Vol. 05 No. 03 (2026) : 20-29 e-ISSN: 2964-0131
p-ISSN-2964-1748
UNISAN JURNAL: JURNAL MANAJEMEN DAN PENDIDIKAN
e-ISSN: 2964-0131 p-ISSN-2964-1748
Available online at https://journal.an-nur.ac.id/index.php/unisanjournal

DINAMIKA HUKUM SIBER *(CYBER LAW)* DALAM MENANGGAPI KEJAHATAN DIGITAL DI ERA MODERN

Dani Amran Hakim
UIN Raden Intan Lampung
Email: daniamranhakim@radenintan.ac.id

Abstrak

Perkembangan teknologi digital yang pesat telah memunculkan berbagai bentuk kejahatan siber yang semakin kompleks dan sulit dikendalikan oleh sistem hukum konvensional. Kondisi ini menuntut adanya dinamika hukum siber yang adaptif dan responsif terhadap perubahan zaman. Penelitian ini bertujuan untuk menganalisis dinamika hukum siber dalam menanggapi kejahatan digital di era modern, mengidentifikasi kelemahan dalam regulasi dan implementasi hukum, serta merumuskan model penguatan hukum yang lebih efektif. Metode yang digunakan adalah studi kepustakaan (library research) dengan pendekatan historis dan konseptual, menggunakan sumber data berupa jurnal ilmiah lima tahun terakhir, buku, serta dokumen hukum yang relevan. Analisis data dilakukan secara kualitatif melalui teknik analisis isi (content analysis). Hasil penelitian menunjukkan bahwa hukum siber di Indonesia masih menghadapi berbagai tantangan, seperti kelemahan regulasi, keterbatasan kapasitas penegak hukum, kurangnya integrasi teknologi, serta kendala yurisdiksi lintas negara. Oleh karena itu, diperlukan penguatan hukum siber melalui pembaruan regulasi, peningkatan kapasitas sumber daya manusia, integrasi teknologi, serta kerja sama lintas sektor dan internasional. Kesimpulan penelitian ini menegaskan bahwa hukum siber harus terus berkembang secara dinamis agar mampu menjawab tantangan kejahatan digital secara efektif dan berkelanjutan di era modern.
Kata Kunci: Hukum Siber, Kejahatan Digital, Cybercrime, Penegakan Hukum, Transformasi Digital

Abstract

The rapid development of digital technology has led to increasingly complex forms of cybercrime that are difficult to control using conventional legal systems. This condition requires a dynamic cyber law framework that is adaptive and responsive to contemporary changes. This study aims to analyze the dynamics of cyber law in addressing digital crimes in the modern era, identify weaknesses in legal regulations and implementation, and formulate a more effective legal strengthening model. The research employs a library research method with historical and conceptual approaches, utilizing data sources from recent scientific journals (last five years), books, and relevant legal documents. Data analysis is conducted qualitatively using content analysis techniques. The results indicate that cyber law in Indonesia still faces several challenges, including regulatory weaknesses, limited capacity of law enforcement, lack of technological integration, and cross-border jurisdiction issues. Therefore, strengthening cyber law is necessary through regulatory reform, enhancement of human resources, technological integration, and cross-sectoral and international cooperation. In conclusion, cyber law must continuously evolve to effectively and sustainably address digital crime challenges in the modern era.
Keywords: Cyber Law, Digital Crime, Cybercrime, Law Enforcement, Digital Transformation

PENDAHULUAN

Perkembangan teknologi informasi di era modern telah mendorong transformasi besar dalam berbagai aspek kehidupan, termasuk dalam bidang hukum. Digitalisasi yang masif tidak hanya menghadirkan kemudahan, tetapi juga memunculkan bentuk kejahatan baru yang dikenal sebagai kejahatan siber (cybercrime). Kejahatan ini memiliki karakteristik lintas batas, anonim, dan kompleks sehingga sulit ditangani dengan pendekatan hukum konvensional. Fenomena seperti peretasan sistem, pencurian data pribadi, dan penipuan digital terus meningkat dan menuntut respons hukum yang lebih adaptif (Saputra, 2025). Oleh karena itu, kajian mengenai dinamika hukum siber menjadi sangat penting dalam menghadapi tantangan kejahatan digital.

Indonesia menghadapi tantangan serius dalam penegakan hukum siber seiring meningkatnya jumlah pengguna internet. Regulasi yang ada seperti Undang-Undang Informasi dan Transaksi Elektronik belum sepenuhnya mampu menjawab kompleksitas kejahatan digital. Permasalahan seperti multitafsir norma hukum, lemahnya penegakan hukum, serta keterbatasan sumber daya manusia menjadi hambatan utama (Wibowo, 2023). Selain itu, kendala dalam pembuktian digital dan kurangnya koordinasi antar lembaga penegak hukum juga memperparah kondisi tersebut (Hidayat, 2024). Hal ini menunjukkan adanya kesenjangan antara perkembangan teknologi dan kesiapan sistem hukum.

Hukum siber merupakan cabang hukum yang mengatur aktivitas manusia di ruang digital, termasuk transaksi elektronik, perlindungan data, dan kejahatan siber. Dalam perspektif teori hukum responsif, hukum harus mampu menyesuaikan diri dengan perubahan sosial dan teknologi yang cepat. Selain itu, teori kejahatan transnasional menjelaskan bahwa cybercrime merupakan ancaman global yang membutuhkan kerja sama lintas negara. Pendekatan hukum modern tidak hanya bersifat represif, tetapi juga preventif dan adaptif melalui integrasi teknologi dan penguatan kelembagaan (Nasution, 2026).

Penelitian oleh (Prasetyo, 2022) mengkaji regulasi cybercrime di Indonesia, namun masih terbatas pada analisis normatif tanpa melihat implementasi. Selanjutnya, penelitian (Lestari, 2025) membahas tantangan hukum siber di era digital, tetapi belum mengintegrasikan aspek teknologi secara komprehensif. Penelitian (Yuliana, 2024) mengenai perlindungan data pribadi lebih menekankan pada aspek privasi tanpa mengkaji dinamika penegakan hukum. Gap dari ketiga penelitian ini adalah belum adanya pendekatan yang menyeluruh dalam melihat hukum siber. Novelty penelitian ini terletak pada pendekatan integratif antara regulasi, teknologi, dan praktik hukum.

Penelitian (Ramadhan, 2026) menyoroti kebijakan penegakan hukum cybercrime, tetapi belum mengkaji implementasi di lapangan. Sementara itu, penelitian (Putra, 2023) membahas pembuktian digital dalam kejahatan siber, namun tidak menghubungkannya dengan reformasi hukum secara luas. Penelitian (Sari, 2025) menunjukkan bahwa penegakan hukum cybercrime masih menghadapi kendala struktural dan teknis. Gap dari penelitian ini adalah kurangnya integrasi antara aspek kebijakan, teknis, dan kelembagaan. Novelty penelitian ini adalah menggabungkan ketiga aspek tersebut dalam satu analisis komprehensif.

Penelitian (Firmansyah, 2024) membahas pertanggungjawaban pidana dalam kasus kejahatan siber, tetapi belum menyentuh aspek perkembangan teknologi terbaru. Di sisi lain, penelitian (Maharani, 2022) mengkaji yurisdiksi dalam cybercrime dan menemukan adanya kendala dalam penegakan hukum lintas negara. Gap dari kedua penelitian ini adalah belum adanya model harmonisasi hukum yang adaptif terhadap perkembangan global. Novelty penelitian ini adalah menawarkan pendekatan harmonisasi hukum nasional dan internasional yang berbasis teknologi.

Berdasarkan delapan penelitian terdahulu, terlihat bahwa kajian hukum siber masih bersifat parsial dan belum terintegrasi. Sebagian besar penelitian hanya fokus pada satu aspek tertentu seperti regulasi, pembuktian, atau yurisdiksi. Oleh karena itu, penelitian ini menghadirkan kebaruan berupa pendekatan multidimensional yang mengintegrasikan aspek regulasi, teknologi, kelembagaan, dan kerja sama internasional dalam satu kerangka analisis yang utuh. Penelitian ini bertujuan untuk menganalisis dinamika hukum siber dalam menanggapi kejahatan digital di era modern, mengidentifikasi kelemahan dalam regulasi dan implementasi hukum, serta merumuskan model penguatan hukum yang adaptif dan responsif terhadap perkembangan teknologi. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan hukum siber di Indonesia baik secara teoritis maupun praktis.

METODE

Penelitian ini menggunakan metode studi kepustakaan (library research) yang mengandalkan sumber-sumber bibliografi berupa artikel jurnal ilmiah terbaru, buku, serta dokumen hukum yang relevan dengan dinamika hukum siber dan kejahatan digital, dengan tujuan untuk mengkaji secara mendalam konsep, teori, serta perkembangan regulasi terkait cyber law dalam merespons fenomena kejahatan digital di era modern melalui pembacaan kritis terhadap pemikiran para ahli dengan pendekatan konstruktif dan interpretatif terhadap substansi permasalahan (Nasution, 2009); selain itu,

penelitian ini juga memadukan pendekatan historis dan konseptual, di mana pendekatan historis digunakan untuk menelusuri evolusi regulasi dan kebijakan hukum siber baik secara global maupun di Indonesia, sementara pendekatan konseptual dimanfaatkan untuk menganalisis berbagai konsep hukum yang berkaitan dengan cybercrime, perlindungan data pribadi, serta penegakan hukum digital; sumber data penelitian ini terdiri dari jurnal-jurnal ilmiah lima tahun terakhir yang membahas hukum siber dan kejahatan digital, dilengkapi dengan buku-buku hukum, dokumen peraturan perundang-undangan, serta laporan resmi yang relevan, dengan fokus pada dinamika regulasi, tantangan penegakan hukum, dan perkembangan teknologi yang memengaruhi hukum siber; teknik pengumpulan data dilakukan melalui metode dokumentasi dengan cara mengidentifikasi, mengumpulkan, dan mengklasifikasikan literatur yang sesuai dengan topik penelitian, kemudian dilakukan reduksi data untuk memilih informasi yang relevan dengan fokus kajian, yang selanjutnya disajikan secara sistematis guna mempermudah proses analisis; analisis data dilakukan secara kualitatif melalui teknik analisis isi (content analysis) dengan mengkaji secara kritis berbagai sumber, membandingkan pandangan dan temuan penelitian terdahulu untuk menemukan pola, kesenjangan (gap), serta peluang pengembangan hukum siber, sekaligus mengaitkan antara teori hukum, regulasi yang berlaku, dan realitas praktik penegakan hukum di lapangan; pada tahap akhir, peneliti memberikan interpretasi terhadap data secara objektif dan sistematis guna menghasilkan pemahaman yang komprehensif mengenai dinamika hukum siber serta merumuskan konsep penguatan hukum yang adaptif dan responsif terhadap perkembangan kejahatan digital, sehingga hasil penelitian ini diharapkan memiliki validitas ilmiah yang kuat dan tidak bersifat subjektif.

HASIL DAN PEMBAHASAN

Dinamika Hukum Siber dalam Menanggapi Kejahatan Digital di Era Modern

Dinamika hukum siber di era modern menunjukkan perkembangan yang sangat signifikan seiring dengan pesatnya transformasi digital dalam berbagai sektor kehidupan. Hukum tidak lagi hanya berfungsi sebagai alat pengatur perilaku konvensional, tetapi juga harus mampu menjangkau ruang virtual yang kompleks dan terus berkembang. Kejahatan digital seperti peretasan, pencurian identitas, penyebaran malware, dan penipuan berbasis daring menuntut adanya pembaruan hukum yang tidak hanya bersifat normatif, tetapi juga adaptif terhadap perubahan teknologi. Dalam konteks ini, hukum siber

menjadi instrumen penting dalam menjaga stabilitas dan keamanan ruang digital.

Perkembangan regulasi hukum siber di Indonesia menunjukkan adanya upaya serius dari pemerintah dalam merespons ancaman kejahatan digital. Kehadiran berbagai peraturan perundang-undangan terkait teknologi informasi mencerminkan komitmen negara dalam memberikan perlindungan hukum bagi masyarakat. Namun demikian, dinamika yang terjadi di lapangan menunjukkan bahwa regulasi yang ada masih menghadapi berbagai tantangan, seperti ketertinggalan dalam mengikuti perkembangan teknologi serta adanya celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan digital.

Selain itu, dinamika hukum siber juga terlihat dari perubahan paradigma dalam penegakan hukum. Jika sebelumnya penegakan hukum lebih bersifat reaktif, maka saat ini mulai bergeser ke arah preventif dan proaktif. Penegak hukum dituntut untuk tidak hanya menindak pelaku kejahatan, tetapi juga mampu melakukan pencegahan melalui edukasi digital, penguatan sistem keamanan, serta pemanfaatan teknologi dalam proses penyelidikan dan penyidikan. Hal ini menunjukkan bahwa hukum siber tidak dapat berdiri sendiri, melainkan harus didukung oleh berbagai elemen lain, termasuk teknologi dan sumber daya manusia yang kompeten.

Di sisi lain, dinamika hukum siber juga dipengaruhi oleh sifat kejahatan digital yang lintas batas negara. Cybercrime tidak mengenal batas geografis, sehingga menimbulkan tantangan dalam hal yurisdiksi dan kerja sama internasional. Penegakan hukum terhadap pelaku kejahatan siber seringkali terkendala oleh perbedaan sistem hukum antarnegara, serta keterbatasan mekanisme kerja sama yang efektif. Oleh karena itu, diperlukan harmonisasi hukum serta penguatan kerja sama internasional untuk mengatasi permasalahan tersebut.

Selanjutnya, dinamika hukum siber juga mencerminkan adanya kebutuhan akan integrasi antara aspek hukum dan teknologi. Penggunaan teknologi seperti digital forensik, artificial intelligence, dan big data analytics menjadi sangat penting dalam mendukung proses penegakan hukum siber. Tanpa dukungan teknologi yang memadai, penegakan hukum akan sulit dilakukan secara efektif, mengingat kompleksitas kejahatan digital yang semakin tinggi. Oleh karena itu, pengembangan kapasitas teknologi menjadi bagian yang tidak terpisahkan dari dinamika hukum siber.

Secara keseluruhan, dinamika hukum siber di era modern menunjukkan bahwa hukum harus terus beradaptasi dengan perkembangan zaman. Hukum tidak lagi bersifat statis, tetapi harus mampu mengikuti perubahan yang terjadi di masyarakat, khususnya dalam ruang digital. Dengan demikian, dinamika hukum siber menjadi cerminan dari upaya negara dalam menjaga keamanan dan keadilan di era digital, sekaligus menunjukkan pentingnya inovasi dalam sistem hukum untuk menghadapi tantangan kejahatan digital yang semakin kompleks.

Kelemahan Regulasi dan Model Penguatan Hukum Siber yang Adaptif dan Responsif

Hasil penelitian menunjukkan bahwa salah satu kelemahan utama dalam hukum siber di Indonesia terletak pada aspek regulasi yang belum sepenuhnya mampu mengakomodasi perkembangan kejahatan digital. Meskipun telah terdapat berbagai peraturan yang mengatur aktivitas di ruang digital, namun masih ditemukan adanya ketidakjelasan norma serta multitafsir dalam penerapannya. Hal ini menyebabkan ketidakpastian hukum yang dapat menghambat proses penegakan hukum serta membuka peluang terjadinya penyalahgunaan kewenangan. Selain itu, kelemahan juga terlihat pada aspek implementasi hukum yang masih menghadapi berbagai kendala teknis dan struktural. Keterbatasan sumber daya manusia yang memiliki kompetensi di bidang teknologi informasi menjadi salah satu faktor utama yang memengaruhi efektivitas penegakan hukum siber. Penegak hukum seringkali mengalami kesulitan dalam mengumpulkan dan menganalisis alat bukti digital, yang pada akhirnya berdampak pada rendahnya tingkat keberhasilan penanganan kasus kejahatan siber.

Kelemahan lain yang ditemukan adalah kurangnya koordinasi antar lembaga dalam penegakan hukum siber. Penanganan kejahatan digital memerlukan kerja sama yang erat antara berbagai instansi, baik di tingkat nasional maupun internasional. Namun, dalam praktiknya, koordinasi tersebut masih belum berjalan secara optimal, sehingga menghambat proses penanganan kasus serta memperlambat respon terhadap ancaman kejahatan digital. Dalam menghadapi berbagai kelemahan tersebut, diperlukan model penguatan hukum siber yang adaptif dan responsif terhadap perkembangan teknologi. Model ini harus mencakup pembaruan regulasi yang lebih jelas dan komprehensif, peningkatan kapasitas sumber daya manusia, serta penguatan infrastruktur teknologi yang mendukung penegakan hukum. Selain itu,

diperlukan juga pengembangan sistem hukum yang mampu mengintegrasikan berbagai aspek, baik hukum, teknologi, maupun kelembagaan.

Penguatan hukum siber juga harus dilakukan melalui pendekatan kolaboratif yang melibatkan berbagai pihak, termasuk pemerintah, sektor swasta, akademisi, dan masyarakat. Kerja sama ini penting untuk menciptakan ekosistem digital yang aman dan berkelanjutan. Selain itu, kerja sama internasional juga perlu ditingkatkan untuk mengatasi kejahatan siber yang bersifat lintas negara, melalui perjanjian bilateral maupun multilateral yang mendukung penegakan hukum global.

Dengan demikian, model penguatan hukum siber yang adaptif dan responsif tidak hanya berfokus pada aspek regulasi, tetapi juga mencakup penguatan kapasitas kelembagaan, pemanfaatan teknologi, serta kerja sama lintas sektor dan negara. Pendekatan ini diharapkan dapat meningkatkan efektivitas penegakan hukum siber serta mampu menjawab tantangan kejahatan digital di era modern secara lebih komprehensif dan berkelanjutan.

Pembahasan

Pembahasan mengenai dinamika hukum siber dalam menanggapi kejahatan digital menunjukkan bahwa temuan penelitian ini sejalan dengan teori hukum responsif yang menekankan bahwa hukum harus mampu beradaptasi dengan perubahan sosial dan teknologi yang cepat (Nonet & Selznick, 2001). Dalam konteks ini, dinamika hukum siber yang terus berkembang mencerminkan upaya sistem hukum untuk menyesuaikan diri dengan kompleksitas ruang digital. Hasil penelitian ini menguatkan pandangan bahwa hukum tidak lagi bersifat statis, melainkan harus fleksibel dan inovatif dalam menghadapi kejahatan digital, sebagaimana juga ditegaskan dalam penelitian Saputra (2025) yang menyatakan bahwa peningkatan cybercrime menuntut pembaruan hukum yang berkelanjutan agar tetap relevan dengan kondisi masyarakat digital.

Lebih lanjut, hasil penelitian ini menunjukkan bahwa regulasi hukum siber di Indonesia masih menghadapi berbagai kelemahan, terutama dalam hal multitafsir norma dan keterbatasan implementasi. Temuan ini sejalan dengan penelitian Wibowo (2023) yang menyoroti kelemahan regulasi dalam menghadapi kejahatan digital yang semakin kompleks. Selain itu, Hidayat (2024) juga menegaskan bahwa kendala pembuktian digital menjadi salah satu hambatan utama dalam penegakan hukum siber. Namun demikian, penelitian ini memberikan penekanan lebih pada dinamika implementasi hukum di

lapangan, yang menunjukkan adanya kesenjangan antara norma hukum dan praktik penegakan hukum, sehingga memperluas kajian sebelumnya.

Dari perspektif teori kejahatan transnasional, hasil penelitian ini juga memperkuat pandangan bahwa cybercrime merupakan kejahatan lintas batas yang membutuhkan kerja sama internasional (Bossler & Holt, 2012). Temuan mengenai kendala yurisdiksi dan keterbatasan kerja sama antarnegara sejalan dengan penelitian Maharani (2022) yang mengungkapkan bahwa perbedaan sistem hukum menjadi penghambat utama dalam penanganan cybercrime global. Namun, penelitian ini menawarkan perspektif baru dengan menekankan perlunya model hukum yang tidak hanya harmonis secara normatif, tetapi juga adaptif terhadap perkembangan teknologi global.

Selain itu, hasil penelitian ini menunjukkan bahwa penegakan hukum siber memerlukan integrasi antara aspek hukum dan teknologi. Temuan ini mendukung teori yang menyatakan bahwa efektivitas penegakan hukum siber sangat bergantung pada kemampuan teknologi seperti digital forensik dan analisis data (Brenner, 2010). Penelitian Putra (2023) juga menunjukkan bahwa pembuktian dalam kejahatan siber memerlukan pendekatan berbasis teknologi yang kuat. Namun, penelitian ini menambahkan dimensi baru dengan menekankan bahwa integrasi teknologi harus menjadi bagian dari sistem hukum secara menyeluruh, bukan hanya sebagai alat bantu teknis.

Dalam aspek kelembagaan, hasil penelitian ini mengungkapkan bahwa lemahnya koordinasi antar lembaga menjadi salah satu faktor penghambat utama dalam penegakan hukum siber. Temuan ini sejalan dengan penelitian Sari (2025) yang menunjukkan bahwa fragmentasi kelembagaan menghambat efektivitas penanganan cybercrime. Selain itu, Ramadhan (2026) menegaskan bahwa kebijakan penegakan hukum masih belum terintegrasi secara optimal. Penelitian ini kemudian memperluas kajian tersebut dengan menekankan pentingnya pendekatan kolaboratif lintas sektor, termasuk keterlibatan pemerintah, swasta, dan masyarakat dalam membangun sistem hukum yang responsif.

Secara keseluruhan, pembahasan ini menunjukkan bahwa penelitian ini tidak hanya mengonfirmasi temuan-temuan sebelumnya, tetapi juga memberikan kontribusi baru dalam bentuk pendekatan multidimensional terhadap hukum siber. Dengan mengintegrasikan aspek regulasi, teknologi, kelembagaan, dan kerja sama internasional, penelitian ini menawarkan model penguatan hukum siber yang lebih komprehensif. Hal ini melengkapi penelitian sebelumnya seperti Prasetyo (2022) dan Lestari (2025) yang masih

bersifat parsial, sehingga penelitian ini menghadirkan kebaruan dalam bentuk analisis yang lebih holistik dan integratif dalam memahami dinamika hukum siber di era modern.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan dalam menafsirkan hasil kajian. Pertama, penggunaan metode studi kepustakaan (library research) menyebabkan penelitian ini sangat bergantung pada ketersediaan dan kualitas sumber literatur, sehingga tidak secara langsung menggambarkan kondisi empiris di lapangan. Kedua, keterbatasan dalam mengakses data terkini terkait praktik penegakan hukum siber, khususnya yang bersifat internal lembaga, membuat analisis lebih berfokus pada aspek normatif dan konseptual. Ketiga, dinamika teknologi yang berkembang sangat cepat berpotensi menyebabkan sebagian temuan menjadi kurang relevan dalam waktu yang relatif singkat. Selain itu, penelitian ini belum secara mendalam mengkaji perbandingan hukum antarnegara secara komprehensif, sehingga generalisasi hasil penelitian masih terbatas pada konteks tertentu, khususnya di Indonesia.

Adapun kebaruan (novelty) penelitian ini terletak pada pendekatan multidimensional yang mengintegrasikan aspek regulasi, teknologi, kelembagaan, dan kerja sama internasional dalam satu kerangka analisis yang utuh. Berbeda dengan penelitian sebelumnya yang cenderung parsial—hanya menyoroti satu aspek seperti regulasi, pembuktian digital, atau kebijakan—penelitian ini menawarkan perspektif yang lebih komprehensif dalam memahami dinamika hukum siber. Selain itu, penelitian ini juga menghadirkan konsep penguatan hukum siber yang bersifat adaptif dan responsif terhadap perkembangan teknologi digital, dengan menekankan pentingnya sinergi antara hukum dan teknologi dalam penegakan hukum. Dengan demikian, penelitian ini tidak hanya memberikan kontribusi teoretis, tetapi juga menawarkan implikasi praktis dalam pengembangan sistem hukum siber yang lebih efektif di era modern.

KESIMPULAN

Hasil penelitian menunjukkan bahwa dinamika hukum siber dalam menanggapi kejahatan digital di era modern mengalami perkembangan yang signifikan, namun masih menghadapi berbagai tantangan, terutama pada aspek regulasi yang belum sepenuhnya adaptif, kelemahan dalam implementasi penegakan hukum, keterbatasan kapasitas sumber daya manusia, serta kurangnya integrasi teknologi dalam sistem hukum; selain itu, kendala yurisdiksi lintas negara dan lemahnya koordinasi antar lembaga turut

memperburuk efektivitas penanganan cybercrime. Berdasarkan temuan tersebut, dapat disimpulkan bahwa hukum siber di Indonesia masih berada dalam tahap transisi menuju sistem yang lebih responsif dan adaptif terhadap perkembangan teknologi digital, sehingga diperlukan pembaruan hukum yang komprehensif dan berkelanjutan. Oleh karena itu, penelitian ini merekomendasikan perlunya penguatan regulasi yang lebih jelas dan tidak multitafsir, peningkatan kompetensi aparat penegak hukum melalui pelatihan berbasis teknologi, pengembangan infrastruktur digital forensik, serta penguatan kerja sama lintas sektor dan internasional guna menciptakan sistem hukum siber yang efektif, terintegrasi, dan mampu menjawab tantangan kejahatan digital secara berkelanjutan di era modern.

DAFTAR PUSTAKA

Brenner, S. W. (2010). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press.

Bossler, A. M., & Holt, T. J. (2012). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Hidayat, R. (2024). Tantangan pembuktian digital dalam penegakan hukum kejahatan siber di Indonesia. *Jurnal Hukum Digital*, 5(2), 120–134.

Lestari, D. (2025). Dinamika hukum siber dalam masyarakat digital: Tantangan dan peluang. *Jurnal Ilmu Hukum Modern*, 7(1), 45–60.

Maharani, S. (2022). Yurisdiksi hukum dalam penanganan cybercrime lintas negara. *Jurnal Hukum Internasional*, 6(2), 88–102.

Nasution, S. (2009). *Metode research (penelitian ilmiah)*. Bumi Aksara.

Nonet, P., & Selznick, P. (2001). *Law and society in transition: Toward responsive law*. Transaction Publishers.

Prasetyo, A. (2022). Analisis regulasi cybercrime di Indonesia dalam perspektif hukum positif. *Jurnal Hukum Nasional*, 4(1), 1–15.

Putra, R. (2023). Pembuktian digital dalam tindak pidana siber di Indonesia. *Jurnal Hukum dan Teknologi*, 3(2), 67–80.

Ramadhan, F. (2026). Kebijakan penegakan hukum terhadap kejahatan siber di era digital. *Jurnal Kebijakan Publik*, 8(1), 22–37.

Saputra, M. (2025). Perkembangan kejahatan siber dan implikasinya terhadap hukum nasional. *Jurnal Kriminologi Indonesia*, 9(1), 10–25.

Sari, N. (2025). Hambatan kelembagaan dalam penegakan hukum cybercrime di Indonesia. *Jurnal Sosio-Legal*, 6(1), 55–70.

Wibowo, A. (2023). Evaluasi regulasi hukum siber di Indonesia dalam menghadapi kejahatan digital. *Jurnal Legislasi Indonesia*, 10(2), 200–215.