Al-Dalil
Jurnal Ilmu Sosial, Politik, dan Hukum
Vol. 2, No. 2, Juli 2024 ISSN: 2987-0976

Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia

Adinda Lola Sariani[1]
[123]Program Studi Ilmu Hukum, Universitas Islam Indragiri
sarianiadindalola@gmail.com[1]

Abstract (Bahasa Inggris)

This study analyzes the effectiveness of law enforcement against cybercrime in Indonesia during the digital transformation era. The research methods include literature review and descriptive analysis of existing regulations and current law enforcement practices. The main findings reveal challenges in cyber law enforcement, such as a lack of regulatory harmonization and limited technical capabilities of law enforcement officers. While the establishment of the National Cyber and Crypto Agency (BSSN) is a concrete step, this study highlights the need for capacity building and more adaptive regulations to address the continuously evolving dynamics of cybercrime. In conclusion, collaboration between the government, private sector, and society, as well as intensive cybersecurity education and training, is crucial for enhancing awareness and skills in dealing with cyber threats.

Kata Kunci:

Tindak Pidana Siber
Penegakan Hukum
Transformasi Digital
Keamanan Siber
Regulasi.

Abstrak (Bahasa Indonesia)

Penelitian ini menganalisis efektivitas penegakan hukum terhadap tindak pidana siber di Indonesia dalam era transformasi digital. Metode penelitian melibatkan studi literatur dan analisis deskriptif terhadap regulasi yang ada serta praktik penegakan hukum. Temuan utama menunjukkan tantangan dalam penegakan hukum siber, seperti kurangnya harmonisasi regulasi dan keterbatasan kapabilitas teknis aparat penegak hukum. Meskipun pendirian Badan Siber dan Sandi Negara (BSSN) merupakan langkah konkret, penelitian ini menyoroti perlunya peningkatan kapasitas dan regulasi yang lebih adaptif untuk mengatasi dinamika kejahatan siber yang terus berkembang. Kesimpulannya, kolaborasi antara pemerintah, sektor swasta, dan masyarakat, serta pendidikan dan pelatihan keamanan siber yang intensif, sangat penting untuk meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman siber.

Corresponding Author:

Adinda Lola Sariani
Fakultas Hukum
Universitas Islam Indragiri
Email: sarianiadindalola@gmail.com

1. PENDAHULUAN

Kejahatan siber atau tindak pidana dunia maya menjadi fokus serius di Indonesia seiring dengan kemajuan teknologi informasi dan komunikasi yang pesat. Penanganan kejahatan siber di Indonesia mencakup beragam aspek, mulai dari penyusunan peraturan hukum hingga penguatan lembaga penegak hukum, serta kerjasama lintas negara (Rahardjo, 1987). Perkembangan teknologi yang cepat di Indonesia menimbulkan kebutuhan akan upaya penegakan hukum yang lebih efektif terhadap kejahatan siber. Era digital ini memberikan dampak yang signifikan terhadap keamanan nasional, terutama dalam sektor ekonomi yang semakin rentan terhadap serangan kejahatan siber yang semakin canggih. Tidak hanya berdampak pada

kerugian finansial, tetapi juga mengganggu stabilitas sosial dan mengancam keamanan nasional (Widodo, 2011). Oleh karena itu, diperlukan upaya rekonstruksi dalam penegakan hukum untuk menghadapi tantangan ini secara efektif dan tepat.

Semakin mendesaknya perlunya tindakan ini semakin terbukti dengan tingginya besarnya kerugian yang ditimbulkan oleh kejahatan siber, yang mencakup tidak hanya kerugian finansial yang signifikan, tetapi juga gangguan terhadap aktivitas bisnis serta ancaman terhadap stabilitas keamanan nasional. Pada tahun 2016, pemerintah Indonesia menetapkan Undang-Undang Nomor 19 Tahun 2016 yang mengubah ketentuan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), menjadi landasan hukum utama dalam penanganan kejahatan siber di negeri ini. Selain UU ITE, terdapat juga peraturan-peraturan lain yang turut mendukung upaya penegakan hukum terhadap kejahatan siber, seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Maramis, 2016). Dengan demikian, langkah-langkah hukum yang telah diambil oleh pemerintah Indonesia mencerminkan komitmen serius dalam menanggulangi ancaman kejahatan siber dan memperkuat infrastruktur hukum yang diperlukan untuk melindungi kepentingan nasional di era digital ini.

Penegakan hukum terhadap kejahatan siber di Indonesia merupakan upaya kolaboratif yang melibatkan sejumlah lembaga, termasuk Kepolisian Republik Indonesia (POLRI), Kejaksaan Agung, dan Komisi Pemberantasan Korupsi (KPK). Dalam kaitannya dengan kejahatan dunia maya, POLRI menegakkan peran penting melalui Direktorat Tindak Pidana Siber Bareskrim Polri, sebuah unit khusus yang didedikasikan untuk menyelidiki dan menangani kejahatan di ranah digital. Sementara itu, Kejaksaan Agung turut berperan dalam proses penuntutan terhadap para pelaku kejahatan siber, memastikan bahwa mereka dihadapkan pada konsekuensi hukum yang sesuai dengan perbuatannya.

Dalam konteks globalisasi yang semakin erat dan tingginya tingkat konektivitas, kerjasama internasional menjadi suatu keharusan dalam menangani ancaman kejahatan siber. Indonesia telah aktif berpartisipasi dalam upaya kolaboratif dengan negara-negara lain, terutama dalam hal pertukaran informasi dan bukti elektronik terkait kejahatan siber, pelatihan bagi aparat penegak hukum terkait teknik investigasi dan penuntutan dalam ranah digital, serta penyusunan regulasi bersama untuk mengatasi tantangan yang dihadapi secara bersama-sama. Melalui upaya kolaboratif ini, diharapkan dapat terwujud lingkungan digital yang lebih aman dan terlindungi bagi masyarakat Indonesia serta komunitas global secara luas.

Reformasi dalam penegakan hukum terhadap kejahatan siber menjangkau beberapa dimensi utama yang krusial. Pertama, perlunya peningkatan dalam aspek keamanan teknologi informasi menjadi sangat penting. Ini mengharuskan penguatan sistem keamanan siber guna melindungi infrastruktur yang kritis dan juga data-data yang memiliki sensitivitas tinggi dari serangan digital. Kedua, upaya untuk meningkatkan literasi keamanan siber di kalangan masyarakat menjadi sebuah kebutuhan mendesak. Hal ini bertujuan agar masyarakat memiliki pemahaman yang lebih baik mengenai ancaman digital dan mampu meresponsnya dengan tindakan yang bijak dan tepat.

Kolaborasi yang aktif antara pemerintah, lembaga keamanan, dan masyarakat menjadi landasan yang tak tergantikan dalam menghadapi kompleksitas kejahatan siber. Kerjasama yang erat ini memungkinkan bagi pertukaran informasi yang lebih efektif dan penyelenggaraan upaya penanggulangan yang terkoordinasi. Tidak kalah pentingnya adalah pembentukan kebijakan dan regulasi yang responsif terhadap perubahan dinamika kejahatan siber. Kebijakan tersebut harus mampu beradaptasi dengan perkembangan teknologi, mendukung penegakan hukum yang efektif, serta melibatkan partisipasi aktif dari masyarakat dalam upaya pencegahan dan perlindungan.

Dengan mengimplementasikan rekonstruksi yang komprehensif dalam penegakan hukum terhadap kejahatan siber di Indonesia, yang melibatkan penetapan peraturan hukum yang berkeadilan, profesionalisme yang tinggi dari lembaga penegak hukum, serta kerjasama internasional yang erat, diharapkan dapat menggalang efektivitas yang lebih besar dalam menanggulangi ancaman kejahatan dunia maya. Hal ini diarahkan untuk menciptakan lingkungan digital yang aman dan dapat dipercaya bagi seluruh masyarakat.

Langkah-langkah konkret dalam rekonstruksi ini mencakup pembentukan tim yang terlatih khusus dalam operasi militer siber, penerapan sistem pemantauan aktif terhadap potensi serangan siber, dan respons yang cepat terhadap kejahatan siber yang teridentifikasi. Peningkatan kapabilitas dalam bidang penegakan hukum, baik dalam hal teknis maupun sumber daya manusia, menjadi bagian tak terpisahkan dari upaya rekonstruksi ini.

Dalam konteks penelitian ini, urgensi untuk memperkuat penegakan hukum terhadap kejahatan siber di Indonesia sangatlah nyata. Tujuan dari penelitian ini adalah untuk melakukan analisis mendalam terhadap kelemahan yang ada dalam sistem penegakan hukum siber di Indonesia dan memberikan rekomendasi konkret untuk perbaikan yang diperlukan. Dengan menggali literatur terbaru, penelitian ini juga bertujuan untuk mengisi celah yang belum terjamah oleh penelitian sebelumnya, sambil menyajikan solusi praktis yang dapat diimplementasikan untuk meningkatkan tingkat keamanan siber di Indonesia.

2. METODE PENELITIAN

Penelitian merupakan suatu upaya yang bertujuan untuk menemukan, mengembangkan, dan menguji kebenaran suatu pengetahuan sesuai dengan tujuan yang telah ditetapkan. Penelitian ini dilakukan dengan menggunakan pendekatan ilmiah yang dikenal sebagai metodologi penelitian, yang mengikuti langkah-langkah sistematis untuk mengumpulkan dan menganalisis data. Dalam konteks ini, jenis penelitian yang dipilih adalah metode penelitian hukum normatif, yang memanfaatkan data empiris untuk mengevaluasi dan menganalisis permasalahan hukum yang terkait dengan peraturan perundang-undangan yang berlaku.

Metode penelitian hukum normatif ini mengutamakan analisis terhadap bahan hukum yang tersedia dengan menggunakan data empiris sebagai landasan utama. Teknik pengumpulan data dilakukan melalui studi kepustakaan, di mana peneliti menggali informasi dari berbagai sumber dokumen atau bahan pustaka yang relevan dengan topik penelitian. Dalam konteks penelitian normatif, fokus utama teknik pengumpulan data terbatas pada studi dokumen atau bahan pustaka, yang sering kali merujuk pada data hukum sekunder.

3. PEMBAHASAN

3.1 Penerapan Hukum Siber di Era Digital di Indonesia

Di tengah perkembangan terus-menerus dalam era digital, tindak pidana siber di Indonesia telah menjadi ancaman serius, terutama di sektor ekonomi yang rentan. Kejahatan siber seperti pencurian data nasabah, penipuan online, perdagangan ilegal, dan serangan terhadap sistem perbankan semakin meningkat. Tren ini menciptakan dampak yang luas, tidak hanya dalam bentuk kerugian finansial bagi masyarakat, tetapi juga mengancam stabilitas keamanan nasional dan menimbulkan risiko yang signifikan terhadap pertumbuhan ekonomi negara.

Penegakan hukum terhadap kejahatan siber ini dihadapkan pada berbagai tantangan, terutama dalam upaya untuk mengharmonisasikan regulasi yang berkaitan dengan penggunaan internet. Dalam menghadapi ancaman yang semakin kompleks ini, upaya penegakan hukum perlu disesuaikan dan diperkuat agar mampu mengatasi tantangan yang dihadapi dalam lingkungan digital yang terus berubah dan berkembang pesat.

Pada masa kini, praktek dalam menangani tindak pidana seperti penipuan, perjudian, dan pornografi masih mengacu pada ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP). Meskipun demikian, dengan adanya kemajuan teknologi informasi dan komunikasi yang terus berkembang, pola transaksi, pembelian, investasi, serta operasional bisnis telah mengalami perubahan signifikan. Perkembangan ini juga membuka pintu bagi maraknya kejahatan siber, seperti serangan terhadap sektor perbankan, pencurian data, dan perdagangan ilegal.

Oleh karena itu, diperlukan langkah-langkah konkret untuk melindungi sistem komputer, jaringan, perangkat elektronik, serta data dari berbagai ancaman siber yang ada. Upaya-upaya ini menjadi sangat penting untuk menghadapi tantangan baru yang muncul seiring dengan perkembangan teknologi, sehingga sistem hukum perlu terus diperbaharui dan disesuaikan agar mampu menjawab kebutuhan dan tantangan zaman yang terus berubah dengan cepat.

Keamanan siber memiliki tujuan utama untuk memelihara kerahasiaan, integritas, dan ketersediaan informasi yang bersifat sensitif, serta untuk menjaga infrastruktur teknologi informasi dari serangan yang dapat menyebabkan kerusakan pada sistem atau menimbulkan kerugian yang signifikan. Di tengah kompleksitas ancaman yang terus berkembang, kolaborasi antara pemerintah, sektor swasta, dan masyarakat menjadi semakin penting dalam upaya menjaga keamanan dan kedaulatan negara dari potensi ancaman serta gangguan.

Dalam konteks ini, diperkuatnya program pendidikan dan pelatihan keamanan siber menjadi suatu langkah yang strategis. Melalui peningkatan kesadaran dan keterampilan dalam menghadapi ancaman siber, diharapkan masyarakat dapat lebih responsif dan proaktif dalam mengatasi berbagai tantangan yang muncul dalam ranah digital. Upaya ini tidak hanya mencakup pelatihan teknis, tetapi juga penyuluhan tentang pentingnya menjaga keamanan informasi dan melindungi infrastruktur teknologi dari potensi serangan yang merugikan.

Meskipun demikian, fenomena kejahatan siber terus mengalami perkembangan dan meningkat menjadi lebih kompleks dari waktu ke waktu. Salah satu aspek yang mendapat perhatian serius adalah cyberbullying yang terjadi melalui media sosial, mengingat pentingnya menjaga keseimbangan antara kebebasan berekspresi dan perlindungan terhadap korban. Dalam konteks ini, pelaksanaan penegakan hukum pidana terhadap kasus cyberbullying memerlukan pertimbangan yang matang, terutama dalam menangani delik aduan yang melibatkan tindakan seperti body shaming, penghinaan, pencemaran nama baik, dan ancaman kepada korban.

Pemerintah Indonesia telah memberikan respons yang tegas terhadap meningkatnya ancaman kejahatan siber dengan mengadopsi kebijakan dan regulasi yang bertujuan untuk meningkatkan keamanan siber serta melindungi infrastruktur informasi yang kritis. Salah satu langkah konkret yang diambil adalah pendirian Badan Siber dan Sandi Negara (BSSN), sebuah lembaga yang dibentuk secara khusus untuk menghadapi berbagai ancaman dalam ranah digital. Meskipun demikian, tantangan yang dihadapi tetap

signifikan, dan upaya pembaruan terus-menerus dalam regulasi serta peningkatan kapabilitas dalam penegakan hukum menjadi sangat penting. Hal ini diperlukan untuk menjaga keamanan nasional serta meminimalkan risiko kejahatan siber yang dapat mengganggu stabilitas dan keamanan di Indonesia.

Perkembangan teknologi informasi dan internet telah membawa dampak yang signifikan dalam berbagai aspek kehidupan, dengan sejumlah manfaat yang dihasilkan, namun juga menghadirkan konsekuensi negatif yang tidak dapat diabaikan. Salah satu dampak negatif yang semakin merisaukan masyarakat adalah kemudahan bagi para pelaku kejahatan untuk melakukan aksi kriminal melalui ruang siber, yang dikenal dengan istilah cyber crime. Meskipun kejahatan siber pada umumnya merujuk pada aktivitas kriminal yang menggunakan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga mencakup kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan sebagai alat untuk memfasilitasi atau meningkatkan efisiensi dari tindakan kejahatan tersebut.

Fungsi sanksi dalam hukum pidana tidak hanya untuk menakut-nakuti atau mengancam para pelanggar, tetapi juga harus dapat mendidik dan memperbaiki pelaku. Berkembangnya konsep untuk mencari alternatif dari pidana perampasan kemerdekaan dalam bentuk sanksi alternatif (alternative sanction) menjadi penting. Rudolph B. Schesinger menjelaskan bahwa perbandingan hukum adalah metode penyelidikan untuk memperoleh pengetahuan yang lebih dalam tentang bahan-bahan hukum tertentu. Perbandingan hukum bukanlah perangkat peraturan dan asas-asas hukum serta bukan suatu cabang hukum, melainkan teknik untuk menghadapi unsur hukum asing dari suatu masalah hukum.

Menurut Munir Fuady, perbandingan hukum merupakan sebuah disiplin ilmu dan metode dalam studi hukum yang melibatkan peninjauan lebih dari satu sistem hukum. Pendekatan ini dilakukan dengan menganalisis berbagai kaidah, aturan hukum, yurisprudensi, dan pandangan ahli yang terkemuka dalam berbagai sistem hukum, dengan tujuan untuk mengidentifikasi persamaan dan perbedaan di antara mereka. Dengan demikian, melalui perbandingan tersebut, kita dapat mengambil kesimpulan serta mengembangkan konsep-konsep tertentu, sambil memahami penyebab munculnya persamaan dan perbedaan tersebut secara historis, sosiologis, analitis, maupun normatif.

Menurut ketentuan yang tercantum dalam Pasal 5 Kitab Undang-Undang Hukum Pidana (KUHP), hukum pidana Indonesia memiliki cakupan yang berlaku bagi setiap warga negara Indonesia yang melakukan tindak pidana tertentu di luar wilayah Indonesia. Adapun tindak pidana yang dimaksud mencakup berbagai perbuatan, antara lain yang berkaitan dengan keamanan negara, pelanggaran terhadap martabat Presiden dan Wakil Presiden, hasutan untuk melakukan tindak pidana, penyebaran tulisan yang bertujuan untuk menimbulkan hasutan, tindakan sengaja untuk membuat diri sendiri atau orang lain tidak dapat memenuhi kewajiban militer, melakukan perkawinan dengan mengetahui bahwa perkawinan yang ada menjadi hambatan yang sah untuk itu, serta berbagai tindak pidana lainnya yang dianggap sebagai kejahatan menurut Undang-Undang Pidana Indonesia serta diancam dengan pidana oleh negara tempat tindak pidana dilakukan.

Di Indonesia, banyak aspek hukum yang memiliki akar dari peraturan-peraturan hukum yang berasal dari Belanda, hal ini dikarenakan proses pembuatan aturan hukum yang memakan waktu yang cukup lama dan melibatkan partisipasi dari berbagai elemen masyarakat di Indonesia. Implementasi hukum di Indonesia seringkali mengambil landasan dari undang-undang atau regulasi yang diwarisi dari sistem hukum Belanda. Namun, seiring dengan perubahan zaman dan evolusi sosial, terjadi revisi-revisi yang dilakukan guna menyesuaikan dengan kebutuhan dan perilaku masyarakat Indonesia.

Contoh konkret dari adaptasi hukum terhadap perkembangan zaman dapat ditemukan dalam Undang-Undang No. 44 Tahun 2008 tentang Pornografi. Di dalamnya, terdapat ketentuan mengenai tindak pidana yang juga mencakup aspek kejahatan siber. Pengertian pornografi yang disebutkan dalam Pasal 1 ayat 1 diperluas tidak hanya mencakup materi cetak, tetapi juga mencakup berbagai bentuk media komunikasi, termasuk internet. Begitu pula dengan definisi jasa pornografi yang tercantum dalam Pasal 1 angka 2, yang mencakup layanan yang disediakan melalui internet dan media komunikasi elektronik lainnya.

Dari definisi yang disebutkan, tindakan yang masuk dalam lingkup kriminalisasi berdasarkan Undang-Undang Pornografi dapat diartikan sebagai tindakan yang melibatkan teknologi informasi dan komunikasi. Terdapat berbagai perbuatan yang dianggap sebagai pelanggaran dalam undang-undang tersebut, yang meliputi aktivitas seperti produksi, pembuatan, duplikasi, penyebaran, siaran, impor, ekspor, penawaran, perdagangan, penyewaan, atau penyediaan materi pornografi yang eksplisit.

Substansi hukum pidana materiil, beserta prinsip-prinsip dasar yang mendasarinya, dirumuskan dengan mempertimbangkan berbagai gagasan dan ide dasar tentang keseimbangan, termasuk dalam proses perumusan Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUU KUHP).

Pencarian keseimbangan dalam konteks hukum mencakup sejumlah aspek yang kompleks dan beragam. Ini melibatkan harmonisasi antara pertimbangan moralitas yang terkait dengan kepentingan negara, kepentingan umum masyarakat, dan hak-hak individu; serta seimbangnya perlindungan terhadap kepentingan publik, hak-hak pelaku tindak pidana, dan kepentingan korban kejahatan. Dalam proses ini, perlu ada penyeimbangan antara unsur-unsur objektif dan subjektif dalam pengambilan keputusan, serta antara kriteria formal dan substansial dalam penerapan hukum. Selain itu, keseimbangan juga harus ditemukan antara

kepastian hukum yang diinginkan, fleksibilitas yang diperlukan untuk menangani situasi-situasi khusus, dan prinsip-prinsip keadilan yang mendasari sistem hukum.

Tidak hanya itu, ada juga upaya untuk mencapai keseimbangan antara kearifan lokal, nilai-nilai nasional yang khas, dan prinsip-prinsip nilai global yang berlaku secara umum. Dalam menjaga keseimbangan ini, hukum memainkan peran sentral dalam menyelaraskan berbagai kepentingan dan nilai-nilai yang terlibat, untuk memastikan bahwa keputusan yang diambil mencerminkan nilai-nilai yang dianggap penting oleh masyarakat serta memenuhi standar keadilan yang adil dan setara bagi semua individu.

Hingga saat ini, Indonesia belum memiliki undang-undang khusus atau cyber law yang secara spesifik mengatur tentang kejahatan siber. Meskipun demikian, beberapa hukum positif yang ada dapat diterapkan terhadap pelaku kejahatan siber, terutama dalam kasus yang melibatkan penggunaan teknologi komputer dan sejenisnya. Dalam konteks ini, penguatan hukum terhadap individu yang terlibat dalam tindak kejahatan siber menjadi penting, terutama bagi mereka yang saat ini tidak dapat dipertanggungjawabkan atas tindakan mereka berdasarkan ketentuan yang terdapat dalam Pasal 44 Kitab Undang-Undang Hukum Pidana. Pasal ini menyatakan bahwa seseorang tidak dapat dipidana jika dalam melakukan tindak kejahatan tersebut, mereka tidak memiliki kesadaran atau kontrol penuh atas tindakan yang dilakukan.

Menurut Martiman Prodjohamidjojo, kejahatan terkait dapat diidentifikasi melalui dua faktor utama: adanya tindakan yang bertentangan dengan hukum dan keberadaan unsur kesalahan dalam bentuk kesengajaan atau kealpaan. Tindakan yang melanggar hukum dapat diatribusikan secara individu kepada pelaku. Ketika membicarakan subyek hukum yang terlibat dalam kejahatan siber, fokusnya selalu mengacu pada kapasitas individu untuk bertanggung jawab atas perbuatannya.

Pertanggungjawaban atas kejahatan memiliki dua dimensi penting: tanggung jawab dan karakter kejahatan itu sendiri. Konsep tanggung jawab, menurut W.J.S. Poerwadarminta, merujuk pada kondisi di mana seseorang harus mempertanggungjawabkan segala tindakannya, dapat dikenai tuntutan, penyalahan, atau tindakan hukum lainnya.

Dari analisis ini, menjadi jelas bahwa urgensi dalam pengembangan hukum pidana siber tidak dapat dipandang remeh, terutama di era transformasi digital saat ini. Perlunya penegakan hukum yang efisien dan responsif terhadap kejahatan di ranah siber menjadi suatu keharusan yang tak terbantahkan. Kehadiran hukum pidana khusus untuk dunia maya menjadi sangat vital dalam upaya melindungi masyarakat luas dan lembaga-lembaga dari ancaman berbagai bentuk kejahatan di ranah siber.

Dalam konteks ini, perlunya penanganan serius terhadap berbagai jenis kejahatan siber seperti pencurian data, penipuan online, dan ancaman siber lainnya menjadi semakin mendesak. Tindakan-tindakan kriminal semacam itu dapat berdampak merugikan tidak hanya individu, tetapi juga organisasi, bahkan dapat mengancam stabilitas keamanan nasional.

Keberlangsungan dari penegakan hukum, khususnya dalam konteks digital, menjadi sangat penting guna memastikan bahwa ketertiban dan keadilan tetap terjaga di tengah pesatnya perkembangan teknologi. Dalam menghadapi dinamika tersebut, penyelarasan antara perkembangan hukum dan evolusi teknologi menjadi suatu keharusan agar hukum tetap relevan dan efektif dalam melindungi masyarakat dari ancaman kejahatan siber.

3.2 Analisis Efektivitas Penegakan Hukum Tindak Pidana Siber Di Indonesia Saat Ini

Di era digitalisasi yang berkembang dengan cepat, Indonesia dihadapkan pada tantangan serius yang berasal dari peningkatan kejahatan siber yang semakin meluas, terutama di sektor ekonomi. Ancaman ini mencakup berbagai jenis seperti serangan terhadap infrastruktur perbankan, pencurian data nasabah, penipuan daring, dan perdagangan ilegal yang terjadi di dunia maya. Kehadiran kejahatan siber ini menjadi fokus perhatian yang mendalam secara nasional.

Dampaknya dapat sangat merugikan bagi masyarakat secara luas, mengancam stabilitas keamanan nasional, dan menimbulkan risiko yang signifikan terhadap pertumbuhan ekonomi negara. Oleh karena itu, upaya perlindungan terhadap masyarakat dan infrastruktur nasional dari ancaman kejahatan siber menjadi sangat penting untuk dilakukan. Dalam menjalankan penegakan hukum terhadap kejahatan siber, berbagai tantangan muncul, terutama terkait dengan penyelarasan regulasi dalam penggunaan internet.

Saat ini, pendekatan terhadap penanganan tindak pidana seperti penipuan, perjudian, dan pornografi masih mengacu pada ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP). Namun, dengan berkembangnya teknologi informasi dan komunikasi, terjadi transformasi dalam cara transaksi, berbelanja, berinvestasi, dan menjalankan operasi bisnis. Hal ini membuka pintu bagi kejahatan siber untuk berkembang dan menyebar.

Dalam menghadapi ancaman siber, diperlukan langkah-langkah konkret untuk memastikan perlindungan yang efektif terhadap sistem komputer, jaringan, perangkat elektronik, dan data yang tersimpan di dalamnya. Keamanan siber menjadi hal yang sangat krusial karena bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang sensitif, serta untuk melindungi infrastruktur teknologi informasi dari berbagai serangan yang dapat mengakibatkan kerusakan pada sistem atau menimbulkan kerugian yang

signifikan. Oleh karena itu, implementasi strategi keamanan siber yang kuat menjadi suatu keharusan untuk memastikan bahwa sistem teknologi informasi dapat beroperasi secara aman dan efisien di lingkungan yang terus berubah dan berkembang pesat.

Sinergi antara pemerintah, sektor swasta, dan masyarakat menjadi semakin kuat dalam menjaga keamanan dan kedaulatan negara dari ancaman siber. Langkah-langkah yang diambil meliputi peningkatan program pendidikan dan pelatihan keamanan siber guna meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman di ranah digital. Meskipun upaya-upaya tersebut dilakukan, fenomena kejahatan siber terus berkembang dan menjadi lebih kompleks seiring berjalannya waktu.

Isu *cyberbullying* yang terjadi melalui platform media sosial menjadi sorotan utama, khususnya dalam konteks penghormatan terhadap hak kebebasan berekspresi sekaligus perlindungan terhadap korban yang terkena dampaknya. Dalam menjalankan penegakan hukum terhadap cyberbullying, penting untuk mempertimbangkan berbagai delik aduan yang melibatkan tindakan seperti body shaming, penghinaan, pencemaran nama baik, dan ancaman. Hal ini menekankan perlunya tindakan hukum yang efektif dan sensitif dalam menangani kasus-kasus cyberbullying untuk memastikan bahwa hak-hak individu terlindungi dan keadilan terwujud.

Respons terhadap meningkatnya ancaman kejahatan siber di Indonesia telah tercermin melalui langkah-langkah yang diambil oleh pemerintah, yang meliputi adopsi kebijakan dan regulasi untuk meningkatkan keamanan siber serta melindungi infrastruktur informasi yang kritis. Salah satu tindakan konkret yang diambil adalah pendirian Badan Siber dan Sandi Negara (BSSN), yang menjadi bukti komitmen serius pemerintah dalam menghadapi ancaman tersebut. Namun, sementara langkah-langkah ini telah diambil, tantangan-tantangan baru terus muncul, dan hal ini menuntut pembaruan regulasi yang terus-menerus serta peningkatan kapabilitas penegakan hukum untuk memastikan keamanan nasional tetap terjaga dan risiko kejahatan siber dapat diminimalkan di Indonesia.

Perkembangan teknologi informasi dan internet telah membawa dampak negatif yang cukup signifikan, di mana semakin mudahnya akses para pelaku kejahatan untuk melakukan aksi kriminal yang meresahkan masyarakat. Penyalahgunaan ruang siber yang terjadi di dalamnya seringkali disebut sebagai cybercrime. Meskipun istilah ini sering dikaitkan dengan aktivitas kriminal yang terjadi secara daring, yang melibatkan komputer atau jaringan komputer sebagai bagian utamanya, namun, konsep cybercrime juga mencakup kejahatan konvensional di mana teknologi informasi dan jaringan komputer dimanfaatkan untuk memfasilitasi atau memungkinkan terjadinya tindak kejahatan tersebut.

Peran sanksi dalam sistem hukum pidana tidak terbatas pada upaya untuk menakut-nakuti atau mengintimidasi pelanggar, tetapi juga mencakup fungsi mendidik dan memperbaiki perilaku para pelaku kejahatan. Konsep yang berkembang untuk mencari alternatif dari hukuman penjara dalam bentuk sanksi alternatif merupakan bagian dari upaya yang terus-menerus dalam memperbaiki sistem penegakan hukum. Langkah-langkah ini bertujuan untuk memberikan opsi yang lebih bervariasi dalam penegakan hukum, dengan fokus pada rehabilitasi dan reintegrasi sosial pelaku kejahatan ke dalam masyarakat.

Menurut Rudolph B. Schesinger, perbandingan hukum merupakan suatu metode investigasi yang bertujuan untuk memperluas pemahaman terhadap berbagai materi hukum yang ada. Proses perbandingan hukum tidak hanya berfokus pada pengembangan peraturan dan prinsip-prinsip hukum, tetapi juga merupakan sebuah teknik yang digunakan untuk menghadapi beragam aspek hukum yang berasal dari berbagai sistem hukum di seluruh dunia. Dengan demikian, perbandingan hukum bukan sekadar alat untuk menghasilkan aturan-aturan hukum, melainkan merupakan pendekatan yang digunakan untuk memahami dan menangani aspek-aspek hukum yang bersifat internasional atau asing dalam konteks permasalahan hukum yang spesifik.

Pentingnya hukum pidana siber mencakup perlunya sistem penegakan hukum yang tidak hanya efektif tetapi juga responsif terhadap berbagai jenis kejahatan siber di era transformasi digital saat ini. Kehadiran hukum pidana yang mengatur dunia maya menjadi sangat penting dalam melindungi masyarakat dan lembaga-lembaga dari ancaman berbagai kejahatan di ranah digital, seperti pencurian data, penipuan daring, dan serangan siber lainnya. Kontinuitas dalam penegakan hukum di tengah dinamika teknologi yang terus berkembang menjadi suatu keharusan untuk memastikan bahwa ketertiban dan keadilan tetap terjaga di era digital ini.

Menghadapi tantangan yang semakin kompleks di era digital, muncul kebutuhan mendesak untuk merekonstruksi konsep penegakan hukum terhadap tindak pidana siber di Indonesia. Seiring dengan perkembangan teknologi yang terus maju, kejahatan siber berkembang secara cepat dan menghadirkan risiko baru yang mengancam baik masyarakat maupun pemerintah. Dalam usaha merekonstruksi konsep penegakan hukum ini, diperlukan langkah-langkah yang progresif untuk meningkatkan kapasitas hukum dalam mengantisipasi serta menanggapi berbagai bentuk kejahatan siber yang terus berkembang.

Upaya ini harus didasarkan pada kerjasama yang erat antara berbagai lembaga penegak hukum, sektor swasta, dan pihak-pihak terkait lainnya, demi menciptakan lingkungan digital yang lebih aman dan terpercaya bagi semua pihak yang terlibat. Pentingnya penyusunan regulasi yang lebih presisi dan responsif

terhadap perubahan dinamika kejahatan siber menjadi sangat nyata dalam menjaga keamanan siber dan melindungi masyarakat.

Dengan melakukan rekonstruksi ini, diharapkan penegakan hukum terhadap tindak pidana siber dapat menjadi lebih efektif, adaptif, dan mampu menjawab tantangan yang muncul seiring perkembangan teknologi. Upaya ini bertujuan untuk menjaga stabilitas dan keamanan dalam lingkup digital di Indonesia dengan mengakomodasi berbagai perubahan dan inovasi yang terjadi dalam ranah kejahatan siber. Konsep penegakan hukum terhadap kejahatan siber di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016, yang merupakan hasil dari revisi terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Melalui UU ITE ini, upaya penegakan hukum dapat lebih terfokus pada berbagai bentuk pelanggaran di dunia maya, serta memberikan kerangka perlindungan hukum dan sanksi pidana bagi para pelaku kejahatan siber. Berbagai pasal dalam UU ITE mengatasi tindak pidana peretasan, yang mencakup elemen-elemen seperti tindakan akses ilegal dan tanpa izin terhadap komputer dan sistem elektronik yang dimiliki oleh orang lain.

Dalam konteks kelembagaan, di Indonesia saat ini terdapat beberapa kepolisian daerah yang telah membentuk unit Cybercrime, seperti Polda Metro Jaya dan Polda Jawa Timur. Namun, dalam penanganan tindak pidana siber, seringkali pendekatan yang digunakan masih sama dengan kasus-kasus tindak pidana konvensional lainnya. Data terkait tindak pidana siber menunjukkan bahwa masih banyak kejadian yang tidak terdeteksi karena berbagai faktor, termasuk keterbatasan dalam kecepatan operasional dan kapasitas penyimpanan perangkat komputer, serta kurangnya keahlian teknis dari aparat penegak hukum.

Dalam Undang-Undang No. 44 Tahun 2008 tentang Pornografi, terdapat ketentuan yang juga mencakup tindak pidana siber. Hal ini mengindikasikan bahwa kriminalisasi perbuatan yang diatur dalam Undang-Undang Pornografi dapat mencakup aktivitas yang dilakukan melalui teknologi informasi dan komunikasi. Contohnya adalah kegiatan seperti pembuatan, penyebaran, dan perdagangan materi pornografi melalui internet. Dengan demikian, Undang-Undang Pornografi juga memiliki relevansi dalam konteks kejahatan siber, karena memperhatikan perkembangan teknologi informasi dan komunikasi.

Kesimpulan dari analisis ini menegaskan pentingnya perubahan konseptual dalam penegakan hukum terhadap kejahatan siber di masa mendatang. Diperlukan pemikiran yang cermat dan transformasi dalam pendekatan hukum untuk menghadapi tantangan yang semakin kompleks di era digital. Rekonstruksi ini menuntut adaptasi hukum yang cepat dan responsif terhadap perkembangan teknologi serta dinamika kejahatan siber yang terus berubah.

Upaya tersebut sangat vital dalam menjaga keamanan nasional, melindungi masyarakat dari ancaman cybercrime, dan memastikan bahwa sistem hukum mampu mengatasi tantangan baru yang muncul seiring dengan kemajuan teknologi informasi dan komunikasi. Perubahan yang komprehensif dalam kerangka hukum menjadi landasan bagi negara untuk menegakkan keadilan dan keamanan dalam era digital yang terus berkembang.

Penegakan hukum terhadap kejahatan siber di Indonesia saat ini dihadapkan pada tantangan yang semakin kompleks. Oleh karena itu, dibutuhkan upaya kolaboratif antara pemerintah, sektor swasta, dan masyarakat untuk meningkatkan efektivitas penegakan hukum di ranah siber. Fokus pada peningkatan kapasitas hukum, penyusunan regulasi yang lebih tepat dan fleksibel, serta penguatan melalui pendidikan dan pelatihan keamanan siber menjadi kunci utama dalam menjaga stabilitas dan kedaulatan negara di era digital ini. Dengan melakukan rekonstruksi konsep penegakan hukum, diharapkan Indonesia dapat menjadi lebih responsif dan efektif dalam menghadapi tantangan yang terus berkembang dari kejahatan siber. Langkah-langkah ini diharapkan dapat memberikan perlindungan yang lebih baik terhadap masyarakat dan infrastruktur digital negara.

4. KESIMPULAN DAN SARAN/REKOMENDASI

4.1 Kesimpulan

Penegakan hukum terhadap tindak pidana siber di Indonesia dalam era transformasi digital menghadapi tantangan yang kompleks. Meskipun kemajuan teknologi informasi memberikan banyak manfaat, namun juga memfasilitasi terjadinya kejahatan siber yang meresahkan masyarakat, seperti pencurian data, penipuan online, dan perdagangan ilegal. Ancaman tersebut mengancam sektor ekonomi dan keamanan nasional, serta membawa risiko bagi pertumbuhan ekonomi. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat dalam melindungi keamanan dan kedaulatan negara dari ancaman siber semakin diperkuat, termasuk dengan adopsi kebijakan dan regulasi serta pendirian Badan Siber dan Sandi Negara (BSSN). Di samping itu, penegakan hukum terhadap kejahatan siber masih sering mengacu pada ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Penggunaan teknologi informasi yang berkembang terus membuka peluang bagi kejahatan siber, sehingga langkah-langkah konkret dalam melindungi sistem komputer, jaringan, perangkat elektronik, dan data dari ancaman siber menjadi sangat penting. Urgensi hukum pidana siber terletak pada

kebutuhan akan penegakan hukum yang efektif dan responsif terhadap kejahatan siber di era digital, termasuk dengan pengembangan konsep sanksi alternatif untuk mendidik pelaku kejahatan. Peningkatan kapasitas hukum dan penyusunan regulasi yang lebih presisi dan adaptif terhadap dinamika kejahatan siber diperlukan untuk menjaga keamanan siber dan melindungi masyarakat. Dalam konteks ini, rekonstruksi konsep penegakan hukum terhadap tindak pidana siber menjadi suatu keharusan untuk menghadapi tantangan di era digital dan memastikan bahwa sistem hukum mampu mengatasi tantangan baru serta menjaga keamanan nasional serta melindungi masyarakat.

4.2 Saran/Rekomendasi

Berbagai langkah dapat diambil untuk meningkatkan penegakan hukum terhadap tindak pidana siber di Indonesia. Pertama, pemerintah harus mempercepat harmonisasi regulasi terkait kejahatan siber untuk menciptakan kerangka hukum yang adaptif terhadap perkembangan teknologi. Kedua, aparat penegak hukum perlu diberikan pelatihan teknis yang intensif dalam bidang keamanan siber untuk menghadapi kejahatan yang semakin kompleks. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat harus diperkuat untuk membangun ekosistem keamanan siber yang tangguh. Peningkatan kesadaran publik tentang risiko kejahatan siber juga penting melalui program pendidikan dan kampanye publik. Evaluasi berkala terhadap regulasi dan strategi penegakan hukum yang ada, serta penguatan Badan Siber dan Sandi Negara (BSSN), juga menjadi kunci. Dengan mengimplementasikan langkah-langkah ini, diharapkan penegakan hukum terhadap kejahatan siber dapat lebih efektif, melindungi masyarakat dan aset nasional dari ancaman di dunia maya.

REFERENSI

Agis, A. (2017). Peranan-Kepolisian-Dalam-Penyidikan-Penyalahgunaan Informasi Elektronik (ite). *Al Hikam*, *1*(2), 37–57.

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1), 2.

Annisa Dwi Amalia, D., & Hafidh Prasetyo, M. (2021). Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terrorism. *Jurnal Pembangunan Hukum Indonesia*, *3*(2), 228–239. https://ejournal2.undip.ac.id/index.php/jphi/article/download/11091/5554

Badan Siber dan Sandi Negara. (2016). Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://jdih.kominfo.go.id/produk_hukum/view/id/30/t/uu

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, DanPerkembangannya. *Technology and Economics Law Journal*, *2*(2), 299–317. https://www.google.com/search?q=Kejahatan+Siber+Terhadap+Individu%3A+Jenis%2C+Analisis%2C+Dan+Perkembangannya&rlz=1C5CHFA_enID876ID882&oq=Kejahatan+Siber+Terhadap+Individu%3A+Jenis%2C+Analisis%2C+Dan+Perkembangannya&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQRRg

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding SAINTEK: Sains Dan Teknologi*, *2*(1), 216–221. https://www.jurnal.pelitabangsa.ac.id/index.php/SAINTEK/article/view/2159

Jendraningrat, B. A. (2021). Efektifitas Penegakan Hukum Tindak Pidana Cyber Gambling Endorsement Di Indonesia. In *Yustisia Tirtayasa: Jurnal Tugas Akhir* (Vol. 1, Issue 1). https://doi.org/10.51825/yta.v1i1.11333

Mafazi, A., Sudarmanto, H. L., Widayati, S. C., & Hanum, F. (2023). Prevention of Terrorism with a Regulatory Model of Violent-Based Extremism that Leads to Terrorism. *Jurnal Cakrawala Hukum*, *14*(2), 126–133. https://doi.org/10.26905/idjch.v14i2.10814

Nomor, V., Issn, D., Hukum, F., Ekasakti, U., No, J. V., Bar, K. P., Padang, K., & Barat, S. (2023). *Rio Law Jurnal PERLINDUNGAN HUKUM TERHADAP KORBAN PADA KASUS CYBER SABOTAGE AND EXTORTATION MENURUT HUKUM POSITIF DI INDONESIA Kata Kunci : Perlindungan , Tindak Pidana , Cyber Sabotage and Extortation*.

Nuzulia, A. (1967). 済無No Title No Title No Title. In *Angewandte Chemie International Edition, 6(11), 951–952.* (Vol. 7, Issue 3).

Nuzulia, A., Richter, L. E., Carlos, A., Beber, D. M., Saputra, A., Kristiawanto, K., Ismed, M., Utin Indah Permata Sari, & Jendraningrat, B. A. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum*, *1*(1), 58–68. https://doi.org/10.51825/yta.v1i1.11333

Pada, P., Pandemi, M., Indonesia, D. I., Sosio, J., No, Y., & Yogyakarta, D. I. (2021). *ALSA LC UGM Law Journal*. *2*(November), 1–18.

Poerwadarminta, W. J. S. (1983). Kamus Umum Bahasa Indonesia. Penerbit Balai Pustaka.

Prodjohamidjojo, M. (2010). Asas-Asas Hukum Pidana Indonesia. Penerbit Buku Kompas.

Putra, E. N. (2016). Pengiriman E-Mail Spam Sebagai Kejahatan Cyber Di Indonesia. *Jurnal Cakrawala*

Hukum, *7*(2), 169–182. https://doi.org/10.26905/idjch.v7i2.1906

RI, U. N. 19 T. 2016. (2016). Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *UU No. 19 Tahun 2016*, *1*, 1–31.

Richter, L. E., Carlos, A., & Beber, D. M. (n.d.). *No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title*. *18*.

Suhariyanto, D. (2022). JPH: Jurnal Pembaharuan Hukum Volume 9, Number 1, April 2022. *Pembaharuan Hukum*, *15*(1), 16–25.

Utin Indah Permata Sari. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. In *Jurnal Studia Legalia* (Vol. 2, Issue 01). https://doi.org/10.61084/jsl.v2i01.7

(*11333-28797-2-SP*, n.d.; Jendraningrat, 2021; Nuzulia, 1967; Nuzulia et al., 2021; Richter et al., n.d.; Utin Indah Permata Sari, 2022)

(Agis, 2017; Aldriano & Priyambodo, 2022; Annisa Dwi Amalia & Hafidh Prasetyo, 2021; Butarbutar, 2023; Hidayatullah, 2023; Mafazi et al., 2023; Nomor et al., 2023; Nuzulia et al., 2021; Pada et al., 2021; Putra, 2016; RI, 2016; Richter et al., n.d.; Suhariyanto, 2022) Badan Siber dan Sandi Negara. (2016). Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://jdih.kominfo.go.id/produk_hukum/view/id/30/t/uu