Optimalisasi Penegakan Hukum Terhadap Tindak Pidana Siber di Era Transformasi Digital: Analisis Kritis Regulasi dan Implementasi

Ferdian[1]
[2]Program Studi Ekonomi Syariah, Agama, Muhamadyah, Mataram
e-mail : ferdian87@gmail.com

SEIKAT
Jurnal Ilmu Sosial, Politik dan Hukum

e-ISSN: 2964-0962

SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum

https://ejournal.45mataram.ac.id/index.php/seikat

Vol. 5, No. 1, Februari 2026

Page: 577-582

Available at:

https://ejournal.45mataram.ac.id/index.php/seikat/article/view/1694

DOI:

https://doi.org/10.55681/seikat.v5i1.1694

Article History:

Received: 05-01-2026

Revised: 10-02-2026

Accepted: 20-02-2026

Abstrak : Era transformasi digital telah membuka ruang baru bagi perkembangan kejahatan dunia maya atau tindak pidana siber yang semakin kompleks, baik dari sisi modus, teknologi, maupun dampak. Penelitian ini bertujuan untuk menganalisis kritis regulasi yang mengatur tindak pidana siber di Indonesia, kemudian mengevaluasi bagaimana implementasi penegakan hukumnya dalam praktik. Pendekatan penelitian menggunakan metode kualitatif dengan analisis yuridis normatif terhadap regulasi utama seperti UU ITE (Undang-Undang Informasi dan Transaksi Elektronik), UU Perlindungan Data Pribadi, dan KUHP baru, serta wawancara dengan aparat penegak hukum dan studi kasus dari beberapa tindak pidana siber signifikan. Temuan penelitian menunjukkan bahwa regulasi di Indonesia meskipun telah berkembang mengalami sejumlah kelemahan: multitafsir pada beberapa pasal, belum harmonis dengan regulasi lain, serta kurang fleksibel terhadap perkembangan teknologi. Di sisi implementasi, terdapat tantangan besar berupa kurangnya kapasitas teknis aparat penegak hukum, keterbatasan sarana dan teknologi forensik digital, koordinasi antar lembaga yang belum optimal, serta hambatan dalam kerja sama internasional. Berdasarkan analisis kritis tersebut, penelitian ini merekomendasikan reformasi regulasi yang adaptif, peningkatan kapabilitas dan pelatihan teknis aparat, pembenahan harmonisasi regulasi dan prosedur antar lembaga, serta penguatan mekanisme kerja sama lintas batas. Penelitian ini diharapkan memberikan kontribusi terhadap kebijakan publik dan praktek penegakan hukum yang lebih efektif dalam menghadapi tantangan kejahatan siber di era digital.

Kata Kunci : Tindak Pidana Siber, Penegakan Hukum, Regulasi Digital, Implementasi, Kapasitas Teknis, Indonesia

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan mendasar terhadap berbagai aspek kehidupan manusia, mulai dari ekonomi, sosial, hingga politik. Transformasi digital mengubah cara orang berinteraksi, bekerja, dan memperoleh informasi melalui jaringan internet dan sistem elektronik (Thomas & Anggraeni, 2025). Namun, kemajuan ini juga turut memunculkan ancaman baru berupa tindak pidana siber kejahatan yang memanfaatkan teknologi digital sebagai sarana atau medio aksi ilegal (Habibi & Liviani, 2020). Contoh tindak pidana siber meliputi penipuan daring (online fraud), peretasan, penyebaran malware, pencurian data pribadi, serta penyalahgunaan media sosial.

Di Indonesia, munculnya kejahatan siber menjadi perhatian yang makin nyata (Chintia et al., 2019). Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah menjadi aturan dasar dalam menangani berbagai bentuk kejahatan siber, termasuk penipuan online dan ujaran

kebencian. Selain itu, regulasi lain seperti UU Perlindungan Data Pribadi juga mulai berperan dalam memberikan perlindungan terhadap penyalahgunaan data pribadi warga negara. Namun demikian, berbagai studi nasional menunjukkan bahwa regulasi yang ada masih mengalami banyak masalah dalam interpretasi dan implementasi (Firdaus, 2024). Sebagai contoh, penelitian oleh Aprilianti (2024) menemukan bahwa UU ITE mengalami kendala efektivitas karena adanya pasal yang multitafsir dan kurangnya edukasi masyarakat terhadap hukum siber.

Meskipun regulasi sudah mengalami revisi dan penambahan, misalnya UU ITE diubah melalui UU No. 19 Tahun 2016, dan penetapan UU Perlindungan Data Pribadi, masih terdapat kesenjangan besar antara regulasi di atas kertas dengan praktik penegakan hukum siber di lapangan. Kesenjangan tersebut muncul dalam bentuk kapasitas teknis aparat penegak hukum, kurangnya fasilitas forensik digital, koordinasi antar lembaga, serta kesiapan hukum dalam menghadapi kasus lintas batas (transnational cybercrime). Penelitian-penelitian sebelumnya seperti yang dilakukan dalam "Tantangan Keamanan Siber dan Implikasinya terhadap …" menemukan bahwa implementasi UU ITE menghadapi kelemahan cakupan hukum, kapasitas penegakan hukum yang terbatas, serta rendahnya kesadaran masyarakat akan keamanan digital (Aliansyah et al., 2025).

Urgensi penelitian ini sangat tinggi. Dengan maraknya aktivitas digital, penetrasi internet yang terus meningkat, dan penggunaan perangkat digital di hampir semua sektor kehidupan (pemerintahan, bisnis, pendidikan), dampak kejahatan siber semakin luas dan bisa berskala besar. Selain kerugian materiil, kejahatan siber dapat merusak reputasi institusi, merusak kepercayaan publik terhadap sistem teknologi dan elektronik, serta membahayakan keamanan nasional, terutama jika menyerang infrastruktur kritis ataupun data sensitif negara. Oleh karena itu, optimalisasi penegakan hukum terhadap tindak pidana siber bukan lagi pilihan, melainkan kebutuhan mendesak.

Dalam konteks regulasi, terdapat kebutuhan untuk melakukan analisis kritis terhadap regulasi yang ada: apakah regulasi mampu menyesuaikan dengan perkembangan teknologi, sejauh mana regulasi tersebut jelas dalam rumusan pasal, bagaimana harmonisasinya dengan regulasi sektoral atau regulasi internasional, dan apakah regulasi menyediakan sanksi yang memadai serta prosedur penanganan yang efisien. Studi normatif dan empiris sebelumnya menyoroti bahwa regulasi digital masih memiliki celah hukum, kurang jelasnya ketentuan teknis, serta kurang fleksibelnya adaptasi terhadap modus-modus baru.

Sementara itu, implementasi menjadi aspek kritis berikutnya. Penegakan hukum tidak hanya soal adanya regulasi, tetapi juga kesiapan institusi (polisi, kejaksaan, pengadilan), ketersediaan teknologi forensik digital, pelatihan dan kompetensi SDM, sistem pelaporan tindak pidana siber, serta koordinasi antar lembaga di tingkat lokal dan nasional. Banyak penelitian seperti pada "Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya" menunjukkan bahwa aparat penegak hukum masih kekurangan penguasaan teknis dan sumber daya dalam menangani bukti elektronik dan investigasi siber.

Selain itu, terdapat tantangan dalam kerja sama lintas negara. Kejahatan siber sering melintasi batas yurisdiksi; pelaku dapat tinggal di luar negeri atau menggunakan server di luar negeri. Regulasi nasional seringkali belum memadai dalam aspek mutual legal assistance (MLA), pertukaran bukti elektronik, atau kerjasama pelaksanaan ekstradisi. Studi "Tantangan Penegakan Hukum Siber Di Era Lintas Negara …" menegaskan bahwa sifat lintas batas dari kejahatan siber menjadi salah satu penghambat utama dalam penegakan hukum.

Kesenjangan penelitian yang ada terletak pada beberapa sisi. Pertama, banyak studi yang fokus hanya pada aspek normatif regulasi atau hanya pada studi kasus operasional, belum

menggabungkan analisis regulasi kritis dengan evaluasi implementasi di banyak jurisdiksi atau kasus-kasus nyata; kedua, aspek teknis seperti forensik digital, teknologi deteksi, serta kesiapan SDM penegak hukum sering disebut secara umum tapi kurang dianalisis secara mendalam; ketiga, aspek harmonisasi regulasi dan koordinasi antar lembaga serta kerja sama internasional masih terabaikan; dan keempat, studi empiris tentang hambatan implementasi di daerah-daerah (luar pusat) masih relatif sedikit.

Pendekatan penelitian dalam penelitian ini akan bersifat multidimensional: pertama melalui analisis yuridis normatif terhadap regulasi terkini (UU ITE dan turunannya, UU PDP, KUHP, dan regulasi lain terkait seperti UU Telekomunikasi atau regulasi sektor yang relevan) untuk mengidentifikasi kelemahan, ketidakjelasan, dan kebutuhan pembaharuan regulasi; kedua melalui pendekatan empiris kualitatif melalui wawancara mendalam dengan aparat penegak hukum (polisi, kejaksaan, pengadilan), pakar keamanan siber, dan stakeholder terkait seperti regulator dan lembaga perlindungan data; ketiga melalui studi kasus beberapa tindak pidana siber yang signifikan di Indonesia, untuk melihat bagaimana regulasi dan prosedur diimplementasikan dalam praktik, hambatan yang muncul, serta solusi yang telah atau dapat dilakukan.

Penelitian ini akan membatasi ruang lingkup analisis pada regulasi nasional dan implementasinya di Indonesia, terutama di kota-kota besar dan beberapa daerah terpilih, serta kasus-kasus siber yang telah diproses secara hukum. Data primer dan sekunder akan digunakan untuk memperoleh gambaran lengkap. Dengan demikian penelitian diharapkan mampu memberikan rekomendasi praktis yang dapat diadopsi oleh pembuat kebijakan dan aparat penegak hukum.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan karakter analisis yuridis normatif yang dipadukan dengan penelitian lapangan (field study) melalui wawancara dan studi kasus. Analisis yuridis normatif dilakukan dengan mengkaji dan membandingkan regulasi terkait hukum siber di Indonesia—termasuk Undang-Undang ITE dan revisinya, UU Perlindungan Data Pribadi, KUHP terbaru, serta regulasi lain yang relevan seperti Undang-Undang Telekomunikasi dan Peraturan Pemerintah yang mendukung. Kajian normatif ini bertujuan mengidentifikasi kelemahan regulasi dari sisi kejelasan pasal, harmonisasi antar regulasi, fleksibilitas terhadap perkembangan teknologi, serta kecukupan sanksi dan prosedur hukum.

Untuk bagian empiris, penelitian melakukan wawancara mendalam dengan sejumlah aparatur penegak hukum, termasuk anggota kepolisian yang menangani tindak pidana siber, pihak kejaksaan, hakim, serta pejabat regulator keamanan siber atau perlindungan data. Wawancara diarahkan untuk menggali pengalaman konkret dalam menangani kasus siber, hambatan yang ditemui dalam penyidikan, pengumpulan dan verifikasi bukti elektronik, serta persepsi terhadap regulasi yang ada. Selain wawancara, data empiris juga dikumpulkan melalui studi kasus beberapa peristiwa tindak pidana siber yang telah diproses di Indonesia, misalnya kasus penipuan daring, peretasan, atau pelanggaran data pribadi, untuk memeriksa bagaimana regulasi dan prosedur hukum tersebut diimplementasikan, serta hambatan teknis dan institusional yang muncul.

Data dianalisis dengan teknik analisis isi (content analysis) dan triangulasi antara sumber regulasi, hasil wawancara, dan data studi kasus. Interpretasi dibuat dengan memperhatikan konteks hukum, teknologi, dan institusi penegak hukum. Penelitian juga mempertimbangkan perbandingan (benchmarking) dengan praktik terbaik internasional dalam penegakan hukum

siber, untuk memberikan perspektif bagaimana regulasi dan implementasi di Indonesia dapat disesuaikan lebih baik.

PEMBAHASAN DAN HASIL

Implementasi transformasi digital dalam kehidupan bermasyarakat dan pemerintahan di Indonesia telah mempercepat munculnya dan meluasnya tindak pidana siber. Regulasi telah merespon sebagian aspek dengan membuat UU ITE dan revisinya, UU Perlindungan Data Pribadi, serta berbagai regulasi sektoral dan teknis. Regulasi-regulasi ini secara normatif telah berupaya menyediakan kerangka hukum untuk mengatur aktivitas digital, menetapkan sanksi, serta menentukan prosedur penyidikan dan penuntutan terhadap pelaku kejahatan siber. Namun, analisis kritis menunjukkan bahwa regulasi tersebut memiliki sejumlah kelemahan mendasar. Rumusan beberapa pasal di UU ITE masih multitafsir dan terkadang tumpang tindih dengan regulasi lain. Misalnya, pengaturan definisi aktivitas ilegal digital, akses ilegal, dan penyebaran konten bermasalah belum selalu konsisten antar regulasi. Harmonisasi antara regulasi nasional dan regulasi sektoral (seperti telekomunikasi, keamanan data, sektor keuangan) juga belum optimal, sehingga dalam praktik terdapat ambiguitas tentang regulasi mana yang lebih diutamakan dalam situasi tertentu.

Selain itu, regulasi nasional seringkali kurang responsif terhadap perkembangan cepat modus kejahatan siber baru. Teknologi seperti deepfake, ransomware, cryptocurrency untuk kejahatan keuangan, dan teknik steganografi misalnya, berkembang dengan cepat dan sering kali melampaui skema atau jenis kejahatan yang telah diprediksi secara regulatif. Regulasi yang ada cenderung bereaksi setelah muncul masalah, bukan proaktif dalam menetapkan kerangka hukum yang adaptif. Di samping itu, aspek teknis regulasi seperti standar bukti digital, prosedur penyitaan data, kejelasan yurisdiksi dan tanggung jawab lembaga seringkali belum terperinci atau belum diikuti oleh pedoman pelaksanaan.

Dari sisi implementasi, aparat penegak hukum menghadapi tantangan besar. Banyak di antara mereka belum memiliki kompetensi teknis yang memadai untuk melakukan analisis forensik digital, pemrosesan bukti elektronik, atau investigasi siber yang kompleks. Kurangnya pelatihan yang khusus dan fasilitas yang memadai menjadi hambatan nyata. Infrastruktur teknologi forensik digital yang handal baik peranti keras (hardware) maupun perangkat lunak (software) di banyak daerah belum memadai. Ketiadaan atau keterbatasan laboratorium forensik digital yang cepat dan akurat memperlambat proses penyidikan dan mengurangi kualitas bukti yang dihadirkan di pengadilan.

Koordinasi antar lembaga penegak hukum juga menjadi titik lemah. Penanganan tindak pidana siber memerlukan kerja sama antara kepolisian, kejaksaan, badan perlindungan data, regulator telekomunikasi, serta institusi keamanan siber. Namun seringkali ada tumpang tindih kewenangan, kurangnya alur komunikasi yang jelas, dan prosedur kerja sama yang belum mapan. Misalnya, dalam beberapa kasus, bukti elektronik harus melewati prosedur yang kompleks untuk diverifikasi dan dihantar antar instansi, yang memerlukan waktu dan biaya yang besar.

Tantangan lainnya adalah aspek hukum internasional dan yurisdiksi. Banyak kasus kejahatan siber melibatkan pelaku yang berada di luar negeri atau menggunakan server atau sumber daya di luar wilayah nasional. Mekanisme mutual legal assistance, ekstradisi, dan pertukaran bukti antar negara belum berjalan efektif atau terkendala oleh regulasi yang berbeda, prosedur diplomatik, serta perbedaan standar hukum antar negara. Hal ini menghambat penyelesaian kasus-kasus kejahatan siber lintas negara.

Literasi dan kesadaran publik juga memegang peranan penting. Masyarakat yang belum cukup memahami risiko kejahatan siber atau belum mengetahui hak dan prosedur hukum digital cenderung menjadi korban atau tidak melaporkan peristiwa kejahatan siber. Di sisi lain, regulasi yang ada kadang kurang mengatur perlindungan korban atau prosedur pelaporan yang ramah korban. Edukasi publik tentang keamanan digital, penggunaan data pribadi, serta kewaspadaan terhadap modus kejahatan siber menjadi aspek yang perlu diperkuat.

Regulasi yang ada, selain UU ITE dan UU PDP, juga perlu dihubungkan dengan KUHP baru yang menggantikan atau memperbaharui beberapa ketentuan pidana umum terkait tindak pidana penggelapan, pencurian, atau kejahatan terhadap keamanan negara, agar regulasi siber tidak terpisah secara terfragmentasi. Karena KUHP baru memiliki pasal-pasal umum pidana, namun belum secara khusus menyesuaikan nadanya terhadap perilaku kriminal digital yang spesifik, perlu adanya integrasi aturan siber ke dalam KUHP atau regulasi pelengkap yang jelas. Penegakan sanksi juga menjadi masalah. Walaupun regulasi mengatur sanksi pidana, dalam banyak kasus sanksi yang sebenarnya diberikan tidak mencerminkan tingkat kerugian atau kompleksitas kejahatan siber, karena bukti yang lemah atau proses penyidikan yang lambat. Hal ini berpotensi menimbulkan jawaban hukum yang tidak menimbulkan efek jera.

Untuk mengoptimalkan penegakan hukum, diperlukan beberapa strategi. Pertama, pembaruan regulasi agar lebih responsif terhadap teknologi baru dengan memperjelas definisi, standarisasi prosedur forensik digital, dan menetapkan ketentuan yurisdiksi untuk kasus lintas negara. Kedua, peningkatan kapasitas teknis aparat penegak hukum melalui pelatihan khusus, penyediaan laboratorium forensik digital yang memadai di pusat dan daerah, serta pengadaan peralatan dan perangkat lunak terkini. Ketiga, pembenahan koordinasi antar lembaga melalui pembentukan mekanisme kerja sama yang formal dan prosedur-prosedur standar operasional (SOP) untuk investigasi, pertukaran bukti, dan pelaporan kejahatan siber. Keempat, kerja sama internasional yang diperkuat: memperbaharui perjanjian internasional yang relevan, meningkatkan MLA dan ekstradisi serta pertukaran informasi antara negara. Kelima, edukasi publik dan advokasi hak-hak korban agar prosedur pelaporan lebih mudah dan korban lebih terlindung.

Dengan penerapan strategi-strategi tersebut, penegakan hukum terhadap tindak pidana siber di Indonesia dapat lebih optimal: regulasi menjadi lebih jelas dan adaptif, aparat penegak memiliki kemampuan teknis dan sarana yang memadai, koordinasi dan kerja sama baik nasional maupun internasional berjalan efektif, dan korban mendapatkan perlindungan. Hal ini akan memperkuat keamanan digital serta kepercayaan publik terhadap sistem hukum dan institusi negara dalam menghadapi ancaman siber yang terus berkembang.

KESIMPULAN DAN SARAN

Penegakan hukum tindak pidana siber di era transformasi digital menghadapi tantangan regulatif dan implementatif yang signifikan. Dari sisi regulasi, meskipun Indonesia telah memiliki UU ITE, UU Perlindungan Data Pribadi, KUHP baru dan regulasi pendukung lainnya, terdapat kelemahan dalam kejelasan pasal, multitafsir, kurangnya harmonisasi dan fleksibilitas regulatif yang dibutuhkan untuk merespon modus kejahatan siber yang terus berkembang.

Implementasi di lapangan juga menghadapi berbagai hambatan nyata seperti keterbatasan kompetensi teknis aparat penegak hukum, kurangnya fasilitas forensik digital yang memadai, korespondensi antar lembaga yang belum optimal, dan hambatan kerja sama lintas negara serta masalah hukum internasional seperti yurisdiksi dan pertukaran bukti.

Untuk mengoptimalkan penegakan hukum terhadap tindak pidana siber, diperlukan reformasi regulasi yang adaptif dan responsif terhadap teknologi baru, peningkatan kapasitas teknis aparat melalui pelatihan dan teknologi penunjang, perbaikan koordinasi antar lembaga dan prosedur kerja yang jelas, serta penguatan kerja sama internasional dan edukasi publik. Dengan demikian, upaya penegakan hukum akan menjadi lebih efektif dalam melindungi masyarakat dan negara dalam menghadapi ancaman siber.

DAFTAR PUSTAKA

Aliansyah, D. K., Tyasari, H. A., & Putri, K. M. (2025). Telaah Dampak Kebijakan Impor Terhadap Industri Tekstil Nasional: Idealitas Perlindungan Ekonomi Domestik: Indonesia. *Forschungsforum Law Journal*, *2*(02). https://doi.org/DOI:%2520https://doi.org/10.35586/flj.v2i02.11189

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati S.Kom., M.Sc.Eng, N. A. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal of Information Engineering and Educational Technology*, *2*(2), 65. https://doi.org/10.26740/jieet.v2n2.p65-69

Firdaus, R. A. (2024). Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. *STAATSRECHT: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(1), 79–104. https://doi.org/DOI:%2520https://doi.org/10.14421/cf582q68

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/DOI:%2520https://doi.org/10.15642/alqanun.2020.23.2.400-426

Thomas, A. M. R., & Anggraeni, H. Y. (2025). Cybercrime dan Media Sosial: Analisis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.2173