AKSIOMA

Volume 2 No. 12, Desember 2025, 2579 - 2591
DOI: https://doi.org/10.62335

Jurnal Sains Ekonomi dan Edukasi
https://manggalajournal.org/index.php/AKSIOMA
E-ISSN 3031-9404

# Tantangan Penegakan Hukum di Era Globalisasi Digital: Strategi Nasional Menghadapi Kejahatan Siber Lintas Batas

**Zahra Pitaloka Islami**[a*]
[a] *Program Studi Magister Ilmu Hukum, Universitas Brawijaya Kampus Jakarta, Indonesia*

INFO ARTIKEL

***Riwayat Artikel:***
*Receied : 15-11-2025*
*Reised : 29-12-2025*
*Accepted :01-12-2025*

***Keywords: Cyber Crime, Digital Globalization, Law Enforcement***

**Kata Kunci: Globalisasi Digital, Penegakan Hukum, Pidana Siber**

*Corresponding Author:*
*zahra.pitaloka@gmail.com*[*]

***DOI: https://doi.org/10.62335***

ABSTRACT

*The rapid advancement of digital technology and cyber globalization has accelerated the emergence of a new order of social, economic, and political interactions that increasingly depend on cross-border data flows, thereby giving rise to new configurations of crime that are no longer subject to the physical territorial boundaries of the state. In this context, cybercrime, data theft, attacks on critical infrastructure, misuse of digital identities, as well as various forms of manipulation of information systems challenge the classical paradigm of national law enforcement, which rests on the principles of territoriality, personality, and the protection of state interests that were designed for an analog world. The situation becomes even more complex when offenders, victims, servers, service providers, and the impacts of crime are dispersed across multiple jurisdictions, while national legal instruments, criminal procedure rules, and the institutional capacity of law-enforcement agencies still operate within a framework that assumes that the locus and tempus delicti can be clearly determined within a single sovereign territory. This paper seeks to identify the weaknesses of the national legal system in responding to global cybercrime and to formulate law-enforcement strategies that are adaptive to the characteristics of the digital space, which does not recognize state borders, by analyzing the dimensions of legal substance, institutional structure, and legal culture that shape the way the state responds to these threats. The approach employed is normative juridical, supported by a criminal-policy perspective, by revisiting the principles of jurisdiction, extradition, mutual legal assistance, and due process of law in the context of digital transformation, while at the same time weighing the need for regulatory harmonization, the strengthening of the technical capacity of law-enforcement agencies, and the establishment of agile cross-border cooperation mechanisms that nonetheless respect human rights and the protection of personal data. The*

*results of the discussion show that an effective national law-enforcement strategy in the era of digital globalization cannot stop at merely revising individual criminal provisions, but instead presupposes a comprehensive reconstruction of how the state understands sovereignty in cyberspace, designs procedures for electronic evidence, manages cooperation with global private actors, and integrates the role of society in preventing and reporting cybercrime. This paper then offers a series of normative and practical recommendations that include updating the regulatory framework, strengthening institutions, developing multi-stakeholder digital governance, and improving digital literacy as efforts to build a law-enforcement architecture that is more responsive, adaptive, and just amid the challenges of digital globalization.*

ABSTRAK

Percepatan perkembangan teknologi digital dan globalisasi siber telah mengakselerasi lahirnya tatanan interaksi sosial, ekonomi, dan politik yang semakin bergantung pada arus data lintas negara, sehingga memunculkan konfigurasi baru kejahatan yang tidak lagi tunduk pada batas-batas fisik teritorial negara. Dalam konteks ini, kejahatan siber, pencurian data, serangan terhadap infrastruktur kritis, penyalahgunaan identitas digital, serta berbagai bentuk manipulasi sistem informasi menantang paradigma klasik penegakan hukum nasional yang bertumpu pada asas teritorial, personal, dan perlindungan kepentingan negara yang dibangun untuk dunia analog. Situasi menjadi kian kompleks ketika pelaku, korban, server, penyedia layanan, dan dampak kejahatan tersebar di berbagai yurisdiksi, sementara perangkat hukum nasional, prosedur acara pidana, dan kapasitas institusional aparatur penegak hukum masih bekerja dalam kerangka yang mengandaikan bahwa locus dan tempus delicti dapat ditentukan secara jelas dalam satu wilayah kedaulatan. Makalah ini berupaya mengidentifikasi kelemahan sistem hukum nasional dalam merespons kejahatan siber global dan merumuskan strategi penegakan hukum yang adaptif terhadap karakter ruang digital yang tidak mengenal batas negara, melalui analisis terhadap dimensi substansi hukum, struktur kelembagaan, serta kultur hukum yang membentuk cara negara merespons ancaman tersebut. Pendekatan yang digunakan bersifat yuridis normatif dengan dukungan perspektif kebijakan kriminal (criminal policy), dengan cara membaca kembali asas-asas yurisdiksi, ekstradisi, mutual legal assistance, serta prinsip due process of law dalam konteks transformasi digital, sambil menimbang kebutuhan akan harmonisasi regulasi, penguatan kapasitas teknis penegak hukum, dan pembentukan mekanisme kerja sama lintas negara yang lincah namun tetap menghormati hak asasi manusia serta perlindungan data pribadi. Hasil pembahasan menunjukkan bahwa

strategi penegakan hukum nasional yang efektif di era globalisasi digital tidak bisa berhenti pada revisi pasal-pasal pidana semata, melainkan mengandaikan rekonstruksi menyeluruh atas cara negara memahami kedaulatan di ruang siber, merancang prosedur pembuktian elektronik, mengelola kerja sama dengan aktor privat global, dan mengintegrasikan peran masyarakat dalam pencegahan serta pelaporan kejahatan siber. Makalah ini kemudian menawarkan serangkaian rekomendasi normatif dan praktis yang mencakup pembaruan kerangka regulasi, penguatan kelembagaan, pengembangan tata kelola multi-pemangku kepentingan, serta peningkatan literasi digital sebagai upaya membangun arsitektur penegakan hukum yang lebih responsif, adaptif, dan berkeadilan di tengah tantangan globalisasi digital.

## PENDAHULUAN

Memasuki era globalisasi digital, hampir seluruh aspek kehidupan manusia mengalami pergeseran fundamental dari pola interaksi yang bersifat fisik menuju ekosistem yang bertumpu pada jaringan komputer, internet, dan platform digital. Aktivitas ekonomi, layanan publik, transaksi keuangan, komunikasi pribadi, hingga proses politik dan demokrasi semakin bergantung pada infrastruktur siber yang tersebar dan saling terhubung lintas batas negara.

Konsekuensinya, kejahatan yang tadinya berlangsung di ruang fisik dengan jejak yang relatif kasatmata, kini bermigrasi ke ruang digital dengan karakter yang lebih cair, anonim, dan sulit dilacak. Kejahatan siber tidak lagi terbatas pada tindakan peretasan sederhana, tetapi mencakup serangan sistematis terhadap lembaga keuangan, pencurian massal data pribadi, sabotase infrastruktur kritis, penipuan berbasis rekayasa sosial, eksploitasi kelemahan sistem informasi pemerintah, serta pemerasan digital melalui malware dan ransomware yang dapat melumpuhkan organisasi dalam hitungan jam.

Dalam lanskap ini, hukum nasional yang disusun untuk menghadapi kejahatan konvensional mendapati dirinya berada dalam posisi tertinggal, bukan saja karena kekurangan norma substantif, tetapi juga karena keterbatasan prosedural dan teknis dalam mengakomodasi karakteristik unik kejahatan siber.

Lebih jauh, globalisasi digital mengaburkan batas-batas kedaulatan yang selama ini menjadi fondasi konseptual bagi sistem hukum pidana nasional. Asas teritorial, yang selama ini menempatkan locus delicti sebagai titik tolak utama penentuan yurisdiksi, menjadi problematis ketika suatu serangan siber dilakukan dari satu negara, memanfaatkan server di negara lain, menargetkan korban di berbagai yurisdiksi, dan menimbulkan kerugian ekonomi maupun sosial yang tersebar secara global.

Dalam situasi demikian, pertanyaan mengenai negara mana yang berwenang

menyidik, menuntut, dan mengadili, serta standar apa yang digunakan untuk menetapkan yurisdiksi, menjadi persoalan krusial yang tidak selalu memiliki jawaban sederhana. Di sisi lain, mekanisme kerja sama internasional yang tersedia, seperti ekstradisi dan bantuan hukum timbal-balik, sering kali dirancang untuk jenis kejahatan tradisional dan prosedur yang membutuhkan waktu panjang, sehingga tidak sejalan dengan kebutuhan penanganan kejahatan siber yang menuntut kecepatan dan kelincahan dalam mengamankan barang bukti elektronik yang mudah hilang atau dimanipulasi.

Dalam konteks ini, penegakan hukum nasional berada di persimpangan antara tuntutan untuk melindungi warga negara dan kepentingan nasional dari ancaman siber global, dengan kewajiban untuk menghormati kedaulatan negara lain, prinsip non-intervensi, serta standar internasional mengenai hak asasi manusia dan perlindungan data pribadi.

Setiap tindakan untuk memperluas kewenangan penegakan hukum di ruang digital berpotensi menimbulkan ketegangan baru: di satu sisi dianggap perlu untuk menjamin keamanan dan ketertiban, di sisi lain dikhawatirkan mengarah pada praktik pengawasan berlebihan dan pelanggaran privasi. Oleh karena itu, penelitian mengenai strategi penegakan hukum di era globalisasi digital menjadi sangat relevan, bukan hanya dari sudut pandang teknis penanggulangan kejahatan, tetapi juga dari perspektif teori hukum, filsafat kedaulatan, dan etika penggunaan kekuasaan negara di ruang siber.

Urgensi penelitian ini dapat ditelusuri dari fakta bahwa kebergantungan negara dan masyarakat terhadap infrastruktur digital tidak diikuti secara seimbang oleh kemampuan sistem hukum untuk mengatur, mengendalikan, dan melindungi ruang digital tersebut secara efektif.

Di satu sisi, negara mendorong digitalisasi layanan publik, transaksi keuangan, dan ekosistem ekonomi berbasis platform sebagai strategi untuk meningkatkan efisiensi, daya saing, dan inklusi; di sisi lain, sistem hukum baik pada tingkat legislasi, kelembagaan, maupun budaya penegakan belum sepenuhnya siap menghadapi konsekuensi negatif berupa meningkatnya kerentanan terhadap kejahatan siber lintas batas. Ketidakseimbangan ini menciptakan "defisit perlindungan hukum" bagi warga negara, di mana individu dan entitas bisnis menanggung risiko yang tinggi atas kebocoran data, penipuan siber, serta serangan terhadap sistem informasi, sementara mekanisme penegakan hukum sering kali tidak mampu memberikan respon yang cepat, pasti, dan memberikan efek jera. Dalam jangka panjang, defisit semacam ini berpotensi melemahkan kepercayaan publik terhadap negara dan hukum, serta mendorong tumbuhnya budaya ketidakpedulian atau skeptisisme terhadap prosedur hukum formal.

Selain itu, urgensi penelitian ini juga terkait dengan kebutuhan mendesak untuk merumuskan kerangka kebijakan kriminal jangka panjang yang konsisten dan adaptif terhadap perubahan teknologi. Tanpa analisis yang mendalam mengenai kelemahan

struktural dan substantif sistem hukum nasional dalam menghadapi kejahatan siber global, reformasi hukum yang dilakukan berisiko bersifat reaktif, parsial, dan fragmentaris, sekadar menjawab kasus-kasus tertentu tanpa membangun fondasi yang kokoh untuk menghadapi tantangan yang akan datang. Padahal, globalisasi digital bersifat dinamis dan evolutif; setiap inovasi teknologi baru seperti kecerdasan buatan, komputasi awan generasi berikutnya, internet of things, dan teknologi blockchain selalu membuka peluang baru bagi pelaku kejahatan untuk mengeksploitasi celah keamanan, memodifikasi modus operandi, dan mengakali mekanisme kontrol yang sudah ada.

Tanpa kerangka kebijakan hukum yang sistematis dan visioner, negara akan terus berada dalam posisi "pemadam kebakaran" yang selalu tertinggal satu langkah, sekadar merespon kerusakan yang sudah terjadi tanpa mampu mencegah atau memitigasi risiko secara struktural. Inilah alasan mengapa penelitian yang berfokus pada pemetaan tantangan penegakan hukum dan perumusan strategi nasional menghadapi kejahatan siber lintas batas menjadi begitu penting secara teoritis maupun praktis.

Berdasarkan latar belakang dan urgensi yang telah dikemukakan, maka pokok persoalan yang hendak dijawab dalam makalah ini dapat dirumuskan secara terarah agar pembahasan tetap fokus dan tidak melebar.

Pertama, bagaimana karakteristik kejahatan siber lintas batas dalam konteks globalisasi digital menantang paradigma tradisional penegakan hukum nasional, khususnya yang berlandaskan pada asas teritorialitas, personalitas, dan perlindungan kepentingan nasional, serta kelemahan apa saja yang tersingkap pada tingkat substansi hukum, struktur kelembagaan penegak hukum, dan kultur hukum dalam merespon bentuk-bentuk kejahatan baru tersebut.

Kedua, bagaimana strategi penegakan hukum nasional yang komprehensif, adaptif, dan berorientasi ke depan dapat dirancang untuk menjawab tantangan kejahatan lintas batas di ruang digital yang tidak mengenal yurisdiksi tradisional, dengan memadukan pembaruan regulasi, penguatan kapasitas institusional dan teknologi, serta pengembangan mekanisme kerja sama internasional dan tata kelola multi-pemangku kepentingan yang sejalan dengan prinsip negara hukum dan penghormatan terhadap hak asasi manusia.

## METODE

Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu pendekatan penelitian hukum yang bertumpu pada studi terhadap norma-norma hukum positif, asas-asas hukum, dan doktrin-doktrin yang berkembang dalam ilmu hukum, bukan pada pengumpulan data empiris di lapangan. Dalam kerangka yuridis normatif, objek kajian utama adalah sistem norma yang mengatur penegakan hukum dan kejahatan siber, baik yang terdapat dalam peraturan perundang-undangan nasional, instrumen hukum

internasional, maupun kebijakan-kebijakan yang terkait dengan tata kelola ruang digital. Penelitian ini memandang hukum sebagai kaidah atau "law in books" yang perlu dibaca secara sistematis, dikonstruksi, dan dievaluasi kesesuaiannya dengan perkembangan fenomena globalisasi digital serta kebutuhan penanggulangan kejahatan siber lintas batas. Dengan demikian, analisis yang dilakukan berfokus pada bagaimana sistem norma dirancang, bagaimana hubungan hierarkis dan horizontal antaraturan, serta sejauh mana norma-norma tersebut memadai atau justru menyisakan kekosongan dan disharmoni dalam menghadapi dinamika kejahatan siber.

Dalam pelaksanaannya, penelitian yuridis normatif ini menggunakan beberapa pendekatan (*approach*) sekaligus yang saling melengkapi. Pertama, pendekatan perundang-undangan (*statute approach*), yakni dengan mengkaji secara mendalam peraturan perundang-undangan yang relevan dengan penegakan hukum di ruang siber, baik yang bersifat umum (misalnya ketentuan hukum pidana dan hukum acara pidana) maupun yang bersifat khusus yang mengatur teknologi informasi, perlindungan data, dan keamanan siber. Kedua, pendekatan konseptual (*conceptual approach*), dengan menelusuri dan mengkritisi konsep-konsep kunci seperti kedaulatan siber, yurisdiksi lintas batas, locus dan tempus delicti dalam konteks digital, due process of law, serta tanggung jawab pidana korporasi, untuk kemudian disistematisasi dan dihubungkan dengan realitas globalisasi digital. Ketiga, apabila diperlukan, digunakan pendekatan komparatif (*comparative approach*) dengan cara membandingkan pengaturan dan kebijakan penegakan hukum siber di beberapa negara atau rezim internasional, guna memperoleh gambaran praktik baik (*best practices*) dan celah kelemahan yang bisa menjadi bahan rekomendasi bagi perbaikan sistem hukum nasional.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan, instrumen hukum internasional, serta putusan-putusan pengadilan yang relevan dengan isu penegakan hukum terhadap kejahatan siber dan kerja sama lintas negara. Bahan hukum sekunder berupa literatur ilmiah, buku teks, artikel jurnal, laporan kebijakan, dan pendapat para ahli yang memberikan penjelasan, kritik, maupun interpretasi terhadap bahan hukum primer. Bahan hukum tersier mencakup kamus hukum, ensiklopedia, dan sumber penunjang lain yang membantu menjelaskan istilah teknis atau memberikan konteks tambahan terhadap konsep yang digunakan. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), dengan menelusuri, menginventarisasi, dan mengklasifikasikan bahan hukum berdasarkan tema-tema utama penelitian, seperti pengaturan *cybercrime*, yurisdiksi lintas batas, mekanisme mutual legal assistance, dan perlindungan hak asasi manusia di ruang digital.

Analisis terhadap bahan hukum dilakukan secara kualitatif normatif, yaitu dengan menafsirkan dan menilai norma-norma hukum melalui teknik penafsiran gramatikal,

sistematis, historis, dan teleologis, serta mengaitkannya dengan kerangka teori kebijakan kriminal dan teori penegakan hukum. Hasil interpretasi tersebut kemudian disusun secara logis dan argumentatif untuk menggambarkan struktur kelemahan sistem hukum nasional dalam menghadapi kejahatan siber global, sekaligus merumuskan alternatif solusi normatif dan institusional yang lebih adaptif. Dengan pendekatan ini, penelitian diharapkan tidak hanya menghasilkan deskripsi mengenai kondisi pengaturan yang ada, tetapi juga memberikan analisis kritis dan rekomendasi preskriptif mengenai bagaimana sistem hukum nasional seharusnya dikembangkan agar mampu merespons tantangan penegakan hukum di era globalisasi digital secara lebih efektif, konsisten, dan berkeadilan.

## HASIL DAN PEMBAHASAN

Dalam rangka menjawab rumusan masalah pertama, perlu dipahami bahwa kejahatan siber lintas batas memiliki karakteristik yang secara fundamental berbeda dari kejahatan konvensional, karena bertumpu pada logika jaringan (*network logic*) dan arsitektur sistem informasi yang terdistribusi. Pelaku kejahatan siber dapat memanfaatkan serangkaian teknik seperti anonymization, enkripsi berlapis, penggunaan server proxy di berbagai negara, pemanfaatan jaringan botnet, serta pembayaran melalui mata uang kripto untuk memutus hubungan langsung antara tindakan kriminal dan identitas nyata pelaku. Lebih rumit lagi, alur kejahatan dapat disusun sedemikian rupa sehingga melibatkan sejumlah yurisdiksi: perencanaan serangan di satu negara, penyebaran malware dari server di negara lain, infeksi sistem korban di berbagai negara berbeda, serta pencucian hasil kejahatan melalui platform keuangan digital global.

Dalam konfigurasi ini, perumusan locus delicti tidak lagi sesederhana menentukan tempat di mana perbuatan dilakukan atau akibat dirasakan, karena seluruh rangkaian peristiwa terjadi secara simultan dalam ruang siber yang lintas batas. Konsekuensinya, ketika hukum pidana nasional tetap bertumpu pada konsep negara-bangsa dengan batas geografis yang tegas, ia menghadapi kesulitan mendasar untuk mengklaim yurisdiksi dan menegakkan sanksi terhadap pelaku yang beroperasi di luar wilayah kedaulatannya.

Selanjutnya, pada tingkat substansi hukum, banyak sistem hukum nasional yang pada awalnya dirancang untuk mengatur kejahatan konvensional harus melakukan penyesuaian signifikan agar mampu mengkriminalkan perilaku baru di ruang digital. Tantangannya tidak hanya terletak pada menambahkan jenis tindak pidana baru ke dalam undang-undang, tetapi juga pada mendefinisikan unsur-unsur delik secara tepat agar tidak terlalu sempit sehingga banyak perbuatan berbahaya yang lolos, maupun terlalu luas sehingga berpotensi mengkriminalisasi perilaku sah yang dilindungi oleh hak-hak dasar, seperti kebebasan berekspresi dan hak atas privasi. Di samping itu, hukum acara pidana juga harus mengakomodasi kebutuhan teknis dalam proses pengumpulan dan

pengamanan barang bukti elektronik, yang pada dasarnya merupakan data yang mudah berubah, dapat direplikasi, dipalsukan, atau dimusnahkan dengan cepat, serta sering kali berada dalam penguasaan pihak ketiga di negara lain. Ketiadaan pengaturan yang rinci mengenai prosedur penyitaan data, penggeledahan sistem komputer, dan pemeliharaan integritas bukti digital mengakibatkan lemahnya posisi penegak hukum ketika berhadapan dengan pembelaan di pengadilan, terutama terkait keabsahan dan kekuatan pembuktian alat bukti elektronik.

Pada dimensi struktur kelembagaan, kelemahan sistem hukum nasional dalam menghadapi kejahatan siber global tampak dari belum meratanya kapasitas aparat penegak hukum untuk memahami secara teknis cara kerja sistem jaringan, teknik forensik digital, dan metodologi analisis data yang diperlukan untuk melacak jejak kejahatan di ruang siber. Aparat penegak hukum yang selama ini terbiasa menangani kejahatan konvensional, seperti pencurian fisik atau penganiayaan, kini dituntut untuk memahami log file, header email, hash nilai file, rekonstruksi paket data, dan berbagai aspek teknis lain yang menjadi kunci bagi pembuktian tindak pidana siber.

Tanpa pelatihan yang intensif dan dukungan infrastruktur laboratorium forensik digital yang memadai, penegak hukum terancam hanya menjadi "penonton" di tengah meningkatnya kompleksitas serangan siber, bergantung pada bantuan teknis pihak luar, dan sulit mengambil inisiatif dalam investigasi lintas batas. Keterbatasan ini kemudian diperparah oleh minimnya koordinasi antar lembaga penegak hukum, misalnya antara kepolisian, kejaksaan, otoritas perlindungan data, dan lembaga pengawas sektor tertentu, sehingga respons terhadap sebuah insiden siber sering kali berjalan terpisah-pisah, tidak sinkron, dan menimbulkan kebingungan mengenai siapa yang memegang mandat utama penanganan.

Tidak kalah penting adalah dimensi kultur hukum, yaitu bagaimana pola pikir, sikap, dan kebiasaan aparat penegak hukum, pembuat kebijakan, dan hakim dalam memandang ruang digital dan alat bukti elektronik.

Di banyak yurisdiksi, masih terdapat kecenderungan untuk menganggap kejahatan siber sebagai "kejahatan kelas dua" atau sekadar perpanjangan dari penipuan konvensional, sehingga tidak mendapat prioritas yang sebanding dengan dampak yang ditimbulkannya terhadap stabilitas ekonomi, keamanan nasional, dan hak-hak warga negara. Di tingkat pengadilan, sebagian hakim mungkin belum sepenuhnya familiar dengan terminologi teknis dan metodologi forensik digital, sehingga menimbulkan keraguan terhadap keabsahan alat bukti atau memberikan bobot pembuktian yang tidak proporsional. Kultur hukum yang belum sepenuhnya "melek digital" ini menyebabkan implementasi norma-norma yang sudah relatif maju di atas kertas tidak diterjemahkan secara optimal dalam praktik penegakan hukum, dan pada gilirannya menurunkan efek jera yang diharapkan dari suatu rezim hukum pidana siber.

Menjawab rumusan masalah kedua, strategi penegakan hukum nasional yang adaptif terhadap globalisasi digital harus dirancang secara komprehensif dengan memadukan pembaruan regulasi, penguatan kelembagaan, dan rekayasa mekanisme kerja sama internasional. Pada tataran regulasi, negara perlu menyusun kerangka hukum cybercrime yang tidak hanya mencantumkan jenis-jenis tindak pidana siber, tetapi juga mengatur dengan rinci aspek yurisdiksi, tanggung jawab pidana korporasi, prosedur penyitaan dan penggeledahan sistem elektronik, standar integritas barang bukti digital, serta perlindungan hak-hak subjek data. Regulasi tersebut idealnya diselaraskan dengan prinsip-prinsip dan praktik baik internasional, untuk memudahkan kerja sama lintas negara dalam konteks ekstradisi, bantuan hukum timbal-balik, dan pengakuan timbal-balik terhadap alat bukti elektronik. Selain itu, pembaruan hukum acara pidana harus mencakup pengaturan mengenai teknik investigasi khusus di ruang siber, seperti pemeliharaan data secara cepat, pengumpulan real-time traffic data, ataupun akses jarak jauh yang dalam kondisi tertentu dapat digunakan dengan pengawasan ketat dan jaminan akuntabilitas.

Pada tingkat kelembagaan, strategi nasional perlu mencakup pembentukan atau penguatan unit-unit khusus penanganan kejahatan siber di tubuh kepolisian dan kejaksaan, yang dilengkapi dengan sumber daya manusia yang terlatih secara teknis dan integritas profesional yang tinggi. Laboratorium forensik digital harus dikembangkan dengan standar yang dapat dipertanggungjawabkan, baik dari sisi metodologi analisis, keamanan data, maupun akreditasi, sehingga hasil pemeriksaan dapat diterima di pengadilan tanpa menimbulkan sengketa atas keandalannya.

Di samping itu, mekanisme koordinasi antar lembaga penegak hukum perlu dirancang ulang, misalnya melalui pembentukan pusat komando insiden siber nasional yang berfungsi sebagai simpul koordinasi ketika terjadi serangan besar, sehingga respons yang diambil tidak terfragmentasi dan dapat mempertimbangkan dimensi hukum, teknis, serta kebijakan publik secara bersamaan.

Strategi penegakan hukum nasional di era globalisasi digital juga tidak bisa dilepaskan dari kerja sama dengan aktor privat, terutama perusahaan penyedia layanan internet, platform media sosial, penyedia layanan komputasi awan, dan operator infrastruktur digital lainnya. Banyak barang bukti penting dalam perkara kejahatan siber justru berada dalam penguasaan sektor privat, baik berupa log akses, metadata komunikasi, maupun data pelanggan yang disimpan di pusat data tertentu. Oleh karena itu, negara perlu mengembangkan kerangka hukum yang jelas dan seimbang mengenai kewajiban penyedia layanan untuk menyimpan data tertentu selama jangka waktu tertentu, prosedur penyerahan data kepada aparat penegak hukum, serta mekanisme pengawasan dan akuntabilitas atas penggunaan kewenangan tersebut agar tidak menimbulkan praktik penyalahgunaan dan pelanggaran privasi.

Dalam konteks enkripsi, dibutuhkan dialog berkesinambungan antara penegak hukum dan perusahaan teknologi untuk mencari titik temu antara kebutuhan investigasi dan kewajiban melindungi keamanan serta kerahasiaan komunikasi pengguna, tanpa jatuh pada solusi sederhana yang justru melemahkan keamanan keseluruhan ekosistem digital.

Akhirnya, strategi nasional yang efektif harus menempatkan masyarakat sebagai bagian integral dari penegakan hukum di ruang digital. Masyarakat yang memiliki literasi digital rendah cenderung menjadi korban empuk kejahatan siber, baik dalam bentuk penipuan, phishing, maupun eksploitasi data pribadi, dan pada saat yang sama enggan melaporkan insiden yang dialaminya karena ketidaktahuan, rasa malu, atau ketidakpercayaan terhadap aparat penegak hukum.

Oleh karena itu, program pendidikan publik mengenai keamanan siber, etika berinternet, dan hak-hak hukum korban kejahatan siber perlu menjadi bagian dari kebijakan kriminal preventif. Dengan meningkatkan kesadaran dan kapasitas masyarakat dalam mengenali, mencegah, dan melaporkan kejahatan siber, negara tidak hanya memperkuat daya tangkal kolektif terhadap ancaman siber, tetapi juga memperluas basis informasi yang dapat dimanfaatkan oleh aparat penegak hukum dalam mendeteksi pola serangan, mengidentifikasi pelaku, dan memitigasi dampak kejahatan secara lebih dini.

## SIMPULAN, KETERBATASAN DAN SARAN

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan bahwa tantangan penegakan hukum di era globalisasi digital memiliki dimensi yang jauh melampaui persoalan teknis mengenai kemampuan melacak pelaku kejahatan di dunia maya. Pada tingkat konseptual, globalisasi digital mengguncang fondasi paradigma klasik penegakan hukum yang bertumpu pada kedaulatan teritorial dan batas geografis negara, karena kejahatan siber lintas batas beroperasi di ruang yang tidak mengenal sekat fisik dan memanfaatkan struktur jaringan global yang kompleks. Pada tingkat normatif, sistem hukum nasional menghadapi pekerjaan besar untuk menyesuaikan substansi hukum pidana dan acara pidana dengan karakteristik kejahatan di ruang digital, sekaligus menghindari jebakan overcriminalization dan pelanggaran hak asasi manusia. Pada tingkat kelembagaan, negara harus berhadapan dengan tuntutan untuk membangun kapasitas teknis forensik digital, meningkatkan koordinasi antar lembaga penegak hukum, dan memperkuat mekanisme kerja sama internasional yang selama ini cenderung lamban dan birokratis. Pada tingkat kultur hukum, penegak hukum dan hakim perlu mengembangkan perspektif baru yang lebih akrab dengan teknologi, sehingga mampu menilai dan memanfaatkan alat bukti elektronik secara tepat dan adil.

Dengan demikian, strategi penegakan hukum nasional yang efektif di era globalisasi digital harus dipahami sebagai kebijakan yang bersifat multidimensi dan

berlapis, tidak cukup hanya dengan menambahkan pasal-pasal baru tentang cybercrime ke dalam undang-undang, tetapi menuntut rekonstruksi menyeluruh atas cara negara mengelola ruang digital sebagai domain baru kehidupan sosial yang membutuhkan regulasi, perlindungan, dan penegakan hukum. Strategi tersebut harus mengintegrasikan pembaruan regulasi, penguatan kelembagaan, kerja sama internasional, kemitraan dengan sektor privat, dan partisipasi masyarakat melalui peningkatan literasi digital, sehingga penegakan hukum tidak hanya muncul sebagai respons represif terhadap kejahatan yang sudah terjadi, melainkan sebagai bagian dari desain tata kelola digital yang menjamin keamanan, keadilan, dan penghormatan terhadap hak-hak dasar individu di tengah arus globalisasi siber yang tak terelakkan.

**Saran dan Rekomendasi**

Sebagai tindak lanjut konseptual dan praktis dari kesimpulan tersebut, beberapa saran dan rekomendasi kebijakan dapat diajukan.

Pertama, negara perlu melakukan revisi komprehensif terhadap kerangka regulasi yang mengatur kejahatan siber dan penegakan hukum di ruang digital, dengan memastikan bahwa definisi tindak pidana, unsur-unsur delik, dan sanksi pidana dirumuskan secara jelas, proporsional, dan selaras dengan prinsip negara hukum dan hak asasi manusia. Revisi tersebut hendaknya mencakup pengaturan rinci mengenai yurisdiksi dalam kasus kejahatan lintas batas, tanggung jawab pidana korporasi terhadap pengelolaan sistem informasi dan data pribadi, serta prosedur pengumpulan, penyitaan, dan penyajian barang bukti elektronik di pengadilan.

Kedua, pemerintah perlu menyusun sebuah strategi nasional penegakan hukum siber yang terintegrasi, yang bukan hanya berupa dokumen kebijakan formal, tetapi benar-benar diposisikan sebagai rujukan utama bagi seluruh lembaga penegak hukum dan pemangku kepentingan lain dalam merespons insiden siber, lengkap dengan pembagian peran, mekanisme koordinasi, standar operasional prosedur, serta indikator kinerja yang dapat diukur secara periodik.

Ketiga, dalam ranah kelembagaan, disarankan agar negara meningkatkan investasi pada pengembangan kapasitas teknis aparat penegak hukum melalui program pelatihan berkelanjutan, rekrutmen tenaga ahli di bidang teknologi informasi dan forensik digital, serta pengadaan infrastruktur laboratorium forensik yang memenuhi standar profesional. Peningkatan kapasitas tersebut perlu diiringi dengan pembangunan kultur organisasi yang adaptif terhadap perubahan teknologi, sehingga aparat penegak hukum didorong untuk terus belajar dan berinovasi, bukan sekadar menerapkan prosedur lama pada masalah baru.

Keempat, negara hendaknya memperkuat dan memperluas kerja sama internasional dalam penanganan kejahatan siber melalui partisipasi aktif dalam forum regional dan

global, penyusunan perjanjian bilateral dan multilateral yang memudahkan pertukaran informasi dan data elektronik, serta pengembangan mekanisme bantuan hukum timbal balik yang lebih cepat dan efisien, tanpa mengabaikan prinsip kedaulatan dan perlindungan hak-hak individu.

Kelima, diperlukan kerangka tata kelola multi-pemangku kepentingan yang jelas dan terukur, yang mempertemukan peran negara, sektor privat, komunitas profesional keamanan siber, akademisi, dan masyarakat sipil dalam merumuskan standar teknis, kode etik, serta praktik terbaik untuk menjaga keamanan dan integritas ruang digital.

Keenam, di tingkat masyarakat, pemerintah perlu merancang program peningkatan literasi digital secara sistematis melalui kurikulum pendidikan formal, pelatihan bagi kelompok rentan, dan kampanye publik yang berkelanjutan, sehingga warga negara memiliki keterampilan dasar untuk melindungi diri dari ancaman siber, memahami hak-haknya terkait perlindungan data pribadi, serta mengetahui saluran pelaporan dan mekanisme bantuan jika menjadi korban kejahatan siber.

Ketujuh, perlu dikembangkan mekanisme pemulihan yang lebih sensitif terhadap kebutuhan korban, baik dalam bentuk layanan bantuan hukum, dukungan psikologis, maupun mekanisme kompensasi dan pemulihan data, agar penegakan hukum tidak berhenti pada pemidanaan pelaku, tetapi juga memastikan pemulihan kondisi korban dan pemulihan kepercayaan terhadap sistem hukum. Dengan mengimplementasikan seluruh rekomendasi ini secara konsisten dan berkesinambungan, diharapkan negara mampu membangun arsitektur penegakan hukum yang kokoh dan adaptif di tengah derasnya arus globalisasi digital, menjadikan ruang siber bukan sebagai arena tanpa hukum, melainkan sebagai bagian integral dari ruang kehidupan yang berada di bawah naungan keadilan dan perlindungan hukum yang efektif.

## DAFTAR PUSTAKA

Alfi, Muhammad, Ni Putu Yundari, and Ahnaf Tsaqif. "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 2 (2023): 5.

Cahyono, Soetardi Tri, Wina Erni, and Taufik Hidayat. "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (2025): 1-23.

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun. "Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis." *Jurnal Konstituen* 5, no. 1 (2023): 1-17.

Hasan, Zainudin, Wiryadi Wiryadi, Arkaan Fadhulrrahman, Muhammad Dimas, dan

Ronald Dzaky Al Jabbar. "Regulasi Penggunaan Teknologi Blockchain Dan Mata Uang Kripto Sebagai Tantangan Di Masa Depan Dalam Hukum Siber." *Birokrasi: Jurnal Ilmu Hukum Dan Tata Negara* 2, no. 2 (2024): 55-69.

Mardiyati, Siti. "Implementasi dan Penegakan Hukum Tata Negara dalam Konteks Globalisasi." *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum Sumpah Pemuda* 30, no. 3 (2024): 79-90.

Mustaqimah, Lailatul. "Penerapan Asas Nasionalitas Pasif Terhadap Tindak Pidana Teknologi Informasi." *Badamai Law Journal* 1, no. 2 (2016): 322-342.

Nasional, Badan Pembinaan Hukum. "Dokumen Pembangunan Hukum Nasional Tahun 2023: Pembangunan Budaya Hukum di Indonesia." (2023).

Nugroho, Dewi Rahmaningsih, and Suteki Suteki. "Membangun Budaya Hukum Persidangan Virtual (Studi Perkembangan Sidang Tindak Pidana via Telekonferensi)." *Jurnal Pembangunan Hukum Indonesia* 2, no. 3 (2020): 291-304.

Pakaya, Rio Dirgantara, and Ahmad Mahyani. "Landasan Perumusan Locus Delicti Dalam Surat Dakwaan Pada Kejahatan Siber." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 1 (2022): 673-686.

Saleh, Indah Nur Shanty, Loso Judijanto, Nurul Widhanita Y. Badilla, Novea Elysa Wardhani, H. Hartawan, and Isnayani Isnayani. *Hukum dan Peradilan di Indonesia:: Kajian Teori dan Praktik Hukum di Indonesia*. PT. Sonpedia Publishing Indonesia, 2025.

Sukmana, Oman, Tri Sulistyaningsih, Fritz Hotman S. Damanik, Fidela Dzatadini Wahyudi, Atma Ras, Fardila Astari, Andi Dody May Putra Agustang et al. *Sosiologi Digital: Transformasi Sosial di Era Teknologi*. Star Digital Publishing,, 2025.

Wibowo, Agus. "Hukum di era globalisasi digital." *Penerbit Yayasan Prima Agus Teknik* (2023): 1-185.

Zaman, Angelina Agung Putri. "Keabsahan Pembuktian Digital Forensik Terhadap Tindak Pidana Pencucian Uang Melalui Mata Uang Virtual (Cryptocurrency)(Studi Komparatif Di Beberapa Negara)." (2025).