum, termasuk dalam pengawasan digital, tetap berada dalam pengawasan yang ketat dan sesuai dengan prinsip-prinsip hak asasi manusia. Penggunaan spyware oleh kepolisian siber harus dilakukan dengan mekanisme yang transparan dan akuntabel, agar tidak disalahgunakan untuk

[1] Abidin, D. Z. (2015). Kejahatan dalam teknologi informasi dan komunikasi. *Jurnal Processor*, *10*(2), 509-516.
[2] Arafat, M., & Wirasto, A. T. E. (2024). Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia. *Equality: Journal of Law and Justice, 1*(2), 220-241.

kepentingan pribadi atau politik. Salah satu cara untuk mencapai hal ini adalah dengan menetapkan lembaga pengawas yang independen yang dapat memantau dan menilai setiap penggunaan spyware oleh aparat kepolisian. Dengan adanya pengawasan yang efektif, masyarakat akan merasa lebih aman bahwa hak-hak privasi mereka tidak akan dilanggar tanpa alasan yang sah dan jelas. Di sisi lain, aspek ketiga yang perlu dianalisis adalah potensi dampak sosial dari penggunaan spyware oleh kepolisian siber[3].

Meskipun spyware dapat digunakan untuk tujuan yang sah, seperti mendeteksi dan mencegah kejahatan siber, penggunaan perangkat ini dalam jangka panjang dapat menimbulkan ketidakpercayaan masyarakat terhadap institusi penegak hukum. Masyarakat mungkin merasa bahwa privasi mereka terancam dan kebebasan individu mereka terbatasi jika penggunaan spyware tidak diawasi dengan ketat[4]. Penting untuk memastikan bahwa regulasi mengenai penggunaan spyware oleh kepolisian siber tetap seimbang, yaitu dapat memberikan keamanan yang dibutuhkan dalam menghadapi ancaman siber, namun juga tetap menjaga hak-hak fundamental warga negara. Kajian mengenai perbandingan dengan regulasi di negara lain yang lebih dulu mengatur penggunaan spyware dalam pengawasan digital dapat memberikan wawasan yang berharga bagi Indonesia dalam merumuskan kebijakan yang lebih baik. Negara-negara seperti Amerika Serikat dan Inggris sudah lebih dulu memiliki regulasi yang mengatur penggunaan spyware oleh lembaga penegak hukum, dengan mempertimbangkan prinsip-prinsip hak asasi manusia dan perlindungan privasi[5].

Oleh karena itu, penelitian ini bertujuan untuk memberikan analisis mendalam mengenai pengaturan hukum penggunaan spyware oleh kepolisian siber di Indonesia, dengan meninjau regulasi yang ada, tantangan yang dihadapi dalam penerapannya, serta potensi dampak sosial dan hukum yang timbul. Melalui kajian ini, diharapkan dapat ditemukan solusi yang lebih tepat guna untuk mengatur penggunaan spyware dalam pengawasan digital oleh kepolisian siber, yang tidak hanya efektif dalam mencegah kejahatan siber, tetapi juga tetap menghormati hak-hak privasi dan kebebasan individu. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi positif bagi pengembangan regulasi yang lebih baik di Indonesia dalam menghadapi tantangan pengawasan digital di era modern ini.

METODE

Penelitian ini menggunakan metode pendekatan normatif, yang berfokus pada kajian terhadap peraturan perundang-undangan yang berlaku, doktrin hukum, serta literatur yang relevan mengenai penggunaan spyware oleh kepolisian siber dalam pengawasan digital. Pendekatan ini bertujuan untuk menganalisis secara komprehensif mengenai pengaturan hukum yang ada, baik di Indonesia maupun di negara lain, terkait penggunaan perangkat pengintai lunak oleh aparat penegak hukum. Sumber data utama yang digunakan adalah peraturan perundang-undangan, termasuk Undang-Undang Informasi dan Transaksi Elektronik (ITE), serta peraturan lain yang relevan, seperti undang-undang mengenai privasi dan hak asasi manusia. Selain itu, penelitian ini juga menggunakan studi pustaka yang mencakup jurnal akademik, artikel, dan laporan yang membahas tentang regulasi pengawasan digital, serta praktik penggunaan spyware oleh kepolisian di negara-negara lain. Teknik analisis yang digunakan adalah analisis kualitatif dengan pendekatan deskriptif-analitis untuk mengevaluasi keabsahan dan implikasi hukum dari penggunaan spyware dalam konteks pengawasan digital. Dengan demikian, penelitian ini

[3] Almira, S. D. A., Wardah Yuspin, S. H., & Muchamad Iksan, S. H. (2025). Perlindungan Hukum Terhadap Pengguna E-Wallet Dalam Menghadapi Risiko Cyber Crime di Indonesia (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

[4] Romadhonia, A., Nahdliyin, S. H., & Janah, M. (2024). Peran Literasi Digital Bagi Masyarakat Dalam Mengurangi Dampak Kejahatan Transaksi Elektronik Illegal. *Jurnal Hukum Ius Publicum, 5*(1), 176-201.

[5] Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4*(1), 165-189.

berusaha memberikan pemahaman yang lebih jelas mengenai batasan-batasan hukum yang ada dan perlunya regulasi yang lebih tegas dalam mengatur penggunaan spyware oleh kepolisian siber.

HASL DAN PEMBAHASAN

Implementasi teknologi informasi dalam konteks keamanan nasional dan penegakan hukum pada era digital menjadi konsekuensi logis dari meningkatnya kompleksitas ancaman siber yang bersifat dinamis, adaptif, dan sulit dideteksi melalui metode konvensional, sehingga mendorong lembaga penegak hukum, termasuk kepolisian siber, untuk mengoptimalkan perangkat digital dalam tugas intelijen dan pengawasan terhadap aktivitas masyarakat di ruang siber; pada tataran global, penggunaan teknologi pengawasan seperti spyware telah lama menjadi instrumen strategis untuk mendeteksi potensi ancaman, aktivitas kriminal, dan ragam kejahatan berbasis teknologi informasi yang berkembang cepat, namun sekaligus menimbulkan dilema etis dan hukum terkait privasi warga, proportionality, necessity, serta akuntabilitas institusi pengguna[6], perkembangan kejahatan siber yang mencakup penyalahgunaan data, pembobolan sistem elektronik, manipulasi informasi, phishing, malware, hingga penipuan daring menuntut aparat penegak hukum meningkatkan kemampuan deteksi dini (early warning) dan kewaspadaan (situational awareness), terutama karena kejahatan tersebut memiliki karakteristik transnasional, berjejaring, serta menggunakan modus serangan yang berkembang sangat cepat; fungsi intelijen kepolisian menjadi salah satu instrumen yang diharapkan mampu mengantisipasi pola ancaman tersebut, mengingat intelijen kepolisian dalam perspektif hukum merupakan bagian dari intelijen penegakan hukum (law enforcement intelligence), yang bekerja untuk menghimpun, mengolah, menganalisis, dan menyampaikan informasi secara sistematis guna mendukung proses penegakan hukum, keamanan, dan ketertiban masyarakat[7].

Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia mengatur bahwa kepolisian memiliki fungsi pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, serta memberikan perlindungan dan pelayanan kepada masyarakat, serta berwenang melakukan kegiatan intelijen (Pasal 13 dan Pasal 14), yang secara normatif memberi dasar bagi pemanfaatan teknologi penunjang, termasuk perangkat pengawasan digital[8] di sisi lain, Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara memberikan mandat bahwa aktivitas intelijen harus dilakukan berdasarkan prinsip profesionalitas, kepastian hukum, akuntabilitas, dan penghormatan terhadap hak asasi manusia, sehingga setiap tindakan pengumpulan informasi, termasuk melalui instrumen TI, wajib mematuhi batasan hukum untuk mencegah penyalahgunaan kewenangan; penggunaan spyware oleh kepolisian siber dalam praktik pengawasan digital sesungguhnya muncul dari kebutuhan operasional intelijen untuk mendeteksi potensi ancaman yang menyangkut ideologi, politik, ekonomi, sosial, budaya, dan keamanan, sebagaimana menjadi salah satu fungsi intelijen dalam mendeteksi isu-isu strategis di masyarakat, khususnya dalam konteks ruang digital yang memfasilitasi penyebaran radikalisme, propaganda, penipuan terorganisasi, hingga aktivitas kriminal terstruktur—namun kebutuhan tersebut tidak dapat dijadikan alasan pembenar untuk menggunakan alat pengintai lunak berbahaya tanpa mekanisme pengawasan dan kepatuhan hukum[9].

Indonesia telah mengatur prinsip-prinsip perlindungan data dan privasi dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, yang menegaskan bahwa setiap pihak dilarang mengakses sistem elektronik tanpa hak (Pasal 30), memanipulasi, mengubah, atau mencuri data (Pasal 32), serta melakukan intersepsi ilegal (Pasal 31),

[6] Rolando, D. M., Aulia, H. H., & Andini, M. T. (2023). Tranformasi Digital dan Ancaman Cybercrime. *Siyasah, 3*(1), 68-84.
[7] Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. In *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia p-ISSN* (Vol. 2086, p. 5805).
[8] Sanusi, S., La Dee, M., Widyastuti, T. V., & Lubis, A. F. (2023). Ilmu Hukum Implikasi Teknologi dalam Perubahan Hukum. *Malang: Penerbit Literasi Nusantara Abadi Group*.
[9] Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding Sains dan Teknologi, 2*(1), 216-221.

sehingga penggunaan spyware oleh aparat penegak hukum harus didasarkan pada kewenangan resmi, mekanisme perintah pengadilan (lawful interception), serta prosedur penegakan hukum yang sah; kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) semakin menegaskan bahwa data pribadi hanya dapat diproses berdasarkan persetujuan, perintah undang-undang, atau kepentingan penegakan hukum yang memenuhi prinsip proporsionalitas, legalitas, dan akuntabilitas, sehingga penggunaan spyware yang memiliki kemampuan mengakses informasi secara diam-diam, memantau aktivitas perangkat, dan mengumpulkan data sensitif merupakan bentuk pemrosesan data pribadi yang sangat intrusif dan berpotensi melanggar hak atas privasi jika dilakukan tanpa dasar hukum yang eksplisit; pada intelijen kepolisian, kebutuhan akan data dan informasi spesifik untuk mendukung proses penegakan hukum memang merupakan bagian integral dari strategi *law enforcement*[10], karena berbagai kasus kejahatan digital seperti terorisme siber, peretasan, penipuan daring, dan penyebaran konten terlarang membutuhkan pembuktian yang bersifat elektronik dan seringkali hanya dapat diperoleh melalui teknik digital surveillance yang canggih, namun urgensi tersebut tetap harus diseimbangkan dengan perlindungan hak-hak sipil warga negara sebagaimana dijamin dalam Undang-Undang Dasar 1945 Pasal 28G yang melindungi hak atas privasi, rasa aman, dan perlindungan dari ancaman penyalahgunaan wewenang[11].

Penggunaan spyware oleh kepolisian siber yang tidak diatur secara tegas dalam peraturan perundang-undangan akan menimbulkan sejumlah persoalan, mulai dari risiko penyalahgunaan (abuse of power), ketidakjelasan batas kewenangan, lemahnya mekanisme oversight, hingga potensi pelanggaran HAM, terutama karena spyware memiliki kemampuan teknis seperti *keylogging, remote access*, pengendalian kamera atau mikrofon, pengambilan file, hingga monitoring komunikasi yang apabila tidak diatur secara ketat dapat menciptakan praktik surveillance state yang bertentangan dengan prinsip negara hukum, maka, diperlukan regulasi khusus atau penguatan pada peraturan pelaksana yang mengatur penggunaan perangkat pengintai oleh aparat penegak hukum, termasuk definisi spyware, mekanisme permohonan izin, batas waktu penggunaan, tujuan penggunaan, verifikasi kebutuhan intelijen, perlindungan data subjek, mekanisme penghancuran data, hingga pengawasan eksternal oleh lembaga independen guna menjamin kesesuaian dengan prinsip-prinsip legalitas dan akuntabilitas; secara normatif, praktik pengawasan digital yang dilakukan kepolisian siber perlu diarahkan pada model yang selaras dengan standar internasional[12], seperti *International Principles on the Application of Human Rights to Communications Surveillance* (2013) yang mensyaratkan adanya *legality, legitimate aim, necessity, adequacy, proportionality, dan oversight* dalam setiap tindakan pengawasan; dalam konteks Indonesia, absennya pengaturan khusus terkait spyware menyebabkan proses penegakan hukum bergantung pada tafsir umum dari UU ITE, UU Kepolisian, UU Intelijen, dan UU PDP, yang belum memberikan kerangka hukum yang komprehensif[13].

Pengaturan hukum penggunaan spyware oleh kepolisian siber bukan hanya menyangkut kebutuhan teknis dalam peningkatan efektivitas intelijen penegakan hukum, tetapi juga mengenai urgensi harmonisasi regulasi untuk memberikan batasan, kepastian hukum, dan perlindungan hak warga negara, sehingga tindakan pengawasan digital oleh aparat tetap berada dalam koridor negara hukum yang demokratis, responsif terhadap perkembangan teknologi, dan menjunjung tinggi asas proporsionalitas demi mencegah potensi penyalahgunaan kekuasaan dalam praktik pengawasan siber.

[10] Sulaeman, D., & Kemala, A. P. (2025). Analisis Hukum terhadap Tindak Pidana Pencurian Identitas di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 3*(2), 133-148.
[11] Kusumoningtyas, A. A. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. *Jurnal Adhikari, 2*(3), 416-433.

[12] Yusuf, A., & Harahap, M. E. M. (2025). Formulasi Tindak Pidana Siber Menggunakan Malware Menurut Hukum Pidana Islam. *PUSKAPSI Law Review, 5*(1), 247-262.
[13] Putra, R. T. Y., & Rusmawan, T. (2024). Strategi Kepolisian Negara Republik Indonesia Dalam Menegakkan Hukum Penyebaran Pornografi Anak Melalui Platform Digital Berdasarkan UU ITE. *Brand Communication, 3*(1), 76-91.

SIMPULAN

Penggunaan perangkat pengintai lunak berbahaya (spyware) oleh kepolisian siber dalam aktivitas pengawasan digital pada dasarnya lahir dari kebutuhan operasional intelijen penegakan hukum untuk merespons laju perkembangan kejahatan siber yang semakin kompleks, adaptif, dan sulit ditangani dengan metode konvensional. Fungsi intelijen kepolisian yang berorientasi pada penghimpunan serta analisis informasi strategis menjadikan teknologi informasi sebagai instrumen yang hampir tidak dapat dipisahkan dari tugas pemeliharaan keamanan dan penegakan hukum. Meskipun demikian, penggunaan spyware yang bersifat intrusif harus ditempatkan dalam kerangka hukum yang jelas, karena saat ini tidak ada regulasi khusus yang secara eksplisit mengatur mekanisme, batas kewenangan, dan prosedur pengawasan terhadap penggunaan perangkat tersebut. Padahal, prinsip-prinsip dasar yang tercantum dalam UU Kepolisian, UU Intelijen Negara, UU ITE, serta UU Perlindungan Data Pribadi mewajibkan aparat untuk menghormati legalitas, akuntabilitas, proporsionalitas, dan perlindungan hak atas privasi warga negara. Tanpa regulasi yang komprehensif, penggunaan spyware berpotensi menimbulkan penyalahgunaan wewenang, pelanggaran hak asasi manusia, dan ketidakpastian hukum dalam praktik pengawasan digital. Oleh karena itu, diperlukan pembentukan atau penguatan regulasi khusus yang mengatur secara rinci penggunaan spyware oleh aparat penegak hukum, sehingga kebutuhan operasional intelijen kepolisian dapat berjalan secara efektif namun tetap berada dalam koridor negara hukum yang demokratis dan menghormati hak-hak fundamental warga negara.

REFERENSI

Arafat, M., & Wirasto, A. T. E. (2024). Kebijakan kriminal dalam penanganan siber di era digital: Studi kasus di Indonesia. *Equality: Journal of Law and Justice, 1*(2), 220-241.

Abidin, D. Z. (2015). Kejahatan dalam teknologi informasi dan komunikasi. *Jurnal Processor, 10*(2), 509-516.

Almira, S. D. A., Wardah Yuspin, S. H., & Muchamad Iksan, S. H. (2025). Perlindungan Hukum Terhadap Pengguna E-Wallet Dalam Menghadapi Risiko Cyber Crime di Indonesia (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4*(1), 165-189.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. In *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia p-ISSN* (Vol. 2086, p. 5805).

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding Sains dan Teknologi, 2*(1), 216-221.

Kusumoningtyas, A. A. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. *Jurnal Adhikari, 2*(3), 416-433.

Putra, R. T. Y., & Rusmawan, T. (2024). Strategi Kepolisian Negara Republik Indonesia Dalam Menegakkan Hukum Penyebaran Pornografi Anak Melalui Platform Digital Berdasarkan UU ITE. *Brand Communication, 3*(1), 76-91.

Romadhonia, A., Nahdliyin, S. H., & Janah, M. (2024). Peran Literasi Digital Bagi Masyarakat Dalam Mengurangi Dampak Kejahatan Transaksi Elektronik Illegal. *Jurnal Hukum Ius Publicum, 5*(1), 176-201.

Rolando, D. M., Aulia, H. H., & Andini, M. T. (2023). Tranformasi Digital dan Ancaman Cybercrime. *Siyasah, 3*(1), 68-84.

Sanusi, S., La Dee, M., Widyastuti, T. V., & Lubis, A. F. (2023). Ilmu Hukum Implikasi Teknologi dalam Perubahan Hukum. *Malang: Penerbit Literasi Nusantara Abadi Group*.

Sulaeman, D., & Kemala, A. P. (2025). Analisis Hukum terhadap Tindak Pidana Pencurian Identitas di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 3*(2), 133-148.

Yusuf, A., & Harahap, M. E. M. (2025). Formulasi Tindak Pidana Siber Menggunakan Malware Menurut Hukum Pidana Islam. *PUSKAPSI Law Review, 5*(1), 247-262.