DINAMIKA HUKUM PIDANA DALAM MENANGGAPI KEJAHATAN SIBER DI ERA DIGITAL

Mahesa Dhio Syahputra
dhiomahesa141@gmail.com
Universitas Muhammadiyah Magelang

ABSTRAK

Perkembangan teknologi informasi telah menyebabkan munculnya kejahatan siber yang menjadi tantangan besar bagi sistem hukum pidana Indonesia. Meskipun Indonesia telah mengatur kejahatan siber melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), terdapat berbagai masalah dalam penerapannya. Penelitian ini bertujuan untuk menganalisis dinamika hukum pidana Indonesia dalam menangani kejahatan siber, termasuk regulasi, penegakan hukum, dan peran lembaga terkait. Metode yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan komparatif. Hasil penelitian menunjukkan bahwa regulasi yang ada masih belum memadai untuk mengatasi perkembangan pesat kejahatan siber. Diperlukan pembaruan dan harmonisasi hukum untuk menanggulangi tantangan tersebut. Penelitian ini memberikan kontribusi bagi pengembangan hukum pidana yang lebih responsif terhadap kejahatan digital.

Kata Kunci: Kejahatan Siber, Hukum Pidana, UU ITE, Penegakan Hukum, Regulasi.

ABSTRACT

The development of information technology has led to the emergence of cybercrime, which poses a significant challenge to Indonesia's criminal justice system. Although Indonesia has regulated cybercrime through Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law), various issues persist in its implementation. This study aims to analyze the dynamics of Indonesian criminal law in addressing cybercrime, including regulations, law enforcement, and the role of related institutions. The research method employed is normative legal research with a legislative and comparative approach. The findings indicate that existing regulations are insufficient to tackle the rapid growth of cybercrime. There is a need for legal reform and harmonization to address these challenges. This research contributes to the development of criminal law that is more responsive to digital offenses.

Keywords: *Cybercrime, Criminal Law, ITE Law, Law Enforcement, Regulation.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, termasuk dalam bidang hukum pidana. Internet sebagai tulang punggung era digital telah menciptakan ruang baru bernama dunia siber (cyberspace), yang memungkinkan interaksi lintas batas negara, waktu, dan ruang. Namun, kemajuan teknologi ini tidak hanya membawa manfaat, tetapi juga memunculkan tantangan baru berupa kejahatan yang bersifat digital, atau yang sering disebut dengan kejahatan siber (cybercrime). Kejahatan ini memiliki karakteristik yang unik, seperti tidak mengenal batas yurisdiksi, menggunakan teknologi canggih, serta memiliki potensi kerugian yang besar baik secara ekonomi maupun sosial (Arief, 2018).

Kejahatan siber mencakup berbagai bentuk pelanggaran hukum, mulai dari penipuan online (online fraud), peretasan sistem komputer (hacking), pencurian identitas (identity theft), penyebaran malware dan ransomware, hingga penyebaran informasi bohong (hoaks) dan ujaran kebencian (hate speech) melalui media sosial. Karakteristik utama dari kejahatan siber adalah penggunaan perangkat elektronik dan jaringan internet sebagai sarana utama dalam melakukan tindak pidana. Dalam konteks ini, hukum pidana konvensional sering kali mengalami kesulitan dalam menjangkau dan mengadili pelaku

kejahatan siber, mengingat bentuk dan modus operandi dari kejahatan ini yang terus berkembang secara dinamis (Marzuki, 2021).

Di Indonesia, upaya penanggulangan kejahatan siber telah diakomodasi melalui berbagai regulasi, di antaranya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui dengan Undang-Undang Nomor 19 Tahun 2016. Meski demikian, regulasi tersebut masih menyisakan sejumlah persoalan, seperti multitafsir terhadap beberapa pasal, belum optimalnya perlindungan terhadap korban, serta keterbatasan kapasitas aparat penegak hukum dalam menghadapi kejahatan siber yang bersifat lintas negara dan sangat teknis. Selain itu, masih terdapat kesenjangan antara perkembangan teknologi digital dan kecepatan legislasi yang dibuat oleh negara (Sihombing, 2020).

Hukum pidana sebagai alat pengendali sosial (social control) dituntut untuk adaptif dan responsif terhadap transformasi sosial yang dihasilkan oleh teknologi digital. Hal ini selaras dengan prinsip lex temporis, yakni hukum pidana harus senantiasa relevan dengan zaman dan kebutuhan masyarakat. Namun, di sisi lain, hukum pidana juga dihadapkan pada prinsip nullum crimen sine lege yang membatasi perluasan interpretasi hukum secara berlebihan agar tidak menimbulkan ketidakpastian hukum dan pelanggaran terhadap hak asasi manusia (Sudarto, 1983).

Dalam konteks tersebut, penting untuk menganalisis bagaimana dinamika hukum pidana nasional dalam menghadapi kejahatan siber di era digital, baik dari aspek regulasi, penegakan hukum, hingga peran kelembagaan yang berwenang. Kajian ini tidak hanya penting secara akademik, tetapi juga memiliki urgensi praktis dalam mendorong pembaruan hukum pidana yang mampu menjawab tantangan zaman, sekaligus melindungi masyarakat dari ancaman kejahatan digital yang semakin kompleks.

Dengan demikian, tulisan ini bertujuan untuk menelaah secara kritis perkembangan hukum pidana Indonesia dalam merespons fenomena kejahatan siber, mengidentifikasi hambatan-hambatan yang dihadapi, serta merumuskan gagasan pembaruan yang diperlukan agar hukum pidana dapat menjalankan fungsinya secara optimal di tengah transformasi digital yang terus berlangsung.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu metode yang menitikberatkan pada studi terhadap norma-norma hukum yang tertuang dalam peraturan perundang-undangan dan literatur hukum sebagai bahan utama dalam menganalisis permasalahan (Soekanto & Mamudji, 2004). Pemilihan metode ini didasarkan pada fokus penelitian yang hendak mengkaji efektivitas hukum pidana Indonesia dalam merespons kejahatan siber, yang pada dasarnya memerlukan analisis terhadap sistematika hukum, asas-asas hukum pidana, dan keterkaitan antara norma hukum positif dengan perkembangan teknologi informasi.

Pendekatan yang digunakan dalam penelitian ini mencakup pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan komparatif (comparative approach). Pendekatan perundang-undangan dilakukan dengan menelaah regulasi yang relevan seperti KUHP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan dan peraturan pelaksananya. Pendekatan konseptual digunakan untuk memahami teori dan doktrin terkait kejahatan siber, prinsip pertanggungjawaban pidana, serta asas legalitas dalam hukum pidana. Sementara itu, pendekatan komparatif dimanfaatkan untuk membandingkan sistem hukum pidana siber Indonesia dengan negara lain yang telah memiliki sistem regulasi yang lebih mapan seperti Singapura, Estonia, dan negara-negara

anggota Uni Eropa yang telah meratifikasi Budapest Convention (Salim & Nurbani, 2013; Suryani, 2020).

Bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup peraturan perundang-undangan yang berlaku dan putusan pengadilan terkait perkara kejahatan siber. Bahan hukum sekunder meliputi buku, jurnal ilmiah, artikel hukum, serta pendapat para pakar di bidang hukum pidana dan hukum teknologi informasi. Sementara itu, bahan hukum tersier digunakan sebagai pelengkap berupa kamus hukum, ensiklopedia hukum, dan data statistik yang relevan.

Pengumpulan data dilakukan melalui studi kepustakaan (library research) yang bersumber dari database hukum nasional maupun internasional, termasuk jurnal yang terindeks dalam Google Scholar, SINTA, DOAJ, serta bahan literatur dari perpustakaan akademik. Teknik analisis yang digunakan adalah teknik preskriptif-analitis, yang bertujuan tidak hanya untuk menggambarkan keadaan hukum yang berlaku saat ini, tetapi juga untuk memberikan argumentasi hukum dan solusi normatif terhadap kelemahan atau kekosongan pengaturan dalam penanganan kejahatan siber di Indonesia (Marzuki, 2017).

Dengan metode ini, penelitian ini diharapkan mampu memberikan kontribusi teoritik dan praktis dalam pengembangan hukum pidana yang adaptif terhadap tantangan zaman digital serta mampu menjembatani kebutuhan perlindungan masyarakat terhadap ancaman kejahatan berbasis teknologi.

Dalam menganalisis data hukum, pendekatan preskriptif tidak hanya digunakan untuk mendeskripsikan dan menjelaskan substansi hukum yang berlaku, tetapi juga untuk memberikan argumentasi normatif yang diarahkan pada pembentukan hukum yang ideal sesuai dengan kebutuhan masyarakat. Teknik analisis ini memungkinkan penulis untuk mengidentifikasi kekosongan hukum (legal gap), ketidaksesuaian norma (norm conflict), dan kelemahan struktur penegakan hukum dalam konteks kejahatan siber. Dengan demikian, hasil penelitian ini diharapkan tidak hanya berkontribusi pada ranah akademik, tetapi juga memberikan rekomendasi konkret yang dapat dijadikan dasar pembaruan kebijakan pidana nasional (Salim & Nurbani, 2013; Marzuki, 2017)

HASIL DAN PEMBAHASAN

Tantangan Hukum Pidana dalam Menghadapi Kejahatan Siber

Kejahatan siber (cybercrime) merupakan fenomena kriminalitas kontemporer yang tidak hanya berdampak pada keamanan digital, tetapi juga mengancam tatanan hukum, sosial, dan ekonomi suatu negara. Di Indonesia, kejahatan siber berkembang seiring meningkatnya penetrasi internet dan digitalisasi berbagai sektor kehidupan, yang kemudian membuka ruang baru bagi pelaku kejahatan untuk memanfaatkan celah hukum dan teknologi dalam melancarkan aksinya (Suryani, 2020). Bentuk kejahatan siber pun sangat beragam, mulai dari pencurian data pribadi, penipuan daring (online fraud), peretasan sistem informasi, penyebaran konten ilegal, hingga serangan siber terhadap infrastruktur vital negara.

Dalam konteks hukum pidana, tantangan utama dalam menghadapi kejahatan siber terletak pada karakteristiknya yang berbeda dengan kejahatan konvensional. Kejahatan siber bersifat tidak terbatas oleh ruang dan waktu (borderless), dapat dilakukan secara anonim, dan seringkali melibatkan pelaku lintas negara. Hal ini menyebabkan kesulitan dalam menentukan yurisdiksi, pembuktian, serta penegakan hukum secara efektif (Wall, 2007). Sistem hukum pidana Indonesia yang berbasis teritorial menjadi kurang memadai dalam menghadapi kejahatan digital yang transnasional. Selain itu, banyak peraturan pidana yang ada saat ini masih berorientasi pada bentuk kejahatan fisik, sehingga belum

mampu mengakomodasi kompleksitas tindak pidana yang terjadi dalam dunia maya.

Kelemahan Regulasi Hukum Pidana Positif terhadap Kejahatan Siber

Meskipun Indonesia telah memiliki instrumen hukum seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016, namun dalam praktiknya UU tersebut belum sepenuhnya efektif dalam menangani seluruh dimensi kejahatan siber. UU ITE cenderung menitikberatkan pada aspek perlindungan data, transaksi elektronik, dan sanksi administratif, tetapi belum mampu menjangkau secara menyeluruh modus-modus kejahatan siber yang terus berkembang, seperti phishing, malware, ransomware, dan serangan siber terhadap sistem siber kritis nasional (Setiadi, 2022).

Di sisi lain, KUHP sebagai induk hukum pidana nasional masih belum secara eksplisit mengatur tindak pidana siber. KUHP yang saat ini berlaku merupakan produk kolonial yang disusun dalam konteks abad ke-19, sehingga wajar apabila banyak substansi normatifnya tidak mampu menyesuaikan diri dengan perkembangan teknologi informasi dan komunikasi. Upaya pembaruan melalui Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP) memang telah dilakukan, namun ketentuan yang berkaitan dengan kejahatan siber di dalamnya masih terbatas dan belum komprehensif dalam menjangkau berbagai bentuk kejahatan digital kontemporer (Marzuki, 2017).

Perlunya Harmonisasi dan Reformasi Regulasi Hukum Pidana Nasional

Menghadapi realitas tersebut, Indonesia memerlukan reformasi regulasi hukum pidana secara menyeluruh yang tidak hanya memperbarui isi KUHP, tetapi juga melakukan harmonisasi terhadap seluruh peraturan perundang-undangan yang mengatur ranah digital. Harmonisasi ini penting mengingat kejahatan siber sering kali melintasi banyak sektor, seperti perbankan, perlindungan konsumen, keamanan negara, dan hak asasi manusia. Oleh karena itu, pendekatan sistemik dalam perumusan hukum pidana harus dilakukan, termasuk integrasi antara hukum pidana umum dengan hukum administrasi, hukum internasional, dan kebijakan keamanan siber nasional (Salim & Nurbani, 2013).

Dalam kerangka tersebut, konsep technological neutrality dan future-proof legislation harus diadopsi dalam menyusun regulasi hukum pidana siber. Konsep ini mengandaikan bahwa norma hukum tidak seharusnya bersifat terlalu teknis dan kaku, agar tetap relevan dengan perubahan teknologi di masa depan (Brenner, 2010). Regulasi yang terlalu cepat usang karena perkembangan teknologi justru akan menciptakan kekosongan hukum dan ketidakpastian dalam penegakan hukum pidana.

Perbandingan dengan Sistem Hukum Siber Negara Lain

Untuk memperoleh perspektif yang lebih luas, penting untuk membandingkan sistem hukum pidana Indonesia dengan negara-negara lain yang telah berhasil mengembangkan instrumen hukum yang efektif dalam menanggulangi kejahatan siber. Singapura, misalnya, telah memiliki Computer Misuse Act sejak 1993 yang terus diperbarui secara berkala sesuai dengan dinamika teknologi dan pola kejahatan digital. Negara tersebut juga memiliki Cyber Security Agency yang berfungsi sebagai lembaga nasional yang menangani insiden keamanan digital dan koordinasi antar sektor (CSA Singapore, 2021).

Sementara itu, negara-negara Uni Eropa telah menunjukkan komitmen tinggi dalam penanggulangan kejahatan siber melalui adopsi Budapest Convention on Cybercrime yang menjadi instrumen internasional utama dalam koordinasi penegakan hukum lintas negara. Indonesia hingga saat ini belum meratifikasi konvensi tersebut, padahal keikutsertaan dalam konvensi ini akan memperkuat posisi hukum Indonesia dalam kerja sama internasional dalam pemberantasan kejahatan siber lintas yurisdiksi (UNODC, 2021).

Peran Aparat Penegak Hukum dan Kapasitas Penegakan

Di luar aspek normatif, penegakan hukum terhadap kejahatan siber juga sangat bergantung pada kapasitas dan profesionalitas aparat penegak hukum. Banyak kasus kejahatan digital yang tidak tertangani dengan optimal karena keterbatasan sumber daya manusia yang memahami teknologi informasi secara mendalam. Oleh karena itu, perlu peningkatan kapasitas lembaga-lembaga penegak hukum, seperti POLRI dan Kejaksaan, melalui pelatihan teknis dan kerja sama lintas negara serta sektor swasta (Rahardjo, 2022)

KESIMPULAN

Kejahatan siber (cybercrime) merupakan fenomena hukum modern yang muncul sebagai konsekuensi logis dari kemajuan teknologi informasi dan komunikasi yang pesat. Dalam kerangka sistem hukum pidana Indonesia, kejahatan siber menghadirkan tantangan yang sangat kompleks, baik dari segi substansi hukum, struktur kelembagaan, maupun budaya hukum masyarakat. Secara normatif, hukum pidana Indonesia, yang sebagian besar masih berakar pada Kitab Undang-Undang Hukum Pidana (KUHP) warisan kolonial Belanda, belum sepenuhnya mampu mengakomodasi perkembangan bentuk-bentuk kejahatan siber yang kian variatif dan canggih. Meskipun telah terdapat UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui UU No. 19 Tahun 2016, regulasi tersebut masih menunjukkan banyak kelemahan, baik dari segi definisi delik, ruang lingkup yurisdiksi, hingga mekanisme pembuktian yang sesuai dengan karakteristik digital (Setiadi, 2022).

Kejahatan siber memiliki ciri khas yang membedakannya dari tindak pidana konvensional, seperti sifatnya yang lintas batas yurisdiksi (borderless), tidak mengenal batas waktu (timeless), dan pelakunya yang bisa tersembunyi dalam anonimitas (anonymity) serta menggunakan identitas palsu secara masif dan otomatis (Wall, 2007). Karakteristik tersebut menyebabkan sistem penegakan hukum nasional sering kali tidak efektif dalam menjangkau pelaku kejahatan siber yang berada di luar wilayah hukum Indonesia. Selain itu, mekanisme kerja sama internasional Indonesia dalam memerangi kejahatan siber masih sangat terbatas, terutama karena belum adanya ratifikasi terhadap Budapest Convention on Cybercrime, yang merupakan instrumen hukum internasional utama dalam penanggulangan cybercrime (UNODC, 2021).

Dari aspek penegakan hukum, permasalahan utama terletak pada keterbatasan sumber daya manusia yang menguasai aspek teknis dan forensik digital. Aparat penegak hukum, baik dari kepolisian, kejaksaan, hingga pengadilan, sering kali mengalami kesulitan dalam proses pembuktian perkara siber karena minimnya pemahaman terhadap sistem enkripsi, jejak digital (digital trail), serta keterbatasan perangkat lunak yang mumpuni (Rahardjo, 2022). Hal ini berimbas pada tingginya angka underreporting serta underdetection terhadap kejahatan siber, di mana banyak korban yang enggan melapor karena merasa proses hukum tidak akan memberikan penyelesaian yang memuaskan (Suryani, 2020). Oleh karena itu, peningkatan kapasitas kelembagaan dan SDM yang terlatih dalam bidang keamanan siber menjadi kebutuhan yang mendesak dan harus menjadi prioritas kebijakan nasional.

Kelemahan hukum pidana dalam menanggulangi kejahatan siber juga tampak pada pendekatan yang digunakan, di mana sistem hukum Indonesia masih dominan mengedepankan pendekatan represif dibandingkan preventif. Padahal, mengingat sifat kejahatan siber yang cepat menyebar dan sulit dikendalikan setelah terjadi, pendekatan preventif melalui literasi digital, penguatan sistem keamanan teknologi, dan regulasi internal dalam industri digital merupakan strategi yang jauh lebih efektif (Brenner, 2010). Negara seharusnya tidak hanya hadir sebagai penindak, tetapi juga sebagai fasilitator bagi

masyarakat untuk memahami risiko digital serta meningkatkan kesadaran akan pentingnya perlindungan data pribadi dan etika bermedia sosial.

Di sisi lain, budaya hukum masyarakat Indonesia juga belum mendukung pemberantasan kejahatan siber secara optimal. Banyak masyarakat yang belum memahami bahwa perbuatan-perbuatan seperti pencemaran nama baik melalui media sosial, penyebaran hoaks, atau peretasan data pribadi termasuk ke dalam kategori tindak pidana siber. Kesadaran hukum yang rendah ini semakin diperburuk oleh praktik penegakan hukum yang kerap kali inkonsisten dan terkesan diskriminatif, terutama dalam perkara-perkara siber yang melibatkan tokoh publik atau kepentingan politik tertentu (Marzuki, 2017). Akibatnya, kepercayaan publik terhadap proses hukum dalam penanganan kejahatan siber menjadi rendah dan memperburuk efektivitas hukum pidana secara keseluruhan.

Dengan memperhatikan berbagai persoalan tersebut, maka dapat disimpulkan bahwa efektivitas hukum pidana dalam menghadapi kejahatan siber di Indonesia masih jauh dari ideal. Reformasi hukum pidana tidak hanya perlu dilakukan pada tataran peraturan perundang-undangan, tetapi juga harus mencakup pembenahan kelembagaan, peningkatan literasi digital masyarakat, serta pembangunan infrastruktur teknologi yang mampu mendukung proses penegakan hukum yang adaptif terhadap perkembangan zaman. Selain itu, kerja sama internasional juga harus diperluas melalui ratifikasi instrumen global dan pembentukan protokol bilateral atau multilateral yang menjamin kemudahan pertukaran informasi, ekstradisi pelaku lintas negara, dan harmonisasi norma pidana siber. Tanpa upaya yang sistemik dan terintegrasi, maka kejahatan siber akan terus menjadi ancaman laten yang menggerogoti supremasi hukum dan merusak tatanan sosial digital bangsa.

DAFTAR PUSTAKA

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Greenwood Publishing Group.

Clough, J. (2015). Principles of Cybercrime (2nd ed.). Cambridge University Press.

Nugroho, R. (2020). Urgensi pembentukan UU perlindungan data pribadi dan cybercrime. Jurnal Hukum Internasional, 17(1), 112–129.

Putra, R. A. (2022). Regulasi tindak pidana siber di Indonesia: Sebuah tinjauan kritis. Jurnal Hukum & Pembangunan, 52(3), 317–334.

Soekanto, S., & Mamudji, S. (2001). Penelitian Hukum Normatif. Rajawali Pers.

Tusher, M., & Islam, M. (2019). Cyber crime and legal framework: Bangladesh perspective. International Journal of Law and Management, 61(1), 61–72. https://doi.org/10.1108/IJLMA-11-2017-0262

United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. United Nations. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_210213.pdf