Tantangan Penegakan Hukum terhadap Kejahatan Siber di Era Digital

Ikke Nurjanah[1*]

[1]Universitas Terbuka, Jalan Pondok Cabe Raya, Kec. Ciputat, Tangerang Selatan, Indonesia
*Alamat email penulis koresponden: 055409933@ecampus.ut.ac.id

Abstrak

Penegakan hukum terhadap kejahatan siber di era digital menghadapi tantangan yang kompleks akibat perkembangan teknologi informasi yang pesat dan karakter kejahatan yang lintas yurisdiksi. Artikel ini bertujuan menganalisis pengaturan hukum positif di Indonesia berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), mengidentifikasi kesenjangan hukum (legal gap), serta mengkaji tantangan penegakan hukum oleh aparat penegak hukum. Penelitian ini menggunakan metode hukum normatif dengan pendekatan analisis yuridis kualitatif. Hasil kajian menunjukkan bahwa meskipun UU ITE terbaru memberikan landasan hukum yang lebih komprehensif dan adaptif, masih terdapat kendala implementasi seperti keterbatasan kapasitas teknis aparat, kesulitan koordinasi lintas lembaga dan internasional, serta regulasi yang belum sepenuhnya harmonis. Untuk mengatasi hal tersebut, diperlukan upaya normatif dan strategis berupa penyempurnaan regulasi, peningkatan kompetensi aparat, penguatan infrastruktur forensik digital, serta pengembangan kerja sama nasional dan internasional. Artikel ini menyimpulkan bahwa penegakan hukum kejahatan siber harus mengedepankan prinsip keadilan, kepastian, dan kemanfaatan hukum agar dapat menghadapi dinamika teknologi dan memberikan perlindungan optimal bagi masyarakat.

Kata Kunci: Kejahatan Siber; Penegakan Hukum; Undang-Undang ITE; Teknologi Digital

Abstract

Law enforcement against cybercrime in the digital era faces complex challenges due to the rapid development of information technology and the cross-jurisdictional nature of crimes. This article aims to analyze the positive legal regulations in Indonesia based on Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), identify legal gaps, and examine the challenges faced by law enforcement officers. This research uses a normative legal method with a qualitative juridical analysis approach. The study results show that although the latest ITE Law provides a more comprehensive and adaptive legal basis, there are still implementation obstacles such as the limited technical capacity of officers, difficulties in cross-agency and international coordination, and regulations that are not yet fully harmonized. To address these issues, normative and strategic efforts are required, including regulatory improvements, capacity building for officers, strengthening digital forensic infrastructure, and developing national and international cooperation. This article concludes that cybercrime law enforcement must prioritize principles of justice, legal certainty, and utility in order to respond to technological dynamics and provide optimal protection for society.

Keywords: Cybercrime; Law Enforcement; ITE Law; Digital Technology

1. PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan mendasar pada struktur sosial, ekonomi, dan interaksi manusia di ruang siber. Di satu sisi, era digital membuka peluang besar bagi peningkatan efisiensi, keterhubungan, dan inovasi layanan publik; di sisi lain, selain itu juga memunculkan berbagai bentuk kejahatan siber yang semakin kompleks, lintas yurisdiksi, dan sulit dikendalikan melalui mekanisme konvensional penegakan hukum. Kejahatan seperti peretasan sistem elektronik, pencurian data pribadi, penipuan berbasis online, penyebaran konten hoaks, *cyber-bullying* hingga pengancaman melalui media sosial menuntut aparat penegak hukum untuk beradaptasi dengan cepat terhadap karakteristik ruang digital yang dinamis (Waluyadi, 2024).

Secara normatif, Indonesia telah melakukan pembaruan signifikan melalui UU ITE terbaru, yaitu Undang-Undang Nomor 1 Tahun 2024 yang mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini menambah dan merevisi sejumlah pasal, di antaranya pengaturan alat bukti elektronik, sertifikasi elektronik, tanggung jawab penyelenggara sistem elektronik, serta penambahan pasal baru terkait layanan sertifikasi, pelindungan anak di ruang digital, dan kewajiban pemerintah dalam menciptakan ekosistem digital yang adil, akuntabel dan aman. Meskipun demikian, sejumlah penelitian terdahulu menunjukkan bahwa dalam praktik penegakan hukum terhadap kejahatan siber masih terdapat gap normatif dan implementatif. Sebagai contoh, studi oleh Aprianto dan Putranto (2022) menyoroti bahwa rumusan delik ujaran kebencian melalui media sosial masih menghadapi tantangan multitafsir dan inkonsistensi penerapan. Begitu pula penelitian oleh Santoso & Lestari (2023) mengemukakan bahwa koordinasi antar-lembaga penegak hukum dan pertukaran data lintas yurisdiksi dalam kasus kejahatan siber belum optimal dan sering terhambat karena kerangka regulasi yang belum adaptif terhadap evolusi teknologi.

Dari kajian tersebut muncul *legal gap* penting: pertama, regulasi yang ada meskipun sudah diperbarui melalui UU No 1 tahun 2024 masih belum secara spesifik menangani seluruh aspek kejahatan siber modern seperti *ransomware, deep-fake,* manipulasi algoritma, atau kejahatan berbasis blockchain. Kedua, terdapat kesenjangan antara norma yang tertulis dengan kapasitas institusional penegakan misalnya dalam hal bukti elektronik, yurisdiksi, kerjasama internasional, dan kejelasan kompetensi penegak hukum. Ketiga, meskipun UU ITE terbaru memuat berbagai pembaruan, aspek penerapan dan penegakan di lapangan belum mencerminkan adaptasi penuh terhadap perubahan cepat teknologi digital dan modus kejahatan yang semakin canggih.

Melihat kondisi tersebut, penelitian ini mengambil kebaruan dalam dua hal utama: (1) melakukan analisis normatif terhadap efektivitas UU 1/2024 dalam menjawab tantangan penegakan hukum kejahatan siber, dengan fokus khusus pada aspek bukti elektronik, yurisdiksi digital, dan kerangka tanggung jawab penyelenggara sistem elektronik; (2) menawarkan rekomendasi normatif bagi reformasi hukum dan kebijakan penegakan agar sistem hukum nasional menjadi adaptif terhadap karakteristik kejahatan siber di era digital. Urgensi penelitian ini tidak dapat diabaikan: di tengah percepatan transformasi digital dan meningkatnya interkoneksi global, kegagalan menegakkan hukum secara efektif terhadap kejahatan siber dapat berdampak serius terhadap keamanan nasional, perlindungan hak asasi manusia, kepercayaan publik terhadap sistem digital, hingga stabilitas ekonomi dan sosial. Dengan demikian, penelitian ini diharapkan memberi kontribusi teoretis maupun praktis bagi

pembaruan hukum nasional dan strategi penegakan hukum di ruang siber yang semakin kompleks.

2. METODE

Penelitian ini menggunakan metode penelitian hukum normatif (yuridis normatif), yaitu penelitian yang menitikberatkan pada kajian terhadap norma-norma hukum positif, asas hukum, dan doktrin yang berkaitan dengan penegakan hukum terhadap kejahatan siber di era digital. Pendekatan normatif dipilih karena permasalahan yang dikaji bersifat konseptual dan regulatif, bukan empiris, sehingga analisis difokuskan pada evaluasi terhadap ketentuan hukum yang berlaku dan kesesuaiannya dengan perkembangan bentuk-bentuk kejahatan siber yang terus berevolusi seiring kemajuan teknologi informasi. Penelitian ini memadukan beberapa pendekatan hukum, yaitu pendekatan perundang-undangan, dan pendekatan konseptual. Pendekatan perundang-undangan dilakukan melalui telaah terhadap peraturan perundang-undangan yang relevan, khususnya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-Undang Hukum Pidana (KUHP), serta sejumlah peraturan pelaksana lainnya yang berkaitan dengan aktivitas di ruang digital. Pendekatan konseptual digunakan untuk menelaah asas dan prinsip hukum yang mendasari penegakan hukum siber, seperti asas legalitas, yurisdiksi lintas batas, perlindungan hak privasi, dan prinsip proporsionalitas dalam pembatasan kebebasan berekspresi di dunia maya. Data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh melalui studi kepustakaan. Sumber data meliputi bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa buku, jurnal ilmiah, dan artikel penelitian, sedangkan ahan hukum tersier seperti kamus hukum serta ensiklopedia hukum. Seluruh bahan hukum yang terkumpul kemudian dianalisis menggunakan metode analisis kualitatif, yaitu dengan menafsirkan ketentuan hukum yang ada, membandingkannya dengan teori dan prinsip hukum yang berlaku, serta mengaitkannya dengan dinamika perkembangan kejahatan siber di era digital (Marzuki, P.M., 2017).

3. HASIL DAN PEMBAHASAN

3.1 Pengaturan Hukum Positif Indonesia dalam Mengatur Tindak Pidana Kejahatan Siber Berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan tonggak penting dalam pengaturan hukum positif Indonesia terkait tindak pidana kejahatan siber di era digital. Pembaruan ini dilakukan sebagai respons atas pesatnya perkembangan teknologi informasi dan komunikasi yang membawa konsekuensi kompleks terhadap ranah hukum, khususnya dalam menanggulangi kejahatan yang menggunakan sarana elektronik. Secara normatif, UU ITE versi terbaru ini memperluas definisi dan cakupan tindak pidana siber, menyesuaikan pengaturan dengan modus operandi baru yang muncul akibat kemajuan teknologi digital. Misalnya, dalam Pasal-pasal baru dan revisi, UU ITE mengakomodasi berbagai jenis tindak pidana siber, mulai dari akses ilegal, penyebaran konten berbahaya, pencurian data, manipulasi sistem elektronik, hingga kejahatan yang terkait dengan transaksi elektronik dan penyalahgunaan informasi (Indradjaja, M. A. P., et al., 2024).

Salah satu aspek penting yang diatur dalam UU ITE terbaru adalah penguatan legitimasi bukti elektronik sebagai alat bukti yang sah dalam proses peradilan, sebagaimana diatur dalam pasal yang mengatur tentang alat bukti digital. Hal ini menjadi sangat krusial mengingat karakteristik kejahatan siber yang mengandalkan data elektronik yang bersifat tidak kasat mata dan mudah termanipulasi. Dengan demikian, pembuktian dalam kasus kejahatan siber dapat berjalan lebih efektif dan sesuai dengan prinsip keadilan hukum. Selain itu, UU Nomor 1 Tahun 2024 juga menegaskan tanggung jawab penyelenggara sistem elektronik, mewajibkan mereka untuk menjaga keamanan sistem dan data, sehingga memberikan kerangka hukum yang jelas dalam hal perlindungan konsumen dan pengguna teknologi digital (Waluyadi, 2024).

Meski demikian, tantangan masih muncul dalam praktik penegakan hukum karena beberapa ketentuan dalam UU ITE masih memiliki ruang interpretasi yang dapat menimbulkan multitafsir, terutama dalam pasal-pasal yang mengatur penyebaran informasi yang dapat merugikan pihak lain. Perubahan pasal-pasal tersebut mencoba mengakomodasi perlindungan kebebasan berekspresi sekaligus mengantisipasi penyalahgunaan yang dapat menyebabkan kerugian nyata, namun batasan-batasan ini belum sepenuhnya dapat menjawab kompleksitas permasalahan di lapangan, terutama terkait dengan konten-konten yang bersifat provokatif dan ujaran kebencian di media sosial. Lebih jauh, UU ITE terbaru berupaya mengakomodasi dinamika transformasi digital dengan memasukkan ketentuan yang mengatur mengenai keamanan siber secara lebih rinci dan tanggung jawab pelaku usaha digital. Pengaturan ini penting dalam membangun ekosistem digital yang aman dan terpercaya, sehingga mendukung perkembangan ekonomi digital yang saat ini menjadi salah satu fokus pembangunan nasional. Akan tetapi, peraturan tersebut juga menuntut aparat penegak hukum untuk memiliki kapasitas teknis yang memadai agar dapat mengimplementasikan regulasi secara efektif, termasuk dalam melakukan investigasi dan penindakan terhadap tindak pidana yang bersifat kompleks dan menggunakan teknologi tinggi (Fadli, M. A., 2023 ; Indradjaja, M. A. P., et al., 2024).

Secara keseluruhan, pengaturan hukum positif di Indonesia melalui UU Nomor 1 Tahun 2024 telah menunjukkan kemajuan normatif yang signifikan dalam mengakomodasi kebutuhan penegakan hukum terhadap kejahatan siber di era digital. Regulasi ini memberikan landasan hukum yang lebih kuat dan jelas untuk mengatur tindak pidana siber, mempertegas legalitas alat bukti elektronik, serta memperluas tanggung jawab penyelenggara sistem elektronik. Namun, implementasi di lapangan masih menghadapi berbagai kendala, mulai dari kemampuan teknis aparat penegak hukum, interpretasi hukum yang belum seragam, hingga tantangan teknologi yang terus berkembang. Oleh karena itu, meskipun kerangka hukum positif sudah diperbarui, penegakan hukum terhadap kejahatan siber tetap membutuhkan dukungan berupa peningkatan kapasitas sumber daya manusia, pengembangan teknologi forensik digital, serta integrasi kerja sama lintas lembaga dan internasional agar regulasi dapat diterapkan secara optimal dan efektif dalam menghadapi tantangan kejahatan siber di era digital.

3.2 Bentuk dan Faktor Penyebab Kesenjangan Hukum (Legal Gap) dalam Penegakan Hukum Kejahatan Siber di Indonesia

Kesenjangan hukum (*legal gap*) dalam penegakan hukum terhadap kejahatan siber di Indonesia merupakan salah satu isu krusial yang menghambat efektivitas penerapan hukum di era digital. Istilah *legal gap* mengacu pada ketidaksesuaian antara norma hukum yang berlaku dengan realitas sosial, teknologis, dan praktik penegakan hukum di lapangan. Dalam konteks kejahatan siber, kesenjangan ini muncul karena hukum yang berlaku sering kali tertinggal dari

perkembangan teknologi informasi yang sangat cepat, sementara sistem penegakan hukum belum sepenuhnya siap mengadaptasi diri terhadap karakteristik ruang digital yang lintas batas, anonim, dan berteknologi tinggi. Walaupun Indonesia telah melakukan dua kali revisi terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terakhir melalui Undang-Undang Nomor 1 Tahun 2024 reformasi normatif ini masih menyisakan sejumlah celah hukum yang menyebabkan lemahnya perlindungan hukum terhadap masyarakat digital serta tidak optimalnya proses penegakan hukum terhadap pelaku kejahatan siber.

Bentuk kesenjangan hukum pertama dapat ditemukan pada aspek substansi hukum atau materi peraturan perundang-undangan itu sendiri. Meskipun UU ITE telah mengatur berbagai bentuk tindak pidana siber seperti akses ilegal, intersepsi tanpa izin, perusakan sistem elektronik, serta penyebaran konten bermuatan kebencian atau pencemaran nama baik, regulasi tersebut belum sepenuhnya mencakup bentuk-bentuk kejahatan digital baru yang muncul akibat inovasi teknologi. Fenomena seperti *ransomware*, *phishing* berbasis kecerdasan buatan (AI), *deepfake*, *cyber grooming*, dan manipulasi data berbasis *blockchain* masih belum memiliki dasar pengaturan yang jelas. Kekosongan hukum ini menjadikan aparat penegak hukum sering kali menafsirkan pasal-pasal UU ITE secara ekstensif untuk menjerat pelaku, yang pada akhirnya menimbulkan ketidakpastian hukum dan potensi pelanggaran terhadap asas legalitas. Ketertinggalan regulasi ini menunjukkan bahwa pembentuk undang-undang masih bersifat reaktif terhadap perkembangan teknologi, bukan antisipatif, sehingga hukum selalu berada satu langkah di belakang modus kejahatan siber (Dwiandari, A. S., & Arifin, R., 2021).

Bentuk kedua dari kesenjangan hukum terlihat pada aspek struktural atau kelembagaan penegakan hukum. Penegakan hukum terhadap kejahatan siber memerlukan kapasitas teknis dan sumber daya manusia yang memiliki keahlian di bidang digital forensik, keamanan jaringan, serta teknologi informasi. Namun, dalam praktiknya, banyak aparat penegak hukum di tingkat penyidikan dan penuntutan belum memiliki kompetensi memadai untuk menangani kasus siber yang kompleks. Ketergantungan pada ahli eksternal dalam melakukan analisis data elektronik sering kali memperlambat proses penyidikan dan membuka peluang manipulasi bukti. Selain itu, koordinasi antar lembaga penegak hukum, seperti kepolisian, kejaksaan, dan Kementerian Komunikasi dan Informatika, masih belum berjalan secara efektif. Tidak adanya mekanisme terpadu dalam pertukaran data dan penanganan laporan kejahatan siber menyebabkan penegakan hukum berjalan parsial dan tumpang tindih. Keterbatasan anggaran, minimnya infrastruktur digital forensik di daerah, serta belum adanya sistem nasional yang terintegrasi untuk penanganan tindak pidana siber memperparah ketimpangan ini (Azzahra, M., et al., 2022).

Kesenjangan hukum juga muncul pada aspek kultural dan pemahaman hukum, baik di kalangan penegak hukum maupun masyarakat. Dalam beberapa kasus, aparat penegak hukum masih menafsirkan pasal-pasal UU ITE dengan pendekatan hukum konvensional yang tidak sesuai dengan karakteristik ruang siber. Misalnya, masih sering terjadi kekeliruan dalam membedakan antara pelanggaran etika komunikasi digital dengan tindak pidana siber, sehingga beberapa kasus justru menimbulkan kriminalisasi terhadap ekspresi warga di media sosial. Hal ini memperlihatkan lemahnya pemahaman terhadap asas *ultimum remedium* dalam hukum pidana, di mana penegakan hukum pidana seharusnya menjadi upaya terakhir, bukan alat represif terhadap kebebasan berekspresi. Di sisi lain, kesadaran hukum masyarakat digital juga masih rendah. Banyak pengguna internet yang tidak memahami batasan antara kebebasan berekspresi dan ujaran kebencian, serta tidak menyadari risiko hukum dari aktivitas di ruang siber seperti

penyebaran data pribadi atau informasi hoaks. Kondisi ini menunjukkan adanya kesenjangan pemahaman hukum yang berkontribusi terhadap meningkatnya potensi pelanggaran di dunia maya (Hasri, H., et al., 2021).

Selain kesenjangan substansi, struktur, dan budaya hukum, faktor penyebab lainnya adalah keterbatasan yurisdiksi hukum nasional dalam menangani kejahatan siber lintas batas negara. Sebagian besar kejahatan siber bersifat transnasional, di mana pelaku, korban, dan sistem yang diserang berada di negara yang berbeda. Dalam situasi seperti ini, penegakan hukum nasional tidak dapat berjalan efektif tanpa kerja sama internasional yang kuat. Indonesia sendiri belum menjadi pihak dalam *Budapest Convention on Cybercrime*, sebuah instrumen hukum internasional yang menjadi standar global dalam penanggulangan kejahatan siber lintas negara. Akibatnya, penegakan hukum terhadap pelaku yang beroperasi dari luar wilayah yurisdiksi Indonesia sering kali menemui jalan buntu karena keterbatasan mekanisme *mutual legal assistance* (MLA) dan ekstradisi. Hal ini memperlemah posisi Indonesia dalam menghadapi ancaman kejahatan siber berskala global, sekaligus memperlebar jarak antara norma hukum nasional dan kebutuhan penegakan hukum modern (Fadli, M. A., et al., 2023).

Dari seluruh uraian tersebut, tampak bahwa kesenjangan hukum dalam penegakan kejahatan siber di Indonesia bersifat multidimensional. Di satu sisi, pembaruan hukum positif melalui UU Nomor 1 Tahun 2024 sudah menunjukkan kemajuan normatif yang berarti, terutama dalam memperjelas delik elektronik, memperkuat alat bukti digital, dan menegaskan tanggung jawab penyelenggara sistem elektronik. Namun di sisi lain, penerapannya masih dibatasi oleh kelemahan struktural, rendahnya kapasitas teknis, minimnya kerja sama lintas sektor, dan keterlambatan adaptasi terhadap perubahan teknologi. Dengan demikian, untuk menutup *legal gap* tersebut diperlukan reformasi hukum yang bersifat holistik, mencakup pembaruan substansi hukum yang responsif terhadap inovasi digital, penguatan kapasitas kelembagaan penegak hukum, peningkatan literasi hukum masyarakat, serta integrasi Indonesia dalam kerja sama internasional di bidang keamanan siber. Hanya dengan pendekatan tersebut, hukum nasional dapat menjadi instrumen yang efektif, adil, dan adaptif dalam menegakkan keadilan di ruang siber.

3.3 Tantangan Aparat Penegak Hukum dalam Menerapkan Ketentuan Hukum terhadap Kejahatan Siber yang Bersifat Lintas Yurisdiksi dan Berbasis Teknologi Tinggi

Penegakan hukum terhadap kejahatan siber yang bersifat lintas yurisdiksi dan berbasis teknologi tinggi menghadirkan tantangan kompleks bagi aparat penegak hukum di Indonesia. Karakteristik kejahatan siber yang melibatkan ruang digital tanpa batas geografis membuat proses penyidikan, penuntutan, hingga eksekusi hukum menjadi jauh lebih rumit dibandingkan dengan tindak pidana konvensional. Tantangan ini tidak hanya bersumber dari aspek teknis dan hukum, tetapi juga berasal dari kelembagaan, sumber daya manusia, serta kerangka kerja sama internasional yang belum optimal. Salah satu tantangan utama adalah kerumitan dalam penanganan bukti elektronik yang menjadi kunci dalam penyidikan kejahatan siber. Bukti yang berupa data digital sangat rentan terhadap manipulasi, hilang, atau rusak jika tidak ditangani dengan prosedur forensik yang ketat (Santoso, B., & Lestari, M., 2023). Oleh karena itu, aparat penegak hukum harus memiliki keahlian khusus dalam digital forensik serta pemahaman mendalam tentang teknologi yang digunakan oleh pelaku kejahatan. Namun, kenyataannya kemampuan teknis aparat masih terbatas dan belum merata di seluruh wilayah Indonesia.

Keterbatasan ini mengakibatkan proses pengumpulan dan pengamanan bukti menjadi lambat dan rentan kegagalan pembuktian di pengadilan.

Selain itu, kejahatan siber yang bersifat lintas yurisdiksi memunculkan tantangan besar dalam hal yurisdiksi hukum dan koordinasi antarnegara. Karena pelaku kejahatan, korban, dan sistem yang diserang dapat berada di negara berbeda, penegakan hukum membutuhkan kerja sama internasional yang solid dan mekanisme hukum yang jelas, seperti *mutual legal assistance* (MLA) dan perjanjian ekstradisi. Namun, Indonesia belum menjadi pihak dalam konvensi internasional seperti *Budapest Convention on Cybercrime*, sehingga menghadapi kesulitan dalam melakukan kerja sama hukum lintas batas. Proses hukum internasional sering kali memakan waktu lama dan dipenuhi birokrasi, sehingga pelaku kejahatan dapat leluasa menghindari penangkapan dan penuntutan. Kondisi ini memperlemah efektivitas penegakan hukum di tingkat nasional terhadap kejahatan siber yang melibatkan jaringan global (Indradjaja, M. A. P., et al., 2024).

Tantangan berikutnya adalah perkembangan teknologi yang sangat cepat dan dinamis, sehingga aparat penegak hukum harus selalu memperbarui pengetahuan dan keterampilannya agar dapat mengikuti modus operandi terbaru pelaku kejahatan siber. Misalnya, penggunaan teknik enkripsi canggih, teknologi blockchain, dan kecerdasan buatan dalam aktivitas kriminal digital membutuhkan pemahaman teknis tingkat tinggi. Ketidaksiapan aparat dalam menghadapi teknologi tersebut sering mengakibatkan keterlambatan dalam deteksi dan penanganan kasus. Di samping itu, teknologi yang terus berkembang juga membuka peluang baru bagi pelaku kejahatan untuk melakukan aksi dengan cara yang semakin sulit dilacak dan dibuktikan secara hokum (Hermawati, N., & Santiago, F. 2023).

Dari segi regulasi dan ketentuan hukum, meskipun Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE telah memperbarui banyak aspek hukum siber, masih terdapat kesenjangan normatif yang tidak sepenuhnya mengakomodasi kejahatan siber berbasis teknologi tinggi dan lintas yurisdiksi. Ketidakjelasan definisi dan batasan dalam beberapa pasal menyebabkan aparat penegak hukum mengalami kesulitan dalam menerapkan hukum secara konsisten dan tepat sasaran. Hal ini diperparah dengan masih adanya ketidaksesuaian antara hukum nasional dengan hukum negara lain yang terlibat dalam kasus lintas batas, sehingga sulit menentukan prioritas yurisdiksi dan pelaksanaan hukum bersama (Waluyadi, W., 2024).

Kendala lain yang signifikan adalah terbatasnya sumber daya manusia dan infrastruktur penegakan hukum. Aparat penegak hukum masih kekurangan tenaga ahli yang kompeten di bidang teknologi informasi dan keamanan siber. Selain itu, infrastruktur digital forensik, laboratorium kriminalistik, serta sistem pelaporan dan pengawasan keamanan siber di tingkat nasional maupun daerah masih belum memadai. Ketiadaan fasilitas dan alat yang memadai memperlambat proses identifikasi dan penyidikan kejahatan siber. Ini juga berimbas pada minimnya kapasitas aparat dalam melakukan edukasi dan pencegahan kejahatan siber di masyarakat, yang seharusnya menjadi bagian penting dari strategi penanggulangan (Fitriani, S., 2021).

Secara kelembagaan, tantangan muncul dari koordinasi yang belum optimal antar lembaga terkait seperti kepolisian, kejaksaan, Kementerian Komunikasi dan Informatika, serta instansi pemerintah lainnya yang terlibat dalam penanganan kasus siber. Kurangnya integrasi data dan informasi serta prosedur kerja yang tumpang tindih menyebabkan inefisiensi dan hambatan

dalam proses penyelesaian perkara. Keterbatasan sinergi ini menurunkan efektivitas penegakan hukum dan mengurangi kepercayaan publik terhadap kemampuan negara dalam menangani kejahatan siber (Aprianto, R., & Putranto, D., 2022).

Secara keseluruhan, tantangan yang dihadapi aparat penegak hukum dalam menegakkan ketentuan hukum terhadap kejahatan siber lintas yurisdiksi dan berbasis teknologi tinggi sangat kompleks dan multidimensional. Untuk mengatasinya, diperlukan upaya strategis berupa peningkatan kapasitas teknis aparat melalui pelatihan dan pendidikan khusus, pengembangan infrastruktur digital forensik yang memadai, serta penguatan kerangka hukum nasional yang responsif dan adaptif terhadap perkembangan teknologi. Selain itu, integrasi dan koordinasi antar lembaga penegak hukum perlu diperkuat, disertai dengan perluasan kerja sama internasional guna mempercepat proses hukum lintas negara. Dengan langkah-langkah tersebut, penegakan hukum terhadap kejahatan siber di Indonesia dapat berjalan lebih efektif dan mampu memberikan perlindungan yang optimal bagi masyarakat di era digital.

3.4 Upaya Normatif dan Strategis untuk Memperkuat Efektivitas Penegakan Hukum terhadap Kejahatan

Penegakan hukum terhadap kejahatan siber di era digital menghadapi tantangan yang sangat kompleks, sehingga diperlukan upaya normatif dan strategis yang komprehensif untuk memperkuat efektivitasnya dengan tetap mengedepankan prinsip keadilan, kepastian, dan kemanfaatan hukum. Secara normatif, langkah awal yang krusial adalah melakukan pembaruan dan penyempurnaan regulasi hukum yang adaptif terhadap perkembangan teknologi digital. Pembaruan ini tidak hanya sebatas revisi pasal-pasal dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tetapi juga harus meliputi harmonisasi regulasi lintas sektor yang terkait, seperti perlindungan data pribadi, keamanan siber, dan perlindungan konsumen digital. Harmonisasi ini penting agar tidak terjadi tumpang tindih aturan yang dapat menimbulkan ketidakpastian hukum bagi penegak dan pengguna teknologi digital. Regulasi yang jelas dan komprehensif akan memberikan kepastian hukum bagi masyarakat dan menjadi landasan yang kuat bagi aparat penegak hukum dalam menjalankan tugasnya secara adil dan konsisten (Azzahra, M., et al., 2022).

Selain itu, secara strategis, peningkatan kapasitas sumber daya manusia penegak hukum menjadi hal yang tak kalah penting. Aparat penegak hukum harus dibekali dengan pendidikan dan pelatihan khusus yang berkelanjutan dalam bidang teknologi informasi dan forensik digital agar mampu memahami karakteristik kejahatan siber yang dinamis dan kompleks. Penguasaan teknologi mutakhir akan memudahkan proses investigasi, pengumpulan bukti elektronik yang sah, serta penuntutan yang efektif di pengadilan. Pelatihan ini juga harus mencakup pemahaman terhadap hak asasi manusia dan prinsip keadilan agar penegakan hukum tidak menjadi represif atau diskriminatif terhadap kebebasan berekspresi di dunia maya. Dengan demikian, aparat penegak hukum dapat menjalankan tugasnya secara profesional sekaligus menjaga keseimbangan antara penegakan hukum dan perlindungan hak individu. Kemudian penguatan institusi dan infrastruktur penegakan hukum juga menjadi upaya strategis yang tidak dapat diabaikan. Pengembangan laboratorium forensik digital yang dilengkapi dengan peralatan canggih dan sistem manajemen data terintegrasi akan mempercepat proses analisis bukti serta meningkatkan akurasi dan kredibilitas hasil penyidikan. Lebih jauh, perlu dibangun sistem koordinasi dan sinergi antar lembaga penegak hukum, seperti kepolisian, kejaksaan, dan Kementerian Komunikasi dan Informatika, agar dapat berbagi informasi dan bekerjasama secara efektif dalam menangani kasus kejahatan siber yang sering kali lintas wilayah dan sektor. Sistem terpadu ini akan meminimalisasi duplikasi tugas, mempercepat proses

penyelesaian kasus, serta meningkatkan akuntabilitas dan transparansi penegakan hokum (Fajrin, Y. A., et al., 2023)

Selain upaya internal, penguatan kerja sama internasional menjadi faktor strategis yang tidak kalah penting. Kejahatan siber yang bersifat lintas yurisdiksi menuntut adanya mekanisme kerja sama hukum lintas negara yang efektif, seperti mutual legal assistance (MLA), ekstradisi, dan pertukaran intelijen siber. Indonesia perlu aktif menjadi bagian dari konvensi internasional di bidang keamanan siber, seperti *Budapest Convention on Cybercrime*, guna memperluas jejaring kerja sama dan mempercepat proses hukum terhadap pelaku kejahatan siber yang beroperasi dari luar wilayah nasional. Kerja sama internasional yang solid akan memperkuat kemampuan Indonesia dalam menghadapi kejahatan siber global sekaligus menjaga kedaulatan dan keamanan digital nasional (Indradjaja, M. A. P., et al., 2024).

Dalam konteks masyarakat, peningkatan literasi digital dan kesadaran hukum juga merupakan upaya strategis penting. Pemerintah dan lembaga terkait harus menjalankan program edukasi yang bertujuan meningkatkan pemahaman masyarakat mengenai risiko kejahatan siber, hak dan kewajiban sebagai pengguna teknologi digital, serta tata cara melaporkan tindak pidana siber. Kesadaran hukum yang tinggi akan mendorong partisipasi aktif masyarakat dalam pencegahan kejahatan siber dan mengurangi kerentanan terhadap modus kejahatan digital (Santoso, B., & Lestari, M., 2023). Dengan demikian, penegakan hukum tidak hanya menjadi tanggung jawab aparat saja, tetapi juga melibatkan peran serta seluruh lapisan masyarakat dalam membangun ekosistem digital yang aman dan terpercaya.

Secara keseluruhan, upaya normatif dan strategis yang menyeluruh tersebut merupakan kunci untuk memperkuat efektivitas penegakan hukum terhadap kejahatan siber di era digital. Melalui pembaruan regulasi yang adaptif dan harmonis, peningkatan kapasitas aparat penegak hukum, penguatan institusi dan infrastruktur, pengembangan kerja sama internasional, serta edukasi masyarakat, prinsip keadilan, kepastian, dan kemanfaatan hukum dapat diwujudkan secara optimal. Dengan demikian, penegakan hukum terhadap kejahatan siber tidak hanya menjadi respons terhadap ancaman teknologi, tetapi juga menjadi instrumen yang mampu memberikan perlindungan hukum yang adil, jelas, dan bermanfaat bagi seluruh masyarakat di tengah pesatnya transformasi digital.

4. KESIMPULAN

Penegakan hukum terhadap kejahatan siber di era digital menghadirkan berbagai tantangan yang kompleks, baik dari aspek regulasi, teknis, maupun koordinasi lintas lembaga dan negara. Undang-Undang Nomor 1 Tahun 2024 sebagai revisi terbaru UU ITE telah memberikan kerangka hukum yang lebih kuat dan adaptif dalam mengatur tindak pidana siber, termasuk penguatan legitimasi bukti elektronik dan tanggung jawab penyelenggara sistem elektronik. Namun demikian, masih terdapat kesenjangan hukum dan kendala implementasi yang harus diatasi agar penegakan hukum berjalan efektif dan berkeadilan. Untuk itu, diperlukan upaya normatif berupa penyempurnaan regulasi yang harmonis serta langkah strategis seperti peningkatan kapasitas sumber daya manusia aparat penegak hukum, pengembangan infrastruktur forensik digital, penguatan koordinasi antar lembaga, serta perluasan kerja sama internasional dalam menghadapi kejahatan siber yang lintas yurisdiksi. Selain itu, peningkatan literasi dan kesadaran masyarakat tentang keamanan digital menjadi bagian penting dalam membangun ekosistem yang kondusif bagi penegakan hukum. Dengan kombinasi langkah-langkah tersebut, penegakan hukum terhadap kejahatan siber dapat mewujudkan prinsip keadilan, kepastian, dan kemanfaatan hukum secara optimal di tengah pesatnya perkembangan teknologi informasi dan komunikasi.

DAFTAR PUSTAKA

Aprianto, R., & Putranto, D. (2022). Problematika penegakan hukum terhadap ujaran kebencian di media sosial berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Lespass: Jurnal Hukum dan Masyarakat, 4*(2), 45–58.

Azzahra, M., Nurwati, N., Prasja, T. R., & Aridhayandi, M. R. (2022). Analisis kasus cyber crime di Indonesia dan tantangan penegakan hukum dalam menghadapinya. *Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan, 16*(1), 1–10. https://doi.org/10.32493/jdmhkdmhk.v16i1.47688

Dwiandari, A. S., & Arifin, R. (2021). Criminal law enforcement on digital identity misuse in AI era for commercial interests in Indonesia. *The Indonesian Journal of International Clinical Legal Education, 7*(1), 1–10. https://doi.org/10.15294/iccle.v7i1.25525

Fadli, M. A., Hatta, M., Isvani, I., Dhipinto, A., Anjelia, D., & Sari, R. (2023). Obstacles and challenge of law enforcement in the face of mayantara crime in Indonesia. *International Journal of Law, Crime and Justice, 2*(1), 1–10. https://doi.org/10.62951/ijlcj.v2i1.540

Fajrin, Y. A., Rasyid, M. F. F., Ginting, G., Endrawati, E. A., & Putri, V. S. (2023). Critical analysis of the Republic of Indonesia Police in the implementation of cybercrime law in Indonesia. *Journal Equity of Law and Governance, 4*(1), 119–128. https://doi.org/10.55637/elg.4.1.9510.119-128

Fitriani, S. (2021). Kendala pembuktian tindak pidana siber dalam sistem peradilan pidana di Indonesia. *Jurnal Hukum dan Pembangunan, 51*(3), 321–340.

Hasri, H., Mashendra, M., Hayun, H., & Nisa, F. N. (2021). Kejahatan cybercrime dan penanggulangannya dalam kerangka sistem hukum nasional. *Indonesian Journal of Legality of Law, 7*(2), 1–10. https://doi.org/10.35965/ijlf.v7i2.6240

Hermawati, N., & Santiago, F. (2023). Law enforcement against cybercrime in online activities. *Edunity Kajian Ilmu Sosial dan Pendidikan, 1*(5), 33–42. https://doi.org/10.57096/edunity.v1i05.33

Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi penyidikan terhadap tindak pidana siber dalam perspektif perbandingan hukum: Indonesia dan Inggris Raya. *Jurnal Ilmiah Penegakan Hukum, 11*(2), 162–172. https://doi.org/10.31289/jiph.v11i2.12931

Marzuki, P. M. (2017). *Penelitian hukum (Edisi revisi)*. Jakarta: Kencana Prenada Media Grup.

Rahmadani, A. (2022). Koordinasi antar lembaga penegak hukum dalam penanganan kejahatan siber lintas yurisdiksi di Indonesia. *Jurnal Hukum dan Kebijakan Publik, 8*(1), 77–92.

Santoso, B., & Lestari, M. (2023). Koordinasi antar-lembaga penegak hukum dalam penanganan kejahatan siber lintas yurisdiksi di Indonesia. *Jurnal Hukum dan Kebijakan Publik, 8*(1), 77–92.

Sitompul, F., Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. (2021). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam hukum Indonesia. *Jaksa: Jurnal Kajian Ilmu Hukum dan Politik, 2*(2), 1–10. https://doi.org/10.51903/jaksa.v2i2.1668

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2024). *Lembaran Negara Republik Indonesia Tahun 2024 Nomor 3*.

Waluyadi, W. (2024). Law enforcement against cyber crimes in Indonesia: Analysis of the role of the ITE law in handling cyber crimes. *Indonesian Cyber Law Review, 1*(2), 5–15. https://doi.org/10.59261/iclr.v1i1.5