Volume 4 Number 1 (2026)
January-June 2026
Page: 1177-1188

E-ISSN: 2986-6502
DOI: 10.37680/ssa.10323

Social Science Academic

Cybercrime di Indonesia, Analisis Kriminologi terhadap Ancaman Kejahatan Digital

Neneng Pratiwi Zahra[1], Bima Guntara[1]

[1] Universitas Pamulang, Indonesia

Received: 19/05/2026 Revised: 22/06/2026 Accepted: 14/07/2026

Abstract

The development of information and communication technology has spurred digital transformation in Indonesia, but it has also increased various forms of cybercrime that threaten the security of individuals, businesses, and the state. This study aims to analyze cybercrime in Indonesia from a criminological perspective by identifying the causative factors, the characteristics of the crime, and efforts to counter it. The research uses normative legal methods, including a statutory and conceptual approach. Data were obtained through literature studies of laws and regulations, books, scientific articles, and reports from related institutions, and were analyzed qualitatively and descriptively. The results of the study show that the increase in cybercrime is influenced by technological advances, high internet usage, low digital literacy, weak personal data protection, and opportunities for anonymity in cyberspace. The most dominant forms of crime include online fraud, personal data theft, hacking, malware spread, and ransomware. From a criminological perspective, digital crime is shaped by interactions among perpetrators, victims, and the digital environment, which provides opportunities to commit crimes with relatively low risk. Therefore, countering cybercrime requires a comprehensive approach that strengthens regulations, enhances law enforcement, increases digital literacy, strengthens cybersecurity systems, and fosters collaboration among the government, law enforcement officials, the private sector, and the community to create a safe and sustainable digital ecosystem.

Keywords

Cybercrime, Kriminologi, Kejahatan Digital, Penegakan Hukum, Keamanan Siber

Corresponding Author
Neneng Pratiwi Zahra
Universitas Pamulang, Indonesia; dosen03049@unpam.ac.id

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan masyarakat Indonesia. Digitalisasi tidak hanya memberikan kemudahan dalam aktivitas ekonomi, pendidikan, pemerintahan, dan komunikasi, tetapi juga menciptakan ruang baru yang dimanfaatkan oleh pelaku kejahatan untuk melakukan tindak pidana berbasis teknologi informasi (cybercrime). Karakteristik dunia siber yang bersifat tanpa batas (borderless), cepat, dan anonim menyebabkan kejahatan digital berkembang lebih kompleks dibandingkan kejahatan konvensional. Kondisi tersebut menuntut adanya pembaruan kebijakan

hukum pidana dan pendekatan kriminologi yang mampu menjelaskan dinamika kejahatan di ruang digital (Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, 2024).

Indonesia merupakan salah satu negara dengan jumlah pengguna internet terbesar di dunia. Meningkatnya penetrasi internet dan penggunaan perangkat digital berbanding lurus dengan meningkatnya ancaman kejahatan siber, seperti penipuan daring, pencurian identitas, peretasan sistem elektronik, penyebaran malware, hingga serangan ransomware. Berbagai kasus tersebut tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan data pribadi, stabilitas sistem elektronik, serta kepercayaan masyarakat terhadap ekosistem digital. Oleh karena itu, cybercrime telah menjadi isu strategis yang memerlukan perhatian serius dari pemerintah, aparat penegak hukum, akademisi, dan Masyarakat (A. P. J. I. Indonesia, 2024)

Dalam perspektif hukum pidana, cybercrime merupakan bentuk tindak pidana yang memiliki karakteristik berbeda dengan kejahatan konvensional. Pelaku dapat menjalankan aksinya tanpa harus berada di lokasi yang sama dengan korban, bahkan sering kali melintasi yurisdiksi berbagai negara. Kondisi tersebut menyebabkan proses pembuktian, penelusuran pelaku, serta penegakan hukum menjadi lebih kompleks. Oleh sebab itu, Indonesia telah mengatur berbagai ketentuan mengenai tindak pidana siber melalui Undang-Undang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya sebagai instrumen hukum utama dalam penanggulangan kejahatan digital (Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, 2024)

Kriminologi memandang bahwa kejahatan tidak hanya dipengaruhi oleh faktor individu pelaku, tetapi juga oleh kondisi sosial, ekonomi, budaya, dan lingkungan yang memberikan peluang terjadinya kejahatan. Dalam konteks cybercrime, perkembangan teknologi digital telah menciptakan ruang baru yang memungkinkan pelaku melakukan kejahatan dengan risiko yang relatif lebih rendah dibandingkan kejahatan konvensional. Teori Routine Activity menjelaskan bahwa suatu kejahatan terjadi karena bertemunya pelaku yang termotivasi, sasaran yang sesuai, dan lemahnya pengawasan (capable guardian). Perspektif tersebut relevan untuk menjelaskan meningkatnya kejahatan digital di Indonesia yang dipicu oleh lemahnya literasi digital dan keamanan sistem informasi (Cohen & Felson, 1979)

Selain faktor peluang, cybercrime juga dipengaruhi oleh perkembangan ekonomi digital yang semakin pesat. Aktivitas perdagangan elektronik, layanan keuangan digital, dan penggunaan media sosial membuka ruang interaksi yang luas antara masyarakat dengan teknologi informasi. Di sisi lain, pelaku kejahatan memanfaatkan rendahnya kesadaran masyarakat terhadap keamanan digital melalui berbagai modus, seperti phishing, rekayasa sosial (social engineering), penipuan investasi daring, dan

pencurian data pribadi. Fenomena tersebut menunjukkan bahwa korban cybercrime berasal dari berbagai lapisan masyarakat tanpa memandang usia maupun tingkat Pendidikan (Clarke, 1997)

Pemerintah Indonesia telah melakukan berbagai upaya dalam menanggulangi cybercrime melalui penguatan regulasi, pembentukan lembaga keamanan siber, peningkatan kapasitas aparat penegak hukum, serta kerja sama internasional. Badan Siber dan Sandi Negara (BSSN), Kepolisian Negara Republik Indonesia, dan Kementerian Komunikasi dan Digital memiliki peran strategis dalam mencegah, mendeteksi, dan menangani berbagai insiden siber. Namun demikian, efektivitas penanggulangan cybercrime masih menghadapi berbagai tantangan, antara lain perkembangan teknologi yang sangat cepat, keterbatasan sumber daya manusia, serta karakter kejahatan siber yang bersifat lintas negara (Negara, 2024)

Dari perspektif kriminologi, penanggulangan cybercrime tidak cukup hanya mengandalkan pendekatan penal melalui pemidanaan pelaku. Upaya nonpenal, seperti peningkatan literasi digital, edukasi keamanan informasi, perlindungan data pribadi, serta penguatan sistem keamanan siber juga memiliki peran yang sangat penting dalam mengurangi peluang terjadinya kejahatan. Pendekatan yang komprehensif tersebut sejalan dengan konsep kebijakan kriminal (criminal policy) yang mengintegrasikan sarana hukum pidana dengan kebijakan sosial untuk mencegah terjadinya kejahatan (Arief, 2017)

Penelitian ini bertujuan menganalisis cybercrime di Indonesia melalui perspektif kriminologi dengan mengkaji faktor-faktor yang memengaruhi terjadinya kejahatan digital, karakteristik cybercrime, serta efektivitas upaya penanggulangannya. Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan kajian hukum pidana dan kriminologi, sekaligus menjadi masukan bagi pembuat kebijakan dalam merumuskan strategi penanggulangan cybercrime yang lebih efektif. Selain itu, hasil penelitian diharapkan dapat memperkaya literatur mengenai kejahatan digital di Indonesia yang terus berkembang seiring dengan kemajuan teknologi informasi (T. Santoso & Zulfa, 2023)

2. METODE

Penelitian ini menggunakan metode penelitian hukum normatif (normative legal research), yaitu penelitian yang menempatkan hukum sebagai norma atau kaidah yang berlaku dalam masyarakat. Pendekatan ini dipilih karena penelitian berfokus pada analisis ketentuan hukum yang mengatur kejahatan siber (cybercrime), konsep-konsep kriminologi, serta kebijakan penanggulangan kejahatan digital di Indonesia. Penelitian hukum normatif bertujuan mengkaji asas hukum, sinkronisasi peraturan perundang-undangan, doktrin, serta teori hukum yang berkaitan dengan objek penelitian sehingga dapat memberikan argumentasi hukum yang sistematis terhadap permasalahan yang dikaji (Marzuki,

2021)

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan peraturan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan peraturan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang mengatur tindak pidana siber, antara lain Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, serta peraturan lain yang berkaitan dengan perlindungan data pribadi dan keamanan siber. Sementara itu, pendekatan konseptual digunakan untuk mengkaji teori-teori kriminologi yang menjelaskan penyebab, karakteristik, dan upaya penanggulangan kejahatan digital berdasarkan pandangan para ahli hukum dan kriminologi (Marzuki, 2005)

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan tindak pidana siber, sedangkan bahan hukum sekunder diperoleh dari buku-buku hukum pidana, kriminologi, artikel jurnal ilmiah, hasil penelitian terdahulu, serta laporan resmi yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), Kepolisian Negara Republik Indonesia, dan lembaga internasional. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, serta sumber referensi lain yang berfungsi memberikan penjelasan terhadap bahan hukum primer dan sekunder (Soekanto & Mamudji, 2019)

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) dengan menelusuri berbagai literatur yang relevan, baik dalam bentuk buku, jurnal ilmiah, peraturan perundang-undangan, maupun dokumen resmi yang memiliki keterkaitan dengan cybercrime dan kriminologi. Seluruh bahan hukum yang diperoleh kemudian diklasifikasikan berdasarkan pokok bahasan untuk memudahkan proses identifikasi norma hukum, teori, serta konsep yang relevan dengan permasalahan penelitian. Tahapan ini bertujuan menghasilkan data yang valid, sistematis, dan mampu mendukung analisis secara komprehensif terhadap fenomena kejahatan digital di Indonesia (Muhaimin, 2020)

Analisis bahan hukum dilakukan secara deskriptif kualitatif, yaitu dengan menguraikan dan menginterpretasikan ketentuan hukum, teori kriminologi, serta hasil penelitian terdahulu secara sistematis untuk memperoleh jawaban atas rumusan masalah penelitian. Analisis dilakukan melalui proses inventarisasi, klasifikasi, interpretasi, dan penarikan kesimpulan secara deduktif, yakni berangkat dari ketentuan hukum dan teori yang bersifat umum menuju pembahasan terhadap fenomena cybercrime di Indonesia. Dengan metode tersebut diharapkan penelitian ini mampu menghasilkan rekomendasi yang relevan bagi pengembangan kebijakan hukum pidana dan strategi penanggulangan kejahatan digital dari perspektif kriminologi (Ibrahim, 2019)

3. HASIL DAN PEMBAHASAN

A. Dinamika Cybercrime di Indonesia

Perkembangan teknologi digital telah mengubah pola kehidupan masyarakat Indonesia secara signifikan (Erbito et al., 2025). Pemanfaatan internet dalam berbagai bidang, seperti perdagangan elektronik, layanan keuangan digital, pendidikan, hingga administrasi pemerintahan, memberikan berbagai kemudahan dalam aktivitas sehari-hari. Namun, di balik kemajuan tersebut muncul risiko penyalahgunaan teknologi oleh pihak-pihak yang memanfaatkannya untuk melakukan tindak pidana (Putra, 2023). Cybercrime berkembang menjadi salah satu bentuk kejahatan yang memiliki karakteristik berbeda dengan kejahatan konvensional karena dilakukan melalui sistem elektronik dan jaringan internet.

Karakteristik utama cybercrime terletak pada kemampuannya melintasi batas wilayah negara, dilakukan secara anonim, serta memanfaatkan perkembangan teknologi yang sangat cepat (M. S. I. Wibowo et al., 2024). Pelaku tidak harus berada pada lokasi yang sama dengan korban sehingga proses identifikasi maupun penegakan hukum menjadi lebih kompleks. Kondisi tersebut menyebabkan aparat penegak hukum menghadapi tantangan baru dalam proses penyidikan, pembuktian, dan penuntutan perkara pidana siber (M. S. I. Wibowo et al., 2024). Kompleksitas ini menunjukkan bahwa pendekatan hukum pidana saja belum cukup untuk mengatasi perkembangan kejahatan digital (Cahyono et al., 2025).

B. Bentuk-Bentuk Cybercrime yang Berkembang

Hasil kajian menunjukkan bahwa bentuk cybercrime di Indonesia semakin beragam seiring berkembangnya teknologi informasi (Syah & Hidayah, 2024). Modus yang sering ditemukan meliputi penipuan daring (online fraud), pencurian identitas (identity theft), peretasan (hacking), penyebaran perangkat lunak berbahaya (malware), serangan ransomware, hingga penyalahgunaan data pribadi (Awar, 2023). Setiap bentuk kejahatan tersebut memiliki karakteristik tersendiri, namun seluruhnya memanfaatkan kelemahan sistem keamanan maupun kelalaian pengguna internet. Oleh karena itu, keamanan siber tidak lagi hanya menjadi tanggung jawab pemerintah, melainkan juga seluruh pengguna teknologi digital (Ramadhan & Aminah, 2024) .

Fenomena penipuan daring merupakan bentuk cybercrime yang paling mudah ditemui dalam kehidupan Masyarakat (Sari, 2023). Pelaku memanfaatkan media sosial, aplikasi pesan instan, hingga platform perdagangan elektronik untuk memperoleh keuntungan ekonomi melalui manipulasi informasi (Nugroho & Marlina, 2024). Modus yang digunakan terus berkembang mengikuti perubahan teknologi sehingga masyarakat sering kali kesulitan membedakan transaksi yang sah dengan tindakan penipuan. Kondisi tersebut menunjukkan bahwa rendahnya literasi

digital masih menjadi faktor yang memperbesar peluang terjadinya viktimisasi (Fauzan & Wulandari, 2025).

Tabel 1. Klasifikasi Umum Bentuk Cybercrime

Jenis Cybercrime	Karakteristik	Dampak
Penipuan Daring (Online Fraud)	Manipulasi transaksi elektronik melalui media digital, seperti marketplace, media sosial, atau aplikasi pesan instan dengan tujuan memperoleh keuntungan secara melawan hukum.	Kerugian finansial bagi korban, hilangnya kepercayaan terhadap transaksi elektronik, serta meningkatnya risiko kejahatan digital.
Phishing	Upaya memperoleh informasi sensitif, seperti username, password, PIN, atau data kartu kredit melalui tautan, situs web, email, atau pesan palsu yang menyerupai layanan resmi.	Kebocoran data pribadi, pembobolan rekening, penyalahgunaan akun digital, dan pencurian identitas.
Hacking	Akses tanpa izin terhadap sistem komputer, jaringan, atau basis data dengan mengeksploitasi celah keamanan untuk mengambil, mengubah, atau merusak informasi.	Gangguan operasional sistem informasi, kebocoran data rahasia, kerusakan infrastruktur digital, serta kerugian ekonomi dan reputasi.
Malware/Ransomware	Penyebaran perangkat lunak berbahaya yang bertujuan merusak sistem, mencuri data, atau mengenkripsi data korban sehingga tidak dapat diakses tanpa membayar tebusan.	Kehilangan data, terhentinya aktivitas operasional, kerugian ekonomi, serta meningkatnya biaya pemulihan sistem.
Identity Theft (Pencurian Identitas)	Penyalahgunaan identitas digital seseorang dengan memanfaatkan data pribadi, seperti Nomor Induk Kependudukan (NIK), akun media sosial, atau informasi keuangan tanpa persetujuan pemiliknya.	Penyalahgunaan akun dan dokumen, penipuan atas nama korban, kerugian finansial, serta gangguan terhadap privasi dan reputasi korban.

Sumber : Diolah oleh penulis berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Convention on Cybercrime (Budapest Convention, 2001); dan literatur hukum siber.

C. Analisis Kriminologi terhadap Cybercrime

Dalam perspektif kriminologi, cybercrime tidak hanya dipandang sebagai pelanggaran terhadap hukum pidana, tetapi juga sebagai fenomena sosial yang dipengaruhi oleh berbagai factor (Wall, 2007). Perkembangan teknologi menciptakan ruang interaksi baru yang memungkinkan pelaku melakukan tindak pidana dengan risiko yang relatif lebih kecil dibandingkan kejahatan konvensional. Anonimitas, kemudahan akses teknologi, serta lemahnya pengawasan menjadi faktor yang meningkatkan peluang terjadinya kejahatan digital. Oleh karena itu, cybercrime perlu dianalisis melalui pendekatan multidisipliner yang memadukan aspek hukum, sosial, psikologi, dan teknologi (Holt & Bossler, 2018).

Dari sudut pandang teori Routine Activity, cybercrime terjadi ketika terdapat tiga unsur utama, yaitu pelaku yang memiliki motivasi, target yang sesuai, serta lemahnya sistem pengawasan digital (Cohen & Felson, 1979). Dalam konteks Indonesia, tingginya penggunaan internet dan media sosial menciptakan banyak sasaran potensial bagi pelaku kejahatan. Rendahnya pemahaman masyarakat mengenai keamanan digital turut memperbesar peluang terjadinya tindak pidana. Dengan demikian, pencegahan cybercrime tidak hanya bergantung pada penegakan hukum, tetapi juga pada peningkatan kapasitas masyarakat dalam melindungi data dan aktivitas digitalnya (Maulana & Nurhayati, 2024).

Selain faktor peluang, motif ekonomi menjadi salah satu pendorong utama terjadinya cybercrime (Holt & Freilich, 2020). Pelaku memanfaatkan teknologi untuk memperoleh keuntungan finansial melalui berbagai cara yang sulit dideteksi secara cepat. Perkembangan mata uang digital, sistem pembayaran elektronik, dan transaksi lintas negara semakin memperluas ruang gerak pelaku. Hal tersebut menunjukkan bahwa kejahatan digital berkembang seiring dengan perubahan struktur ekonomi berbasis teknologi (B. Santoso & Anggraeni, 2025).

D. Tantangan Penegakan Hukum

Penegakan hukum terhadap cybercrime menghadapi berbagai kendala, terutama terkait pembuktian digital dan identifikasi pelaku (Hamdan, 2022). Barang bukti elektronik memiliki karakteristik yang berbeda dengan alat bukti konvensional sehingga memerlukan prosedur khusus dalam proses penyitaan, pemeriksaan, dan analisis forensik digital (Ganarsih, 2021). Selain itu, banyak pelaku memanfaatkan server yang berada di luar negeri sehingga menimbulkan persoalan yurisdiksi. Kondisi tersebut menuntut kerja sama internasional yang lebih efektif dalam penanganan kejahatan siber (Agusman, 2022).

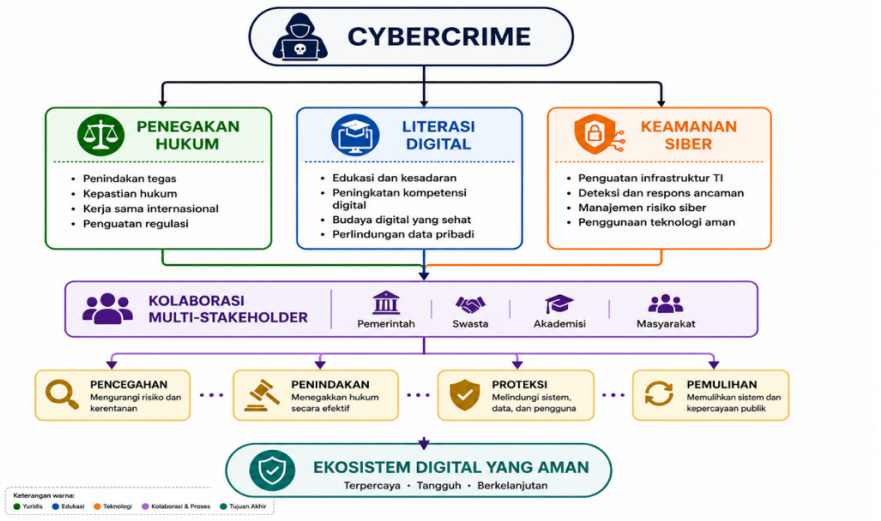
Tantangan lain adalah kecepatan perkembangan teknologi yang sering kali lebih cepat dibandingkan pembentukan regulasi (A. Wibowo, 2023). Modus operandi pelaku cybercrime terus berubah mengikuti inovasi teknologi, sementara aparat penegak hukum memerlukan waktu

untuk menyesuaikan kemampuan teknis maupun perangkat hukumnya. Akibatnya, terdapat kesenjangan antara perkembangan kejahatan digital dengan kapasitas penegakan hukum. Oleh karena itu, pembaruan regulasi dan peningkatan kompetensi aparat menjadi kebutuhan yang tidak dapat diabaikan (Simarmata, 2024).

E. Strategi Penanggulangan Cybercrime

Penanggulangan cybercrime memerlukan pendekatan yang bersifat komprehensif melalui kebijakan penal dan nonpenal (Arief, 2010). Pendekatan penal diwujudkan melalui penerapan hukum pidana terhadap pelaku sebagai bentuk perlindungan terhadap masyarakat. Sementara itu, pendekatan nonpenal dilakukan melalui edukasi keamanan digital, peningkatan literasi digital, penguatan sistem keamanan informasi, dan pembangunan budaya sadar siber. Sinergi kedua pendekatan tersebut diyakini lebih efektif dibandingkan hanya mengandalkan pemidanaan (Djumadi, 2023).

Kolaborasi antara pemerintah, aparat penegak hukum, sektor swasta, akademisi, dan masyarakat menjadi faktor penting dalam membangun ekosistem digital yang aman (Argama, 2023). Dunia usaha memiliki tanggung jawab meningkatkan keamanan sistem informasi, sedangkan pemerintah berperan menyusun regulasi dan kebijakan yang adaptif terhadap perkembangan teknologi. Di sisi lain, masyarakat perlu meningkatkan kesadaran mengenai pentingnya perlindungan data pribadi dan keamanan akun digital (Dewi, 2021). Pendekatan kolaboratif tersebut akan memperkuat upaya pencegahan sekaligus penanggulangan cybercrime secara berkelanjutan (Yusuf & Qomari, 2022).



Bagan 1. Kerangka Penanggulangan Cybercrime

Berdasarkan hasil analisis tersebut, dapat dipahami bahwa cybercrime merupakan bentuk kejahatan yang berkembang seiring dengan kemajuan teknologi dan digitalisasi Masyarakat ((BSSN), 2024). Pendekatan kriminologi menunjukkan bahwa faktor individu, lingkungan,

kesempatan, dan perkembangan teknologi saling berinteraksi dalam mendorong terjadinya kejahatan digital (Makarao & Tolib, 2022). Oleh karena itu, kebijakan penanggulangan cybercrime harus dirancang secara terpadu melalui penguatan regulasi, peningkatan kapasitas penegak hukum, pembangunan literasi digital, serta pengembangan sistem keamanan siber (M. A. R. Indonesia, 2020). Dengan strategi yang terintegrasi, upaya pencegahan dan penindakan terhadap cybercrime di Indonesia diharapkan menjadi lebih efektif dan mampu memberikan perlindungan yang optimal bagi Masyarakat (A. S. Indonesia, 2024).

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa cybercrime di Indonesia merupakan bentuk kejahatan yang berkembang seiring dengan pesatnya transformasi digital dan meningkatnya pemanfaatan teknologi informasi dalam berbagai aspek kehidupan masyarakat. Karakteristik cybercrime yang bersifat lintas batas negara (borderless), memanfaatkan anonimitas, serta didukung oleh kemajuan teknologi menjadikan kejahatan ini lebih kompleks dibandingkan kejahatan konvensional. Bentuk-bentuk cybercrime yang dominan meliputi penipuan daring, phishing, pencurian data pribadi, peretasan, penyebaran malware, dan ransomware, yang tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan informasi, perlindungan data pribadi, dan stabilitas sistem elektronik nasional.

Ditinjau dari perspektif kriminologi, cybercrime dipengaruhi oleh interaksi berbagai faktor, antara lain motivasi pelaku, peluang yang tersedia dalam lingkungan digital, rendahnya literasi digital masyarakat, serta kelemahan sistem keamanan informasi. Fenomena tersebut menunjukkan bahwa perkembangan teknologi telah menciptakan ruang kejahatan baru yang memungkinkan pelaku melakukan tindak pidana dengan tingkat risiko yang relatif rendah. Oleh karena itu, penanggulangan cybercrime tidak dapat hanya mengandalkan pendekatan represif melalui hukum pidana, tetapi juga memerlukan strategi preventif yang berorientasi pada peningkatan kesadaran masyarakat, penguatan keamanan siber, perlindungan data pribadi, serta peningkatan kapasitas aparat penegak hukum dalam bidang forensik digital dan investigasi kejahatan siber.

Dengan demikian, upaya penanggulangan cybercrime di Indonesia harus dilaksanakan secara komprehensif melalui sinergi antara pemerintah, aparat penegak hukum, sektor swasta, akademisi, dan masyarakat. Penguatan regulasi yang adaptif terhadap perkembangan teknologi, peningkatan literasi digital, kerja sama nasional maupun internasional, serta pemanfaatan teknologi keamanan siber menjadi elemen penting dalam membangun sistem perlindungan yang efektif terhadap ancaman kejahatan digital. Pendekatan yang terpadu tersebut diharapkan mampu menciptakan ekosistem digital yang aman, meningkatkan kepercayaan masyarakat terhadap ruang siber, serta mendukung

terwujudnya sistem penegakan hukum yang responsif terhadap dinamika perkembangan cybercrime di Indonesia.

REFERENCE

(BSSN), B. S. dan S. N. (2024). *Indeks Kematangan Keamanan Informasi Indonesia Tahun 2024*. BSSN RI.

Agusman, D. D. (2022). Yurisdiksi dan Kerja Sama Internasional dalam Penanganan Kejahatan Siber Transnasional: Perspektif Hukum Indonesia. *Jurnal Hukum Internasional*, *18*(2), 155–158.

Argama, R. (2023). Tata Kelola Keamanan Siber: Pendekatan Kolaboratif Multipihak (Multi-Stakeholder) dalam Menghadapi Ancaman Digital. *Jurnal Kebijakan Publik*, *14*(2), 110–112.

Arief, B. N. (2010). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Kencana Prenada Media Group.

Arief, B. N. (2017). *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Kencana.

Awar, A. M. T. (2023). Tipologi Kejahatan Siber dalam Perspektif Undang-Undang ITE: Analisis Klasifikasi dan Ancaman terhadap Keamanan Data Pribadi. *Mimbar Hukum*, *35*(3), 41.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law (DJH)*, *1*(1), 15–18.

Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies* (2nd Edition). Harrow and Heston.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Dewi, S. (2021). *Hukum Teknologi Informasi (Information Technology Law)*. PT Refika Aditama.

Djumadi, F. X. (2023). Pendekatan Penal dan Non-Penal dalam Penanggulangan Kejahatan Siber di Indonesia. *Jurnal Hukum Pidana Indonesia*, *5*(1), 45–48.

Erbito, Y., Solikhin, & Purwani, T. (2025). Analisis dan Dampak Ekonomi Digital di Indonesia. *Mount Hope Economic Journal (MEGA)*, *3*(2), 224–225.

Fauzan, A., & Wulandari, R. (2025). Pengaruh Rendahnya Literasi Digital terhadap Viktimisasi Kejahatan Siber pada Masyarakat Indonesia. *Jurnal Sosiologi Digital*, *8*(1), 55–58.

Ganarsih, Y. (2021). Kekuatan Pembuktian Alat Bukti Elektronik dalam Sistem Hukum Acara Pidana Indonesia. *Jurnal Mimbar Hukum*, *33*(1), 88–90.

Hamdan. (2022). Tantangan Penegakan Hukum Pidana terhadap Kejahatan Siber (Cybercrime) di Indonesia. *Jurnal Hukum Ius Quia Iustum*, *29*(2), 245–247.

Holt, T. J., & Bossler, A. (2018). *The Routledge Handbook of Technology, Crime and Justice*. Routledge.

Holt, T. J., & Freilich, R. D. (2020). *Transnational Cybercrime and Terrorism: Motivations, Methods, and Opportunities*. Routledge.

Ibrahim, J. (2019). *Teori dan Metodologi Penelitian Hukum Normatif*. Bayu Media Publishing.

Indonesia, A. P. J. I. (2024). *Survei Penetrasi Internet Indonesia 2024*.

Indonesia, A. S. (2024). *Roadmap Keamanan Siber Nasional 2025-2029: Menuju Ekosistem Digital yang Tangguh*. Asosiasi Siber Indonesia.

Indonesia, M. A. R. (2020). *Pedoman Penyelesaian Sengketa Perbankan Syariah*. Mahkamah Agung RI.

Makarao, E., & Tolib. (2022). *Kriminologi: Teori, Kebijakan, dan Penanggulangan Kejahatan Siber*. Kencana.

Marzuki, P. M. (2005). *Penelitian Hukum*. Kencana.

Marzuki, P. M. (2021). *Penelitian Hukum* (Edisi Revisi). Kencana.

Maulana, A. R., & Nurhayati, S. (2024). Analisis Viktimisasi Kejahatan Siber di Indonesia: Pendekatan Teori Aktivitas Rutin dan Literasi Digital. *Jurnal Kriminologi Dan Kepolisian Indonesia*, *15*(2), 112–115.

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.

Negara, B. S. dan S. (2024). *Lanskap Keamanan Siber Indonesia 2024*. Badan Siber dan Sandi Negara.

Nugroho, F., & Marlina, L. (2024). Eksploitasi Media Sosial dan E-Commerce dalam Tindak Pidana Penipuan Daring: Tinjauan Kriminologis dan Hukum. *Jurnal Hukum & Pembangunan*, *54*(1), 120–122.

Putra, G. R. A. (2023). Tipologi Kejahatan Siber dan Penanggulangannya di Indonesia: Klasifikasi, Modus Operandi, dan Evaluasi Kerangka Hukum dalam Menghadapi Ancaman Digital Kontemporer. *Jurnal Yudisial*, *7*(7), 301.

Ramadhan, R., & Aminah, S. (2024). Tata Kelola Keamanan Siber di Indonesia: Pendekatan Multi-Stakeholder dalam Mencegah Kejahatan Digital. *Jurnal Kebijakan Dan Administrasi Publik*, *28*(2), 178–180.

Santoso, B., & Anggraeni, D. (2025). Ekonomi Digital dan Transformasi Kejahatan Siber: Analisis Motif Ekonomi dalam Cybercrime Kontemporer. *Jurnal Ekonomi Dan Hukum Bisnis*, *9*(1), 78–82.

Santoso, T., & Zulfa, E. A. (2023). *Kriminologi*. Rajawali Pers.

Sari, D. K. (2023). Penipuan Daring (Online Fraud) sebagai Bentuk Kejahatan Siber yang Dominan di Indonesia: Analisis Modus dan Dampak Sosial-Ekonomi. *Jurnal Kriminologi Indonesia*, *19*(2), 89–91.

Simarmata, R. (2024). Urgensi Peningkatan Kapasitas Aparat Penegak Hukum dan Pembaruan Regulasi dalam Menghadapi Kejahatan Siber. *Jurnal Hukum Pidana Dan Kriminologi*, *5*(1), 33–36.

Soekanto, S., & Mamudji, S. (2019). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers.

Syah, M. I., & Hidayah, N. (2024). Evolusi Modus Operandi Kejahatan Siber di Indonesia: Studi Terhadap Tren Cybercrime Pasca Pandemi. *Jurnal Hukum Pidana Dan Penanggulangannya*, *12*(1), 45–47.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (2024).

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Open University Press.

Wibowo, A. (2023). Kesenjangan Regulasi dan Perkembangan Teknologi dalam Penanggulangan Cybercrime di Era Disrupsi. *Jurnal Rechts Vinding*, *12*(1), 45–48.

Wibowo, M. S. I., Munawar, A., & Hidayatullah. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. *Rewang Rencang: Jurnal Hukum Lex Generalis*, *5*(7), 8–12.

Yusuf, M., & Qomari, N. (2022). Strategi Preventif dan Represif dalam Penanggulangan Cybercrime di Indonesia: Sebuah Tinjauan Holistik. *Jurnal Rechts Vinding*, *11*(3), 305–308.