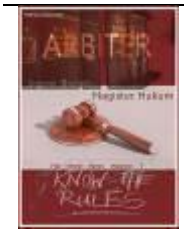

*ARBITER: Jurnal Ilmiah Magister Hukum*, 8 (1) 2026: 1-12
DOI: 10.31289/arbiter.v8i1.6654

***ARBITER: Jurnal Ilmiah Magister Hukum***

*Available online http://jurnalmahasiswa.uma.ac.id/index.php/arbiter*
*Diterima: 04 Oktober 2025; Direview: 24 November 2025; Disetujui: 07 Desember 2025*

# Penegakan Hukum Pidana Siber di Indonesia: Tantangan dan Solusi Era Digital

## *Cybercrime Law Enforcement in Indonesia: Challenges and Solutions in the Digital Era*

**Utami Rahmadiani***
Ilmu hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia

**Abstrak**

Akselerasi digitalisasi di Indonesia mendorong peningkatan kejahatan siber yang mengancam kedaulatan digital nasional, sementara penegakan hukum masih menghadapi kesenjangan kapasitas kelembagaan dalam merespons karakteristik unik cybercrime. Penelitian ini bertujuan menganalisis tantangan multidimensional dalam penegakan hukum pidana siber dan merumuskan strategi penguatan yang adaptif terhadap dinamika kejahatan digital. Penelitian menggunakan pendekatan hukum normatif melalui studi kepustakaan terhadap peraturan perundang-undangan, literatur hukum, dan dokumen resmi yang relevan. Analisis dilakukan dengan metode deskriptif-analitis melalui interpretasi sistematis, gramatikal, dan teleologis, serta didukung perbandingan terbatas dengan praktik terbaik di beberapa yurisdiksi internasional. Hasil penelitian menunjukkan bahwa penegakan hukum pidana siber menghadapi kendala berupa keterbatasan sumber daya manusia dalam forensik digital, lemahnya koordinasi antar-lembaga, volatilitas alat bukti elektronik, anonimitas pelaku, serta rendahnya literasi keamanan siber masyarakat. Undang-Undang Nomor 19 Tahun 2016 telah menyediakan kerangka hukum yang memadai, namun implementasinya terhambat oleh sifat transnasional kejahatan siber. Simpulan penelitian menegaskan perlunya pendekatan holistik melalui penguatan kapasitas SDM, standarisasi infrastruktur forensik digital, penguatan regulasi adaptif, pembangunan ekosistem keamanan siber nasional, dan peningkatan kerja sama internasional.
**Kata Kunci**: Penegakan Hukum Pidana Siber; Cybercrime; Teknologi Forensik Digital; Koordinasi Kelembagaan; Keamanan Siber Nasional.

***Abstract***

*The acceleration of digitalization in Indonesia has led to a significant rise in cybercrime, posing serious threats to national digital sovereignty, while law enforcement agencies continue to face institutional capacity gaps in responding to the unique characteristics of cybercrime. This study aims to analyze the multidimensional challenges in cyber criminal law enforcement and to formulate strategic solutions that are responsive to the dynamics of contemporary digital crime. The research adopts a normative legal approach through a literature review of relevant legislation, legal doctrines, and official documents. Data analysis is conducted using a descriptive-analytical method, employing systematic, grammatical, and teleological interpretations, supported by a limited comparative approach to best practices in selected international jurisdictions. The findings indicate that cybercrime law enforcement is constrained by limited human resource capacity in digital forensics, weak inter-agency coordination, the volatility of electronic evidence, offender anonymity, and low public awareness of cybersecurity. Law Number 19 of 2016 provides a comprehensive legal framework; however, its implementation is hindered by the transnational nature of cybercrime that exceeds national jurisdiction. The study concludes that a holistic approach is required, including strengthening human resource capacity, standardizing digital forensic infrastructure, reinforcing adaptive regulations, developing a national cybersecurity ecosystem, and enhancing international cooperation. This research contributes an integrative analytical framework that supports the institutional capacity building needed to address increasingly complex digital crimes.*
***Keywords:*** *Cyber Criminal Law Enforcement; Cybercrime; Digital Forensics; Cybersecurity; Institutional Coordination*

***How to Cite****:* Rahmadiani, U., (2026), Penegakan Hukum Pidana Siber di Indonesia: Tantangan dan Solusi Era Digital, *ARBITER: Jurnal Ilmiah Magister Hukum, 8 (1): 1-12*

**E-mail: utamirdiani@gmail.com* *ISSN 2722-1865 (Online)*

**PENDAHULUAN**

Akselerasi digitalisasi di Indonesia telah mengkonfigurasi ulang lanskap sosial-ekonomi masyarakat dengan menciptakan ekosistem siber yang menawarkan aksesibilitas informasi sekaligus memunculkan vulnerabilitas keamanan dalam bentuk kejahatan digital yang semakin masif. Penetrasi internet yang eksponensial melahirkan fenomena *cybercrime* dengan ragam modus operandi sophisticated mulai dari *fraud* investasi daring, perjudian *online*, *carding*, *phishing*, hingga terorisme siber yang mengancam kedaulatan dan stabilitas keamanan nasional. Dinamika kejahatan siber tidak hanya memanfaatkan kecanggihan teknologi sebagai instrumen, tetapi juga mengeksploitasi kerentanan regulasi dan keterbatasan kompetensi teknis penegak hukum dalam mengidentifikasi serta memproses bukti digital yang bersifat volatil dan transnasional (Januri et al., 2022; Ginara et al., 2022). Kompleksitas ini diperparah oleh karakteristik *cybercrime* yang melampaui jurisdiksi teritorial konvensional, menciptakan tantangan hukum yang menuntut adaptasi sistem peradilan pidana dari paradigma konvensional menuju responsivitas digital yang komprehensif.

Transformasi paradigmatik kejahatan dari dimensi fisik menuju ruang siber menghadirkan urgensi rekonfigurasi sistem hukum pidana yang mampu mengakomodasi karakteristik unik kejahatan digital. Ketidakjelasan jurisdiksi hukum dan minimnya pengaturan spesifik untuk tipologi kejahatan tertentu seperti *cyber terrorism* menciptakan kekosongan normatif yang berpotensi menghasilkan impunitas hukum bagi pelaku (Jondong, 2020). Implementasi penegakan hukum menghadapi tantangan multidimensional yang meliputi keterbatasan kapasitas sumber daya manusia dalam penguasaan teknologi forensik digital, fragmentasi koordinasi kelembagaan, volatilitas bukti elektronik yang mudah dimanipulasi, anonimitas pelaku yang memanfaatkan enkripsi canggih, serta defisit literasi keamanan siber masyarakat yang memperluas permukaan serangan (*attack surface*) kejahatan digital (Virginia Valentine et al., 2024); (Alief Tanding Pamungkas et al., 2024). Meskipun Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah menyediakan landasan yuridis komprehensif, implementasinya terkendala oleh karakteristik unik *cybercrime* dan dimensi transnasional yang melampaui batas kedaulatan nasional, menciptakan kesenjangan antara norma hukum dengan realitas praktik penegakan hukum di lapangan (Kurniawan et al., 2022; (Saputra et al., 2024).

Meskipun literatur eksisting telah mengidentifikasi tantangan teknis, regulasi, dan kelembagaan dalam penegakan hukum pidana siber secara parsial, belum terdapat kajian komprehensif yang mengintegrasikan dimensi substantif, struktural, dan kultural dalam merumuskan solusi holistik bagi optimalisasi penegakan hukum pidana siber di Indonesia. Gap penelitian ini signifikan mengingat pendekatan fragmentaris yang dominan dalam studi terdahulu cenderung menghasilkan rekomendasi yang bersifat sektoral dan kurang efektif dalam mengatasi kompleksitas multidimensional kejahatan siber kontemporer. Penelitian ini mengisi kekosongan tersebut dengan menganalisis secara komprehensif tantangan penegakan hukum pidana siber melalui pendekatan integratif yang mensinergikan perspektif dogmatik hukum, sosiologi hukum, dan teknologi informasi untuk merumuskan solusi strategis yang responsif terhadap dinamika kejahatan digital di era kontemporer.

Berdasarkan kompleksitas permasalahan tersebut, penelitian ini bertujuan menganalisis tantangan multidimensional penegakan hukum pidana siber di Indonesia dan merumuskan solusi hukum yang efektif dalam menanggulangi *cybercrime*. Kontribusi penelitian ini meliputi pengembangan *framework* analisis holistik bagi penegakan hukum pidana siber serta rekomendasi praktis bagi penguatan kapasitas kelembagaan dalam menghadapi dinamika kejahatan digital kontemporer.

Transformasi digital di Indonesia telah menciptakan ruang siber yang memberikan kemudahan akses informasi sekaligus memunculkan kompleksitas kejahatan baru. Proliferasi cybercrime mencakup berbagai modus dari penipuan online, phishing, carding, hingga terorisme siber yang mengancam stabilitas nasional (Januri et al., 2022; Pande Putu Rastika Paramartha et al., 2021). Kompleksitas ini semakin meningkat ketika pelaku mengeksploitasi celah regulasi dan keterbatasan kapasitas penegak hukum dalam memahami dimensi teknis kejahatan digital (Ginara et al., 2022; Jondong, 2020).

Pergeseran paradigma kejahatan dari konvensional menuju ranah siber menuntut adaptasi sistem hukum pidana yang responsif dan komprehensif. (Ginara et al., 2022) menekankan pentingnya proses kriminalisasi terhadap bentuk-bentuk kejahatan baru seperti carding, yang pada awalnya tidak dikategorikan sebagai tindak pidana namun kemudian berkembang menjadi ancaman serius bagi keamanan transaksi elektronik. Kondisi ini diperparah oleh ketidakjelasan jurisdiksi hukum dan minimnya pengaturan spesifik untuk jenis-jenis kejahatan tertentu, sebagaimana temuan (Jondong, 2020) yang mengungkapkan kekosongan hukum dalam pengaturan cyber terrorism di Indonesia, dimana Kitab Undang-Undang Hukum Pidana maupun regulasi khusus terorisme belum mengakomodasi dimensi kejahatan terorisme yang dilakukan melalui dunia maya. Kesenjangan regulasi ini berpotensi menciptakan impunitas hukum bagi pelaku kejahatan siber akibat ketiadaan unsur melawan hukum yang secara eksplisit dirumuskan dalam peraturan perundang-undangan.

Transformasi digital yang mengakselerasi adopsi teknologi informasi dalam berbagai sektor kehidupan masyarakat Indonesia telah menciptakan ekosistem digital yang semakin kompleks dan interconnected, dimana setiap aktivitas online meninggalkan jejak digital yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk mengembangkan strategi serangan yang lebih sophisticated dan terorganisir. (Virginia Valentine et al., 2024) mengidentifikasi bahwa *cybercrime* telah berkembang menjadi ancaman terbesar di era digital dengan dampak kompleks yang tidak hanya merugikan individu namun juga mengancam stabilitas infrastruktur nasional, menciptakan kerentanan sistemik yang memerlukan pendekatan komprehensif dalam mitigasi risiko keamanan siber. (Saputra et al., 2024) memperkuat temuan tersebut dengan mengungkapkan bahwa kemudahan dan tantangan yang dibawa oleh transformasi teknologi telah menjadikan ancaman kejahatan siber sebagai fokus utama yang terus berkembang, dimana kejahatan siber tidak hanya menggunakan teknologi digital sebagai instrumen namun juga memanfaatkan kerentanan psikologis dan sosial masyarakat dalam mengoptimalkan dampak kerugian yang ditimbulkan. Kompleksitas modus operandi *cybercrime* kontemporer menunjukkan evolusi dari kejahatan oportunistik menuju kejahatan yang terstruktur dan berkesinambungan, dimana pelaku mengembangkan business model kriminal yang memanfaatkan teknologi canggih seperti artificial intelligence, machine learning, dan automation untuk meningkatkan efisiensi dan efektivitas serangan sekaligus meminimalkan risiko deteksi oleh sistem keamanan konvensional. (Alief Tanding Pamungkas et al., 2024) menguraikan bahwa pengaturan hukum saat ini masih memiliki keterbatasan dalam mengantisipasi perkembangan teknologi yang exponential, menciptakan gap antara kecepatan inovasi teknologi dengan kemampuan adaptasi framework hukum yang memerlukan proses legislasi yang relatif lambat dan birokratis. Fenomena ini diperparah oleh karakteristik kejahatan siber yang bersifat transnasional dan mengeksploitasi perbedaan regulasi antar jurisdiksi, sehingga pelaku dapat dengan mudah berpindah base operasi ke negara-negara dengan regulasi cyber security yang lemah atau enforcement yang tidak optimal, menciptakan safe haven bagi aktivitas kriminal digital yang merugikan kedaulatan dan keamanan nasional Indonesia.

Implementasi penegakan hukum terhadap kejahatan siber menghadapi tantangan multidimensional yang meliputi aspek substantif, struktural, dan kultural. (Kesuma et al., 2020) menguraikan kompleksitas penerapan sanksi pidana terhadap penipuan melalui media elektronik yang memerlukan pendekatan berlapis, menggabungkan ketentuan Pasal 378 KUHP dengan Pasal 28 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik. (Purwanti et al., 2023) menambahkan bahwa modus operandi kejahatan phising yang semakin canggih, dengan pelaku menyamar sebagai lembaga resmi melalui telephone, email, atau pesan teks, menunjukkan perlunya strategi penanggulangan komprehensif yang mengintegrasikan pendekatan penal dan non-penal. (Kurniawan et al., 2022) mengidentifikasi berbagai hambatan dalam penegakan hukum pidana siber oleh Kepolisian, mencakup keterbatasan penguasaan teknologi informasi oleh penyidik, minimnya bukti dan saksi, serta lemahnya koordinasi antara aparat penegak hukum dengan provider dan masyarakat. (Januri et al., 2022) memperkuat temuan tersebut dengan mengungkapkan bahwa kendala internal berupa lemahnya pengawasan pemerintah, sifat alat bukti digital yang mudah dimanipulasi, serta kendala eksternal meliputi faktor penegak hukum,

sarana prasarana, dan budaya hukum masyarakat menjadi penghambat signifikan dalam penanggulangan kejahatan siber terorganisir.

Berdasarkan kompleksitas permasalahan tersebut, penelitian ini bertujuan untuk menganalisis secara komprehensif tantangan penegakan hukum pidana siber di Indonesia serta merumuskan solusi hukum yang efektif dalam menanggulangi *cybercrime*. Penelitian ini diharapkan dapat memberikan kontribusi teoretis dalam pengembangan kebijakan hukum pidana siber yang lebih responsif, serta memberikan rekomendasi praktis bagi penguatan kapasitas penegak hukum dalam menghadapi dinamika kejahatan digital di era kontemporer.

## METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan kepustakaan (library research) yang berfokus pada analisis mendalam terhadap peraturan perundang-undangan, literatur hukum, dan sumber-sumber dokumen tertulis yang berkaitan dengan penegakan hukum pidana siber di Indonesia. Metode penelitian hukum normatif dipilih karena penelitian ini berupaya mengkaji dan menganalisis norma-norma hukum positif yang mengatur tentang kejahatan siber serta implementasinya dalam sistem hukum pidana Indonesia (Sugiyono, 2020). Pendekatan normatif memungkinkan peneliti untuk melakukan pengkajian sistematis terhadap hierarki peraturan perundang-undangan secara vertikal maupun harmonisasi peraturan secara horizontal, guna mengidentifikasi konsistensi, kekosongan hukum, dan efektivitas regulasi dalam menanggulangi fenomena *cybercrime* yang terus berkembang. Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh melalui studi dokumentasi terhadap bahan hukum primer, sekunder, dan tersier.

Bahan hukum primer mencakup peraturan perundang-undangan yang relevan, khususnya Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menjadi instrumen hukum utama dalam pengaturan kejahatan siber di Indonesia, serta ketentuan dalam Kitab Undang-Undang Hukum Pidana yang masih berlaku untuk jenis-jenis kejahatan konvensional yang bertransformasi ke ranah digital. Bahan hukum sekunder diperoleh dari jurnal ilmiah terakreditasi, buku-buku teks hukum pidana, hasil penelitian terdahulu, dan artikel ilmiah yang membahas tentang penegakan hukum pidana siber, tantangan implementasi regulasi, serta analisis kasus-kasus kejahatan siber yang telah diputus oleh pengadilan. Bahan hukum tersier berupa kamus hukum, ensiklopedia, dan bahan referensi lainnya yang mendukung pemahaman komprehensif terhadap terminologi dan konsep-konsep hukum pidana siber. Teknik pengumpulan data dilakukan melalui studi kepustakaan dengan mengidentifikasi, menginventarisasi, dan mengklasifikasikan bahan-bahan hukum yang relevan dengan permasalahan penelitian, kemudian dilanjutkan dengan analisis kualitatif untuk menginterpretasikan dan mengevaluasi substansi norma hukum serta implikasinya terhadap penegakan hukum pidana siber. Analisis data menggunakan metode deskriptif-analitis dengan memaparkan secara sistematis ketentuan hukum yang berlaku, mengidentifikasi problematika implementasi, dan merumuskan solusi hukum yang dapat diaplikasikan dalam praktik penegakan hukum untuk menghadapi tantangan kejahatan siber di era digital kontemporer.

Batasan fokus norma hukum dalam penelitian ini mencakup ketentuan substansif dan prosedural dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, khususnya Pasal 26 tentang perlindungan data pribadi, Pasal 31 tentang intersepsi atau penyadapan, Pasal 40 tentang kewenangan pemutus akses konten terlarang, Pasal 43 tentang kewenangan penyidikan khusus, serta Pasal 45, 45A, dan 45B tentang ketentuan pidana terhadap berbagai tipologi kejahatan siber, yang dianalisis dalam konteks relevansinya dengan praktik penegakan hukum kontemporer. Teknik analisis data menggunakan metode interpretasi sistematis dengan mengkaji keterkaitan antar norma hukum secara vertikal dan horizontal untuk mengidentifikasi konsistensi regulasi, interpretasi gramatikal untuk memahami makna tekstual ketentuan pidana siber, serta interpretasi teleologis untuk mengungkap tujuan pembentukan norma dalam konteks perkembangan teknologi informasi. Argumentasi yuridis dibangun melalui silogisme deduktif dengan menjadikan norma hukum sebagai premis mayor, fakta empiris tantangan penegakan hukum sebagai premis minor, dan kesimpulan berupa identifikasi

kesenjangan implementasi serta formulasi solusi hukum yang responsif. Penelitian ini juga menggunakan pendekatan komparatif terbatas dengan membandingkan kerangka hukum pidana siber Indonesia terhadap praktik terbaik (*best practices*) jurisdiksi internasional yang relevan untuk mengidentifikasi aspek-aspek yang dapat diadaptasi dalam konteks sistem hukum nasional, tanpa bermaksud melakukan transplantasi hukum secara langsung mengingat perbedaan konteks sosio-legal antar negara.

## HASIL DAN PEMBAHASAN

### Tantangan Penegakan Hukum Pidana Siber di Era Digital

Penegakan hukum pidana siber di Indonesia menghadapi berbagai tantangan fundamental yang menghambat efektivitas sistem peradilan dalam menangani kejahatan digital. Ancaman kejahatan siber di era transformasi digital telah menjadi fokus utama yang terus berkembang seiring kemudahan dan tantangan yang dibawa oleh teknologi tersebut, dimana kejahatan siber menggunakan teknologi digital dan merugikan secara materiil maupun non-materiil bagi individu, organisasi, dan negara (Saputra et al., 2024). Pengaturan hukum saat ini masih memiliki beberapa kelemahan mendasar, seperti keterbatasan sumber daya manusia yang kompeten, kurangnya fasilitas pendukung teknologi forensik digital, dan keterbatasan alokasi anggaran untuk peningkatan kapasitas penegak hukum (Alief Tanding Pamungkas et al., 2024).

Kompleksitas permasalahan semakin meningkat ketika kejahatan siber terus berkembang menjadi ancaman serius bagi stabilitas sosial dan kedaulatan negara, menciptakan kesenjangan antara kecepatan evolusi modus operandi kejahatan dengan kemampuan adaptasi sistem hukum yang ada. *Cybercrime* merupakan ancaman terbesar di era digital yang memberikan dampak kompleks terhadap individu hingga infrastruktur nasional, dengan faktor-faktor penghambat meliputi cepatnya transformasi digital, rendahnya literasi keamanan siber di kalangan masyarakat, keterbatasan regulasi yang adaptif, serta defisit tenaga ahli yang memiliki kompetensi khusus dalam bidang teknologi informasi dan keamanan siber (Virginia Valentine et al., 2024). Meskipun Indonesia telah memiliki regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik, tantangan besar masih dihadapi dalam implementasi hukum pidana siber yang memerlukan reformasi hukum adaptif serta peningkatan kapasitas aparat penegak hukum dalam menangani kasus kejahatan digital yang semakin kompleks dan canggih (Judijanto, 2025).

Dimensi transnasional kejahatan siber dan karakteristik unik bukti digital menjadi hambatan signifikan dalam proses penegakan hukum yang memerlukan pendekatan khusus berbeda dari penanganan tindak pidana konvensional. Tantangan utama dalam pembuktian kasus kejahatan siber meliputi sifat transnasional kejahatan yang melampaui batas jurisdiksi negara, anonimitas pelaku yang memanfaatkan teknologi enkripsi dan jaringan tersembunyi, volatilitas bukti digital yang mudah dimanipulasi atau dihapus, serta keterbatasan sumber daya dan keahlian penyidik dalam melakukan analisis forensik digital yang memadai (Aini & Lubis, 2024). Hasil penelitian forensik digital menunjukkan bahwa pencarian bukti-bukti digital pada perangkat android dalam keadaan unroot hanya memiliki persentase keberhasilan 40% untuk aplikasi WhatsApp dan 30% untuk aplikasi Line, namun meningkat drastis menjadi 90% pada perangkat yang telah dilakukan root, menunjukkan kompleksitas teknis dalam pengumpulan alat bukti elektronik yang valid (Prasetyawan & Indrayani, 2023).

Faktor-faktor teknis dan prosedural menyulitkan proses pengumpulan dan analisis bukti digital yang dapat diterima sebagai alat bukti sah di pengadilan, menciptakan kesenjangan antara kemampuan teknis investigasi dengan standar pembuktian yang ditetapkan dalam sistem hukum acara pidana Indonesia. Dalam proses penyelidikan kejahatan cyber crime masih terdapat hambatan atau kendala dalam pencarian tersangka, alat bukti, dan saksi, sehingga memerlukan upaya aktif dan pasif serta pelaksanaan secara tim dengan melakukan pelatihan untuk meningkatkan kemampuan personil dan komunikasi antar personal Cyber Nusantara dengan petugas Interpol yang menangani kejahatan dunia maya (Sadar et al., 2023). Meskipun terdapat upaya serius dari berbagai negara termasuk Indonesia dan Amerika dalam menangani kasus cyber crime, terdapat perbedaan signifikan dalam pendekatan hukum dan strategi penegakannya yang memerlukan harmonisasi regulasi dan peningkatan kerjasama internasional untuk mengatasi dimensi transnasional kejahatan siber secara efektif (Aditama et al., 2025).

Keterbatasan literasi keamanan siber di kalangan masyarakat dan minimnya kesadaran hukum terhadap regulasi yang mengatur kejahatan digital menjadi tantangan kultural yang menghambat upaya preventif dan represif dalam penegakan hukum pidana siber. Dalam konteks revolusi industri 5.0, masih banyak mahasiswa sebagai generasi digital yang belum bisa memanfaatkan teknologi secara bijak dan belum mengenal Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, sehingga rentan menjadi pelaku maupun korban dari berbagai bentuk cyber crime yang memanfaatkan platform digital (Elza Aida Putri et al., 2024). Penanganan *cybercrime* membutuhkan pendekatan komprehensif yang menggabungkan teknologi, hukum, pendidikan, dan kerja sama internasional untuk menciptakan ekosistem keamanan digital yang tangguh (Virginia Valentine et al., 2024).

Berdasarkan deskripsi tantangan di atas, analisis mendalam menunjukkan bahwa permasalahan penegakan hukum pidana siber di Indonesia bersifat sistemik dan saling berkaitan. Keterbatasan kapasitas SDM tidak hanya berdampak pada kemampuan teknis investigasi, tetapi juga mempengaruhi kualitas koordinasi kelembagaan dan efektivitas pembuktian di pengadilan. Rendahnya literasi keamanan siber masyarakat memperburuk situasi dengan memperluas permukaan serangan (*attack surface*) yang dapat dieksploitasi pelaku kejahatan digital. Dalam konteks Indonesia, kesenjangan antara kecepatan perkembangan teknologi dengan kapasitas adaptasi kelembagaan penegak hukum menciptakan celah struktural yang dimanfaatkan pelaku untuk mengembangkan modus operandi yang semakin canggih. Implikasinya, diperlukan pendekatan holistik yang tidak hanya memperkuat aspek regulasi, tetapi juga mengintegrasikan peningkatan kapasitas SDM, investasi infrastruktur forensik digital, dan pembangunan ekosistem keamanan siber nasional secara berkelanjutan.

Berdasarkan analisis di atas, dapat disimpulkan bahwa tantangan penegakan hukum pidana siber di Indonesia bersifat multidimensional yang mencakup keterbatasan kapasitas SDM dalam penguasaan teknologi forensik digital, fragmentasi koordinasi kelembagaan, volatilitas bukti digital yang rentan manipulasi, anonimitas pelaku yang memanfaatkan enkripsi canggih, serta minimnya literasi keamanan siber masyarakat yang memperluas eksposur risiko kejahatan digital. Kompleksitas ini diperparah oleh karakteristik transnasional kejahatan siber yang melampaui jurisdiksi nasional dan menciptakan kesulitan dalam proses investigasi lintas batas. Identifikasi tantangan komprehensif ini menjadi basis untuk mengkaji kecukupan dan efektivitas kerangka hukum yang ada dalam mengakomodasi dinamika kejahatan digital kontemporer, sekaligus merumuskan solusi strategis yang responsif terhadap evolusi teknologi dan modus operandi *cybercrime*.

**Kerangka Hukum Penegakan Pidana Siber di Indonesia**

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi instrumen hukum utama dalam pengaturan kejahatan siber di Indonesia yang memberikan landasan yuridis komprehensif bagi penegakan hukum pidana digital. Regulasi ini lahir untuk menjawab perkembangan teknologi informasi dan transaksi elektronik yang menimbulkan tantangan baru dalam penegakan hukum, dengan perubahan dilakukan karena adanya permasalahan implementasi UU ITE 2008 termasuk uji materi di Mahkamah Konstitusi terkait delik aduan, penyadapan, dan alat bukti elektronik yang memerlukan kepastian hukum lebih tinggi. (Judijanto, 2025) mengidentifikasi bahwa meskipun Indonesia telah memiliki regulasi seperti UU ITE, tantangan besar masih dihadapi dalam implementasi hukum pidana siber yang memerlukan reformasi hukum adaptif untuk mengakomodasi perkembangan teknologi dan modus operandi kejahatan yang terus berevolusi.

Pasal 26 UU No. 19 Tahun 2016 mengatur perlindungan data pribadi dengan menetapkan bahwa penggunaan data pribadi harus dengan persetujuan pemilik data, sementara penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan data yang tidak relevan atas permintaan pengguna melalui putusan pengadilan, memberikan jaminan perlindungan privasi dalam ruang digital. (Aditama et al., 2025) menambahkan perspektif komparatif bahwa pengaturan hukum pidana cyber crime di Indonesia memiliki karakteristik unik dibandingkan dengan negara lain seperti Amerika, dimana terdapat perbedaan dalam pendekatan hukum dan strategi penegakan yang memerlukan kajian mendalam untuk optimalisasi sistem hukum nasional. (Elza Aida Putri et al., 2024) menekankan pentingnya sosialisasi

dan peningkatan kesadaran hukum masyarakat terhadap UU ITE sebagai upaya preventif, mengingat masih banyak kalangan masyarakat termasuk generasi muda yang belum memahami ketentuan dan implikasi hukum dari regulasi tersebut dalam aktivitas digital sehari-hari.

Ketentuan sanksi pidana dalam UU No. 19 Tahun 2016 memberikan penegasan terhadap berbagai bentuk kejahatan siber dengan ancaman hukuman yang tegas untuk menciptakan efek jera bagi pelaku kejahatan digital. Pasal 45 mengatur pidana bagi pelanggaran konten elektronik dimana muatan kesusilaan dan perjudian diancam dengan penjara maksimal 6 tahun atau denda Rp1 miliar, sementara penghinaan atau pencemaran nama baik sebagai delik aduan diancam penjara maksimal 4 tahun atau denda Rp750 juta, dan pemerasan atau pengancaman melalui media elektronik diancam penjara maksimal 6 tahun atau denda Rp1 miliar. Pasal 45A secara khusus mengatur penyebaran berita bohong atau menyesatkan dan ujaran kebencian berbasis SARA dengan ancaman penjara maksimal 6 tahun atau denda Rp1 miliar, menunjukkan keseriusan negara dalam melindungi masyarakat dari dampak negatif penyalahgunaan teknologi informasi.

Pasal 45B mengatur ancaman kekerasan atau menakut-nakuti melalui media elektronik dengan pidana penjara maksimal 4 tahun atau denda Rp750 juta, memberikan perlindungan hukum terhadap korban cyberbullying dan intimidasi digital yang semakin marak terjadi. (Saputra et al., 2024) mengidentifikasi bahwa meskipun sanksi pidana telah diatur secara komprehensif, implementasi penegakan hukum masih menghadapi kendala dalam hal pembuktian dan proses penyelidikan yang memerlukan keahlian teknis khusus dalam forensik digital dan analisis bukti elektronik. (Alief Tanding Pamungkas et al., 2024) menambahkan bahwa efektivitas sanksi pidana tidak hanya bergantung pada ketegasan ancaman hukuman, namun juga pada kapasitas sistem peradilan dalam mengungkap, membuktikan, dan memproses kasus kejahatan siber secara profesional dan akuntabel. (Virginia Valentine et al., 2024) menekankan perlunya sinergi antara penegakan hukum represif melalui sanksi pidana dengan upaya preventif melalui edukasi publik dan penguatan infrastruktur keamanan siber nasional untuk menciptakan ekosistem digital yang aman dan kondusif bagi perkembangan ekonomi dan sosial masyarakat.

Berdasarkan analisis kerangka hukum di atas, dapat disimpulkan bahwa Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah memberikan landasan yuridis komprehensif bagi penegakan hukum pidana siber di Indonesia melalui pengaturan sanksi pidana yang tegas, kewenangan penyidikan khusus, dan mekanisme perlindungan data pribadi. Namun, implementasi regulasi ini menghadapi kendala multidimensional yang meliputi kesenjangan antara norma hukum dengan kapasitas kelembagaan, keterbatasan prosedur teknis forensik digital, dan minimnya koordinasi antar lembaga penyidik. Efektivitas kerangka hukum tidak hanya ditentukan oleh ketegasan sanksi pidana, tetapi juga oleh kemampuan sistem peradilan dalam mengadaptasi perkembangan teknologi dan modus operandi kejahatan digital yang terus berevolusi. Temuan ini menjadi landasan untuk merumuskan solusi strategis yang tidak hanya fokus pada penyempurnaan regulasi, tetapi juga pada penguatan kapasitas kelembagaan dan infrastruktur pendukung penegakan hukum pidana siber.

**Solusi Strategis Penguatan Penegakan Hukum Pidana Siber**

Peningkatan kapasitas sumber daya manusia penegak hukum melalui pendidikan, pelatihan berkelanjutan, dan sertifikasi kompetensi khusus dalam bidang teknologi informasi dan forensik digital menjadi solusi fundamental untuk mengatasi keterbatasan kemampuan teknis dalam penanganan kasus kejahatan siber. (Alief Tanding Pamungkas et al., 2024) menekankan perlunya peningkatan kapasitas penegak hukum melalui pelatihan dan penyediaan teknologi yang lebih canggih, alokasi anggaran yang lebih besar, serta penguatan kerjasama internasional untuk menanggulangi kejahatan lintas batas yang memerlukan koordinasi multi-jurisdiksi dalam proses investigasi dan penuntutan. (Virginia Valentine et al., 2024) menambahkan bahwa solusi strategis mencakup penguatan infrastruktur teknologi keamanan siber, edukasi publik yang masif dan berkelanjutan, kolaborasi global antar negara dan lembaga internasional, pengembangan sumber daya manusia yang kompeten, serta pemanfaatan artificial intelligence dalam deteksi dan pencegahan ancaman secara proaktif untuk mengantisipasi perkembangan modus operandi kejahatan yang semakin canggih.

(Sadar et al., 2023) mengidentifikasi bahwa upaya yang efektif meliputi pelaksanaan investigasi secara tim dengan melakukan pelatihan untuk meningkatkan kemampuan personil dan secara teknis

melakukan komunikasi antar personal Cyber Nusantara dengan petugas Interpol, menunjukkan pentingnya koordinasi lintas lembaga baik nasional maupun internasional dalam penanganan kasus kejahatan siber yang kompleks. (Judijanto, 2025) menekankan bahwa diperlukan reformasi hukum yang adaptif terhadap perkembangan teknologi serta peningkatan kapasitas aparat penegak hukum dalam menangani kasus kejahatan digital, yang tidak hanya fokus pada aspek teknis namun juga pemahaman komprehensif terhadap regulasi dan prosedur hukum yang berlaku. (Aini & Lubis, 2024) menambahkan bahwa peningkatan kapasitas penegak hukum harus disertai dengan penyediaan fasilitas dan infrastruktur pendukung yang memadai, termasuk laboratorium forensik digital yang terstandarisasi, perangkat lunak dan perangkat keras investigasi yang mutakhir, serta akses terhadap database dan informasi intelijen kejahatan siber yang terintegrasi secara nasional dan internasional. (Prasetyawan & Indrayani, 2023) memperkuat argumen dengan menekankan pentingnya peningkatan kemampuan analisis forensik digital menggunakan framework yang diakui secara internasional seperti National Institute of Justice untuk memastikan bukti digital yang dikumpulkan memiliki validitas dan dapat diterima dalam proses peradilan, sehingga tidak terjadi kegagalan dalam proses pembuktian yang dapat menyebabkan lepasnya pelaku kejahatan dari jerat hukum.

Penguatan regulasi dan harmonisasi peraturan perundang-undangan terkait kejahatan siber dengan mempertimbangkan perkembangan teknologi dan modus operandi kejahatan yang terus berevolusi menjadi kunci dalam menciptakan kepastian hukum dan efektivitas penegakan hukum pidana digital. (Aditama et al., 2025) mengidentifikasi bahwa perbandingan hukum pidana cyber crime antara Indonesia dan Amerika menunjukkan perbedaan dalam pendekatan hukum dan strategi penegakan yang dapat menjadi pembelajaran untuk perbaikan sistem hukum nasional, dimana diperlukan adaptasi best practices internasional dengan mempertimbangkan konteks hukum dan sosial budaya Indonesia.

(Saputra et al., 2024) menekankan pentingnya pembentukan regulasi efektif yang tidak hanya berfokus pada aspek represif namun juga preventif, dengan mengintegrasikan kerjasama antara pemerintah, otoritas keamanan, dan masyarakat dalam ekosistem keamanan siber nasional yang komprehensif dan responsif terhadap ancaman yang dinamis. (Judijanto, 2025) menambahkan bahwa reformasi hukum yang adaptif harus mampu mengantisipasi perkembangan teknologi seperti artificial intelligence, blockchain, dan Internet of Things yang membawa tantangan baru dalam definisi dan kategorisasi tindak pidana siber serta mekanisme pembuktiannya dalam sistem peradilan. Pasal 40 UU No. 19 Tahun 2016 memberikan kewenangan kepada pemerintah untuk memutus akses terhadap konten bermuatan terlarang seperti pornografi, perjudian, ujaran kebencian, dan berita bohong, namun implementasinya memerlukan mekanisme yang transparan dan akuntabel untuk menghindari penyalahgunaan kewenangan yang dapat mengancam kebebasan berekspresi dan akses informasi publik.

(Alief Tanding Pamungkas et al., 2024) mengidentifikasi bahwa penguatan regulasi harus disertai dengan peningkatan mekanisme pengawasan dan evaluasi implementasi peraturan perundang-undangan, sehingga dapat diidentifikasi kelemahan dan celah hukum yang perlu diperbaiki untuk meningkatkan efektivitas penegakan hukum dalam menangani kejahatan siber yang semakin kompleks dan canggih. (Virginia Valentine et al., 2024) menekankan bahwa regulasi adaptif harus mampu mengakomodasi kebutuhan perlindungan masyarakat dari ancaman kejahatan siber sekaligus memberikan ruang bagi inovasi teknologi dan pengembangan ekonomi digital yang berkelanjutan, sehingga diperlukan pendekatan yang seimbang antara kepentingan keamanan dengan kepentingan pembangunan ekonomi digital nasional.

Pembangunan ekosistem keamanan siber nasional yang terintegrasi melalui kolaborasi multi-stakeholder, peningkatan literasi keamanan siber masyarakat, dan pemanfaatan teknologi canggih dalam deteksi dan pencegahan kejahatan digital menjadi strategi holistik untuk menanggulangi ancaman *cybercrime* secara komprehensif. (Elza Aida Putri et al., 2024) mengidentifikasi urgensi peningkatan kesadaran hukum masyarakat khususnya generasi muda melalui edukasi tentang penggunaan teknologi secara bijak dan pemahaman terhadap UU ITE untuk mencegah terjadinya tindak pidana cyber crime, baik sebagai pelaku maupun korban dari kejahatan digital yang memanfaatkan kerentanan literasi digital masyarakat. (Saputra et al., 2024) menambahkan bahwa fokus pada peningkatan keamanan teknologi informasi dan literasi keamanan siber di kalangan masyarakat menjadi langkah kunci dalam mengantisipasi dan mencegah dampak buruk kejahatan siber, dengan melibatkan partisipasi aktif dari berbagai pihak termasuk sektor pendidikan, industri teknologi, dan organisasi masyarakat sipil.

(Virginia Valentine et al., 2024) menekankan bahwa solusi komprehensif memerlukan integrasi lintas sektor dengan menggabungkan teknologi kecerdasan buatan dan analitik data besar dalam sistem pertahanan siber nasional, pendekatan edukatif yang efektif dalam meningkatkan kesadaran publik, serta kolaborasi global dalam pertukaran informasi intelijen dan penanganan kasus kejahatan siber transnasional. (Fithri et al., 2022) menambahkan perspektif bahwa penanganan modus kejahatan yang memanfaatkan celah sistem memerlukan penguatan kebijakan terkait dan partisipasi aktif dari masyarakat dalam melaporkan indikasi kejahatan serta memberikan informasi yang dapat membantu proses penegakan hukum. (Aini & Lubis, 2024) mengidentifikasi bahwa kerjasama internasional yang solid menjadi prasyarat dalam mengatasi dimensi transnasional kejahatan siber, termasuk mutual legal assistance, ekstradisi pelaku kejahatan lintas negara, dan harmonisasi regulasi untuk memfasilitasi proses investigasi dan penuntutan yang melibatkan multiple jurisdictions. (Alief Tanding Pamungkas et al., 2024) menekankan bahwa pembangunan ekosistem keamanan siber yang tangguh memerlukan komitmen jangka panjang dari pemerintah dalam alokasi anggaran yang memadai, pengembangan infrastruktur teknologi yang modern, serta penciptaan iklim kondusif bagi kolaborasi antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil dalam mewujudkan ruang digital yang aman, adil, dan berkelanjutan bagi seluruh lapisan masyarakat Indonesia.

**Optimalisasi Mekanisme Koordinasi Kelembagaan dalam Penegakan Hukum Pidana Siber**

Kompleksitas penanganan kejahatan siber di Indonesia memerlukan sinergitas kelembagaan yang optimal antara berbagai instansi penegak hukum, regulator, dan stakeholder terkait untuk menciptakan sistem yang responsif dan efektif dalam menghadapi dinamika ancaman digital yang terus berkembang. (Sadar et al., 2023) mengidentifikasi bahwa pelaksanaan penyidikan kejahatan cyber crime memerlukan komunikasi antar personal Cyber Nusantara dengan petugas Interpol, menunjukkan pentingnya koordinasi lintas lembaga dalam mengatasi dimensi transnasional kejahatan digital yang melampaui batas juridiksi nasional. Ketidakselarasan mekanisme koordinasi antar institusi penegak hukum seringkali menjadi penghambat signifikan dalam proses penyelidikan dan penuntutan kasus *cybercrime*, dimana setiap lembaga memiliki kewenangan, prosedur, dan pendekatan yang berbeda dalam menangani permasalahan kejahatan siber yang sama.

(Judijanto, 2025) menekankan bahwa implementasi hukum pidana siber memerlukan reformasi hukum adaptif serta peningkatan kapasitas aparat penegak hukum yang tidak hanya fokus pada aspek teknis individual namun juga pada harmonisasi sistem kerja antar lembaga. (Alief Tanding Pamungkas et al., 2024) menguatkan argumen tersebut dengan mengidentifikasi bahwa penguatan kerjasama internasional menjadi kebutuhan mendesak dalam menanggulangi kejahatan lintas batas yang memerlukan koordinasi multi-jurisdiksi dengan standar operasional prosedur yang terstandarisasi. (Aini & Lubis, 2024) menambahkan bahwa kerjasama internasional yang solid menjadi prasyarat dalam mengatasi dimensi transnasional kejahatan siber, termasuk mutual legal assistance dan harmonisasi regulasi untuk memfasilitasi proses investigasi yang melibatkan multiple jurisdictions secara simultan dan terkoordinasi.

Fragmentasi kewenangan antara Kepolisian, Kejaksaan, dan lembaga-lembaga khusus seperti Badan Siber dan Sandi Negara dalam penanganan kejahatan siber memerlukan reformulasi mekanisme koordinasi yang lebih sistematis dan terintegrasi untuk menghindari tumpang tindih fungsi dan optimalisasi pemanfaatan sumber daya yang terbatas. (Prasetyawan & Indrayani, 2023) mengungkapkan bahwa melakukan tindakan mobile forensik dan digital forensik memerlukan koordinasi yang erat antara penyidik lapangan dengan ahli teknologi forensik untuk memastikan validitas bukti digital yang dikumpulkan sesuai dengan standar internasional yang berlaku. (Saputra et al., 2024) mengidentifikasi bahwa penegakan hukum terhadap kejahatan siber memerlukan sinergi antara pemerintah, otoritas keamanan, dan masyarakat sebagai langkah kunci dalam mengantisipasi ancaman, dimana koordinasi kelembagaan menjadi fondasi utama dalam mengintegrasikan berbagai upaya preventif dan represif secara holistik.

(Virginia Valentine et al., 2024) memperkuat temuan tersebut dengan menekankan bahwa penanganan *cybercrime* membutuhkan pendekatan komprehensif yang menggabungkan teknologi, hukum, pendidikan, dan kerja sama internasional melalui mekanisme koordinasi yang efektif dan berkelanjutan. Kelembagaan yang terkoordinasi secara optimal dapat mengatasi kendala teknis seperti yang diidentifikasi (Kurniawan et al., 2022) mengenai keterbatasan penguasaan teknologi informasi oleh

penyidik dan lemahnya koordinasi antara aparat penegak hukum dengan provider dan masyarakat. (Judijanto, 2025) menambahkan bahwa reformasi kelembagaan harus mampu mengakomodasi perkembangan teknologi dan modus operandi kejahatan yang dinamis melalui pembentukan task force khusus yang terdiri dari multidisiplin expertise dengan kewenangan koordinatif yang jelas dan akuntabel.

Pembentukan sistem informasi terintegrasi dan pusat komando terpadu (command center) untuk koordinasi real-time antar lembaga penegak hukum menjadi solusi strategis dalam mengoptimalkan respons terhadap kejahatan siber yang memerlukan penanganan cepat dan presisi tinggi dengan memanfaatkan teknologi informasi sebagai enabler koordinasi kelembagaan. (Elza Aida Putri et al., 2024) mengidentifikasi pentingnya pemanfaatan teknologi secara bijak dalam konteks revolusi industri 5.0, dimana sistem koordinasi kelembagaan harus mampu mengadaptasi perkembangan teknologi untuk meningkatkan efektivitas penanganan kasus kejahatan siber secara real-time dan terintegrasi. (Fithri et al., 2022) menambahkan perspektif bahwa penanganan modus kejahatan yang kompleks memerlukan partisipasi aktif dari masyarakat dalam melaporkan indikasi kejahatan, yang hanya dapat dioptimalkan melalui sistem koordinasi yang memfasilitasi alur informasi yang efisien dari masyarakat ke berbagai lembaga penegak hukum terkait.

(Virginia Valentine et al., 2024) menekankan bahwa pemanfaatan artificial intelligence dalam deteksi dan pencegahan ancaman secara proaktif memerlukan integrasi sistem antar lembaga untuk memungkinkan sharing data dan intelligence secara real-time dengan tetap memperhatikan aspek keamanan dan privasi informasi. (Aditama et al., 2025) mengidentifikasi bahwa pembelajaran dari best practices negara lain seperti Amerika dalam koordinasi kelembagaan dapat menjadi referensi untuk mengoptimalkan sistem koordinasi nasional dengan adaptasi sesuai konteks hukum dan kelembagaan Indonesia. (Alief Tanding Pamungkas et al., 2024) menegaskan bahwa pembangunan ekosistem koordinasi kelembagaan yang tangguh memerlukan komitmen jangka panjang dalam alokasi anggaran yang memadai untuk pengembangan infrastruktur teknologi koordinasi, standardisasi prosedur operasional, dan penciptaan iklim kondusif bagi kolaborasi efektif antar lembaga dalam mewujudkan penegakan hukum pidana siber yang profesional dan akuntabel di era digital kontemporer.

**Implikasi Praktis dan Teoretis Penelitian**

Implikasi praktis penelitian ini memberikan kontribusi signifikan bagi pengembangan kebijakan hukum pidana siber di Indonesia melalui formulasi rekomendasi strategis yang dapat diimplementasikan oleh instansi penegak hukum dan pembuat kebijakan dalam meningkatkan efektivitas penanganan *cybercrime*. Temuan penelitian mengenai keterbatasan kapasitas sumber daya manusia penegak hukum dalam penguasaan teknologi forensik digital dapat menjadi landasan bagi Kepolisian dan Kejaksaan dalam merancang program pelatihan berkelanjutan dan sertifikasi kompetensi khusus yang terstandarisasi sesuai dengan perkembangan teknologi informasi kontemporer. (Saputra et al., 2024) mengidentifikasi bahwa penegakan hukum terhadap kejahatan siber memerlukan perhatian nasional yang fokus pada peningkatan keamanan teknologi informasi dan literasi keamanan siber, dimana rekomendasi penelitian ini dapat dioperasionalisasikan melalui pembentukan kurikulum pelatihan yang komprehensif dan berkelanjutan.

Implikasi akademis penelitian ini mendorong pengembangan agenda riset masa depan dalam bidang hukum pidana siber yang dapat dieksplorasi melalui pendekatan empiris, komparatif, dan eksperimental untuk memperdalam pemahaman terhadap dinamika kejahatan digital dan efektivitas instrumen hukum dalam era transformasi teknologi yang accelerated. Temuan penelitian mengenai keterbatasan regulasi dalam mengantisipasi evolusi modus operandi *cybercrime* membuka peluang penelitian lanjutan tentang adaptive law-making dan responsive regulation dalam konteks teknologi disruptive seperti artificial intelligence, blockchain, dan quantum computing yang berpotensi menciptakan tantangan baru dalam penegakan hukum pidana siber. (Sadar et al., 2023) mengidentifikasi pentingnya komunikasi antar personal dalam investigasi *cybercrime*, dimana penelitian ini dapat dikembangkan lebih lanjut melalui studi empiris tentang efektivitas protokol koordinasi kelembagaan dan dampaknya terhadap tingkat keberhasilan penyelesaian kasus kejahatan siber di berbagai tingkat jurisdiksi.

**SIMPULAN**

Kompleksitas penegakan hukum pidana siber di Indonesia menghadapi tantangan multidimensional yang meliputi keterbatasan kapasitas sumber daya manusia penegak hukum

dalam penguasaan teknologi forensik digital, fragmentasi koordinasi kelembagaan yang menghambat efektivitas penyelidikan transnasional, serta minimnya literasi keamanan siber masyarakat yang memperburuk proliferasi kejahatan digital dalam ekosistem teknologi informasi kontemporer. Kerangka hukum yang direpresentasikan oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah memberikan landasan yuridis komprehensif dengan sanksi pidana yang tegas, namun implementasinya masih terkendala oleh volatilitas bukti digital, anonimitas pelaku yang memanfaatkan teknologi enkripsi canggih, serta keterbatasan infrastruktur forensik yang memadai untuk mengakomodasi karakteristik unik *cybercrime* yang berbeda fundamental dengan tindak pidana konvensional. Dimensi transnasional kejahatan siber yang melampaui jurisdiksi nasional memerlukan harmonisasi regulasi internasional dan penguatan mekanisme mutual legal assistance untuk mengatasi hambatan investigasi lintas batas yang sering menjadi celah bagi pelaku dalam menghindari jerat hukum melalui eksploitasi perbedaan sistem hukum antar negara.

Solusi strategis yang diperlukan mencakup peningkatan kapasitas sumber daya manusia melalui pendidikan berkelanjutan dan sertifikasi kompetensi khusus dalam bidang teknologi informasi, reformulasi mekanisme koordinasi kelembagaan yang terintegrasi dengan pemanfaatan sistem informasi real-time untuk optimalisasi respons terhadap ancaman siber, serta pembangunan ekosistem keamanan siber nasional yang mensinergikan upaya preventif dan represif melalui kolaborasi multi-stakeholder antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil. Penguatan regulasi adaptif yang mampu mengantisipasi evolusi teknologi dan modus operandi kejahatan digital menjadi prasyarat fundamental dalam menciptakan kepastian hukum dan efektivitas penegakan hukum pidana siber, disertai dengan investasi infrastruktur teknologi forensik yang terstandarisasi internasional dan peningkatan literasi keamanan siber masyarakat sebagai benteng pertahanan pertama dalam menghadapi ancaman *cybercrime*. Implementasi solusi holistik ini memerlukan komitmen jangka panjang dari seluruh elemen bangsa dalam mewujudkan ruang digital yang aman, adil, dan berkelanjutan sebagai fondasi pembangunan ekonomi digital nasional yang berdaya saing tinggi di era transformasi teknologi informasi global yang semakin dinamis dan kompleks.

## DAFTAR PUSTAKA

Aditama, P., Sinaga, E. A., & Putri, C. A. (2025). Perbandingan Hukum Pidana Cyber Crime Dan Pengaruhnya Dalam Penegakan Hukum Antara Indonesia Dan Amerika Comparison of Cyber Crime Criminal Law and Its Impact on Law Enforcement Between Indonesia and America. *Jurnal Kompilasi Hukum*, *10*(1), 58–76. https://jkh.unram.ac.id/index.php/jkh/article/view/202

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *05*(02), 55–63. http://www.journal.cattleyadf.org/index.php/Judge/article/view/566%0Ahttp://www.journal.cattleyadf.org/index.php/Judge/article/download/566/433

Alief Tanding Pamungkas, Andi Muliyono, & Nurjana Lahangatubun. (2024). The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions. *DELICTUM : Jurnal Hukum Pidana Islam*, *2*(2), 71–83. https://doi.org/10.35905/delictum.v2i2.10613

Elza Aida Putri, F., Wedhatami, B., Suran Ningsih, A., Nurul Anggaretno, S. W., Sijbat, S., Fadilah, G., Monica Sari, A., Rusyiana, R., Sinta, D., & Fatika Sari, C. (2024). Peran Mahasiswa UNNES Menjadi Smart & Good Citizen dalam Menghadapi Revolusi Industri 5.0. *Jurnal Pengabdian Kepada Masyarakat Nusantara*, *5*(1), 1147–1152. https://doi.org/10.55338/jpkmn.v5i1.2695

Fithri, B. S., Wahyuni, W. S., & Kartika, A. (2022). Modus Pemanfaatan Koperasi dalam Tindak Pidana Pencucian Uang. *ARBITER: Jurnal Ilmiah Magister Hukum*, *4*(1), 105–113. https://doi.org/10.31289/arbiter.v4i1.617

Ginara, I. G. K., Widyantara, I. M. M., & Styawati, N. K. A. (2022). Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia. *Jurnal Preferensi Hukum*, *3*(1), 138–142. https://doi.org/10.22225/jph.3.1.4673.138-142

I Made Gede Adi Arya Natih, Anak Agung Sagung Laksmi Dewi, & I Gusti Agung Ayu Gita Pritayanti Dinar. (2022). Sanksi Pidana Bagi Pelaku Penipuan Dengan Modus Investasi Online. *Jurnal Preferensi Hukum*, *3*(3), 501–507. https://doi.org/10.55637/jph.3.3.5598.501-507

Januri, J., Melati, D. P., & Muhadi, M. (2022). Upaya Kepolisian Dalam Penanggulangan Kejahatan Cyber Terorganisir. *Audi Et AP : Jurnal Penelitian Hukum*, *1*(02), 94–100.

https://doi.org/10.24967/jaeap.v1i02.1692

Jondong, Z. (2020). Kebijakan Hukum Pidana bagi Tindak Pidana Cyber Terrorism dalam Rangka Pembentukan Hukum Positif di Indonesia. *Jurnal Preferensi Hukum*, *1*(2), 21–27. https://doi.org/10.22225/jph.1.2.2337.21-27

Judijanto, L. (2025). *Hukum Pidana dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital di Era Teknologi*. *5*, 1079–1085. https://www.irje.org/irje/article/view/2114

Kesuma, I. G. M. J., Widiati, I. A. P., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Penipuan Melalui Media Elektronik. *Jurnal Preferensi Hukum*, *1*(2), 72–77. https://doi.org/10.22225/jph.1.2.2345.72-77

Kurniawan, Y., Siregar, T., & Hidayani, S. (2022). Penegakan Hukum Oleh Polri Terhadap Pelaku Tindak Pidana Judi Online (Studi Pada Kepolisian Daerah Sumatera Utara). *ARBITER: Jurnal Ilmiah Magister Hukum*, *4*(1), 28–44. https://doi.org/10.31289/arbiter.v4i1.1203

Pande Putu Rastika Paramartha, Anak Agung Sagung Laksmi Dewi, & I Putu Gede Seputra. (2021). Sanksi Pidana terhadap Para Pemasang dan Promosi Iklan Bermuatan Konten Judi Online. *Jurnal Preferensi Hukum*, *2*(1), 156–160. https://doi.org/10.22225/jph.2.1.3062.156-160

Prasetyawan, R., & Indrayani, R. (2023). Analisis dan Recovery Bukti Digital pada Media Sosial di Perangkat Mobile Berbasis Android. *Explore*, *13*(2), 74–78. https://doi.org/10.35200/ex.v13i2.29

Purwanti, Y., Rachman, F., Gunawan, T., & Kartadinata, A. (2023). Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Daerah Lampung. *Audi Et AP : Jurnal Penelitian Hukum*, *2*(01), 64–71. https://doi.org/10.24967/jaeap.v2i01.2088

Sadar, A., Oner, B., & Almusawir. (2023). *Pelaksanaa Penegakan Hukum Tindak Pidana Cyber Crime Terhadap Pelaku Kejahatan Informasi Data Pribadi*. 382–390.

Saputra, A., Kristiawanto, K., & Ismed, M. (2024). Rekonstruksi Penegakan Hukum Tindak Pidana Siber di Indonesia. *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum*, *3*(1), 63–70. https://doi.org/10.55681/seikat.v3i1.1186

Sugiyono. (2020). *Metodologi Penelitian Kuantitatif, Kualitatif dan R & D*.

Virginia Valentine, Septiani, C. S., & Parshusip, J. (2024). Menghadapi Tantangan Dan Solusi Cybercrime Di Era Digital. *Jurnal Informatika Dan Komputer*, *1*(2), 152–156.