ULIL ALBAB : Jurnal Ilmiah Multidisiplin
Vol.5, No.9, Agustus 2026

Kejahatan Siber dan Respons Hukum Pidana di Era Transformasi Digital: Analisis Normatif terhadap Penegakan Hukum di Indonesia

Ruliyanando Gondo Suhandito
Universitas Widya Mataram, Yogyakarta, Indonesia
E-mail: suhanditoruliyanando21@gmail.com

Article History:
Received: 16 Juli 2026
Revised: 19 Juli 2026
Accepted: 02 Agustus 2026

Keywords: *Kejahatan Siber, Hukum Pidana, Teknologi Informasi, UU ITE, Penegakan Hukum*

Abstrak: *Perkembangan teknologi informasi yang pesat membawa dampak signifikan terhadap pola kejahatan modern. Kejahatan siber (cybercrime) kini menjadi ancaman serius yang melampaui batas-batas yurisdiksi konvensional dan menantang sistem hukum pidana yang ada. Penelitian ini bertujuan untuk menganalisis dua permasalahan utama: pertama, bagaimana hukum pidana Indonesia merespons perkembangan kejahatan siber; dan kedua, bagaimana efektivitas penegakan hukum pidana terhadap pelaku kejahatan siber di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE), masih terdapat sejumlah kekosongan hukum dan tantangan dalam penegakannya. Diperlukan reformasi regulasi yang komprehensif, peningkatan kapasitas aparat penegak hukum, serta kerjasama internasional yang lebih erat untuk menghadapi ancaman kejahatan siber yang terus berkembang.*

PENDAHULUAN

Revolusi digital yang terjadi sejak akhir abad ke-20 telah mengubah hampir seluruh aspek kehidupan manusia secara fundamental. Internet, yang awalnya hanya merupakan jaringan komunikasi militer dan akademis, kini telah bertransformasi menjadi infrastruktur vital yang menopang kehidupan ekonomi, sosial, dan politik global. Di Indonesia, penetrasi internet terus mengalami pertumbuhan yang luar biasa. Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2024, lebih dari 221 juta penduduk Indonesia atau sekitar 79,5 persen dari total populasi telah terhubung dengan internet, menjadikan Indonesia sebagai salah satu pasar digital terbesar di Asia Tenggara. Namun demikian, perkembangan teknologi informasi yang pesat ini ibarat pedang bermata dua. Di satu sisi, teknologi digital membuka peluang tak terbatas bagi pembangunan ekonomi, kemajuan ilmu pengetahuan, dan peningkatan kualitas hidup masyarakat. Di sisi lain, teknologi yang sama juga dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan berbagai bentuk kejahatan baru yang sebelumnya tidak terbayangkan dalam sistem hukum konvensional. Kejahatan siber (cybercrime) telah berkembang menjadi

fenomena kriminal yang kompleks, lintas batas, dan terus berevolusi mengikuti perkembangan teknologi itu sendiri (Fadly et al., 2025).

Indonesia, sebagai negara dengan jumlah pengguna internet yang besar, menghadapi ancaman kejahatan siber yang semakin serius dari tahun ke tahun. Badan Siber dan Sandi Negara (BSSN) mencatat terdapat lebih dari 2,2 miliar anomali trafik yang terindikasi sebagai serangan siber sepanjang tahun 2023. Jenis kejahatan yang terjadi pun sangat beragam, mulai dari penipuan daring, pencurian data pribadi, peretasan sistem informasi, penyebaran konten ilegal, hingga serangan terhadap infrastruktur kritis negara. Kerugian finansial akibat kejahatan siber di Indonesia diperkirakan mencapai miliaran rupiah setiap tahunnya, belum termasuk kerugian non-materiil seperti kerusakan reputasi dan gangguan terhadap kepercayaan publik. Menghadapi tantangan ini, sistem hukum pidana Indonesia dituntut untuk beradaptasi dan merespons secara efektif. Indonesia telah memiliki Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016, dan terakhir diperbarui melalui Undang-Undang Nomor 1 Tahun 2024. Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) yang baru sebagaimana termuat dalam Undang-Undang Nomor 1 Tahun 2023 juga telah mengakomodasi beberapa ketentuan terkait kejahatan siber. Namun, efektivitas regulasi-regulasi tersebut dalam menghadapi dinamika kejahatan siber yang terus berkembang masih menjadi perdebatan di kalangan akademisi dan praktisi hukum (Gladys & Bella, 2025).

Berdasarkan latar belakang tersebut, penelitian ini merumuskan dua permasalahan pokok yang akan dianalisis. Pertama, bagaimana hukum pidana Indonesia merespons perkembangan kejahatan siber ditinjau dari perspektif regulasi yang ada? Kedua, bagaimana efektivitas penegakan hukum pidana terhadap pelaku kejahatan siber di Indonesia dan apa saja faktor-faktor yang mempengaruhinya? Dua rumusan masalah ini dipilih karena dianggap paling representatif dalam mencerminkan hubungan antara perkembangan teknologi informasi dengan sistem hukum pidana Indonesia saat ini (Nai & Hoesein, 2026).

LANDASAN TEORI

1. Teori Kejahatan Siber (Cybercrime)

Kejahatan siber (cybercrime) merupakan bentuk kejahatan yang memanfaatkan teknologi informasi, sistem elektronik, jaringan komputer, dan internet sebagai sarana, sasaran, maupun alat untuk melakukan suatu tindak pidana. Perkembangan teknologi digital yang sangat pesat telah mengubah pola kehidupan masyarakat, baik dalam bidang ekonomi, pendidikan, pemerintahan, maupun komunikasi. Di sisi lain, kemajuan tersebut juga membuka peluang munculnya berbagai bentuk kejahatan baru yang memiliki karakteristik berbeda dengan kejahatan konvensional. Cybercrime tidak lagi dibatasi oleh wilayah geografis sehingga pelaku dapat melakukan tindakan melawan hukum dari lokasi yang berbeda dengan korban maupun tempat terjadinya akibat hukum. Karakteristik tersebut menjadikan kejahatan siber sebagai salah satu tantangan terbesar dalam sistem hukum pidana modern. Secara konseptual, cybercrime mencakup berbagai bentuk tindak pidana yang dilakukan melalui penggunaan teknologi digital. Bentuk-bentuk tersebut meliputi peretasan (hacking), penyebaran malware, pencurian identitas (identity theft), penipuan daring (online fraud), penyebaran berita bohong (hoaks), perjudian daring, serangan ransomware, pencurian data pribadi, hingga penyebaran konten ilegal melalui media elektronik. Seiring berkembangnya teknologi kecerdasan buatan (Artificial Intelligence/AI), muncul pula bentuk kejahatan baru seperti pembuatan deepfake, manipulasi identitas digital, dan serangan otomatis berbasis AI. Ragam bentuk cybercrime menunjukkan bahwa ruang siber telah menjadi lingkungan yang rentan terhadap penyalahgunaan teknologi untuk kepentingan kriminal (Fadly et al., 2025).

Dalam perspektif kriminologi, cybercrime dipandang sebagai kejahatan yang berkembang akibat perubahan sosial dan transformasi digital masyarakat. Modernisasi teknologi menciptakan peluang (opportunity) yang semakin besar bagi pelaku untuk melakukan tindak pidana dengan risiko yang relatif rendah. Pelaku dapat menyamarkan identitas menggunakan virtual private network (VPN), enkripsi, akun anonim, maupun server yang berada di luar yurisdiksi negara korban. Kondisi tersebut menyebabkan proses identifikasi pelaku, pengumpulan alat bukti elektronik, dan penegakan hukum menjadi jauh lebih kompleks dibandingkan dengan kejahatan konvensional. Kejahatan siber juga memiliki dampak yang sangat luas terhadap berbagai aspek kehidupan masyarakat. Dampak ekonomi muncul melalui kerugian finansial akibat pencurian dana, penipuan transaksi elektronik, maupun serangan terhadap sistem perbankan. Dampak sosial terlihat dari meningkatnya penyebaran ujaran kebencian, hoaks, cyberbullying, dan eksploitasi digital yang berpotensi mengganggu ketertiban umum. Selain itu, cybercrime dapat mengancam keamanan nasional melalui serangan terhadap infrastruktur vital, sistem pemerintahan elektronik, maupun kebocoran data strategis negara. Oleh karena itu, cybercrime tidak lagi dipandang sebagai kejahatan individu semata, tetapi telah berkembang menjadi ancaman multidimensional (Gladys & Bella, 2025).

Di Indonesia, perkembangan cybercrime mengalami peningkatan seiring dengan meningkatnya penggunaan internet dan transformasi digital di berbagai sektor. Digitalisasi layanan publik, perdagangan elektronik, media sosial, dan sistem pembayaran elektronik memperluas ruang interaksi masyarakat, namun pada saat yang sama meningkatkan potensi terjadinya tindak pidana siber. Berbagai laporan menunjukkan bahwa kasus pencurian data pribadi, penipuan digital, serangan ransomware, hingga penyalahgunaan media sosial terus mengalami peningkatan dalam beberapa tahun terakhir. Kondisi tersebut menunjukkan bahwa perkembangan teknologi harus diimbangi dengan peningkatan kapasitas regulasi, pengawasan, serta literasi digital masyarakat. Dengan demikian, teori cybercrime menjadi landasan penting dalam penelitian ini karena memberikan pemahaman mengenai karakteristik, bentuk, penyebab, dan dampak kejahatan siber di era transformasi digital. Teori ini menjelaskan bahwa perkembangan teknologi tidak hanya menghasilkan inovasi yang bermanfaat, tetapi juga melahirkan berbagai modus operandi kejahatan baru yang memerlukan respons hukum yang adaptif. Oleh sebab itu, pemahaman terhadap konsep cybercrime menjadi dasar dalam menganalisis efektivitas penegakan hukum pidana terhadap berbagai bentuk kejahatan siber di Indonesia (Nai & Hoesein, 2026).

2. Teori Penegakan Hukum Pidana

Penegakan hukum pidana merupakan proses untuk mewujudkan norma hukum pidana agar dapat diterapkan secara efektif dalam kehidupan masyarakat. Menurut Soerjono Soekanto, penegakan hukum dipengaruhi oleh lima faktor utama, yaitu substansi hukum, aparat penegak hukum, sarana dan prasarana, masyarakat, serta budaya hukum. Kelima faktor tersebut saling berkaitan sehingga keberhasilan penegakan hukum tidak hanya ditentukan oleh kualitas peraturan perundang-undangan, tetapi juga oleh kemampuan aparat, dukungan fasilitas, tingkat kesadaran hukum masyarakat, dan budaya hukum yang berkembang. Dalam konteks hukum pidana, penegakan hukum bertujuan memberikan kepastian hukum, keadilan, dan kemanfaatan bagi masyarakat. Kepastian hukum diwujudkan melalui penerapan aturan secara konsisten terhadap setiap pelanggaran hukum. Keadilan diwujudkan melalui perlakuan yang sama di hadapan hukum tanpa diskriminasi, sedangkan kemanfaatan diarahkan untuk menciptakan ketertiban sosial dan memberikan perlindungan terhadap kepentingan masyarakat. Ketiga tujuan tersebut harus berjalan secara seimbang agar sistem hukum mampu menjawab perkembangan kejahatan yang semakin kompleks (Juniarso & Abdillah, 2026).

Penegakan hukum terhadap cybercrime memiliki karakteristik yang berbeda dibandingkan tindak pidana konvensional. Alat bukti yang digunakan sebagian besar berupa informasi elektronik, dokumen elektronik, log aktivitas digital, metadata, dan bukti digital lainnya yang memerlukan keahlian khusus dalam proses identifikasi maupun analisis forensik digital. Selain itu, lokasi pelaku, korban, dan server sering kali berada pada negara yang berbeda sehingga memerlukan kerja sama internasional dalam proses penyidikan maupun penuntutan. Kompleksitas tersebut menyebabkan efektivitas penegakan hukum sangat bergantung pada kemampuan aparat dalam menguasai perkembangan teknologi informasi. Dalam sistem hukum Indonesia, penegakan hukum terhadap cybercrime dilaksanakan oleh berbagai institusi, seperti Kepolisian Negara Republik Indonesia, Kejaksaan Republik Indonesia, Pengadilan, Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara (BSSN), serta berbagai lembaga terkait lainnya. Setiap institusi memiliki kewenangan yang berbeda namun saling melengkapi dalam upaya pencegahan, penyidikan, penuntutan, hingga pemulihan akibat tindak pidana siber. Koordinasi antarlembaga menjadi faktor penting dalam menciptakan sistem penegakan hukum yang efektif (Savitri, 2025).

Perkembangan teknologi digital menuntut adanya transformasi dalam sistem penegakan hukum pidana. Aparat penegak hukum tidak lagi hanya dituntut memahami aspek hukum substantif, tetapi juga harus memiliki kompetensi di bidang teknologi informasi, keamanan siber, analisis digital forensik, dan penanganan bukti elektronik. Selain peningkatan kapasitas sumber daya manusia, diperlukan pula dukungan infrastruktur teknologi yang memadai, pembentukan regulasi yang adaptif, serta penguatan kerja sama internasional untuk mengatasi kejahatan siber yang bersifat lintas negara. Berdasarkan uraian tersebut, teori penegakan hukum pidana menjadi landasan penting dalam penelitian ini karena memberikan kerangka analisis mengenai bagaimana sistem hukum Indonesia merespons perkembangan cybercrime di era transformasi digital. Teori ini digunakan untuk mengevaluasi efektivitas implementasi regulasi, kapasitas aparat penegak hukum, serta berbagai kendala yang memengaruhi keberhasilan penegakan hukum terhadap tindak pidana siber (Cahyono, 2025).

3. Teori Transformasi Digital dan Hukum

Transformasi digital merupakan proses perubahan menyeluruh dalam berbagai aspek kehidupan melalui pemanfaatan teknologi digital, internet, komputasi awan, big data, kecerdasan buatan, dan teknologi informasi lainnya. Transformasi ini tidak hanya mengubah cara masyarakat berkomunikasi, bekerja, belajar, dan bertransaksi, tetapi juga mengubah cara pemerintah memberikan pelayanan publik serta bagaimana sistem hukum menghadapi perkembangan teknologi. Perubahan tersebut menuntut adanya penyesuaian kebijakan hukum agar tetap mampu memberikan perlindungan terhadap kepentingan masyarakat di era digital. Dalam perspektif hukum, transformasi digital melahirkan berbagai hubungan hukum baru yang sebelumnya tidak dikenal dalam sistem hukum konvensional. Munculnya perdagangan elektronik, kontrak elektronik, pembayaran digital, aset kripto, kecerdasan buatan, komputasi awan, media sosial, hingga perlindungan data pribadi menunjukkan bahwa perkembangan teknologi menciptakan objek pengaturan hukum yang semakin kompleks. Oleh karena itu, hukum dituntut bersifat dinamis agar mampu mengikuti perkembangan masyarakat tanpa menghambat inovasi teknologi (Richardo et al., 2026).

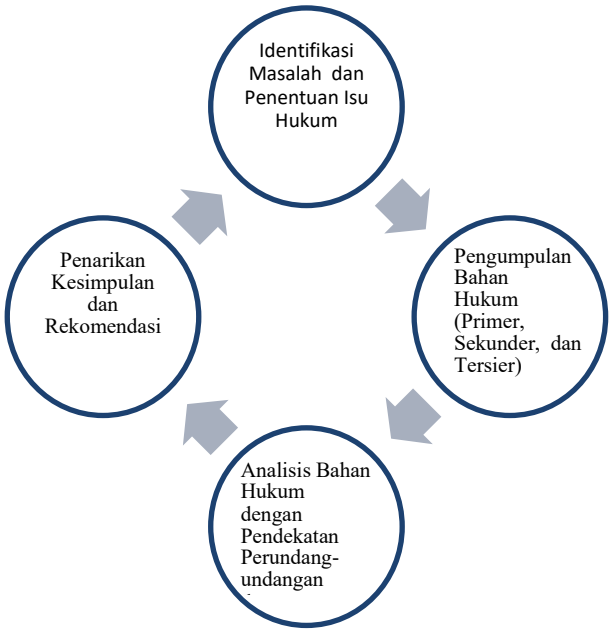
Transformasi digital juga membawa tantangan terhadap konsep yurisdiksi hukum pidana. Aktivitas digital berlangsung secara lintas batas negara sehingga suatu tindak pidana dapat melibatkan pelaku, korban, dan server yang berada di wilayah hukum berbeda. Kondisi ini menimbulkan persoalan mengenai kewenangan negara dalam melakukan penyidikan, penuntutan, maupun pelaksanaan putusan pengadilan. Oleh sebab itu, kerja sama internasional menjadi salah

satu unsur penting dalam sistem penegakan hukum terhadap kejahatan siber. Di Indonesia, respons hukum terhadap transformasi digital diwujudkan melalui pembentukan berbagai regulasi, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, serta berbagai regulasi mengenai perlindungan data pribadi dan keamanan siber. Kehadiran regulasi tersebut menunjukkan bahwa negara berupaya menyesuaikan sistem hukum dengan perkembangan teknologi, meskipun implementasinya masih menghadapi berbagai tantangan (Ferdian, 2026).

Konsep hukum progresif juga relevan dalam menjelaskan respons hukum terhadap transformasi digital. Hukum progresif memandang bahwa hukum harus berkembang mengikuti dinamika masyarakat dan tidak semata-mata terikat pada teks peraturan. Dalam konteks cybercrime, pendekatan ini menekankan pentingnya pembaruan regulasi, peningkatan kualitas penegakan hukum, penguatan perlindungan hak masyarakat, serta pemanfaatan teknologi dalam mendukung proses penyidikan dan pembuktian. Dengan demikian, hukum tidak hanya berfungsi sebagai alat pengendalian sosial, tetapi juga sebagai instrumen adaptasi terhadap perubahan zaman. Berdasarkan uraian tersebut, teori transformasi digital dan hukum menjadi dasar konseptual dalam penelitian ini untuk menjelaskan hubungan antara perkembangan teknologi digital dengan perubahan sistem hukum pidana di Indonesia. Teori ini memberikan pemahaman bahwa efektivitas penegakan hukum terhadap cybercrime tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh kemampuan sistem hukum dalam beradaptasi terhadap inovasi teknologi yang terus berkembang. Dengan demikian, teori ini mendukung analisis mengenai respons hukum pidana terhadap kejahatan siber di era transformasi digital (Morion et al., 2025).

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (normative legal research), yakni penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder. Pendekatan yang digunakan adalah pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah semua undang-undang dan regulasi yang berkaitan dengan isu hukum yang sedang diteliti, khususnya Undang-Undang ITE dan KUHP baru. Pendekatan konseptual dilakukan dengan merujuk pada pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum, khususnya hukum pidana dan hukum teknologi informasi. Bahan hukum yang digunakan dalam penelitian ini terdiri dari tiga jenis. Bahan hukum primer meliputi peraturan perundang-undangan yang berlaku di Indonesia, khususnya Undang-Undang Nomor 1 Tahun 2024 tentang ITE, Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, serta berbagai peraturan pelaksananya. Bahan hukum sekunder meliputi literatur hukum, jurnal ilmiah, hasil penelitian, dan berbagai tulisan dari para ahli hukum yang relevan dengan topik penelitian, dengan rentang waktu publikasi antara tahun 2016 hingga 2024 untuk memastikan kemutakhiran referensi yang digunakan. Bahan hukum tersier meliputi kamus hukum, ensiklopedia, dan berbagai referensi penunjang lainnya. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yaitu dengan mengumpulkan, mengidentifikasi, dan mengklasifikasikan bahan-bahan hukum yang relevan dari berbagai sumber, termasuk basis data jurnal ilmiah nasional dan internasional, publikasi lembaga pemerintah, serta literatur akademis yang dapat diakses secara daring. Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan teknik deskriptif-analitis, yaitu dengan menggambarkan dan menganalisis secara mendalam permasalahan hukum yang diteliti berdasarkan bahan hukum yang telah dikumpulkan (Juniarso & Abdillah, 2026).



Gambar 1. Diagram Alur Metode

HASIL DAN PEMBAHASAN

A. Perkembangan Kejahatan Siber dan Tantangannya terhadap Hukum Pidana

Sebelum menganalisis respons hukum pidana terhadap kejahatan siber, perlu terlebih dahulu dipahami karakteristik dan perkembangan kejahatan siber itu sendiri. Kejahatan siber merupakan kejahatan yang menggunakan teknologi komputer dan jaringan internet sebagai sarana atau objek kejahatan. Definisi ini terus berkembang seiring dengan munculnya bentuk-bentuk kejahatan baru yang belum pernah ada sebelumnya. Dalam perspektif tipologi, kejahatan siber dapat dibedakan menjadi dua kategori utama. Pertama, kejahatan yang menggunakan komputer dan internet sebagai instrumen atau alat untuk melakukan kejahatan konvensional dalam bentuk baru, seperti penipuan daring (online fraud), pencemaran nama baik melalui media sosial, dan pornografi daring. Kedua, kejahatan yang menjadikan komputer atau sistem informasi sebagai target atau objek kejahatan itu sendiri, seperti peretasan (hacking), penyebaran malware, serangan denial-of-service (DDoS), dan pencurian data (data breach) (Savitri, 2025).

Perkembangan kejahatan siber di Indonesia menunjukkan tren yang mengkhawatirkan. Data dari Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menunjukkan bahwa laporan kasus kejahatan siber terus meningkat dari tahun ke tahun. Pada tahun 2022, terdapat lebih dari 8.831 laporan polisi terkait kejahatan siber, meningkat signifikan dibandingkan tahun-tahun sebelumnya. Jenis kejahatan yang paling banyak dilaporkan adalah penipuan daring, pencurian akun media sosial, dan ujaran kebencian (hate speech). Salah satu karakteristik yang membuat kejahatan siber sangat sulit ditangani adalah sifatnya yang melampaui batas yurisdiksi (transnational). Pelaku kejahatan siber dapat berada di satu negara, infrastruktur yang digunakan berada di negara lain, sementara korban berada di negara ketiga. Kondisi ini menimbulkan kebingungan yurisdiksi dan menciptakan celah hukum yang sering dimanfaatkan oleh para pelaku. Indonesia sebagai negara berkembang seringkali menjadi target kejahatan siber dari luar negeri,

namun proses ekstradisi dan kerjasama hukum internasional yang lamban seringkali menghambat proses penegakan hukum (Cahyono, 2025).

Karakteristik lain yang membedakan kejahatan siber dari kejahatan konvensional adalah cepatnya evolusi modus operandi. Pelaku kejahatan siber selalu beradaptasi dengan perkembangan teknologi terbaru, bahkan seringkali memanfaatkan teknologi lebih cepat daripada aparat penegak hukum. Munculnya teknologi kecerdasan buatan (artificial intelligence), blockchain, dan Internet of Things (IoT) membuka dimensi-dimensi baru dalam kejahatan siber yang belum sepenuhnya diantisipasi oleh regulasi yang ada. Deepfake yang digunakan untuk penipuan identitas, penggunaan cryptocurrency untuk pencucian uang hasil kejahatan siber, dan eksploitasi perangkat IoT sebagai zombie dalam serangan DDoS adalah beberapa contoh terkini yang menunjukkan betapa cepatnya evolusi ancaman siber (Cahyono, 2025).

B. Respons Hukum Pidana Indonesia terhadap Kejahatan Siber

Rumusan masalah pertama penelitian ini adalah bagaimana hukum pidana Indonesia merespons perkembangan kejahatan siber. Untuk menjawab pertanyaan ini, perlu dilakukan analisis terhadap regulasi-regulasi yang ada dan sejauh mana regulasi tersebut mampu mengcover berbagai bentuk kejahatan siber yang berkembang. Tonggak utama regulasi kejahatan siber di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini merupakan regulasi pertama yang secara khusus mengatur kejahatan siber di Indonesia. UU ITE mengatur berbagai perbuatan yang dilarang di dunia siber, termasuk akses ilegal (hacking), intersepsi ilegal, gangguan terhadap data dan sistem komputer, penyebaran konten ilegal (pornografi, perjudian, pencemaran nama baik), serta penipuan elektronik. Undang-undang ini kemudian direvisi melalui UU Nomor 19 Tahun 2016 yang terutama mempertegas beberapa ketentuan dan memperjelas mekanisme penghapusan konten (Richardo et al., 2026).

Revisi terbaru UU ITE dilakukan melalui Undang-Undang Nomor 1 Tahun 2024. Perubahan ini membawa sejumlah penyempurnaan yang cukup signifikan. Di antaranya adalah pengaturan yang lebih rinci mengenai perlindungan data pribadi, ketentuan mengenai tanggung jawab platform digital, serta mekanisme yang lebih jelas dalam penyelesaian sengketa terkait konten digital. Selain itu, perubahan ini juga mencoba mengklarifikasi pasal-pasal yang sebelumnya sering disalahgunakan, terutama pasal-pasal terkait pencemaran nama baik yang kerap diperdebatkan dalam konteks kebebasan berekspresi. Di samping UU ITE, Indonesia juga telah memiliki Kitab Undang-Undang Hukum Pidana (KUHP) baru yang tertuang dalam Undang-Undang Nomor 1 Tahun 2023. KUHP baru ini, yang akan mulai berlaku secara penuh pada tahun 2026, mengakomodasi beberapa ketentuan terkait kejahatan siber, meskipun masih bersifat umum. KUHP baru mengatur tentang penyadapan ilegal, penyebaran informasi yang meresahkan, dan beberapa tindak pidana lain yang memiliki dimensi siber. Namun, para akademisi mencatat bahwa KUHP baru belum secara komprehensif mengatur kejahatan siber yang spesifik sebagai lex specialis (Ferdian, 2026).

Regulasi penting lainnya adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Undang-undang ini merupakan langkah maju yang signifikan dalam konteks keamanan siber, khususnya untuk menangani kejahatan yang berkaitan dengan pencurian dan penyalahgunaan data pribadi. UU PDP mewajibkan pengelola data (data controller dan data processor) untuk mematuhi standar perlindungan data tertentu dan memberikan sanksi pidana bagi yang melanggarnya. Ini merupakan pendekatan yang sesuai dengan tren regulasi global, sebagaimana tercermin dalam General Data Protection Regulation (GDPR) Uni Eropa. Dalam konteks hukum internasional, Indonesia juga telah meratifikasi beberapa konvensi

internasional yang relevan dengan kejahatan siber, meskipun Indonesia belum meratifikasi Konvensi Budapest tentang Kejahatan Siber (Budapest Convention on Cybercrime), yang merupakan instrumen hukum internasional paling komprehensif dalam bidang ini. Ketiadaan ratifikasi ini merupakan salah satu kendala dalam kerjasama internasional penegakan hukum terhadap kejahatan siber lintas batas. Analisis terhadap regulasi yang ada menunjukkan bahwa Indonesia telah memiliki kerangka hukum yang cukup untuk menangani berbagai bentuk kejahatan siber. Namun, terdapat beberapa kelemahan yang perlu diperhatikan. Pertama, masih adanya kekosongan hukum (legal gap) untuk beberapa jenis kejahatan siber baru, seperti serangan terhadap infrastruktur kritis menggunakan AI, kejahatan yang memanfaatkan teknologi blockchain, dan berbagai bentuk kejahatan siber yang memanfaatkan teknologi mutakhir lainnya. Kedua, beberapa ketentuan dalam UU ITE masih bersifat multitafsir sehingga menimbulkan ketidakpastian hukum. Ketiga, koordinasi antara berbagai regulasi yang berbeda (UU ITE, UU PDP, KUHP baru) masih perlu ditingkatkan untuk menghindari tumpang tindih dan inkonsistensi (Morion et al., 2025).

Respons hukum pidana Indonesia terhadap kejahatan siber pada dasarnya menunjukkan adanya upaya adaptasi yang cukup progresif terhadap perkembangan teknologi digital. Kehadiran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai regulasi utama menandai pengakuan negara bahwa ruang siber merupakan domain yang membutuhkan pengaturan khusus. Namun demikian, kecepatan perkembangan teknologi sering kali melampaui kemampuan regulasi dalam merespons secara tepat waktu. Perubahan melalui Undang-Undang Nomor 1 Tahun 2024 menunjukkan adanya kesadaran pembentuk undang-undang untuk memperbaiki kelemahan sebelumnya, khususnya terkait perlindungan hak-hak digital dan kejelasan norma hukum. Meskipun demikian, implementasi norma tersebut masih bergantung pada interpretasi aparat penegak hukum, yang dalam beberapa kasus dapat berbeda-beda dan menimbulkan ketidakpastian hukum. Dalam kaitannya dengan hukum pidana umum, Kitab Undang-Undang Hukum Pidana (KUHP) baru memberikan dasar tambahan dalam mengatur perilaku yang memiliki dimensi siber. Akan tetapi, karena sifatnya yang umum, KUHP belum mampu menjangkau secara rinci kompleksitas kejahatan siber modern. Hal ini menegaskan pentingnya keberadaan regulasi khusus sebagai lex specialis yang lebih responsif dan adaptif (Ghiffari, 2025).

Keberadaan Undang-Undang Perlindungan Data Pribadi (UU PDP) juga memperkuat respons hukum pidana terhadap aspek tertentu dari kejahatan siber, khususnya yang berkaitan dengan perlindungan data. UU ini memberikan dasar hukum yang jelas untuk menindak pelanggaran terkait pengelolaan data pribadi, sekaligus mendorong peningkatan standar keamanan data di sektor publik maupun swasta. Namun demikian, pengaturan yang tersebar dalam berbagai undang-undang tersebut juga menimbulkan tantangan harmonisasi. Tumpang tindih norma antara UU ITE, UU PDP, dan KUHP berpotensi menimbulkan konflik interpretasi dalam praktik penegakan hukum. Oleh karena itu, diperlukan sinkronisasi regulasi yang lebih sistematis agar tidak terjadi inkonsistensi dalam penerapan hukum. Selain itu, respons hukum pidana Indonesia masih cenderung bersifat reaktif daripada preventif. Banyak regulasi yang lahir sebagai respons terhadap kasus-kasus yang sudah terjadi, bukan sebagai langkah antisipatif terhadap potensi ancaman di masa depan. Padahal, karakter kejahatan siber yang cepat berkembang menuntut pendekatan hukum yang lebih proaktif dan berbasis prediksi (Fadly et al., 2025).

Kelemahan lain yang cukup signifikan adalah belum optimalnya pengaturan terhadap kejahatan siber berbasis teknologi baru. Misalnya, penggunaan kecerdasan buatan dalam melakukan penipuan digital atau manipulasi informasi belum diatur secara spesifik. Hal ini menunjukkan adanya kesenjangan antara perkembangan teknologi dan kesiapan hukum dalam mengaturnya. Dalam konteks internasional, belum diratifikasinya Budapest Convention on

Cybercrime juga menjadi faktor yang membatasi efektivitas respons hukum Indonesia terhadap kejahatan siber lintas batas. Tanpa keterlibatan dalam kerangka hukum internasional yang komprehensif, Indonesia menghadapi keterbatasan dalam hal akses terhadap bukti dan kerjasama penegakan hukum dengan negara lain. Meskipun demikian, Indonesia telah menunjukkan komitmen untuk terus memperbaiki kerangka hukumnya melalui pembaruan regulasi dan peningkatan kerjasama internasional. Upaya ini perlu terus dilanjutkan dengan memperhatikan praktik terbaik global serta kebutuhan nasional yang spesifik. Secara keseluruhan, respons hukum pidana Indonesia terhadap kejahatan siber dapat dikatakan sudah berada pada jalur yang tepat, namun masih memerlukan penguatan dari segi substansi, harmonisasi regulasi, dan kemampuan adaptasi terhadap perkembangan teknologi. Tanpa pembaruan yang berkelanjutan, hukum pidana akan sulit mengejar kompleksitas dan dinamika kejahatan siber yang terus berkembang (Gladys & Bella, 2025).

C. Efektivitas Penegakan Hukum Pidana terhadap Kejahatan Siber

Rumusan masalah kedua penelitian ini adalah bagaimana efektivitas penegakan hukum pidana terhadap pelaku kejahatan siber di Indonesia dan faktor-faktor apa yang mempengaruhinya. Penegakan hukum pidana merupakan ujung tombak dari sistem hukum pidana itu sendiri. Tanpa penegakan yang efektif, regulasi yang paling komprehensif sekalipun tidak akan bermakna dalam praktik. Dalam mengevaluasi efektivitas penegakan hukum pidana terhadap kejahatan siber, perlu digunakan kerangka teori yang tepat. Teori efektivitas hukum dari Lawrence M. Friedman menyatakan bahwa efektivitas sistem hukum bergantung pada tiga komponen: substansi hukum (legal substance), struktur hukum (legal structure), dan budaya hukum (legal culture). Dalam konteks penegakan hukum terhadap kejahatan siber di Indonesia, ketiga komponen ini masing-masing menghadapi tantangan tersendiri. Dari sisi substansi hukum, sebagaimana telah dianalisis pada bagian sebelumnya, Indonesia memiliki beberapa regulasi terkait kejahatan siber namun dengan berbagai keterbatasan. Masih terdapat kekosongan hukum untuk beberapa jenis kejahatan siber baru, dan beberapa ketentuan yang ada masih bersifat multitafsir. Selain itu, sanksi pidana yang diatur terkadang dianggap belum proporsional dengan dampak yang ditimbulkan oleh kejahatan siber, terutama untuk kasus-kasus yang melibatkan kerugian dalam skala besar atau ancaman terhadap keamanan nasional. Dari sisi struktur hukum, Indonesia telah membentuk berbagai institusi yang secara khusus menangani kejahatan siber. Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri merupakan satuan polisi yang secara khusus menangani kejahatan siber di tingkat nasional. Setiap Polda juga memiliki unit siber tersendiri. Selain kepolisian, Badan Siber dan Sandi Negara (BSSN) memiliki peran penting dalam deteksi dini dan respons terhadap insiden siber, meskipun perannya lebih bersifat teknis dan preventif daripada penindakan pidana (Nai & Hoesein, 2026).

Namun, tantangan yang dihadapi oleh struktur penegak hukum ini cukup signifikan. Pertama, keterbatasan sumber daya manusia yang memiliki keahlian teknis di bidang forensik digital. Investigasi kejahatan siber membutuhkan keahlian yang sangat spesifik dan terus berkembang, sementara pelatihan dan pengembangan kapasitas aparat penegak hukum masih terbatas. Kedua, keterbatasan peralatan forensik digital yang canggih. Investigasi kejahatan siber membutuhkan perangkat keras dan perangkat lunak yang mutakhir, yang membutuhkan investasi finansial yang tidak kecil. Ketiga, permasalahan koordinasi antar lembaga, baik di tingkat nasional (antara kepolisian, BSSN, Kejaksaan, dan Kementerian terkait) maupun di tingkat internasional. Dari sisi budaya hukum, terdapat beberapa permasalahan yang perlu diatasi. Pertama, tingkat kesadaran hukum masyarakat terkait kejahatan siber masih rendah, baik sebagai potensi pelaku maupun sebagai korban. Banyak korban kejahatan siber yang tidak melaporkan kejadian yang

menimpa mereka, baik karena tidak mengetahui prosedur pelaporan, merasa percuma, atau bahkan tidak menyadari bahwa mereka telah menjadi korban kejahatan siber. Kedua, masih ada persepsi di sebagian kalangan bahwa kejahatan siber merupakan kejahatan yang tidak serius atau tanpa korban (victimless crime), padahal dampaknya bisa sangat merugikan (Juniarso & Abdillah, 2026).

Mengukur efektivitas penegakan hukum terhadap kejahatan siber juga menjadi tantangan tersendiri. Statistik kasus yang dilaporkan dan ditangani hanya merupakan sebagian kecil dari keseluruhan kejahatan siber yang terjadi (dark figure of crime). Banyak kasus yang tidak dilaporkan atau tidak berhasil diungkap. Tingkat penyelesaian kasus (case clearance rate) untuk kejahatan siber pun relatif rendah dibandingkan kejahatan konvensional, mengingat kesulitan teknis dalam mengidentifikasi dan menangkap pelaku yang bersembunyi di balik anonimitas dunia digital. Satu aspek penting dalam penegakan hukum kejahatan siber adalah persoalan pembuktian. Kejahatan siber sangat bergantung pada bukti digital yang memiliki karakteristik berbeda dari bukti fisik konvensional. Bukti digital mudah berubah, dapat dihapus, dan dapat dipalsukan. Autentisitas dan integritas bukti digital harus dijaga dengan sangat ketat melalui prosedur forensik digital yang standar. Di Indonesia, pengaturan mengenai bukti digital dalam KUHAP masih terbatas, meskipun UU ITE telah memberikan beberapa ketentuan mengenai nilai pembuktian dokumen elektronik. Standardisasi prosedur forensik digital dan peningkatan kapasitas ahli digital forensik di Indonesia masih menjadi pekerjaan rumah yang penting (Savitri, 2025).

Efektivitas penegakan hukum pidana terhadap kejahatan siber di Indonesia pada akhirnya sangat ditentukan oleh sejauh mana ketiga komponen dalam teori Lawrence M. Friedman dapat berjalan secara selaras. Ketidakseimbangan antara substansi, struktur, dan budaya hukum akan menciptakan celah yang dimanfaatkan oleh pelaku kejahatan siber. Dalam praktiknya, sering kali terlihat bahwa pembaruan regulasi tidak selalu diiringi dengan peningkatan kapasitas aparat maupun perubahan perilaku masyarakat. Dari sisi substansi hukum, keberadaan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memang menjadi landasan utama dalam penanganan kejahatan siber. Namun, dinamika teknologi seperti kecerdasan buatan, serangan ransomware, dan kejahatan berbasis deepfake menunjukkan bahwa regulasi yang ada sering tertinggal dari perkembangan modus operandi kejahatan. Hal ini menyebabkan aparat penegak hukum harus melakukan penafsiran yang luas, yang berpotensi menimbulkan ketidakpastian hukum. Dalam konteks struktur hukum, peran Direktorat Tindak Pidana Siber Bareskrim Polri menjadi sangat strategis sebagai garda terdepan penindakan. Namun, keterbatasan jumlah personel yang memiliki keahlian khusus di bidang keamanan siber dan digital forensik masih menjadi kendala utama. Beban perkara yang terus meningkat tidak selalu sebanding dengan kapasitas institusi yang tersedia (Cahyono, 2025).

Selain itu, Badan Siber dan Sandi Negara (BSSN) berperan penting dalam aspek pencegahan dan mitigasi serangan siber. Akan tetapi, koordinasi antara BSSN dengan aparat penegak hukum dalam proses penindakan pidana masih perlu diperkuat. Kesenjangan antara fungsi teknis dan fungsi yuridis ini sering kali memperlambat respons terhadap insiden siber yang membutuhkan penanganan cepat dan terpadu. Permasalahan koordinasi juga terlihat dalam hubungan antara kepolisian dan Kejaksaan Republik Indonesia, khususnya dalam tahap penuntutan. Perbedaan pemahaman mengenai alat bukti digital dan konstruksi perkara dapat menghambat proses peradilan. Oleh karena itu, diperlukan standardisasi pemahaman lintas lembaga agar proses penegakan hukum dapat berjalan lebih efektif dan efisien. Dari sisi budaya hukum, rendahnya literasi digital masyarakat menjadi faktor yang sangat mempengaruhi efektivitas penegakan hukum. Banyak masyarakat yang belum memahami risiko keamanan digital, seperti phishing, pencurian data, atau penipuan online. Kondisi ini menyebabkan tingginya angka

kejahatan sekaligus rendahnya tingkat pelaporan, sehingga aparat kesulitan memperoleh gambaran utuh mengenai skala permasalahan (Richardo et al., 2026).

Selain itu, persepsi masyarakat terhadap kejahatan siber juga masih menjadi hambatan. Sebagian masyarakat menganggap kejahatan di dunia maya tidak seberbahaya kejahatan konvensional, padahal dampaknya bisa sangat luas, termasuk kerugian finansial besar dan kebocoran data pribadi. Perubahan paradigma ini memerlukan edukasi yang berkelanjutan dan terstruktur dari pemerintah maupun lembaga pendidikan. Dalam aspek pembuktian, tantangan terbesar terletak pada karakteristik bukti digital yang sangat rentan terhadap manipulasi. Oleh karena itu, penerapan standar forensik digital yang ketat menjadi keharusan. Indonesia perlu mengadopsi praktik internasional dalam chain of custody dan penggunaan alat forensik yang terverifikasi untuk memastikan bahwa bukti yang diajukan di pengadilan memiliki kekuatan pembuktian yang tinggi. Efektivitas penegakan hukum juga dipengaruhi oleh kemampuan dalam melakukan pelacakan lintas yurisdiksi. Banyak pelaku kejahatan siber beroperasi dari luar negeri, sehingga membutuhkan kerjasama internasional yang kuat. Tanpa mekanisme kerjasama yang cepat dan efisien, proses penegakan hukum akan terhambat dan pelaku sulit dijangkau oleh hukum nasional. Pada akhirnya, peningkatan efektivitas penegakan hukum pidana terhadap kejahatan siber di Indonesia memerlukan pendekatan yang komprehensif dan berkelanjutan. Reformasi regulasi harus diiringi dengan penguatan kapasitas institusi, peningkatan literasi masyarakat, serta optimalisasi kerjasama nasional dan internasional. Tanpa upaya terpadu tersebut, penegakan hukum akan terus tertinggal dari laju perkembangan kejahatan siber yang semakin kompleks (Ferdian, 2026).

D. Perbandingan dengan Regulasi Internasional dan Praktik Terbaik

Untuk melengkapi analisis mengenai respons hukum pidana dan efektivitas penegakannya, perlu juga dilakukan perbandingan dengan regulasi dan praktik terbaik internasional. Konvensi Budapest (Budapest Convention on Cybercrime) yang diadopsi oleh Dewan Eropa pada tahun 2001 dan telah diratifikasi oleh puluhan negara merupakan kerangka hukum internasional paling komprehensif dalam bidang kejahatan siber. Konvensi ini mengatur harmonisasi hukum materiil dan hukum acara terkait kejahatan siber, serta mekanisme kerjasama internasional antar negara pihak. Beberapa negara di Asia Tenggara telah lebih dahulu meratifikasi Konvensi Budapest dan terbukti mendapatkan manfaat yang signifikan dalam penegakan hukum terhadap kejahatan siber lintas batas. Singapura, misalnya, memiliki regulasi kejahatan siber yang sangat komprehensif dan aparat penegak hukum yang sangat terlatih dan terampil di bidang forensik digital. Malaysia pun memiliki Undang-Undang Kejahatan Komputer (Computer Crimes Act) yang telah teruji dan terus diperbarui sesuai perkembangan teknologi. Indonesia perlu mempertimbangkan ratifikasi Konvensi Budapest sebagai langkah strategis untuk meningkatkan kemampuan penegakan hukum terhadap kejahatan siber, terutama yang bersifat lintas batas (Morion et al., 2025).

Di tingkat ASEAN, terdapat beberapa inisiatif kerjasama dalam bidang keamanan siber yang relevan. ASEAN Cybersecurity Cooperation Strategy dan berbagai perjanjian bilateral di bidang kerjasama hukum pidana (Mutual Legal Assistance Treaty/MLAT) merupakan mekanisme yang dapat dimanfaatkan untuk mengatasi tantangan yurisdiksi lintas batas. Namun, efektivitas mekanisme ini masih perlu terus ditingkatkan melalui kapasitas teknis yang lebih baik dan prosedur yang lebih efisien. Dalam konteks perlindungan data pribadi sebagai bagian dari upaya pencegahan kejahatan siber, Indonesia dapat belajar dari implementasi GDPR di Uni Eropa. GDPR telah terbukti mendorong standar perlindungan data yang tinggi dan memberikan deterrence effect yang signifikan terhadap pelanggaran data. Meskipun UU PDP Indonesia telah mengadopsi beberapa prinsip dari GDPR, implementasinya masih perlu diperkuat melalui pembentukan Komisi

Perlindungan Data Pribadi yang independen dan efektif, sebagaimana diamanatkan oleh undang-undang tersebut. Perbandingan lebih lanjut menunjukkan bahwa Budapest Convention on Cybercrime tidak hanya berfungsi sebagai instrumen harmonisasi hukum, tetapi juga menyediakan kerangka operasional yang konkret dalam proses penyidikan, seperti pengamanan data elektronik secara cepat (expedited preservation) dan akses lintas yurisdiksi terhadap bukti digital. Hal ini menjadi keunggulan utama dibandingkan dengan banyak regulasi nasional yang masih terbatas pada aspek normatif tanpa diikuti prosedur teknis yang memadai. Di negara-negara yang telah meratifikasi konvensi tersebut, koordinasi antar lembaga penegak hukum menjadi jauh lebih efisien. Misalnya, mekanisme 24/7 contact point yang diatur dalam konvensi memungkinkan respons cepat terhadap permintaan bantuan internasional. Indonesia saat ini masih menghadapi kendala birokrasi dalam proses permintaan data lintas negara, yang sering kali memakan waktu lama sehingga berpotensi menghilangkan barang bukti digital yang bersifat volatil (Ghiffari, 2025).

Praktik terbaik juga terlihat dari penguatan kapasitas institusi penegak hukum. Di Singapore, aparat kepolisian memiliki unit khusus seperti Cybercrime Command yang dilengkapi dengan teknologi mutakhir dan tenaga ahli di bidang digital forensik. Pendekatan ini menekankan bahwa keberhasilan penegakan hukum tidak hanya bergantung pada regulasi, tetapi juga pada kesiapan sumber daya manusia dan infrastruktur teknologi. Sementara itu, Malaysia melalui Computer Crimes Act dan kebijakan turunannya terus melakukan pembaruan regulasi agar tetap relevan dengan perkembangan ancaman siber. Pendekatan adaptif ini penting karena karakter kejahatan siber yang sangat dinamis, sehingga regulasi yang statis akan cepat menjadi usang dan tidak efektif dalam menjawab tantangan baru. Di kawasan regional, ASEAN telah mengembangkan berbagai kerangka kerja sama, termasuk ASEAN Cybersecurity Cooperation Strategy. Namun demikian, implementasi di tingkat operasional masih menghadapi tantangan seperti perbedaan kapasitas antar negara anggota, perbedaan sistem hukum, serta keterbatasan dalam berbagi informasi sensitif secara real-time. Selain itu, mekanisme Mutual Legal Assistance Treaty (MLAT) yang dimiliki Indonesia sebenarnya dapat menjadi alat yang efektif dalam penanganan kejahatan siber lintas batas. Namun, prosedur yang kompleks dan waktu pemrosesan yang panjang sering kali menghambat efektivitasnya. Oleh karena itu, diperlukan reformasi prosedural agar lebih responsif terhadap kebutuhan penegakan hukum di era digital. Dalam konteks perlindungan data pribadi, General Data Protection Regulation (GDPR) di Uni Eropa menjadi benchmark global. Regulasi ini tidak hanya menetapkan standar tinggi dalam pengelolaan data, tetapi juga memberikan sanksi yang tegas bagi pelanggaran, sehingga menciptakan efek jera yang signifikan bagi pelaku usaha maupun institusi yang lalai dalam melindungi data pengguna (Fadly et al., 2025).

Indonesia melalui Undang-Undang Perlindungan Data Pribadi (UU PDP) telah mengadopsi sejumlah prinsip penting dari GDPR, seperti consent, purpose limitation, dan data minimization. Namun, tanpa adanya lembaga pengawas yang kuat dan independen, implementasi prinsip-prinsip tersebut berpotensi tidak optimal. Oleh karena itu, pembentukan otoritas pengawas yang efektif menjadi kunci keberhasilan regulasi ini. Lebih jauh, praktik terbaik internasional juga menekankan pentingnya pendekatan multi-stakeholder, yang melibatkan pemerintah, sektor swasta, akademisi, dan masyarakat sipil dalam upaya pencegahan dan penanganan kejahatan siber. Kolaborasi ini penting karena sebagian besar infrastruktur digital dikelola oleh sektor swasta, sehingga keterlibatan mereka menjadi krusial dalam menjaga keamanan ekosistem digital. Sebagai penutup, pembelajaran dari praktik internasional menunjukkan bahwa efektivitas penanggulangan kejahatan siber tidak hanya bergantung pada keberadaan regulasi, tetapi juga pada integrasi antara kerangka hukum yang adaptif, kapasitas institusi yang kuat, mekanisme kerjasama internasional yang

efisien, serta pengawasan yang akuntabel. Indonesia memiliki peluang besar untuk memperkuat sistemnya dengan mengadopsi praktik terbaik tersebut secara kontekstual dan berkelanjutan (Gladys & Bella, 2025).

E. Upaya Pembaruan dan Reformasi Hukum

Menghadapi berbagai tantangan yang telah diidentifikasi, terdapat beberapa upaya pembaruan dan reformasi hukum yang perlu dilakukan untuk meningkatkan respons hukum pidana dan efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. Pertama, penyempurnaan substansi hukum melalui revisi UU ITE yang lebih responsif terhadap perkembangan teknologi terkini, termasuk pengaturan yang lebih spesifik mengenai kejahatan siber yang memanfaatkan AI, blockchain, dan IoT. Harmonisasi antara UU ITE, UU PDP, dan KUHP baru juga perlu diperkuat untuk menghindari tumpang tindih dan memastikan kepastian hukum. Kedua, penguatan kapasitas institusional. Investasi dalam pengembangan sumber daya manusia di bidang forensik digital, keamanan siber, dan penegakan hukum siber merupakan kebutuhan yang mendesak. Program pendidikan dan pelatihan yang terstruktur bagi aparat penegak hukum, jaksa, dan hakim dalam memahami dan menangani perkara kejahatan siber perlu ditingkatkan secara signifikan. Pembentukan laboratorium forensik digital yang modern dan terstandarisasi di seluruh wilayah Indonesia juga merupakan investasi yang penting (Nai & Hoesein, 2026).

Ketiga, peningkatan kerjasama internasional. Pertimbangan untuk meratifikasi Konvensi Budapest perlu dikaji secara serius, dengan mempertimbangkan manfaat yang dapat diperoleh dalam konteks penegakan hukum terhadap kejahatan siber lintas batas. Penguatan perjanjian MLAT dengan negara-negara yang sering menjadi basis kejahatan siber yang menyerang Indonesia juga perlu menjadi prioritas diplomasi hukum Indonesia. Di samping itu, partisipasi aktif dalam forum-forum internasional dan regional di bidang keamanan siber perlu terus ditingkatkan untuk memastikan Indonesia tidak tertinggal dalam perkembangan global. Keempat, penguatan upaya pencegahan dan edukasi masyarakat. Pendekatan hukum pidana yang semata-mata bersifat represif tidak cukup untuk mengatasi kejahatan siber yang kompleks. Upaya preventif melalui edukasi masyarakat mengenai keamanan siber, literasi digital, dan kesadaran hukum perlu ditingkatkan secara masif. Kemitraan antara pemerintah, sektor swasta, dan masyarakat sipil dalam membangun ekosistem keamanan siber yang lebih kokoh merupakan pendekatan yang semakin diadopsi oleh negara-negara yang berhasil dalam mengatasi tantangan kejahatan siber (Juniarso & Abdillah, 2026).

Tabel. 1 Literatur Review

No.	Penulis (Tahun)	Judul Penelitian	Metode Penelitian	Hasil Penelitian	Relevansi dengan Penelitian
1	Cahyono (2025)	Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia	Yuridis normatif	Menunjukkan perlunya rekonstruksi hukum pidana agar mampu mengakomodasi perkembangan kejahatan siber serta memperkuat sistem peradilan pidana Indonesia.	Menjadi dasar dalam memahami kebutuhan pembaruan hukum pidana untuk menghadapi cybercrime.
2	Fadly, Arifin, & Irawan	Analisis tentang Pengaruh Politik Hukum terhadap Penegakan Hukum di	Yuridis normatif	Politik hukum memiliki pengaruh signifikan terhadap efektivitas pembentukan regulasi dan	Memberikan perspektif mengenai hubungan

	(2025)	Bidang Siber		penegakan hukum siber di Indonesia.	kebijakan hukum dengan efektivitas penegakan hukum siber.
3	Ferdian (2026)	Optimalisasi Penegakan Hukum terhadap Tindak Pidana Siber di Era Transformasi Digital: Analisis Kritis Regulasi dan Implementasi	Analisis normatif	Regulasi telah berkembang, namun implementasi penegakan hukum masih menghadapi berbagai kendala seperti kapasitas aparat dan perkembangan teknologi.	Mendukung analisis mengenai tantangan implementasi regulasi cybercrime di era digital.
4	Ghiffari (2025)	Kejahatan Siber dan Tantangan Penegakan Hukum di Indonesia	Studi kepustakaan	Mengidentifikasi berbagai tantangan penegakan hukum, seperti keterbatasan regulasi, pembuktian digital, dan kerja sama lintas negara.	Menjadi referensi mengenai hambatan penegakan hukum terhadap cybercrime di Indonesia.
5	Gladys & Bella (2025)	Penegakan Hukum terhadap Tindak Pidana Cybercrime dalam Kasus Peretasan dan Pelanggaran Data Pribadi oleh Hacker Bjorka	Yuridis normatif (studi kasus)	Kasus Bjorka menunjukkan lemahnya perlindungan data pribadi serta perlunya peningkatan koordinasi antar lembaga penegak hukum.	Memberikan contoh konkret implementasi penegakan hukum terhadap kejahatan siber di Indonesia.
6	Juniarso & Abdillah (2026)	Reformasi Kebijakan Pidana Nasional terhadap Kejahatan Siber Berbasis AI melalui Pendekatan Hukum Progresif	Yuridis normatif	Diperlukan reformasi kebijakan pidana yang adaptif terhadap perkembangan Artificial Intelligence melalui pendekatan hukum progresif.	Menjadi acuan dalam membahas tantangan cybercrime berbasis teknologi AI.
7	Morion, Thomas, & Anggraeni (2025)	Cybercrime dan Media Sosial: Analisis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital	Analisis yuridis	Peningkatan penggunaan media sosial berbanding lurus dengan meningkatnya tindak pidana siber sehingga diperlukan penguatan regulasi dan literasi digital.	Mendukung pembahasan mengenai perkembangan bentuk-bentuk cybercrime di media sosial.
8	Nai & Hoesein (2026)	Analisis Yuridis terhadap Perlindungan Hukum bagi Korban Kejahatan Siber di Indonesia	Yuridis normatif	Perlindungan hukum bagi korban cybercrime masih belum optimal sehingga diperlukan penguatan regulasi dan mekanisme pemulihan korban.	Memberikan landasan mengenai aspek perlindungan hukum bagi korban kejahatan siber.
9	Richard	Analisis Normatif	Yuridis	Teknologi deepfake	Menambah

	o, Wanggai, Hartono, Parwati (2026)	terhadap Penyebaran Deepfake sebagai Bentuk Kejahatan Siber di Indonesia	normatif	menimbulkan tantangan baru yang belum sepenuhnya diatur dalam regulasi nasional sehingga diperlukan pembaruan hukum.	kajian mengenai bentuk cybercrime berbasis teknologi kecerdasan buatan.
10	Savitri (2025)	Perkembangan Regulasi dan Tantangan Penegakan Hukum Kejahatan Siber di Indonesia: Keseimbangan antara Inovasi dan Kepastian Hukum	Studi kepustakaan	Regulasi cybercrime harus mampu menjaga keseimbangan antara inovasi teknologi, kepastian hukum, dan perlindungan hak masyarakat.	Menjadi referensi dalam menganalisis perkembangan regulasi cybercrime dan tantangan implementasinya.

KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap dua rumusan masalah yang menjadi fokus penelitian ini, dapat ditarik beberapa kesimpulan yang saling berkaitan. Pertama, terkait respons hukum pidana Indonesia terhadap perkembangan kejahatan siber, Indonesia telah memiliki kerangka regulasi yang cukup memadai, dengan UU ITE (terakhir diperbarui melalui UU Nomor 1 Tahun 2024) sebagai pilar utamanya, didukung oleh UU PDP dan KUHP baru. Namun, kerangka regulasi ini masih menghadapi beberapa kelemahan, termasuk kekosongan hukum untuk beberapa jenis kejahatan siber baru yang memanfaatkan teknologi mutakhir seperti AI dan blockchain, ketentuan yang masih bersifat multitafsir sehingga menimbulkan ketidakpastian hukum, dan koordinasi yang perlu diperkuat antara berbagai regulasi yang ada. Diperlukan pembaruan regulasi yang berkelanjutan dan responsif terhadap dinamika perkembangan teknologi untuk memastikan kerangka hukum pidana Indonesia tetap relevan dan efektif dalam menghadapi kejahatan siber yang terus berevolusi. Kedua, terkait efektivitas penegakan hukum pidana terhadap kejahatan siber, penegakan hukum di Indonesia masih menghadapi berbagai tantangan yang signifikan. Dari aspek substansi hukum, masih adanya kekosongan hukum dan ketidakpastian interpretasi menjadi kendala tersendiri. Dari aspek struktur hukum, keterbatasan sumber daya manusia yang terampil di bidang forensik digital, keterbatasan peralatan teknis, dan permasalahan koordinasi antar lembaga menjadi faktor yang menghambat efektivitas penegakan hukum. Dari aspek budaya hukum, rendahnya pelaporan kasus dan kesadaran masyarakat terhadap kejahatan siber merupakan tantangan yang perlu diatasi melalui upaya edukasi yang sistematis dan berkelanjutan.

Untuk meningkatkan respons hukum pidana dan efektivitas penegakan hukum terhadap kejahatan siber, diperlukan pendekatan yang komprehensif dan multi-dimensi. Reformasi regulasi yang berkelanjutan, penguatan kapasitas institusional aparat penegak hukum, peningkatan kerjasama internasional, dan penguatan upaya pencegahan melalui edukasi masyarakat merupakan empat pilar yang harus dijalankan secara simultan dan sinergis. Keberhasilan dalam menghadapi tantangan kejahatan siber tidak dapat hanya mengandalkan pendekatan represif melalui hukum pidana semata, melainkan harus dipadukan dengan pendekatan preventif dan restoratif yang melibatkan seluruh pemangku kepentingan dalam ekosistem digital Indonesia. Penelitian ini memberikan kontribusi berupa analisis normatif yang komprehensif terhadap permasalahan hukum pidana dan perkembangan IT di Indonesia. Penelitian lanjutan yang bersifat empiris mengenai implementasi dan efektivitas regulasi yang ada di lapangan sangat diperlukan untuk melengkapi

pemahaman yang lebih holistik mengenai permasalahan ini. Selain itu, kajian komparatif yang lebih mendalam dengan negara-negara yang telah berhasil dalam mengatasi tantangan kejahatan siber dapat memberikan pelajaran berharga bagi pembaruan sistem hukum pidana Indonesia di era digital.

DAFTAR REFERENSI

Cahyono, S. T. (2025). RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA. *DJH Dame Journal Hukum*, *1*(1), 111–133.

Fadly, D., Arifin, F., & Irawan, D. (2025). ANALISIS TENTANG PENGARUH POLITIK HUKUM TERHADAP PENEGAKAN HUKUM DI BIDANG SIBER. *Jurnal Kajian Islam Politik Dan Sosial*, *1*(2), 32–47.

Ferdian. (2026). Optimalisasi Penegakan Hukum Terhadap Tindak Pidana Siber di Era Transformasi Digital : Analisis Kritis Regulasi dan Implementasi. *SEIKAT*, *5*(1), 577–582.

Ghiffari, A. Al. (2025). Kejahatan Siber dan Tantangan Penegakan Hukum di Indonesia. *JPIM: Jurnal Penelitian Ilmiah Multidisipliner*, *02*(02), 1295–1299.

Gladys, W., & Bella, O. (2025). PENEGAKAN HUKUM TERHADAP TINDAK PIDANA CYBERCRIME DALAM KASUS PERETASAN DAN PELANGGARAN DATA PRIBADI OLEH HACKER BJORKA. *Jurnal Review Pendidikan Dan Pengajaran*, *8*(4), 8284–8292.

Juniarso, D., & Abdillah, J. (2026). Reformasi Kebijakan Pidana Nasional Terhadap Kejahatan Siber Berbasis Ai Melalui Pendekatan Hukum Progresif. *Jurnal Impresi Indonesia (JII)*, *5*(1), 77–88.

Morion, A., Thomas, R., & Anggraeni, Y. (2025). CYBERCRIME DAN MEDIA SOSIAL ANALIS HUKUM TERHADAP TREN PENINGKATAN TINDAK PIDANA DI ERA DIGITAL CYBERCRIME. *Rewang Rencang : Jurnal Hukum Lex Generalis*, *6*(7), 1–22.

Nai, M. A., & Hoesein, Z. A. (2026). Analisis Yuridis Terhadap Perlindungan Hukum Bagi Korban Kejahatan Siber di Indonesia. *Journal of Innovative and Creativity*, *6*(1), 1637–1644.

Richardo, F., Wanggai, M., Hartono, M. S., Putu, N., & Parwati, E. (2026). Analisis Normatif terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber di Indonesia. *Majelis : Jurnal Hukum Indonesia*, *3*(1), 1–9.

Savitri, F. N. M. (2025). PERKEMBANGAN REGULASI DAN TANTANGAN PENEGAKAN HUKUM KEJAHATAN SIBER DI INDONESIA: KESEIMBANGAN ANTARA INOVASI DAN KEPASTIAN HUKUM. *Lontar Merah*, *8*(2), 1–12.