Website Justitiable: https://ojs.ejournalunigoro.com/index.php/JUSTITIABLE
Jurnal Justitiable 8 (2), Januari 2026, Pages 114-126
Doi: https://doi.org/10.56071/justitiable.v7i2.1153

Cybercrime dan Tantangan Perlindungan Individu dalam Kerangka Sistem Hukum di Indonesia

La Idul, Dinda Dwi Deninta, Zahra Siti Fatimah, Donny Aliandi, Andreas Andri Muliawan, Nugraha Pranadita
Universitas Langlangbuana
E-mail: laidul69@gmail.com

ABSTRAK

Transformasi ruang siber sebagai ruang sosial dan hukum baru telah meningkatkan ketergantungan masyarakat terhadap teknologi digital sekaligus memperluas risiko kejahatan siber yang menempatkan individu pada posisi rentan. Cybercrime berkembang sebagai fenomena struktural yang diproduksi oleh karakter ruang siber yang terbuka, lintas batas, dan asimetris. Penelitian ini mengkaji bagaimana cybercrime dalam struktur ruang siber meningkatkan kerentanan individu, bagaimana orientasi pengaturan cyber law Indonesia dalam memberikan perlindungan, serta faktor-faktor yang menyebabkan ketidakefektifan perlindungan tersebut. Penelitian ini bertujuan menganalisis kerentanan individu sebagai konsekuensi struktural ruang siber dan mengevaluasi orientasi normatif cyber law dalam sistem hukum Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual, menggunakan bahan hukum primer, sekunder, dan tersier, serta dianalisis secara deskriptif-analitis. Hasil penelitian menunjukkan bahwa cyber law Indonesia masih didominasi pendekatan kriminalisasi dan keamanan negara (state-centric), sehingga perlindungan individu dan pemulihan korban belum menjadi pusat pengaturan. Penelitian ini merekomendasikan reorientasi cyber law menuju pendekatan perlindungan subjek hukum yang lebih protektif, adaptif, dan responsif terhadap dinamika ruang siber.

Kata kunci: cybercrime; perlindungan individu; cyber law

ABSTRACK

The transformation of cyberspace into a new social and legal sphere has intensified society's reliance on digital technology while simultaneously expanding the risks of cybercrime that place individuals in vulnerable positions. Cybercrime has evolved into a structural phenomenon shaped by the open, borderless, and asymmetrical nature of cyberspace. This study examines how cybercrime within the structure of cyberspace increases individual vulnerability, how Indonesian cyber law is oriented toward individual protection, and why such protection remains ineffective. This research aims to analyze individual vulnerability as a structural consequence of cyberspace and to evaluate the normative orientation of cyber law within Indonesia's legal system. This study employs a normative juridical method with statutory and conceptual approaches, utilizing primary, secondary, and tertiary legal materials analyzed through descriptive-analytical techniques. The findings indicate that Indonesian cyber law remains predominantly state-centric and offender-oriented, causing individual protection and victim recovery to remain peripheral. This study recommends reorienting cyber law toward a subject-centered protection approach that is more protective, adaptive, and responsive to the dynamics of cyberspace.

Keywords: *cybercrime; individual protection; cyber law*

Website Justitiable: https://ojs.ejournalunigoro.com/index.php/JUSTITIABLE
Jurnal Justitiable 8 (2), Januari 2026, Pages 114-126
Doi: https://doi.org/10.56071/justitiable.v7i2.1153

Pendahuluan

Perkembangan ruang siber sebagai ruang sosial dan hukum baru tidak dapat dilepaskan dari proses panjang transformasi teknologi yang berakar pada revolusi industri. Revolusi industri menandai peralihan mendasar dari penggunaan tenaga manusia menuju penggunaan mesin dalam proses produksi, yang tidak hanya mengubah cara kerja manusia, tetapi juga membentuk ulang struktur sosial, ekonomi, dan politik masyarakat (Ardyawati et al. 2025). Perkembangan revolusi industri lanjutan yang ditandai oleh kemajuan teknologi informasi dan komunikasi melahirkan ruang interaksi baru yang dikenal sebagai ruang siber *(cyberspace),* di mana relasi manusia tidak lagi terbatas pada ruang fisik, tetapi dimediasi oleh jaringan digital yang bersifat global, cepat, dan tanpa batas teritorial.

Ekspansi ruang siber ditopang oleh pertumbuhan signifikan jumlah pengguna Internet secara global. Laporan ITU mencatat bahwa pada tahun 2025 sekitar 6 miliar orang telah terhubung ke Internet. Di Indonesia, tingkat penetrasi internet mencapai 229.428.417 jiwa atau 80,66% dari total populasi, menunjukkan bahwa ruang siber telah menjadi medium utama dalam penyelenggaraan layanan publik, transaksi ekonomi digital, dan pembentukan relasi sosial sehari-hari (Amelia 2024).

Tingginya penetrasi internet berimplikasi langsung pada meningkatnya eksposur individu terhadap risiko kejahatan siber *(cybercrime). Cybercrime* tidak lagi terbatas pada serangan terhadap sistem teknologi, tetapi semakin menargetkan individu sebagai korban langsung melalui penipuan daring, pencurian data pribadi, peretasan akun digital, hingga kejahatan berbasis manipulasi psikologis. Dalam konteks sistem peradilan pidana siber Indonesia, posisi korban cybercrime mengalami ambivalensi problematis (Salim and Hakim 2024). Meskipun korban diakui secara normatif, dalam praktik penegakan hukum korban lebih diposisikan sebagai objek perkara ketimbang subjek aktif yang memiliki hak-hak prosedural memadai. Pengaturan dalam UU ITE dan KUHP baru masih bersifat *state-centric,* menempatkan kepentingan penegakan hukum dan stabilitas sistem sebagai prioritas utama, sementara kepentingan pemulihan korban berada di posisi sekunder.

Hak-hak korban dalam sistem peradilan pidana siber Indonesia masih sangat terbatas. UU ITE maupun KUHP baru belum secara eksplisit mengatur mekanisme restitusi otomatis, kompensasi langsung, atau perlindungan khusus bagi korban cybercrime. Kondisi ini menunjukkan bahwa perlindungan hukum tidak dapat disamakan dengan kriminalisasi pelaku semata. Perlindungan individu dalam cybercrime harus dipahami sebagai upaya sistemik yang mencakup aspek protektif (pencegahan), responsif (penanganan cepat), dan restoratif (pemulihan korban) yang menempatkan korban sebagai subjek aktif dengan hak-hak yang dijamin secara prosedural dan substantif (Khaidir, Kurnia, and Erawaty 2025).

Indonesia telah mengembangkan kerangka regulasi siber yang relatif komprehensif melalui UU Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE, KUHP baru, Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional, dan Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber (Ganjar 2025). Namun pendekatan pertahanan yang dominan menegaskan bahwa kebijakan siber Indonesia masih kuat dalam perspektif state-centric, sehingga individu sebagai korban langsung cybercrime berpotensi terpinggirkan.

Keberadaan berbagai regulasi tersebut menunjukkan bahwa persoalan perlindungan individu bukan terletak pada ketiadaan regulasi, melainkan pada orientasi dan efektivitas pengaturannya. Fragmentasi regulasi, dominasi pendekatan kriminalisasi dan keamanan negara, serta lemahnya fokus pada pemulihan korban memperlihatkan kesenjangan antara kerangka normatif cyber law dan realitas perlindungan individu di ruang siber. Penelitian ini mengkaji: (1) bagaimana *cybercrime* dalam struktur ruang siber meningkatkan kerentanan individu; (2) bagaimana orientasi pengaturan cyber law dalam melindungi individu dari cybercrime; dan (3) mengapa cyber law belum efektif dalam merespons krisis perlindungan individu di ruang siber.

Metode Penelitian

Penelitian ini merupakan penelitian yuridis normatif, yang berfokus pada pengkajian norma hukum positif terkait kejahatan siber dan perlindungan individu dalam kerangka sistem hukum Indonesia. Pendekatan normatif dipilih karena tujuan utama penelitian ini bukan untuk mengukur frekuensi atau pola empiris cybercrime, melainkan untuk menelaah orientasi, konstruksi, dan efektivitas pengaturan hukum *(cyber law)* dalam merespons kerentanan individu di ruang siber (Wiraguna 2024).

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan *(statute approach)* dan pendekatan konseptual *(conceptual approach)*. Pendekatan perundang-undangan dilakukan dengan menelaah secara sistematis berbagai regulasi yang berkaitan langsung maupun tidak langsung dengan kejahatan siber dan perlindungan individu, antara lain Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Kitab Undang-Undang Hukum Pidana baru, Undang-Undang Perlindungan Data Pribadi, serta kebijakan strategis dan peraturan pelaksana di bidang keamanan siber. Melalui pendekatan ini, penelitian menilai koherensi, konsistensi, dan orientasi normatif regulasi cyber law dalam sistem hukum nasional.

Hasil dan Pembahasan

A. Cybercrime sebagai Fenomena Struktural Ruang Siber

Ruang siber merupakan hasil evolusi historis dari Revolusi Industri ketiga *(digital revolution)* dan Revolusi Industri keempat (Industry 4.0), ketika teknologi komputasi, otomasi, dan jaringan telekomunikasi terintegrasi membentuk suatu medium interaksi global yang tidak lagi bergantung pada batas geografis dan ruang fisik (L. Hadi Adha, Zaeni Asyhadie 2020). Revolusi Industri ketiga ditandai oleh digitalisasi melalui penemuan transistor, sirkuit terpadu, dan mikroprosesor yang memungkinkan komputasi personal dan otomasi berbasis elektronik. Sementara itu, Revolusi Industri keempat memperluas transformasi tersebut melalui integrasi *artificial intelligence* (AI), big data, Internet of Things (IoT), komputasi awan (cloud computing), dan sistem siber-fisik yang semakin mengaburkan batas antara dunia fisik dan digital. Secara historis, pengembangan ARPANET pada akhir 1960-an

menjadi tonggak lahirnya internet modern, yang kemudian berevolusi menjadi infrastruktur komunikasi global berbasis protokol TCP/IP. Infrastruktur ini menciptakan ruang interaksi baru ruang siber yang bersifat terbuka, terdistribusi, dan lintas yurisdiksi (Salsabila 2024). Tidak seperti ruang fisik yang tunduk pada kedaulatan teritorial negara, ruang siber beroperasi melalui arsitektur jaringan global yang memungkinkan komunikasi dan pertukaran data berlangsung secara instan tanpa batas negara.

Karakter ruang siber yang terbuka, anonim, dan tidak berbatas tersebut secara struktural menciptakan peluang sekaligus risiko. Di satu sisi, ia mendorong pertumbuhan ekonomi digital, inovasi, dan partisipasi sosial (Mahu 2014). Di sisi lain, karakter tersebut menyediakan kondisi kriminogenik bagi berkembangnya cybercrime. Kongres PBB X Tahun 2000 mendefinisikan cybercrime dalam arti sempit sebagai perbuatan melawan hukum yang menyerang keamanan sistem komputer dan data *(computer-related crime),* serta dalam arti luas sebagai segala bentuk perbuatan ilegal yang dilakukan melalui atau dengan bantuan sistem komputer dan jaringan. Definisi ini menunjukkan perluasan spektrum kejahatan dari sekadar serangan terhadap sistem menjadi penggunaan sistem digital sebagai instrumen kejahatan (Amalia and Atman 2025).

Goodman dan Brenner mengklasifikasikan cybercrime ke dalam dua kategori besar (Ayubi 2025): (1) komputer sebagai target (computer as a target), seperti peretasan, malware, dan serangan denial-of-service; dan (2) komputer sebagai alat (computer as a tool), yaitu kejahatan konvensional yang bermigrasi ke ruang digital seperti penipuan, pemerasan, distribusi konten ilegal, dan pencucian uang. Perkembangan selanjutnya bahkan menunjukkan bentuk hibrida, di mana teknologi digital tidak hanya menjadi alat, tetapi juga menciptakan jenis kejahatan baru yang sebelumnya tidak dikenal dalam hukum konvensional. Sifat global internet menjadikan cybercrime sebagai kejahatan transnasional yang kompleks. Pelaku, korban, server, dan dampak kejahatan dapat berada di yurisdiksi yang berbeda, sehingga menimbulkan persoalan konflik hukum, ekstradisi, pembuktian elektronik, dan kerja sama internasional. Mekanisme penegakan hukum berbasis teritorial menjadi kurang efektif karena ruang siber beroperasi dalam logika jaringan

(network logic) yang tidak mengenal batas negara secara fisik. Selain itu, anonimitas pengguna, penggunaan enkripsi, *cryptocurrency,* serta keberadaan dark web semakin memperkuat posisi pelaku dan menyulitkan identifikasi maupun penuntutan. Kondisi ini menunjukkan adanya ketimpangan struktural antara kemampuan negara dalam mengatur dan kecepatan inovasi teknologi yang dimanfaatkan pelaku kejahatan.

Manifestasi konkret cybercrime menunjukkan eskalasi baik dari sisi kuantitas maupun kualitas dampaknya. Kasus kebocoran data (data breaches) seperti Tokopedia yang melibatkan sekitar 90 juta akun dan BPJS Kesehatan dengan ratusan juta data penduduk memperlihatkan tingginya risiko terhadap perlindungan data pribadi dan keamanan informasi nasional. Serangan ransomware yang mengenkripsi sistem dan menuntut tebusan telah menargetkan institusi pemerintah, rumah sakit, dan sektor strategis lainnya, sehingga berdampak langsung pada layanan publik dan stabilitas ekonomi (Wati et al. 2024). Selain itu, penipuan *daring, phishing, dan social engineering* memanfaatkan kelemahan psikologis dan literasi digital masyarakat. menunjukkan bahwa faktor manusia tetap menjadi titik paling rentan dalam keamanan siber. Serangan terhadap infrastruktur kritis seperti sistem keuangan, energi, transportasi, dan layanan publik menunjukkan bahwa cybercrime tidak lagi sekadar isu kriminalitas individu, melainkan telah berkembang menjadi ancaman terhadap keamanan nasional dan ketahanan negara. Dalam konteks ini, ruang siber menjadi domain strategis yang setara dengan darat, laut, udara, dan luar angkasa.

Kerentanan individu dalam ruang siber merupakan konsekuensi struktural dari desain arsitektur digital yang asimetris. Platform digital dan korporasi teknologi menguasai data dalam skala besar, sementara pengguna sering kali berada pada posisi subordinat dengan keterbatasan kontrol dan pemahaman terhadap pemrosesan data mereka. Ketidakseimbangan informasi (*information asymmetry*), praktik pengumpulan data masif, serta lemahnya literasi digital memperbesar risiko eksploitasi (Mulya, Saputra, and Rahmadzani 2025). Oleh karena itu, diperlukan kerangka perlindungan hukum yang protektif, responsif, dan adaptif terhadap dinamika teknologi. Perlindungan tersebut tidak hanya mencakup kriminalisasi dan

penegakan hukum terhadap pelaku, tetapi juga penguatan rezim perlindungan data pribadi, mekanisme pemulihan korban (*victim redress*), jaminan hak atas privasi, hak atas rasa aman, serta peningkatan literasi dan kesadaran digital masyarakat. Pendekatan regulatif harus diimbangi dengan kerja sama internasional, harmonisasi hukum lintas negara, serta penguatan kapasitas kelembagaan agar negara mampu merespons kompleksitas cybercrime yang bersifat transnasional dan dinamis. Dengan demikian, ruang siber sebagai produk kemajuan teknologi modern tidak hanya menghadirkan peluang transformasi sosial-ekonomi, tetapi juga menuntut rekonstruksi paradigma hukum dan tata kelola keamanan yang mampu menjawab tantangan kejahatan digital secara komprehensif dan berkelanjutan.

B. Orientasi Cyber Law dalam Perlindungan Individu: Analisis Normatif

Cyber law lahir sebagai respons normatif negara terhadap transformasi struktur sosial dan pola kejahatan akibat perkembangan teknologi informasi. Perubahan dari ruang fisik ke ruang digital tidak hanya menggeser medium interaksi, tetapi juga mengubah karakter delik, locus delicti, alat bukti, hingga subjek hukum yang terdampak. Dalam konteks ini, hukum dituntut beradaptasi untuk menjaga ketertiban, melindungi hak individu, serta memastikan kepastian hukum dalam ekosistem digital. Di Indonesia, respons normatif terhadap fenomena tersebut terkonsolidasi melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian mengalami perubahan melalui UU Nomor 19 Tahun 2016 dan pembaruan terbaru melalui UU Nomor 1 Tahun 2024 (MS 2025). Secara konseptual, desain UU ITE mengadopsi tipologi kejahatan siber sebagaimana dirumuskan dalam *European Convention on Cybercrime* (Budapest Convention), meliputi: *illegal access, illegal interception, data interference,* system *interference, misuse of devices, serta computer-related fraud and forgery.* Selain itu, UU ITE juga mengatur konten ilegal *(illegal content)* yang mencakup muatan kesusilaan, perjudian, penghinaan dan/atau pencemaran nama baik, pemerasan, serta penyebaran informasi yang menimbulkan kebencian atau permusuhan berbasis SARA.

Namun, secara normatif, orientasi awal cyber law Indonesia menunjukkan dominasi pendekatan kriminalisasi *(criminalization-oriented approach).* Struktur UU ITE menempatkan perumusan larangan dalam Pasal 27–35 dan ancaman pidana dalam Pasal 45–52 sebagai inti pengaturan. Model ini mencerminkan paradigma hukum pidana klasik yang berfokus pada kepastian rumusan delik *(lex certa dan lex stricta),* dengan menekankan penindakan terhadap pelaku (Suhaemin 2023). Perlindungan terhadap individu sebagai subjek yang rentan belum menjadi poros utama dalam konstruksi regulasi. Jika dibandingkan dengan *Budapest Convention,* terdapat perbedaan orientasi normatif. Konvensi tersebut menempatkan serangan terhadap sistem dan data *(illegal access, data interference)* sebagai prioritas utama karena dianggap mengancam integritas dan kepercayaan terhadap infrastruktur digital (Ayu et al. 2023). Sebaliknya, UU ITE justru membuka pengaturan dengan delik kesusilaan, perjudian, dan pencemaran nama baik (Pasal 27). Hal ini menunjukkan kecenderungan "digitalisasi delik konvensional" yakni memindahkan delik lama ke medium elektronik alih-alih membangun arsitektur hukum yang sepenuhnya berangkat dari karakteristik spesifik ruang siber. Kecenderungan tersebut berdampak pada praktik penegakan hukum yang kerap menempatkan individu sebagai objek kriminalisasi, khususnya dalam perkara pencemaran nama baik atau ekspresi di ruang digital. Kritik akademik menyoroti potensi overcriminalization dan multitafsir dalam beberapa norma UU ITE, yang berimplikasi pada ketegangan antara penegakan hukum dan perlindungan kebebasan berekspresi sebagai bagian dari hak asasi manusia.

Perkembangan regulasi selanjutnya menunjukkan adanya upaya perluasan pendekatan. Integrasi ketentuan terkait teknologi informasi dalam KUHP 2023 memperlihatkan pengakuan bahwa dimensi digital telah menjadi bagian inheren dari sistem hukum pidana nasional. Selain itu, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional serta Permenhan Nomor 82 Tahun 2014 tentang Pertahanan Siber memperkuat kerangka keamanan siber dalam perspektif strategis dan pertahanan negara (Anggreini 2025). Regulasi-regulasi ini menggeser sebagian orientasi dari semata-mata represif menuju pendekatan preventif, manajerial risiko, dan penguatan kapasitas kelembagaan. Akan tetapi, secara

konseptual, desain regulasi tersebut masih cenderung *state-centric.* Fokus utama diarahkan pada stabilitas sistem, perlindungan infrastruktur kritis, dan keamanan nasional. Perlindungan individu sering kali ditempatkan sebagai konsekuensi turunan dari keamanan sistem, bukan sebagai tujuan normatif utama. Dalam paradigma ini, negara diposisikan sebagai aktor sentral penjaga ketertiban siber, sementara individu berada dalam posisi yang relatif pasif.

Padahal, dalam perspektif hak asasi manusia, perlindungan individu merupakan fondasi legitimasi *cyber law.* Hak atas privasi, yang dirumuskan oleh Warren dan Brandeis sebagai *"the right to be let alone",* menjadi prinsip dasar dalam relasi antara individu, negara, dan korporasi digital. Dalam konteks Indonesia, jaminan konstitusional tersebut tercermin dalam Pasal 28G ayat (1) UUD 1945 yang menjamin perlindungan diri pribadi, keluarga, kehormatan, martabat, dan rasa aman (Burju 2026). Penguatan lebih lanjut hadir melalui Undang-Undang Perlindungan Data Pribadi (UU PDP), yang menegaskan hak subjek data atas akses, koreksi, penghapusan, pembatasan pemrosesan, serta mekanisme ganti rugi. Meskipun demikian, secara sistemik masih terdapat fragmentasi pengaturan. Norma terkait perlindungan data tersebar dalam UU ITE, UU PDP, KUHP, regulasi sektoral, serta kebijakan teknis lainnya. Fragmentasi ini berpotensi menimbulkan tumpang tindih kewenangan, inkonsistensi penegakan, dan ketidakpastian hukum bagi individu sebagai korban. Selain itu, ketiadaan ratifikasi *Budapest Convention* membatasi optimalisasi kerja sama internasional dalam penanganan cybercrime yang bersifat lintas negara, termasuk dalam aspek ekstradisi, pertukaran alat bukti elektronik, dan investigasi bersama. Kondisi ini secara tidak langsung berdampak pada efektivitas perlindungan korban di tingkat global.

Dengan demikian, secara normatif dapat disimpulkan bahwa orientasi cyber law Indonesia masih didominasi pendekatan kriminalisasi dan keamanan negara, sementara paradigma perlindungan korban *(victim-oriented approach)* belum sepenuhnya terintegrasi sebagai poros utama. Tantangan ke depan terletak pada rekonstruksi orientasi regulasi menuju model yang lebih seimbang antara keamanan sistem, kepastian hukum, dan perlindungan hak individu (Nai and Hoesein 2026). Hal ini mencakup harmonisasi regulasi, penguatan mekanisme pemulihan korban,

peningkatan akuntabilitas pengendali data, serta perluasan kerja sama internasional agar perlindungan individu di ruang siber tidak hanya bersifat deklaratif, tetapi juga efektif secara substantif.

C. Krisis Efektivitas Cyber Law dalam Ruang Siber: Kesenjangan Norma dan Realitas

Efektivitas cyber law dapat diukur melalui empat dimensi utama. Pertama, preventive efficacy, yakni kemampuan hukum mencegah cybercrime melalui norma berbasis risiko, kewajiban keamanan sistem, mekanisme early warning, dan literasi digital. Kedua, *enforcement efficacy,* yaitu kapasitas mendeteksi, menginvestigasi, dan menghukum pelaku dengan dukungan rumusan delik yang jelas, koordinasi kelembagaan, serta forensik digital yang memadai. Ketiga, *restorative efficacy,* kemampuan memberikan pemulihan nyata bagi korban melalui restitusi, kompensasi, dan rehabilitasi. Keempat, *legal certainty efficacy,* yaitu koherensi regulasi, konsistensi interpretasi, dan adaptabilitas terhadap perkembangan teknologi (Aprilianti 2024).

Dalam konteks Indonesia, krisis efektivitas muncul dari ketegangan antara desain normatif dan realitas empiris. Sejak UU ITE 2008 hingga perubahan melalui UU 1/2024, pendekatan yang dominan masih berorientasi pada kriminalisasi dan pengetatan sanksi. Revisi norma memang memberi klarifikasi, tetapi kasus kriminalisasi konten, kebocoran data massal, dan serangan ransomware menunjukkan adanya implementation gap dan regulatory lag. Karakter regulasi yang reaktif dibentuk pasca-kejadian berbeda dengan model anticipatory governance seperti GDPR atau NIST Framework yang berbasis manajemen risiko (Nurdiyanti and Prastyanti 2025). Fragmentasi kewenangan antara BSSN, Kepolisian, dan Kemenkominfo memperlemah koordinasi, sementara belum diratifikasinya *Convention on Cybercrime* membatasi kerja sama internasional. Rendahnya tingkat conviction juga mencerminkan keterbatasan kapasitas forensik digital. Secara konseptual, desain *cyber law* Indonesia masih *offender-centric,* sehingga perlindungan korban belum optimal dan berpotensi menimbulkan secondary victimization. Reformasi ke depan menuntut pergeseran menuju victim-

centered approach, penguatan restitusi dan tanggung jawab pengendali sistem, serta harmonisasi internasional agar hukum siber tidak hanya kuat secara normatif, tetapi juga efektif secara substantif.

Kesimpulan

Perkembangan ruang siber sebagai produk Revolusi Industri ketiga dan keempat telah melahirkan medium interaksi global yang melampaui batas teritorial negara. Karakteristiknya yang terbuka, anonim, dan terdesentralisasi menciptakan peluang transformasi sosial-ekonomi sekaligus kondisi kriminogenik bagi munculnya cybercrime yang bersifat transnasional dan kompleks. Dalam konteks ini, negara dituntut membangun kerangka hukum yang mampu merespons perubahan struktur kejahatan sekaligus melindungi individu sebagai subjek yang rentan. Secara normatif, cyber law Indonesia melalui UU ITE dan regulasi turunannya menunjukkan upaya adaptasi terhadap tipologi kejahatan siber global. Namun, orientasinya masih didominasi pendekatan kriminalisasi dan keamanan negara *(state-centric dan offender-centric),* sementara perlindungan individu dan korban belum sepenuhnya menjadi poros utama. Fragmentasi regulasi, keterbatasan koordinasi kelembagaan, serta belum optimalnya kerja sama internasional memperlihatkan bahwa desain hukum belum sepenuhnya selaras dengan karakter ruang siber yang lintas batas. Krisis efektivitas cyber law tampak pada kesenjangan antara konstruksi normatif dan implementasi empiris ditandai oleh kebocoran data massal, serangan ransomware, kriminalisasi berbasis konten, serta lemahnya pemulihan korban. Hal ini menunjukkan bahwa penguatan sanksi pidana semata tidak cukup. Diperlukan pergeseran paradigma menuju pendekatan yang lebih preventif, adaptif, dan berorientasi pada korban *(victim-centered approach),* disertai harmonisasi regulasi dan penguatan kapasitas institusional. Dengan demikian, masa depan cyber law Indonesia bergantung pada kemampuannya merekonstruksi orientasi dari sekadar instrumen penindakan menjadi kerangka perlindungan hak individu yang komprehensif dan efektif dalam menghadapi dinamika ruang siber global.

Daftar Pustaka

Amalia, Aminarti Fithri, and Wira Atman. 2025. "Strategi Detterence Siber Indonesia Terhadap Ancaman Proxy State Actor," 262–77.

Amelia, Selvi. 2024. "Ruang Cyber vs Kebebasan Berpendapat : Menyeimbangkan Regulasi Dan Ekspresi Di Era Digital Banyak Manfaat Bagi Masyarakat , Terdapat Juga Kekhawatiran Yang Valid" 4 (2).

Anggreini, Bunga. 2025. "Penguatan Hukum Pidana Indonesia Dalam Menghadapi Kejahatan Siber Era Digital." *Jurnal Terekam Jejak* 3 (3): 8–20.

Aprilianti, Astri. 2024. "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia:Tantangan Dan Solusi." *Begawan Abioso* 15 (3).

Ardyawati, Atha Hukama, Sahara Islami Syahidana, Miranda Eryna, and Vimala Bulan. 2025. "Media Hukum Indonesia (MHI) Eksistensi Hukum Dalam Hidup Bermasyarakat Di Era Digitalisasi The Role and Existence of Law in Society in the Digital Era Media Hukum Indonesia (MHI) Tradisional." 3 (4): 433–39.

Ayu, Ida, Agung Rasmi, Ni Luh, Gede Astariyani, Fakultas Hukum, and Universitas Udayana. 2023. "Urgensi Dalam Meratifikasi Convention On Cybercrime Sebagai Pemenuhan HAM Di Indonesia Abstrak" 45 (2).

Ayubi, Adim Isral. 2025. "Kejahatan Cyber: Motif Dan Implikasi Terhadap Keamanan Nasional." *QISTINA* 4 (1): 158–67.

Burju, Johanes Maruli. 2026. "Analisis Peran Hukum Siber Dalam Menjaga Privasi Pengguna Di Indonesia Pada Era Digital," no. November 2025.

Ganjar, Silawati Dayang. 2025. "Urgensi Pembaruan Hukum Pidana Dalam Menanggulangi Kejahatan Siber : Tinjauan Kritis Terhadap Kesesuaian KUHP Nasional Dan Perubahan UU ITE" 4 (3): 197–208.

Khaidir, Annisa, Mahendra Putra Kurnia, and Rika Erawaty. 2025. "Perlindungan Hukum Terhadap Korban Kejahatan Siber Di Indonesia Dalam Perspektif Hukum Internasional," 10563–73.

L. Hadi Adha, Zaeni Asyhadie, Rahmawati Kusuma. 2020. "INDUSTRIAL DIGITALIZATION AND ITS IMPACT ON LABOR AND EMPLOYMENT RELATIONSHIPS IN INDONESIA." *Jurnal Kompilasi Hukum* V (2).

Mahu, Aprianus O. 2014. "Ruang Siber Dan Kehidupan Remaja Dalam Novel Sweet Sixteen Karya Birgit Vanderbeke," 32–49.

MS, Nuruzzaman. 2025. "The Harmonization of Administrative Regulatory Arrangements Toward Public Institutional Accountability in Handling Cybercrime in Indonesia." *Mendapo* 6: 144–62.

Mulya, Ilham Indra, Muhammad Dewanto Adi Saputra, and Muhammad Rahmadzani. 2025. "Analisis Kerentanan Siber Kebocoran Data Polri Oleh Bjorka" 4 (1): 202–8.

Nai, Makkamadin Aras, and Zainal Arifin Hoesein. 2026. "Analisis Yuridis Terhadap Perlindungan Hukum Bagi Korban Kejahatan Siber Di Indonesia." *Journal of Innovative and Creativity* 6 (1): 1637–44.

Nurdiyanti, Erlinda Putri, and Rina Arum Prastyanti. 2025. "Efektivitas Penegakan Hukum Telematika Terhadap Pelanggaran Hak Cipta Di Media Digital : Studi Kasus Streaming Ilegal." *Jurnal Ilmu Sosial, Politik Dan Humaniora* 5 (1): 1–11.

Salim, Lukman, and Nur Hakim. 2024. "Penurunan Etika Sebagai Dampak Kejahatan Siber Terhadap Generasi Muda Di Indonesia" 2 (1): 628–36.

Salsabila, Alivia Fitri. 2024. "Pengaruh Revolusi Industri 4 . 0 Terhadap Hubungan Komunikasi Antarmanusia Dalam Implikasi Perubahan Sosial Di Era Digital" 2 (1).

Suhaemin, Amin. 2023. "Karakteristik Cybercrime Di Indonesia." *EduLaw* 5 (2): 15–26.

Wati, Dwi Shinta, Siti Nurhaliza, Mulia Wulan Sari, and Rizka Amallia. 2024. "Dampak Cyber Crime Terhadap Keamanan Nasional Dan Strategi Penanggulangannya : Ditinjau Dari Penegakan Hukum" 02 (01): 44–55.

Wiraguna, Sidi Ahyar. 2024. "Metode Normatif Dan Empiris Dalam Penelitian Hukum : Studi Eksploratif Di Indonesia." *Jurnal Sosial Politik, Pemerintahan Dan Hukum* 3 (3). https://doi.org/10.59818/jps.v3i3.1390.