JIRK
Journal of Innovation Research and Knowledge
Vol.6, No.4, September 2026
https://doi.org/10.53625/jirk.v1i1.13274

Kriminologi Dalam Era Digital Antara Perkembangan Kejahatan *Cyber* Dan Kesiapan Sistem Hukum

Tommy Adhiyaksah Putra[1]*, Reynaldo Setiawan[2], Alvi Syahrin Putra[3]
[1,2,3]Program Magister Hukum, Universitas Pasundan Bandung
Penulis Korespondensi: gerry0505@icloud.com

Received: 30/07/2026 | Accepted: 01/09/2026 | Publication: 05/09/2026

Abstract: *Advances in information technology have transformed patterns of social interaction, economic transactions, and information dissemination, while at the same time creating new spaces for the development of cybercrime. Cybercrime is no longer limited to simple fraud but encompasses illegal access, data theft, identity theft, carding, digital extortion, the dissemination of fake news, hate speech, and other forms of crime that utilize computers and networks as either means or targets. This study aims to analyze law enforcement against perpetrators of cybercrime in Indonesia and the regulation of cybercrime within the Indonesian criminal justice system. The study employs a normative juridical method using a statutory approach and a conceptual approach, supported by a literature review of relevant books, journals, and legal sources. The findings indicate that law enforcement against cybercrime faces several challenges, including limited law enforcement capacity, digital forensic technology, laboratory facilities, investigation costs and time, as well as victims' tendency not to report incidents. From a regulatory perspective, cybercrime provisions are dispersed across several legal instruments, requiring harmonization to keep pace with the characteristics of digital crimes, which are cross-border, rapidly evolving, and technology-based. Strengthening the legal system should be pursued through updates to legal substance, improvements in law enforcement structures, strengthening legal culture and digital literacy, and enhanced national and international cooperation. Victim protection should also be positioned as an integral part of cybercrime prevention and control policies.*
Keywords: *Criminology, Victimology, Cybercrime, Law Enforcement, Criminal Law System*

How to Cite: Putra, T. A., Setiawan, R., & Putra, A. S. (2026). Kriminologi dalam era digital antara perkembangan kejahatan cyber dan kesiapan sistem hukum. *Journal of Innovation Research and Knowledge, 6*(4), 2367–2378. https://doi.org/10.53625/jirk.v1i1.13274

PENDAHULUAN

Perkembangan teknologi digital merupakan salah satu perubahan sosial paling signifikan dalam kehidupan masyarakat modern. Internet, komputer, telepon pintar, platform media sosial, dan berbagai sistem elektronik telah mempercepat komunikasi serta mempermudah transaksi ekonomi. Aktivitas yang sebelumnya membutuhkan pertemuan fisik kini dapat dilakukan melalui ruang digital. Perubahan tersebut membawa manfaat besar bagi masyarakat, tetapi sekaligus menciptakan ruang baru yang dapat dimanfaatkan untuk melakukan kejahatan.

Fenomena *cyber crime* menunjukkan bahwa teknologi tidak hanya digunakan sebagai instrumen pembangunan, tetapi juga dapat digunakan untuk melakukan perbuatan melawan hukum. Kejahatan siber mempunyai karakter berbeda dari kejahatan konvensional karena

pelaku dapat menyembunyikan identitas, menggunakan jaringan anonim, memanfaatkan perangkat lunak tertentu, dan menjalankan aksinya dari wilayah yang berbeda dengan lokasi korban. Karena itu, ruang digital membuat batas geografis menjadi semakin kurang relevan dalam proses terjadinya kejahatan.

Dalam bahan kajian yang menjadi dasar artikel ini, perkembangan *cyber crime* di Indonesia digambarkan melalui berbagai modus, antara lain phishing, pencurian identitas, peretasan akun, malware, penipuan berbasis aplikasi, pemalsuan dan pencurian kartu kredit atau carding, serta pembobolan rekening. Perkembangan tersebut menunjukkan bahwa objek yang diserang tidak hanya harta benda, tetapi juga data, identitas, privasi, sistem elektronik, dan kepercayaan masyarakat terhadap ruang digital.

Dari perspektif kriminologi, *cyber crime* tidak cukup dipahami hanya sebagai pelanggaran terhadap ketentuan pidana. Kejahatan merupakan gejala sosial yang dipengaruhi faktor individual, psikologis, ekonomi, lingkungan, teknologi, kesempatan, dan budaya. Perkembangan teknologi dapat menciptakan kesempatan baru bagi pelaku karena biaya melakukan kejahatan tertentu relatif rendah, korban dapat dijangkau dalam jumlah besar, dan pelaku dapat beroperasi tanpa harus berhadapan langsung dengan korbannya.

Perspektif viktimologi melengkapi analisis tersebut dengan menempatkan korban sebagai bagian penting dalam sistem penanggulangan kejahatan. Korban *cyber crime* dapat mengalami kerugian finansial, kehilangan data, gangguan privasi, kerusakan reputasi, tekanan psikologis, bahkan hilangnya rasa aman dalam menggunakan teknologi. Oleh karena itu, kebijakan penegakan hukum tidak semestinya hanya berorientasi pada penangkapan dan penghukuman pelaku, tetapi juga harus memperhatikan pemulihan korban.

Permasalahan menjadi lebih kompleks karena hukum pidana harus mampu mengikuti perubahan teknologi. Bahan awal penelitian menegaskan adanya kesenjangan antara hukum ideal dan realitas penegakan hukum, khususnya terkait keterlambatan harmonisasi regulasi, kapasitas aparat, fasilitas penyidikan, dan rendahnya literasi hukum masyarakat mengenai keamanan digital. Kondisi tersebut memperlihatkan bahwa persoalan *cyber crime* merupakan persoalan sistem hukum secara keseluruhan, bukan sekadar persoalan ada atau tidak adanya suatu ketentuan pidana.

Indonesia telah memiliki ketentuan mengenai informasi dan transaksi elektronik yang menjadi salah satu dasar penanggulangan *cyber crime*. Namun, karakter kejahatan digital yang terus berkembang menuntut pembacaan hukum secara sistematis. Ketentuan mengenai akses ilegal, intersepsi, gangguan data dan sistem, pemalsuan, penipuan, konten tertentu, dan berbagai perbuatan melalui sistem elektronik harus ditempatkan dalam kerangka kebijakan kriminal yang lebih luas.

Selain aspek substansi hukum, kesiapan struktur hukum juga menjadi persoalan. Penanganan perkara digital memerlukan kemampuan khusus dalam pengamanan barang bukti elektronik, digital forensics, analisis jaringan, pelacakan transaksi, serta koordinasi dengan penyedia layanan. Keterbatasan laboratorium *cyber crime* dan tenaga yang mempunyai kompetensi khusus dapat memperlambat penyelidikan dan pembuktian. Bahan awal penelitian juga mencatat bahwa fasilitas laboratorium belum tersedia secara merata sehingga dapat menimbulkan kendala waktu dan biaya.

JIRK
Journal of Innovation Research and Knowledge
Vol.6, No.4, September 2026
https://doi.org/10.53625/jirk.v1i1.13274

Dalam konteks budaya hukum, keberhasilan penanggulangan *cyber crime* juga ditentukan oleh perilaku masyarakat. Masyarakat yang tidak memahami keamanan akun, autentikasi, phishing, privasi, dan penggunaan data pribadi dapat menjadi lebih rentan. Pada sisi lain, korban yang enggan melapor karena alasan privasi, ekonomi, atau kurang percaya terhadap kemampuan aparat menyebabkan sebagian kejahatan tidak tercatat secara optimal. Karena itu, literasi digital dan kepercayaan terhadap institusi penegak hukum merupakan bagian dari kebijakan pencegahan.

Atas dasar persoalan tersebut, artikel ini diarahkan untuk mengkaji dua persoalan utama. Pertama, bagaimana penegakan hukum terhadap pelaku tindak pidana *cyber crime* di Indonesia. Kedua, bagaimana pengaturan *cyber crime* dalam sistem hukum pidana Indonesia. Kedua persoalan tersebut dianalisis dengan menghubungkan perspektif kriminologi, viktimologi, teori *cyber crime*, dan teori sistem hukum agar diperoleh gambaran yang lebih menyeluruh mengenai kesiapan hukum Indonesia menghadapi perkembangan kejahatan digital.

Berdasarkan uraian di atas, rumusan masalahnya adalah:

1. Bagaimana penegakan hukum terhadap pelaku tindak pidana *cyber crime* di Indonesia?
2. Bagaimana pengaturan *cyber crime* dalam sistem hukum pidana Indonesia?

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian yang menempatkan hukum sebagai norma yang dikaji melalui peraturan perundang-undangan, doktrin, konsep, dan bahan kepustakaan yang relevan. Metode ini dipilih karena fokus penelitian berada pada pengaturan *cyber crime* dan penegakan hukum terhadap pelaku dalam sistem hukum pidana Indonesia. Penelitian tidak diarahkan untuk mengukur perilaku masyarakat secara statistik, melainkan untuk menganalisis norma hukum dan keterkaitannya dengan perkembangan kejahatan digital.

Pendekatan yang digunakan adalah pendekatan peraturan perundang-undangan *(statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan peraturan perundang-undangan digunakan untuk mengidentifikasi ketentuan hukum yang berkaitan dengan informasi dan transaksi elektronik, pembuktian, tindak pidana yang dilakukan dengan atau melalui sistem elektronik, serta kebijakan penanggulangan kejahatan. Pendekatan konseptual digunakan untuk memahami konsep *cyber crime*, kriminologi, viktimologi, penegakan hukum, dan sistem hukum. Bahan hukum primer berupa peraturan perundang-undangan yang berkaitan dengan tindak pidana siber dan sistem hukum pidana Indonesia. Bahan hukum sekunder berupa buku-buku kriminologi, viktimologi, hukum pidana, hukum siber, serta artikel jurnal yang membahas *cyber crime* dan perlindungan korban. Bahan hukum tersier digunakan untuk membantu memahami istilah dan konsep yang berkaitan dengan penelitian.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan. Bahan yang diperoleh kemudian diinventarisasi, diklasifikasikan berdasarkan tema, dan dianalisis secara kualitatif. Analisis dilakukan dengan menghubungkan norma hukum dengan karakteristik *cyber crime* dan kebutuhan penegakan hukum. Dengan demikian, penelitian tidak hanya

JIRK
Journal of Innovation Research and Knowledge
Vol.6, No.4, September 2026
https://doi.org/10.53625/jirk.v1i1.13274

mendeskripsikan ketentuan hukum, tetapi juga menilai kecukupan dan kesiapan sistem hukum dalam merespons perkembangan kejahatan digital.

Analisis menggunakan kerangka sistem hukum yang memandang keberhasilan penegakan hukum melalui keterkaitan antara substansi hukum, struktur hukum, dan budaya hukum. Kerangka tersebut dipadukan dengan perspektif viktimologi agar kepentingan korban tidak terpisah dari proses penegakan hukum. Hasil analisis selanjutnya disusun secara sistematis berdasarkan dua rumusan masalah.

HASIL DAN PEMBAHASAN

1. Penegakan Hukum terhadap Pelaku Tindak Pidana *Cyber crime* di Indonesia

Penegakan hukum *cyber crime* pada dasarnya merupakan rangkaian kegiatan untuk memastikan bahwa perbuatan pidana yang menggunakan atau menyerang teknologi informasi dapat diidentifikasi, diselidiki, dibuktikan, dituntut, dan diputus sesuai hukum yang berlaku. Kekhususan perkara siber terletak pada karakter alat bukti dan cara pelaku melakukan kejahatan. Barang bukti dapat berbentuk data elektronik, log aktivitas, akun, perangkat komputer, telepon pintar, alamat jaringan, rekaman komunikasi, transaksi elektronik, dan berbagai informasi digital lainnya.

Ketentuan mengenai alat bukti elektronik menjadi penting karena *cyber crime* sering kali tidak meninggalkan jejak dalam bentuk konvensional. Bahan penelitian menjelaskan bahwa ketentuan mengenai informasi elektronik, data elektronik, dan hasil cetaknya memperluas ruang pembuktian dalam perkara pidana. Hal tersebut merupakan perkembangan penting karena proses penegakan hukum terhadap kejahatan siber sangat bergantung pada kemampuan aparat mengidentifikasi, mengamankan, memeriksa, dan menyajikan bukti digital secara sah.

Dalam tahap penyelidikan dan penyidikan, aparat harus mampu membedakan antara aktivitas digital yang sah dan aktivitas yang memenuhi unsur tindak pidana. Misalnya, akses terhadap sistem elektronik tidak selalu merupakan kejahatan. Persoalan pidana muncul ketika akses dilakukan dengan sengaja, tanpa hak atau melawan hukum, termasuk apabila dilakukan untuk memperoleh informasi atau menerobos sistem pengamanan. Kerangka demikian menunjukkan pentingnya ketelitian aparat dalam mengonstruksikan unsur tindak pidana.

Penegakan hukum juga menghadapi persoalan kompetensi. Kejahatan siber dapat dilakukan oleh pelaku yang mempunyai kemampuan teknis tinggi, menggunakan identitas palsu, memanfaatkan server atau akun yang berada di luar wilayah Indonesia, serta menghapus atau memindahkan jejak digital. Oleh karena itu, penyidik memerlukan pengetahuan mengenai jaringan komputer, sistem operasi, enkripsi, analisis perangkat, transaksi digital, serta prosedur digital forensik. Bahan penelitian menempatkan keterbatasan keterampilan aparat sebagai salah satu hambatan utama penegakan hukum *cyber crime*.

Persoalan sarana dan prasarana juga mempengaruhi efektivitas penegakan hukum. Laboratorium *cyber crime* diperlukan untuk mempercepat pemeriksaan perangkat dan data digital. Apabila fasilitas hanya terkonsentrasi pada lembaga atau kota tertentu, penyidikan perkara yang berada jauh dari pusat fasilitas dapat memerlukan waktu dan biaya lebih besar.

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)

Dalam perkara digital, keterlambatan dapat mengurangi peluang memperoleh bukti karena data dapat dihapus, dipindahkan, atau berubah akibat aktivitas sistem.

Dari perspektif viktimologi, keberhasilan penegakan hukum tidak boleh hanya diukur dari keberhasilan menemukan pelaku. Korban harus memperoleh informasi, perlindungan, kesempatan untuk didengar, serta mekanisme pemulihan kerugian. Kajian viktimologi dalam bahan penelitian menegaskan bahwa korban merupakan subjek yang memiliki hak atas informasi, perlindungan, kompensasi, dan restitusi.

Dalam *cyber crime*, kebutuhan pemulihan korban dapat sangat beragam. Korban pencurian identitas membutuhkan pemulihan identitas dan keamanan akun; korban penipuan membutuhkan mekanisme penelusuran transaksi dan pemulihan kerugian; korban kebocoran data membutuhkan perlindungan terhadap penggunaan data lebih lanjut; sedangkan korban ancaman atau pemerasan digital membutuhkan perlindungan dari intimidasi. Dengan demikian, pendekatan korban harus disesuaikan dengan karakter kerugian yang dialami.

Faktor pelaporan juga menjadi bagian penting. Tidak semua korban segera mengadukan kejahatan karena merasa malu, khawatir terhadap privasi, menganggap kerugiannya terlalu kecil, atau tidak yakin bahwa pelaku dapat ditemukan. Dalam kasus tertentu, korban juga tidak mengetahui kepada siapa harus melapor. Rendahnya pelaporan dapat menimbulkan fenomena dark figure of cybercrime, yaitu kejahatan yang terjadi tetapi tidak tercatat dalam sistem penegakan hukum. Karena itu, penyederhanaan mekanisme pelaporan dan peningkatan kepercayaan publik menjadi langkah strategis.

Penegakan hukum *cyber crime* juga membutuhkan koordinasi antarlembaga. Satu perkara dapat melibatkan penyedia platform, perbankan, operator telekomunikasi, aparat penegak hukum, dan lembaga lain yang memiliki data relevan. Koordinasi yang lambat dapat menghambat pelacakan akun, transaksi, alamat jaringan, dan data lainnya. Pada kasus lintas negara, kebutuhan kerja sama menjadi lebih besar karena penyedia layanan, server, pelaku, dan korban dapat berada di negara berbeda.

Karena sifat *cyber crime* yang lintas batas, kerja sama internasional merupakan unsur penting. Bahan penelitian menyarankan peningkatan kerja sama bilateral, regional, dan multilateral, termasuk melalui mekanisme ekstradisi dan bantuan hukum timbal balik. Kerja sama tersebut dibutuhkan agar proses memperoleh bukti dan mengejar pelaku tidak berhenti pada batas yurisdiksi nasional.

Penegakan hukum juga perlu dibedakan antara pendekatan represif dan pencegahan. Pendekatan represif diperlukan untuk memberikan pertanggungjawaban pidana kepada pelaku. Namun, jika kebijakan hanya berorientasi pada penghukuman setelah kejahatan terjadi, kerugian korban tetap akan muncul. Oleh karena itu, kebijakan preventif perlu dikembangkan melalui penguatan keamanan sistem, literasi digital, edukasi masyarakat, dan peningkatan kapasitas institusi.

Secara kriminologis, pencegahan harus memperhatikan kesempatan yang memungkinkan kejahatan terjadi. Pelaku akan lebih mudah melakukan *cyber crime* ketika sistem memiliki kelemahan, pengguna memiliki literasi rendah, dan pengawasan tidak efektif. Karena itu, keamanan teknologi perlu diposisikan sebagai bagian dari strategi

pencegahan. Bahan penelitian menyebut beberapa langkah teknis seperti pembaruan sistem, kebijakan keamanan, intrusion detection dan prevention system, firewall, serta antivirus.

Pendekatan lain yang relevan adalah keadilan restoratif, khususnya untuk perkara tertentu yang secara hukum memungkinkan penyelesaian berorientasi pemulihan. Dalam perspektif viktimologi, keadilan restoratif dapat memberikan ruang bagi korban untuk menyampaikan kerugian dan kebutuhan pemulihan. Namun penerapannya harus memperhatikan karakter tindak pidana, kepentingan korban, dampak masyarakat, serta ketentuan hukum yang berlaku. Pendekatan tersebut tidak dapat dipahami sebagai pengganti penegakan hukum terhadap seluruh *cyber crime*, melainkan sebagai salah satu pendekatan yang dapat digunakan secara selektif.

Dengan demikian, penegakan hukum terhadap *cyber crime* di Indonesia membutuhkan pendekatan yang terpadu. Peningkatan kapasitas aparat harus berjalan bersama pembaruan regulasi, penguatan digital forensics, pemerataan fasilitas, perbaikan mekanisme pelaporan, perlindungan korban, koordinasi antarlembaga, dan kerja sama internasional. Tanpa integrasi tersebut, peningkatan jumlah dan kompleksitas kejahatan digital akan lebih cepat daripada kemampuan sistem hukum untuk meresponsnya.

2. Pengaturan *Cyber crime* dalam Sistem Hukum Pidana Indonesia

Cyber crime merupakan konsep yang berkembang seiring perubahan teknologi. Dalam bahan penelitian, *cyber crime* dipahami sebagai aktivitas kejahatan yang menempatkan komputer atau jaringan komputer sebagai alat, sasaran, atau tempat terjadinya kejahatan. Dengan karakter tersebut, *cyber crime* dapat mencakup penipuan kartu kredit, pencurian identitas, pemalsuan, penipuan melalui surat elektronik, pembobolan rekening, akses ilegal, perusakan situs, dan berbagai bentuk penyalahgunaan sistem informasi.

Secara konseptual, *cyber crime* dapat dibedakan menjadi kejahatan yang menggunakan teknologi informasi sebagai fasilitas dan kejahatan yang menjadikan sistem teknologi informasi sebagai sasaran. Pembedaan ini penting karena strategi penanggulangannya berbeda. Pada kategori pertama, teknologi digunakan sebagai sarana melakukan tindak pidana yang pada dasarnya dapat memiliki padanan dalam kejahatan konvensional. Pada kategori kedua, sistem komputer atau data justru menjadi objek serangan.

Perkembangan pengaturan *cyber crime* di Indonesia menunjukkan bahwa hukum pidana harus menghadapi persoalan baru yang sebelumnya tidak dikenal dalam bentuk yang sama. Akses ilegal, intersepsi, gangguan data, gangguan sistem, penyalahgunaan perangkat, pemalsuan data, dan penipuan berbasis komputer membutuhkan perumusan unsur tindak pidana yang dapat diterapkan terhadap perbuatan digital. Bahan penelitian mengaitkan beberapa kategori tersebut dengan kualifikasi *cyber crime* yang berkembang dalam hukum internasional.

Ketentuan mengenai akses ilegal merupakan salah satu contoh penting. Bahan penelitian menjelaskan bahwa Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik mengatur akses terhadap komputer atau sistem elektronik milik orang lain secara sengaja dan tanpa hak atau melawan hukum, termasuk akses untuk memperoleh informasi atau dokumen elektronik serta tindakan menerobos atau menjebol sistem pengamanan. Ketentuan tersebut memperlihatkan bahwa hukum pidana telah mengakui karakter khusus serangan terhadap sistem elektronik.

Selain akses ilegal, sistem hukum juga harus mampu merespons penggunaan teknologi untuk melakukan penghinaan, pemerasan atau pengancaman, penyebaran berita palsu, ujaran kebencian, perjudian, pelanggaran kesusilaan, dan bentuk perbuatan lainnya. Pengaturan yang tersebar menunjukkan bahwa *cyber crime* tidak merupakan satu jenis tindak pidana tunggal, melainkan cara atau lingkungan baru untuk melakukan berbagai perbuatan pidana.

Masalah yang muncul kemudian adalah harmonisasi. Jika ketentuan tersebar dalam beberapa peraturan, aparat harus menentukan hubungan antara aturan khusus dan aturan umum, menghindari tumpang tindih, serta memastikan unsur tindak pidana dapat dibuktikan secara tepat. Harmonisasi menjadi semakin penting ketika hukum pidana nasional mengalami perubahan dan ketika ketentuan mengenai teknologi informasi berinteraksi dengan hukum pidana umum.

Dalam perspektif teori sistem hukum, pengaturan *cyber crime* tidak dapat dilihat hanya dari substansi peraturan. Hans Kelsen memandang hukum sebagai sistem norma yang tersusun secara hierarkis, sedangkan pengembangan teori sistem hukum dalam konteks Indonesia menuntut perhatian terhadap dinamika pembentukan dan penerapan norma. Bahan penelitian juga menekankan bahwa sistem hukum Indonesia tidak hanya berkaitan dengan norma tertulis, tetapi berinteraksi dengan nilai keadilan, hukum yang hidup dalam masyarakat, dan praktik penegakan hukum.

Jika konsep sistem hukum diterapkan pada *cyber crime*, terdapat tiga dimensi yang perlu diperhatikan. Pertama, substansi hukum harus mampu memberikan dasar kriminalisasi, pertanggungjawaban, pembuktian, perlindungan korban, dan sanksi. Kedua, struktur hukum harus memiliki aparat, laboratorium, prosedur, dan mekanisme koordinasi yang memadai. Ketiga, budaya hukum harus mendorong masyarakat menggunakan teknologi secara bertanggung jawab serta melaporkan kejahatan yang dialami.

Dari sisi substansi, pembaruan hukum perlu mengantisipasi bentuk kejahatan yang terus berkembang. Teknologi seperti kecerdasan buatan, otomatisasi, enkripsi, jaringan anonim, dan layanan digital lintas negara dapat digunakan untuk meningkatkan kemampuan pelaku. Hukum yang terlalu bergantung pada bentuk teknologi tertentu berisiko cepat tertinggal. Karena itu, perumusan norma sebaiknya menekankan unsur perbuatan dan akibat hukum dengan tetap memberikan kepastian hukum.

Dari sisi struktur, diperlukan aparat yang mampu melakukan penyelidikan dan penyidikan berbasis bukti digital. Pelatihan tidak cukup diberikan satu kali, karena teknologi dan modus operandi berkembang dengan cepat. Kompetensi perlu diperbarui secara berkala melalui pendidikan, simulasi kasus, pengembangan laboratorium, dan kerja sama dengan pihak yang menguasai teknologi.

Dari sisi budaya hukum, literasi digital merupakan bagian dari pencegahan. Masyarakat perlu memahami bahwa keamanan digital bukan hanya tanggung jawab pemerintah atau perusahaan teknologi. Pengguna juga mempunyai peran dalam menjaga kata sandi, autentikasi, perangkat, dan data pribadi. Edukasi tersebut harus dilakukan dengan pendekatan yang mudah dipahami agar tidak berhenti pada pemahaman teknis, tetapi berkembang menjadi kesadaran hukum.

Pengaturan *cyber crime* juga harus berorientasi pada perlindungan korban. Ketika terjadi pencurian data atau penipuan digital, korban tidak cukup diberi status sebagai saksi. Sistem hukum perlu menyediakan mekanisme yang memungkinkan korban memperoleh informasi mengenai perkembangan perkara, perlindungan dari ancaman lanjutan, dan pemulihan kerugian sesuai ketentuan yang tersedia. Perspektif viktimologi menuntut pergeseran dari sistem yang berorientasi pada pelaku semata menuju sistem yang menyeimbangkan kepentingan pelaku, korban, dan masyarakat.

Perlindungan korban menjadi semakin penting karena *cyber crime* dapat menghasilkan dampak yang berlangsung lama. Data yang telah tersebar di internet sulit ditarik kembali. Identitas yang dicuri dapat digunakan untuk tindakan lain. Foto atau informasi pribadi yang disalahgunakan dapat mempengaruhi reputasi korban. Karena itu, pemulihan dalam perkara digital sering kali tidak selesai hanya dengan menghukum pelaku.

Dalam kerangka kebijakan kriminal, pengaturan *cyber crime* harus ditempatkan dalam strategi penal dan non-penal. Kebijakan penal mencakup kriminalisasi, penyidikan, penuntutan, pemeriksaan pengadilan, dan pemidanaan. Kebijakan non-penal mencakup pendidikan, keamanan siber, desain sistem yang aman, pengawasan, peningkatan literasi, dan penguatan ketahanan masyarakat. Bahan penelitian menegaskan perlunya pembaruan hukum pidana nasional dan hukum acara, peningkatan keamanan jaringan, peningkatan keahlian aparat, peningkatan kesadaran warga, serta kerja sama antarnegara.

Pengaturan yang efektif juga harus mampu menjaga keseimbangan antara penegakan hukum dan hak-hak warga. Ruang digital merupakan bagian dari kehidupan masyarakat sehingga penanggulangan *cyber crime* tidak boleh menghasilkan penggunaan kewenangan yang berlebihan. Setiap tindakan penegakan hukum harus memiliki dasar hukum, prosedur yang jelas, dan mekanisme pengawasan. Kepastian hukum diperlukan agar masyarakat memperoleh perlindungan sekaligus mengetahui batas perilaku yang dilarang.

Dengan demikian, kesiapan sistem hukum Indonesia menghadapi *cyber crime* harus dipahami sebagai kesiapan yang bersifat menyeluruh. Hukum substantif perlu harmonis dan adaptif; struktur penegakan hukum perlu kompeten dan didukung teknologi; sedangkan budaya hukum perlu diperkuat melalui literasi dan partisipasi masyarakat. Ketiga unsur tersebut harus bergerak bersama. Apabila salah satunya tertinggal, efektivitas penanggulangan *cyber crime* akan tetap terbatas.

Pada akhirnya, perkembangan *cyber crime* memperlihatkan bahwa perubahan teknologi memaksa hukum untuk terus melakukan adaptasi. Adaptasi tersebut bukan berarti setiap perkembangan teknologi harus selalu diikuti oleh undang-undang baru, melainkan membangun sistem hukum yang mampu menerapkan prinsip pidana secara tepat terhadap modus baru, sekaligus menyediakan ruang pembaruan ketika norma yang ada tidak lagi memadai. Inilah makna kesiapan sistem hukum dalam menghadapi kejahatan digital.

Kriminologi memberikan kerangka untuk memahami mengapa *cyber crime* terjadi dan bagaimana kondisi sosial menciptakan kesempatan bagi pelaku. Bahan penelitian menjelaskan bahwa kriminologi mempelajari kejahatan sebagai gejala sosial, termasuk faktor penyebab, dampak, dan upaya penanggulangannya. Pendekatan ini penting karena kejahatan digital tidak hanya muncul akibat niat individu, tetapi juga akibat kesempatan yang diciptakan oleh teknologi dan lingkungan sosial

Viktimologi kemudian memperluas sudut pandang dengan bertanya mengenai siapa yang menjadi korban, mengapa seseorang rentan menjadi korban, bagaimana hubungan korban dan pelaku, serta bagaimana dampak kejahatan dipulihkan. Dalam konteks digital, kerentanan dapat muncul karena rendahnya literasi, penggunaan kata sandi yang lemah, kepercayaan terhadap pesan palsu, keterbukaan data di media sosial, atau kelemahan sistem yang dikelola penyedia layanan. Namun, kerentanan tersebut tidak boleh digunakan untuk menyalahkan korban. Tanggung jawab utama tetap berada pada pelaku dan pada sistem perlindungan yang seharusnya mencegah penyalahgunaan.

Hubungan antara kriminologi dan viktimologi dengan sistem hukum menghasilkan pendekatan yang lebih lengkap. Kriminologi membantu memahami sebab dan pola kejahatan; viktimologi menjelaskan pengalaman dan kebutuhan korban; sedangkan hukum memberikan mekanisme untuk menentukan perbuatan yang dilarang, pertanggungjawaban, proses pembuktian, sanksi, serta pemulihan. Ketiganya harus ditempatkan dalam satu kebijakan kriminal.

Dalam praktik, pendekatan tersebut dapat diterapkan melalui siklus pencegahan, penindakan, dan pemulihan. Pencegahan dilakukan dengan mengurangi kesempatan melakukan kejahatan. Penindakan dilakukan dengan memperkuat kemampuan menemukan dan membuktikan tindak pidana. Pemulihan dilakukan dengan memastikan korban memperoleh perlindungan dan pemulihan sesuai hukum. Siklus tersebut membuat penanggulangan *cyber crime* tidak berhenti pada tahap pemidanaan.

Perspektif tersebut juga menunjukkan bahwa kesiapan sistem hukum tidak identik dengan banyaknya peraturan. Sistem dapat memiliki banyak aturan tetapi tetap tidak efektif apabila aparat tidak kompeten, fasilitas tidak tersedia, koordinasi lemah, dan masyarakat tidak percaya kepada institusi hukum. Oleh karena itu, ukuran kesiapan harus dilihat dari kemampuan sistem menghasilkan respons hukum yang cepat, tepat, adil, dan dapat dipertanggungjawabkan.

Penelitian ini juga menunjukkan pentingnya pembaruan hukum acara. Kejahatan digital menghasilkan bukti yang mudah berubah dan dapat berada di berbagai lokasi. Prosedur pengamanan, pemeriksaan, penyimpanan, dan penyajian bukti elektronik harus memberikan kepastian sehingga bukti dapat digunakan secara sah. Dalam perkara lintas batas, mekanisme memperoleh data dari luar negeri juga harus efisien tanpa mengabaikan kedaulatan negara dan perlindungan hak.

Pada tingkat kebijakan, pemerintah perlu mengembangkan strategi nasional yang mengintegrasikan penegakan hukum, keamanan siber, perlindungan korban, dan pendidikan masyarakat. Strategi tersebut perlu melibatkan lembaga negara, aparat penegak hukum, sektor teknologi, perbankan, akademisi, dan masyarakat sipil. Pendekatan kolaboratif menjadi penting karena *cyber crime* tidak berada dalam satu sektor saja.

Pada tingkat individu, masyarakat perlu diposisikan sebagai bagian dari sistem pencegahan. Pengguna harus mampu mengenali modus phishing, menjaga kredensial, menggunakan autentikasi yang memadai, memperbarui perangkat, dan melaporkan insiden. Perusahaan dan penyedia platform juga perlu membangun keamanan sejak desain sistem. Dengan demikian, pencegahan tidak dibebankan hanya kepada korban setelah kejadian.

Keseluruhan analisis menunjukkan bahwa *cyber crime* merupakan tantangan yang bersifat multidimensional. Karena itu, respons hukum juga harus multidimensional. Hukum pidana diperlukan, tetapi tidak berdiri sendiri. Ia harus didukung kriminologi untuk membaca perkembangan kejahatan, viktimologi untuk melindungi korban, teknologi untuk mengamankan bukti dan sistem, serta kerja sama kelembagaan dan internasional untuk menghadapi karakter lintas batas.

KESIMPULAN

1. Penegakan hukum terhadap pelaku *cyber crime* di Indonesia telah memiliki dasar hukum dan mekanisme yang dapat digunakan untuk menangani berbagai bentuk kejahatan digital, tetapi efektivitasnya masih menghadapi kendala kapasitas aparat, pemerataan sarana digital forensik dan laboratorium *cyber crime*, kompleksitas alat bukti elektronik, biaya dan waktu penyidikan, serta rendahnya pelaporan korban. Penegakan hukum perlu dikembangkan secara terpadu dengan memperkuat kemampuan aparat, teknologi forensik, koordinasi antarlembaga, kerja sama internasional, dan perlindungan serta pemulihan korban.
2. Pengaturan *cyber crime* dalam sistem hukum pidana Indonesia pada dasarnya tersebar dalam berbagai ketentuan yang mengatur perbuatan terkait sistem elektronik, akses ilegal, gangguan data dan sistem, penipuan, pemerasan atau pengancaman, penyebaran informasi tertentu, dan bentuk kejahatan lainnya. Tantangan utamanya adalah harmonisasi, adaptasi terhadap perkembangan teknologi, dan keseimbangan antara kepastian hukum dengan kebutuhan penanggulangan kejahatan. Kesiapan sistem hukum harus dibangun melalui pembaruan substansi, penguatan struktur penegakan hukum, dan peningkatan budaya hukum serta literasi digital.

Saran

1. Pemerintah dan aparat penegak hukum perlu memperkuat kapasitas penanganan *cyber crime* melalui pendidikan dan pelatihan digital forensik secara berkelanjutan, pemerataan laboratorium *cyber crime*, peningkatan kualitas mekanisme pelaporan, penguatan koordinasi antarlembaga, serta kerja sama bilateral, regional, dan multilateral untuk perkara lintas batas. Kebijakan penegakan hukum juga perlu memberi ruang yang memadai bagi perlindungan dan pemulihan korban.
2. Pembentuk undang-undang perlu terus melakukan harmonisasi dan pembaruan hukum pidana serta hukum acara agar mampu mengikuti perkembangan teknologi tanpa mengorbankan kepastian hukum dan hak warga negara. Di sisi lain, pemerintah, institusi pendidikan, sektor teknologi, dan masyarakat perlu memperluas literasi digital agar pencegahan *cyber crime* tidak hanya bergantung pada tindakan represif setelah kejahatan terjadi.

DAFTAR PUSTAKA

Apandi, M., K. Rahayu, W. Agus Prayugo, dan L. Ariany. 2025. "Kekaburan Norma dalam Kebebasan Berekspresi di Era Digital: Analisis Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik." Jurnal Hukum Lex Generalis, Vol. 5, No. 12.

Arief, Barda Nawawi. 1996. Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara. Semarang: Badan Penerbit Universitas Diponegoro.

Arifah, Dista Amalia. 2011. "Kasus Cybercrime di Indonesia." Jurnal Bisnis dan Ekonomi (JBE), Vol. 18, No. 2.

Asshiddiqie, Jimly dan Ali Safa'at. 2012. Teori Hans Kelsen tentang Hukum. Cetakan Kedua. Jakarta: Konstitusi Press.

Chazawi, Adami. 2013. Hukum Pidana Positif Penghinaan. Edisi Revisi. Malang: Media Nusa Creative.

Desembriyanti, S., R. F. Folasimo, Z. Zhafira, A. N. Oktafia, dan T. Supriyadi. 2024. "Pengaruh Faktor Lingkungan terhadap Perilaku Kriminalitas Anak." Corona: Jurnal Ilmu Kesehatan Umum, Psikolog, Keperawatan dan Kebidanan, Vol. 2, No. 2.

Dewi, M. P. dan B. Santoso. 2021. "Cybercrime di Indonesia: Studi Kasus dan Aspek Kriminologis." Jurnal Keamanan Nasional, Vol. 7, No. 2.

Dirdjosisworo, Soedjono. 1969. Doktrin-Doktrin Kriminologi. Jakarta: Alumni.

Hurwitz, Stephan. 1982. Kriminologi. Diterjemahkan oleh N. L. Moeljatno. Jakarta: Bina Aksara.

Idris, M., S. Aprita, dan M. Nurlani. "Pengaturan dan Penegakan Hukum Kejahatan Dunia Maya (Cybercrime): Harmonisasi Revisi Undang-Undang ITE dan KUHP."

Ismail, Katsuar. 2022. "Kebebasan Pendapat Hakim dalam Perbedaan Pendapat Dissenting Opinion pada Sebuah Putusan: Studi Perbandingan Indonesia dan Amerika Serikat."

Kelsen, Hans. 1967. Pure Theory of Law. Translated by Max Knight. Berkeley: University of California Press.

Kurniawan, Y. I., A. Rahmawati, N. Chasanah, dan A. Hanifa. 2019. "Application for Determining the Modality Preference of Student Learning." Journal of Physics: Conference Series, Vol. 1367, No. 1.

Muliadi, S. 2012. "Aspek Kriminologis dalam Penanggulangan Kejahatan." Fiat Justitia: Jurnal Ilmu Hukum, Vol. 6, No. 1.

Prakoso, A. 2023. "Kajian Viktimologi dalam Tindak Pidana Penggelapan pada Perusahaan Pembiayaan." Sivis Pacem, Vol. 1, No. 1.

Raharjo, Agus. 2002. Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: Citra Aditya Bakti.

Setiawan, Deris. 2005. Sistem Keamanan Komputer. Jakarta: PT Elex Media Komputindo.

Sihombing, A. dan Y. Nuraeni. 2022. "Korban Perkosaan Ditinjau dari Viktimologi dalam Tindak Pidana Kejahatan Perkosaan." Pakuan Justice Journal of Law, Vol. 3, No. 2.

Silalahi, R. S. 2025. "Analisis Hukum Tindak Pidana Cyber Data Breach di Era Digital Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (Studi Putusan Nomor 2447/Pid.Sus/2024/PN Mdn)." Vol. 4, No. 9, hlm. 2425–2440.

Soepraptomo, Heru. 2000. Peranan Komputer dalam Industri dan Pengaruhnya terhadap Bidang Hukum. Bandung: Alumni.

Soesilo, R. 1985. Kriminologi: Pengetahuan tentang Sebab-Sebab Kejahatan. Bogor: Politeia.

Suseno, Sigid. 2012. Yurisdiksi Tindak Pidana Siber. Bandung: Refika Aditama.

Thantawi. 2014. "Perlindungan Korban Tindak Pidana *Cyber crime* dalam Sistem Hukum Pidana Indonesia." Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala, Vol. 2, No. 1.

Wahid, Abdul dan Mohammad Labib. 2005. Kejahatan Mayantara (*Cyber crime*). Bandung: Refika Aditama.

ISSN 2798-3471 (Cetak)
ISSN 2798-3641 (Online)