

**CYBERCRIME DAN MEDIA SOSIAL ANALIS HUKUM TERHADAP
TREN PENINGKATAN TINDAK PIDANA DI ERA DIGITAL
CYBERCRIME AND SOCIAL MEDIA A LEGAL ANALYSIS OF THE
RISING TREND OF OFFENCES IN THE DIGITAL ERA**

Alejandro Morion Ruben Thomas dan Happy Yulia Anggraeni

Fakultas Hukum Universitas Islam Nusantara Bandung

Korespondensi Penulis : pionaregod@gmail.com, happy.anggraeni@uninus.ac.id

Citation Structure Recommendation :

Thomas, Alejandro Morion Ruben dan Happy Yulia Anggraeni. *Cybercrime dan Media Sosial Analisis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.7 (2025).

ABSTRAK

Meningkatnya kasus kejahatan siber di media sosial menandai lemahnya perlindungan hukum dan kesiapan aparat terhadap dinamika teknologi digital. Penelitian ini menunjukkan tren kenaikan signifikan pada tindak pidana seperti pencurian data, penipuan daring dan peretasan akun, seiring rendahnya literasi digital masyarakat dan lambannya adaptasi regulasi. Analisis hukum terhadap UU ITE dan KUHP memperlihatkan kekosongan norma terhadap modus kejahatan baru seperti *deepfake* dan *social engineering*. Diperlukan pembaruan regulasi berbasis *technology forecasting*, peningkatan kapasitas digital forensik aparat, serta literasi keamanan siber terpadu untuk menekan eskalasi kejahatan digital.

Kata Kunci: Kejahatan Siber, Literasi Digital, Penegakan Hukum

ABSTRACT

The increase in cybercrime cases on social media highlights the weakness of legal protection and the preparedness of authorities in response to the dynamics of digital technology. This study shows a significant upward trend in crimes such as data theft, online fraud, and account hacking, along with low digital literacy among the public and slow regulatory adaptation. A legal analysis of the Electronic Information and Transactions Law (ITE Law) and the Criminal Code (KUHP) reveals a lack of norms addressing new modes of crime such as deepfakes and social engineering. Regulatory updates based on technology forecasting, increased digital forensics capacity among authorities, and integrated cybersecurity literacy are needed to curb the escalation of digital crime.

Keywords: Cybercrime, Digital Literacy, Law Enforcement

A. PENDAHULUAN

Pada era digital yang semakin meluas, penggunaan platform media sosial telah menjadi bagian integral dari kehidupan sehari-hari masyarakat global. Interaksi daring melalui perangkat pintar, aplikasi jejaring sosial dan layanan komunikasi berbasis internet memungkinkan komunikasi instan, penyebaran informasi massal dan koneksi lintas batas secara mudah. Namun demikian, kemajuan teknologi tersebut juga membuka ruang bagi penyalahgunaan dan eksploitasi termasuk munculnya berbagai bentuk kejahatan siber (*cybercrime*) yang memanfaatkan media sosial sebagai alat maupun objeknya (*Impact of Cybercrimes on Social Media Platforms Threats and Consequences, 2024*).¹ Fenomena ini menjadi penting untuk ditelaah dari sisi hukum, karena struktur tradisional tindak pidana tidak sepenuhnya siap menghadapi karakteristik kejahatan yang terjadi di ruang digital. Regulasi, penegakan dan kerja sama internasional menjadi faktor krusial dalam merespon perkembangan ini.²

Seiring dengan peningkatan penggunaan media sosial, muncul modus-operandi baru tindak pidana yang sebelumnya sulit dibayangkan dalam konteks konvensional. Contohnya, pelaku dapat memanfaatkan fitur platform untuk melakukan phishing, penipuan identitas, penyebaran ujaran kebencian, hingga manipulasi konten secara kolektif (*The Dark Side of Social Networking Sites A Review of Cybercrime, 2023*).³ Sifat media sosial yang mudah diakses, berefek viral dan anonim memberikan kesempatan bagi kejahatan siber berkembang dengan skala dan kecepatan yang jauh melampaui kejahatan tradisional. Kondisi ini menimbulkan tantangan besar bagi aparat penegak hukum: dari segi identifikasi pelaku, penanganan bukti digital, hingga pelaksanaan yurisdiksi antar negara. Dalam konteks Indonesia, regulasi harus mampu menyesuaikan dengan dinamika tersebut agar tidak tertinggal dari perkembangan kejahatan siber.⁴

¹ A. Syaputra dan S. Malik, *Efektivitas UU ITE dalam Penanggulangan Cybercrime Berbasis Media Sosial di Indonesia*, Jurnal Hukum Digital Nusantara, Vol.6, No.4 (2024), p.211–27.

² L. D. Astari, *Kebijakan Penegakan Hukum terhadap Kejahatan Siber di Indonesia*, Jurnal Kriminologi Indonesia, Vol.17, No.1 (2021), p.73–86.

³ Dinda A. H. dan Muhamad H. S., *Perlindungan Hukum terhadap Serangan Siber: Tinjauan atas Kebijakan dan Regulasi Terbaru*, CAUSA: Jurnal Hukum dan Kewarganegaraan, Vol.1, No.5 (November 2023).

⁴ Muhammad Abdullah, dkk., *Evolution Cybercrime - Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data*, Analytics, Vol.4, No.3 (September 2025), p.25.

Dalam konteks nasional, negara Indonesia menunjukkan bahwa meskipun telah terdapat kerangka regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan implementasi baru dalam KUHP yang diperbarui, keberhasilan penegakan hukum terhadap kejahatan siber melalui media sosial masih terbatas (Andreas, 2025).⁵ Kajian empiris menunjukkan bahwa banyak kasus kejahatan siber yang melibatkan media sosial tidak hanya melanggar sanksi delik elektronik, tetapi juga berdampak langsung terhadap keamanan data pribadi, reputasi dan stabilitas sosial. Sementara itu, kapasitas institusi penegakan dan sistem pengaduan masih menghadapi kendala teknis dan regulatif. Hal ini menegaskan bahwa kajian hukum mutlak diperlukan untuk mengevaluasi efektivitas regulasi, prosedur investigasi dan pemutakhiran sistem penegakan hukum di era digital.⁶

Salah satu kasus yang pernah terjadi yakni kasus penipuan APK (*Sniffing/Phishing*). Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri membongkar praktik pengelabuan (*phising*) melalui pengiriman berkas paker aplikasi android (*application package file/APK*) modifikasi dan tautan (*link*) ilegal. Para pelaku terdapat dari berbagai daerah seperti Palembang, Makassar dan Banyuwangi. Selama menjalankan kejahatannya, para pelaku berhasil menguras 493 rekening bank milik korban. Para pelaku yang menjadi developer APK dikenakan Pasal 46 ayat (1), (2) dan (3) jo Pasal 30 ayat (1), (2) dan (3) UU ITE terkait akses ilegal (*illegal access*), Pasal 48 ayat (1) jo Pasal 32 ayat (1) UU ITE untuk modifikasi informasi & dokumen elektronik, Pasal 50 jo Pasal 34 ayat (1) UU ITE atas distribusi & menjual perangkat lunak (*software*) ilegal, serta Pasal 3, Pasal 5 dan Pasal 10 UU TPPU. Pelaku diancam hukuman paling lama 10 tahun penjara dan/atau denda maksimal Rp10 miliar. Para pelaku dikenakan pasal-pasal dari UU ITE, UU Transfer Dana, UU TPPU dan KUHP.⁷

⁵ Andreas Fransiskus Hutajulu dan Sri Endah Wahyuningsih, *Penegakan Hukum Pidana terhadap Cyber Crime di Indonesia*, Ensiklopedia of Journal Lembaga Penelitian dan Penerbitan Hasil Penelitian Ensiklopedia, Vol.7, No.3 (2025), p.79–89.

⁶ D. Kusnadi dan G. N. Efendi, *Cybercrime and Digital Society in Indonesia: Legal Challenges and Public Discourse*, Adliya: Jurnal Hukum dan Kemanusiaan, Vol.19, No.1 (Juni 2025), p.139–56.

⁷ Alinea.id, *Polisi Bongkar Penipuan Berkedok Chat WA Kurir Paket, 493 Orang Jadi korban*, diakses dari <https://www.alinea.id/nasional/polisi-bongkar-penipuan-berkedok-chat-wa-kurir-paket-b2hKs9JO8>.

Secara global, laporan dan riset terkini mengungkap bahwa kerentanan terhadap kejahatan siber semakin meningkat dalam skala besar. Berdasarkan laporan World Economic Forum, 45% pemimpin organisasi menyebut gangguan operasional akibat serangan siber sebagai salah satu kekhawatiran besar pada 2024.⁸ Hal ini menunjukkan bahwa kerangka hukum nasional tunggal tidak cukup; diperlukan sinergi internasional untuk menghadapi kejahatan yang lintas batas dan bersifat kompleks. Terlebih lagi, indikator global seperti “*Cybercrime Index*” menunjuk bahwa tidak semua negara memiliki tingkat kesiapan yang sama dalam menghadapi ancaman ini (Oxford University, 2024). Oleh karena itu, aspek kerja sama internasional, harmonisasi regulasi dan penyesuaian konsep yurisdiksi menjadi titik penting dalam analisis hukum ini.

Fokus penelitian ini menyoroti peran media sosial sebagai medium yang memfasilitasi terjadinya kejahatan siber baik dari sisi pelaku, korban maupun platform teknologi. Media sosial tidak sekadar menjadi arena interaksi, tetapi juga platform yang memungkinkan pelaku memanfaatkan jaringan besar, automasi, anonimitas, serta algoritma yang memudahkan penyebaran konten berbahaya atau ilegal (Zulyadi, 2025). Pelaksanaan kejahatan melalui media sosial bisa berupa pengedaran konten terlarang, penipuan massal, atau penyalahgunaan data pribadi. Dengan demikian, analisis hukum terhadap media sosial harus memasukkan elemen teknologi, regulasi platform, perilaku pengguna dan mekanisme penegakan hukum.

Berbagai penelitian sebelumnya telah mengkaji fenomena *cybercrime* dan media sosial dari beragam sudut pandang. Namun, kajian-kajian tersebut masih menyisakan ruang kosong yang perlu diisi melalui penelitian ini. Penelitian yang dilakukan oleh Rafli Hukom dan Martinus Hukmu Setiadi (2025) membahas pengaruh media sosial terhadap pola kejahatan di era digital. Penelitian ini menekankan bahwa media sosial telah menjadi sarana utama terjadinya berbagai tindak pidana siber. Penelitian ini menitik beratkan pada aspek kriminologi dan sosiologis.⁹ Selanjutnya, penelitian Harahap dan Zikri (2025) mengkaji *cybercrime* dari perspektif penyalahgunaan identitas digital (*online identity misuse*).

⁸ Ismail Koto, *Cyber Crime According to the ITE Law*, IJRS, Vol.2, No.2 (2021).

⁹ Rafli Hukom dan Martinus Hukmu Setiadi, *Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi*, Perkara : Jurnal Ilmu Hukum dan Politik, Vol.3, No.1 (Maret 2025), p.750–68.

Penelitian ini menguraikan bahwa anonimitas dan fleksibilitas identitas di media sosial membuka peluang besar bagi pelaku untuk melakukan kejahatan seperti *catfishing*, *doxing*, *cyberbullying* dan penipuan daring.¹⁰ Penelitian lain dilakukan oleh Mulyadi, dkk., (2024) yang meninjau penipuan online melalui media sosial dalam perspektif kriminologi.¹¹ Sementara itu, Firdaus (2024) meneliti bahwa *cybercrime* sebagai kejahatan siber di Indonesia yang terus meningkat dari tahun ke tahunnya. Dalam penelitian ini menitikberatkan pada analisis secara yuridis terhadap peningkatan tindak *cybercrime* ditinjau dari perspektif hukum pidana.¹²

Berdasarkan uraian penelitian terdahulu tersebut, dapat disimpulkan bahwa sebagian besar penelitian masih bersifat parsial, baik dengan fokus pada satu jenis kejahatan, satu aspek penegakan hukum, maupun pendekatan non-yuridis. Oleh karena itu, penelitian ini memiliki kebaharuan dengan menghadirkan analisis hukum pidana yang komprehensif terhadap fenomena peningkatan *cybercrime* di media sosial. Penelitian ini tidak hanya memetakan bentuk dan tren kejahatan, tetapi juga mengkaji kesesuaian regulasi, efektivitas penegakan hukum, serta tantangan normatif yang dihadapi hukum pidana Indonesia dalam merespon dinamika kejahatan di era digital.

Penelitian ini bertujuan melakukan analisis hukum mendalam terhadap tren peningkatan tindak pidana yang memanfaatkan media sosial di era digital. Kajian ini akan mencakup identifikasi bentuk-bentuk kejahatan siber yang terkait media sosial, tinjauan regulasi nasional dan internasional, tantangan penegakan hukum termasuk pembuktian bukti digital, yurisdiksi dan kolaborasi lintas negara serta formulasi rekomendasi kebijakan yang adaptif. Melalui pendekatan normatif-analitis, diharapkan penelitian ini dapat memberi kontribusi baik bagi pengembangan kerangka hukum maupun praktek penegakan di Indonesia dan secara global.

¹⁰ Rahma Hayati Harahap dan Muhammad Adfhol Zikri, *Online Identity and Cybercrime: Unmasking Threats in the Digital Age*, CONTENT: Journal of Communication Studies, Vol.3, No.1 (Mei 2025), p.11–16.

¹¹ Mulyadi, dkk., *Analisis Penipuan Online Melalui Media Sosial dalam Perspektif Kriminologi*, Media Hukum Indonesia (MHI), Vol.2, No.2 (April-Juni 2024), p.74–82.

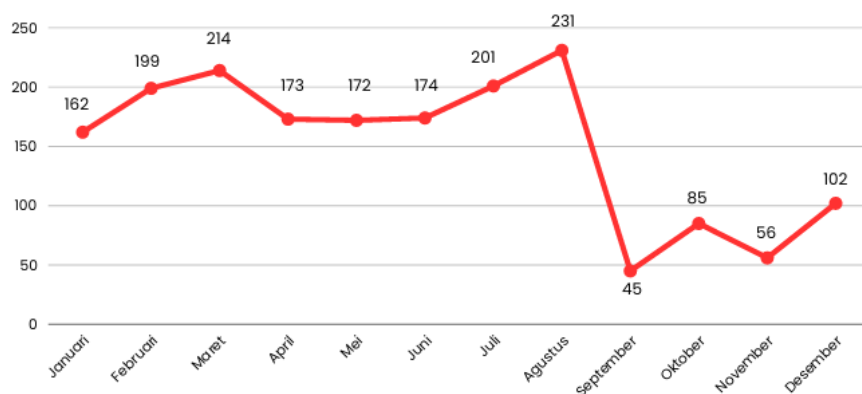
¹² Mohamad Firdaus, *Analisa Yuridis terhadap Peningkatan Tindak Cybercrime Ditinjau dari Perspektif Hukum Pidana*, Multiple Journal of Global and Multidisciplinary, Vol.2, No.3 (Maret 2024), p.1434–45.

Hasil kajian ini diharapkan dapat memperkuat wawasan akademik dan praktis dalam menghadapi tantangan kejahatan siber yang terus berkembang. Era digital menuntut bahwa hukum pidana dan kebijakan keamanan pun harus berevolusi secara proaktif, bukan hanya reaktif terhadap gejala yang muncul. Dengan demikian, regulasi harus bersifat dinamis, penegakan harus kolaboratif antara negara, sektor swasta dan masyarakat, serta literasi digital publik harus ditingkatkan. Hanya dengan demikian, kejahatan siber melalui media sosial tidak hanya dapat ditangani secara hukum tetapi juga dicegah secara komprehensif.

B. PEMBAHASAN

1. Pola Peningkatan Kasus *Cybercrime* di Media Sosial

Peningkatan tindak pidana siber yang memanfaatkan media sosial terlihat jelas seiring bertambahnya populasi digital di Indonesia. Data empiris menunjukkan aktivitas kejahatan siber mengalami kenaikan tajam sepanjang 2020–2024, terutama dalam bentuk *phishing*, pencurian identitas digital, peretasan akun, penipuan transaksi daring, serta penyebaran konten manipulatif yang menyesatkan publik.¹³ BSSN mencatat bahwa laporan aduan siber selama tahun 2024 Tim Pusat Kontak Siber BSSN menerima sebanyak 1.814 aduan siber yang berasal dari berbagai sektor. Adapun aduan terbanyak terdapat pada bulan Agustus dengan jumlah 231 aduan.¹⁴



Gambar 1: Statistik Aduan Siber pada Tahun 2024

¹³ Donna Revilia dan Irwansyah, *Social Media Literacy: Millennial's Perspective Of Security And Privacy Awareness*, Jurnal Penelitian Komunikasi dan Opini Publik, Vol.24, No.1 (Juli 2020), p.1–15.

¹⁴ BSSN, *Laporan Tahunan Keamanan Siber Indonesia*, Kominfo Csirt, Jakarta, 2024.

Dalam perspektif hukum, dinamika kejahatan di media sosial mengalami perkembangan yang jauh lebih cepat daripada respons regulatif negara. Indonesia memiliki rujukan yuridis melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun implementasi pembuktiannya menghadapi tantangan terkait anonimitas pelaku, keberadaan server di luar yurisdiksi nasional, serta bukti elektronik yang mudah dimanipulasi atau dihapus tanpa jejak.¹⁵ Selain itu, beberapa rumusan pasal dinilai belum mampu mengakomodasi modus terkini seperti *social engineering* melalui pesan langsung ataupun *identity takeover* pada akun-akun publik. Kondisi ini memperlihatkan adanya celah hukum yang menuntut pembaruan regulasi secara berkelanjutan sesuai perkembangan teknologi informasi.

Tingkat literasi digital yang masih rendah juga berkontribusi signifikan terhadap banyaknya korban tindak pidana siber. Survei literasi digital menunjukkan bahwa sebagian besar pengguna media sosial belum memahami manajemen keamanan data pribadi, seperti penggunaan autentikasi ganda, kontrol privasi, ataupun kemampuan mengidentifikasi ancaman siber secara mandiri.¹⁶ Rendahnya pemahaman ini berakibat pada tingginya kasus penyalahgunaan data pribadi, *grooming* kejahatan seksual siber dan penipuan finansial yang menyebar masif melalui pesan yang tampak meyakinkan. Dalam konteks sosial, kelompok rentan seperti remaja dan perempuan mengalami risiko lebih tinggi terhadap eksploitasi digital di platform media sosial,¹⁷ sehingga membutuhkan perhatian hukum dan edukatif yang lebih terstruktur.

Dari sisi penegakan hukum, aparat menghadapi tantangan teknis yang tidak ringan karena kejahatan siber bersifat *borderless* dan terselubung. Teknologi *encryption*, *virtual private network*, serta akun palsu memungkinkan pelaku menyamarkan identitas dan lokasi, sehingga proses pelacakan menuntut kolaborasi internasional serta kemampuan investigasi digital lebih canggih.

¹⁵ A. S. Pribowo dan M. N. Alhadi, *Cyber Crime Social Media Account Data Hacking in Indonesia*, TATOHI: Jurnal Ilmu Hukum, Vol.5, No.6 (Agustus 2025), p.271–79.

¹⁶ H. Widiyari dan N. Thalib, *Cybercrime Trends in Southeast Asia*, Jurnal Keamanan Digital ASEAN, Vol.3, No.2 (2024).

¹⁷ R. Butar, *Perilaku Siber dan Kejahatan Media Sosial*, Jurnal Kejahatan Siber Indonesia, Vol.2, No.1 (2025).

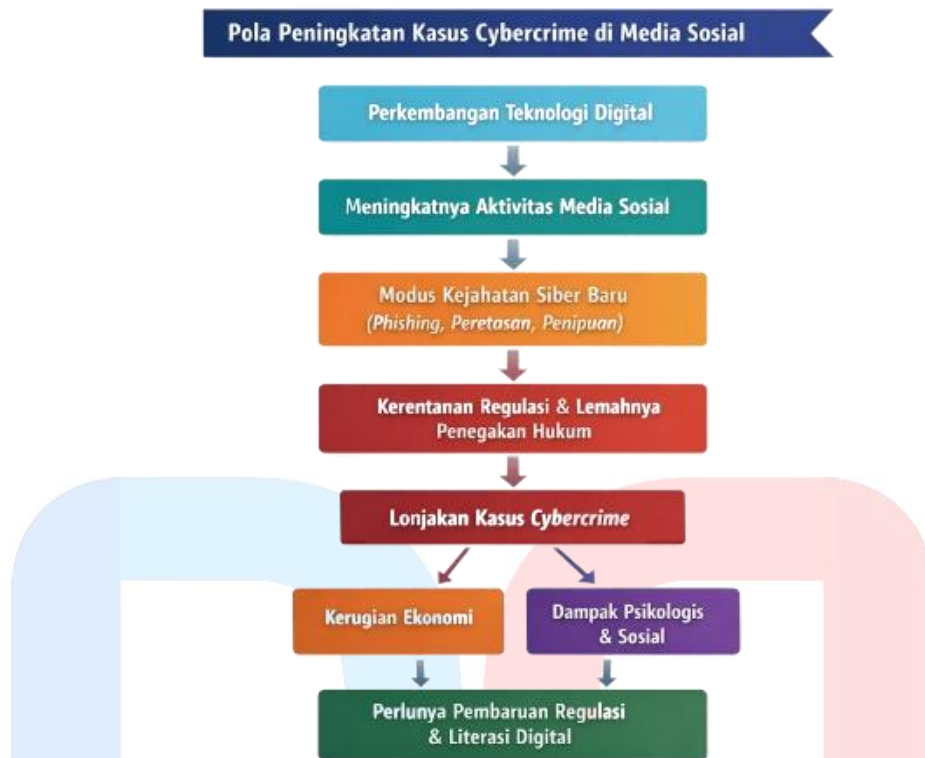
Aparat sering kesulitan mengumpulkan alat bukti yang sah secara forensik karena data elektronik memiliki sifat mudah berubah dan hilang.¹⁸ Di sisi lain, koordinasi antara pemerintah, platform penyedia media sosial dan lembaga penegak hukum juga belum optimal, menyebabkan waktu respons terhadap insiden sering terlambat dan merugikan korban secara berkelanjutan.

Fenomena kejahatan siber di media sosial tidak hanya berimplikasi pada kerugian ekonomi, tetapi juga pada dampak psikologis dan sosial yang mendalam bagi korban. Maraknya kasus penistaan, perundungan digital dan penyebaran konten merugikan martabat individu menimbulkan trauma jangka panjang serta merusak reputasi yang sulit dipulihkan.¹⁹ Kejahatan yang berfokus pada pemerasan data pribadi bahkan dapat mengancam keselamatan dan integritas sosial korban serta keluarganya. Dengan demikian, perkembangan kejahatan siber telah memasuki dimensi baru: bukan hanya melanggar norma hukum, namun merusak struktur kepercayaan masyarakat terhadap ruang digital dan pada akhirnya menghambat kemajuan transformasi digital nasional.

Berdasarkan keseluruhan pemaparan hasil ini, dapat dipahami bahwa peningkatan kejahatan siber pada media sosial bukan sekadar efek samping modernisasi, melainkan ancaman strategis terhadap keamanan digital dan stabilitas hukum. Maka negara perlu memperkuat sinergi kebijakan: mulai dari penyempurnaan perangkat hukum yang adaptif, peningkatan kapasitas penegak hukum dalam *digital forensic*, hingga pendekatan edukatif yang memprioritaskan perlindungan pengguna. Tanpa intervensi kebijakan yang cepat dan efektif, pertumbuhan media sosial akan terus dibayangi risiko kriminalitas yang semakin serius dan sulit dikendalikan.

¹⁸ D. Sutanto, *Digital Forensic Challenges in Cybercrime Investigation*, Indonesian Journal of Cyber Law, Vol.2, No.2 (2023).

¹⁹ A. Firmansyah, *Dampak Psikososial Korban Tindak Pidana Siber*, Jurnal Kriminologi Indonesia, Vol.2, No.2 (2024).



Gambar 2: Gambar Alur Pola Peningkatan Kasus Cybercrime

2. Kerentanan Regulasi terhadap Perkembangan Teknologi

Perkembangan teknologi digital, khususnya media sosial, bergerak secara eksponensial melampaui kemampuan pembuat kebijakan dalam merumuskan regulasi yang setara cepatnya. Inovasi dalam bentuk fitur baru, *algorithmic personalization*, hingga integrasi kecerdasan buatan menyebabkan interaksi antar pengguna semakin kompleks dan penuh risiko hukum, sementara kerangka regulasi seperti UU No. 19 Tahun 2016 masih berlandaskan paradigma kejahatan siber generasi awal.²⁰ Situasi ini menimbulkan celah normatif yang memungkinkan pelaku memanfaatkan ruang-ruang abu-abu hukum yang belum terakomodasi dalam aturan positif. Ketidakseimbangan antara teknologi dan regulasi pada akhirnya memaksa aparat penegak hukum beradaptasi secara reaktif, bukan preventif, sehingga penanganan tindak pidana siber sering berada satu langkah tertinggal dibanding modus kejahatan yang terus berkembang.

²⁰ A. S. Pribowo dan M. N. Alhadi, *Cyber Crime Social Media Account Data Hacking in Indonesia*.

Banyak kasus *identity takeover* dan *social engineering* pada akun media sosial tidak dapat diproses secara optimal karena bukti percakapan digital maupun *metadata* sudah terhapus sebelum proses penyidikan dimulai.²¹ Selain itu, keberadaan server penyedia layanan media sosial di luar negeri memperumit proses permintaan data secara legal, karena harus melibatkan mekanisme *mutual legal assistance* yang memerlukan waktu lama dan birokrasi lintas negara.²² Keadaan ini memperlihatkan adanya *asymmetry of power* antara pelaku yang menguasai teknologi dan aparat hukum yang bergantung pada struktur perundangan serta kerja sama internasional yang tidak selalu responsif terhadap kebutuhan penyidikan.

Kondisi literasi regulasi yang belum merata di masyarakat turut memperluas kerentanan hukum. Banyak pengguna tidak memahami bahwa aktivitas sederhana seperti penyebaran informasi pribadi milik orang lain, atau menyebar konten yang tampak sepele, dapat dikategorikan sebagai tindak pidana menurut norma hukum tertentu.²³ Celah pemahaman ini sering dimanfaatkan pelaku untuk meyakinkan korban memberikan akses terhadap data pribadi atau mengikuti tautan berbahaya yang kemudian digunakan sebagai dasar eksploitasi digital. Hasil penelitian menunjukkan bahwa kelemahan regulasi bukan hanya terletak pada teks pasal, tetapi juga pada implementasi edukatif yang belum mampu memperkuat kesadaran masyarakat mengenai batasan perilaku hukum di ruang siber.²⁴

Di sisi lain, adaptasi hukum yang dilakukan secara tergesa-gesa tanpa memperhatikan konteks perkembangan teknologi justru dapat menciptakan masalah baru dalam penerapan regulasi. Dalam beberapa kasus, aturan yang dirancang untuk mencegah penyalahgunaan informasi digital rentan menimbulkan tumpang tindih norma, terutama dalam isu ekspresi publik dan perlindungan kebebasan berpendapat.²⁵ Hal ini membuktikan bahwa kerentanan regulasi terhadap perkembangan teknologi tidak hanya menimbulkan kekosongan hukum,

²¹ D. Sutanto, *Digital Forensic Challenges in Cybercrime Investigation*.

²² H. Widiyari dan N. Thalib, *Cybercrime Trends in Southeast Asia*.

²³ A. Firmansyah, *Dampak Psikososial Korban Tindak Pidana Siber*.

²⁴ Donna Revilia dan Irwansyah, *Social Media Literacy: Millennial's Perspective Of Security And Privacy Awareness*.

²⁵ R. Butar, *Perilaku Siber dan Kejahatan Media Sosial*.

tetapi juga potensi *over-criminalization* terhadap aktivitas digital yang sebenarnya merupakan bagian dari hak dasar sebagai warga negara. Maka diperlukan desain kebijakan hukum yang adaptif, berbasis *technology-forecasting*, serta didukung riset berkelanjutan mengenai tren *cyber behaviour* masyarakat digital.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE) merupakan instrumen utama penanggulangan kejahatan siber. Namun, UU ini dinilai memiliki sejumlah kerentanan. Pertama, rumusan norma yang bersifat multitafsir, khususnya dalam ketentuan mengenai pencemaran nama baik, ujaran kebencian dan konten bermuatan penghinaan.²⁶ Dalam konteks cybercrime, ketidakjelasan ini menyulitkan aparat penegak hukum dalam mengklasifikasikan perbuatan yang benar-benar memenuhi unsur tindak pidana siber. Kedua, UU ITE belum secara komprehensif mengatur modus kejahatan siber mutakhir, seperti pemanfaatan kecerdasan buatan, *deepfake*, *social engineering* dan lainnya. Akibatnya, banyak kejahatan digital yang hanya dapat diproses melalui penafsiran ekstensif, yang berpotensi bertentangan dengan asas legalitas dalam hukum pidana. Implikasinya, UU ITE sering kali tidak mampu memberikan respons hukum yang cepat dan presisi terhadap bentuk kejahatan baru, sehingga membuka ruang impunitas bagi pelaku atau sebaliknya, berpotensi melahirkan kriminalisasi berlebihan terhadap pengguna media sosial.²⁷

Kemudian, Kitab Undang-Undang Hukum Pidana (KUHP) meskipun telah mengalami pembaruan melalui UU Nomor 1 Tahun 2023, pada dasarnya masih berakar pada paradigma hukum pidana konvensional dan belum menghimpun kejahatan di ruang siber. Kerentanan muncul ketika perbuatan pidana di dunia digital tidak memiliki padanan langsung dengan delik klasik, seperti pencurian data, manipulasi identitas digital, atau peretasan akun media sosial.²⁸

²⁶ Mochamad Januar Rizki, *Pasal Karet dalam UU ITE Terbaru Masih Mengancam Masyarakat yang Kritis*, diakses dari <https://www.hukumonline.com/berita/a/pasal-karet-dalam-uu-ite-terbaru-masih-mengancam-masyarakat-yang-kritis-lt6597e40be9b8c>, diakses pada 16 Januari 2026.

²⁷ Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Cybercrime di Indonesia*, Raja Grafindo Persada, Jakarta, 2014, p.88.

²⁸ Vidya Prahassacitta, *Kesiapan Kitab Undang-Undang Hukum Pidana Nasional dalam Menghadapi Kejahatan Siber di Masa Depan*, Jurnal Hukum & Pembangunan, Vol.53, No.4 (2023), p.440–42.

Akibatnya aparat penegak hukum kerap memaksakan penerapan pasal-pasal konvensional terhadap perbuatan siber, yang secara normatif kurang tepat. Implikasi dari kondisi ini adalah inkonsistensi penegakan hukum, baik dalam penentuan pasal, ancaman pidana, maupun putusan pengadilan. Hal ini berdampak pada lemahnya efek jera dan menurunnya kepercayaan publik terhadap kemampuan hukum pidana dalam melindungi masyarakat di era digital.²⁹

Berdasarkan hasil analisis tersebut, dapat disimpulkan bahwa ketertinggalan regulasi hukum terhadap perkembangan teknologi merupakan faktor kunci yang memperburuk penanggulangan tindak pidana siber di media sosial. Tanpa pembaruan hukum yang progresif, penguatan kapasitas *digital forensic*, serta hubungan koordinatif antara negara dan perusahaan platform digital, upaya penegakan hukum akan terus menghadapi hambatan struktural dan teknis yang signifikan. Dengan demikian, pengembangan regulasi yang adaptif dan inklusif menjadi urgensi strategis untuk mewujudkan keamanan digital yang lebih kuat di era transformasi teknologi yang terus berubah dengan cepat.

3. Peran Literasi Digital dalam Pencegahan Kejahatan Siber

Perkembangan teknologi digital membuat masyarakat semakin aktif berinteraksi melalui internet, namun kesadaran terhadap ancaman siber masih tergolong rendah. Banyak individu membagikan informasi pribadi tanpa memahami risiko penyalahgunaan identitas, pencurian data, hingga penipuan *online*. Di sinilah literasi digital memiliki peran strategis untuk membentuk perilaku aman saat bermedia digital agar kejahatan siber dapat diminimalisir.

Literasi digital tidak hanya mengenai kemampuan mengoperasikan perangkat atau aplikasi, tetapi juga mencakup pemahaman mengenai perlindungan data pribadi, aturan privasi, serta cara menjaga keamanan akun. Masyarakat yang melek keamanan digital akan lebih berhati-hati dalam memberikan akses data, memilih kata sandi yang kuat, mengaktifkan *two-factor authentication* dan mampu mengenali tanda-tanda kejahatan seperti *phishing*, *malware*, maupun *social engineering*. Ketika individu memiliki pengetahuan tersebut, peluang pelaku siber untuk menyerang akan semakin kecil.

²⁹ Sherley, *Tantangan Hukum Pidana dalam Menghadapi Teknologi Deepfake di Indonesia*, Jurnal Hukum & Pembangunan, Vol.53, No.2 (2023), p.152.

Selain itu, literasi digital juga membantu masyarakat mengelola jejak digital (*digital footprint*) dengan bijak. Banyak kasus kebocoran data berawal dari kelalaian pengguna yang sembarangan mengunggah informasi sensitif ke platform publik. Pemahaman tentang identitas digital sangat penting karena data yang tersebar di internet dapat digunakan kembali untuk tindakan kriminal seperti pemalsuan akun dan akses ilegal ke layanan keuangan. Upaya edukasi mengenai etika digital dan keamanan data akan memperkuat budaya waspada di tengah masyarakat.³⁰

Pemerintah melalui Kementerian Komunikasi dan Digital (Kemkomdigi) menjalankan program literasi digital nasional yang disebut Indonesia Makin Cakap Digital. Dengan adanya program ini bertujuan agar masyarakat bisa menggunakan teknologi digital dengan produktif, aman, etis dan terhindar dari konten negatif serta kejahatan digital seperti penipuan, phishing, atau penyalahgunaan data pribadi. Literasi ini mencakup pilar-pilar penting termasuk keamanan digital (*digital safety*) yang membantuk masyarakat memahami risiko dan upaya pencegahan ancaman siber.³¹ Selain itu, Kemkomdigi menguatkan edukasi mengenai empat pilar literasi digital dalam setiap program pelatihan talenta digital untuk memastikan ruang siber Indonesia bida kondusif dan aman bagi masyarakat di tengah potensi ancaman kejahatan.³² Badan Siber dan Sandi Negara (BSSN) melakukan kampanye SIAP #JagaRuangSiber kepada masyarakat luas. SIAP #JagaRuangSiber sendiri merupakan singkatan dari simpan datamu, ikuti literasi, amankan *gadget*-mu dan perkuat *password* (kata sandi).³³

4. Efektivitas Kerja Aparat Penegak Hukum dalam Kasus Dunia Maya

Efektivitas penegakan hukum dalam menangani kejahatan siber bukan hanya persoalan kecanggihan teknologi, melainkan hasil interaksi kompleks antara aturan, institusi dan perilaku masyarakat. Mengacu teori Lawrence M.

³⁰ R. Ismail dan B. Nugroho, *Literasi Digital dan Keamanan Informasi Masyarakat Indonesia*, Jurnal Teknologi Informasi, Vol.11, No.2 (2023), p.55–66.

³¹ Kemkomdigi, *Program Literasi Digital Nasional "Indonesia Makin Cakap Digital"*, diakses dari <https://literasidigital.id/profil>.

³² Livia Kristiani, *Kemkomdigi Perkuat 4 Pilar Literasi Digital Jaga Ruang Siber Kondusif*, diakses dari <https://www.antaranews.com/berita/4879581/kemkomdigi-perkuat-4-pilar-literasi-digital-jaga-ruang-siber-kondusif>, diakses pada 16 Januari 2026.

³³ Farhan Arda Nugraha, *BSSN Menggalakkan Kampanye SIAP #JagaRuangSiber*, diakses dari <https://www.antaranews.com/berita/3632217/bssn-menggalakkan-kampanye-siap-jagaruangsiber>, diakses pada 16 Januari 2026.

Friedman,³⁴ keberhasilan hukum dapat diukur melalui tiga komponen utama yang saling berkaitan: Pertama, Komponen Substansi Hukum (*Legal Substance*). Substansi hukum berkaitan dengan aturan atau regulasi yang menjadi landasan bertindak. Dalam konteks Indonesia, keberadaan UU ITE dan UU Perlindungan Data Pribadi (PDP) telah memberikan payung hukum bagi aparat.³⁵ Namun, efektivitasnya sering kali terbentur oleh sifat kejahatan siber yang *borderless* (tanpa batas).³⁶ Tantangan terbesar pada aspek substansi adalah ketidaksinkronan antara kecepatan regulasi dengan inovasi kejahatan seperti *deepfake extortion* atau pencucian uang melalui *cryptocurrency*.³⁷ Selain itu, prosedur hukum acara terkait *Mutual Legal Assistance* (MLA) yang masih birokratis menyebabkan substansi hukum sering kali kehilangan taringnya saat berhadapan dengan server luar negeri yang membutuhkan respons cepat sebelum jejak digital dihapus.³⁸

Kedua, Komponen Struktur Hukum (*Legal Structure*). Struktur hukum berkaitan dengan institusi penegak hukum, perangkat dan sumber daya manusianya. Di sinilah letak hambatan paling nyata. Meskipun di tingkat pusat (Mabes Polri) telah memiliki unit siber yang mumpuni, terjadi ketimpangan infrastruktur dan keahlian di tingkat daerah. Banyak penyidik yang masih mengandalkan pendekatan konvensional karena keterbatasan sertifikasi digital forensik dan alat investigasi.³⁹ Masalah *chain of custody* (rantai penjagaan bukti) yang sering terputus menunjukkan bahwa struktur kita belum sepenuhnya adaptif terhadap sifat bukti digital yang rapuh.⁴⁰ Tanpa struktur yang kuat dan merata, hukum hanya akan menjadi "macan kertas" yang tidak mampu menjangkau pelaku di ruang digital yang gelap.

³⁴ Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, Russell Sage Foundation, New York, 1975.

³⁵ Indonesia, *Undang-Undang tentang Perubahan Kedua atas UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, UU No.1 Tahun 2024, LN Tahun 2024 No.39, TLN No.6905.

³⁶ A. Syaputra dan S. Malik, *Efektivitas UU ITE dalam Penanggulangan Cybercrime Berbasis Media Sosial di Indonesia*.

³⁷ Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Cybercrime di Indonesia*, p.42.

³⁸ Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta, 2012, p.156.

³⁹ Widodo, *Hukum Pidana di Bidang Teknologi Informasi*, Aswaja Pressindo, Yogyakarta, 2013.

⁴⁰ Mary Helen Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence*, Jones & Bartlett Publishers, New York, 2014.

Masalah terbesar yang dihadapi aparat adalah aspek pembuktian digital yang tidak dapat diperlakukan sama seperti barang bukti fisik. Data elektronik dapat berpindah lokasi dalam hitungan detik, bahkan menghilang jika server luar negeri atau sistem *auto-delete* digunakan. Banyak kasus di Indonesia menunjukkan bahwa laporan masyarakat mengenai peretasan, *phishing*, atau pencurian identitas sering berakhir tanpa hasil karena bukti digital tidak disimpan dengan prosedur teknis forensik yang benar. Ketika *chain of custody* terputus, validitas bukti di pengadilan pun melemah, menjadikan pelaku sulit dijerat hukum meskipun indikasi kejahatan sudah jelas.⁴¹

Ketiga, Komponen Budaya Hukum (*Legal Culture*). Budaya hukum mencakup sikap, nilai dan kesadaran masyarakat, baik masyarakat umum maupun aparat itu sendiri terhadap hukum. Efektivitas penegakan hukum siber sangat bergantung pada bagaimana masyarakat merespons kejahatan. Rendahnya literasi digital menyebabkan banyak korban tidak sadar akan pentingnya menjaga orisinalitas bukti digital, seperti melakukan screenshot yang tidak sesuai standar atau bahkan menghapus jejak percakapan karena malu.⁴² Di sisi lain, budaya hukum aparat yang terkadang masih memprioritaskan kasus fisik dibandingkan kasus digital juga memengaruhi kecepatan penanganan laporan. Sinergi antara masyarakat yang melek hukum digital dan aparat yang proaktif merupakan kunci utama agar sistem hukum ini dapat bernapas dan berfungsi secara efektif.⁴³

Walaupun kondisi ini menghadirkan tantangan besar, upaya peningkatan efektivitas penegakan hukum sebenarnya terus dilakukan melalui pembaruan kebijakan dan penguatan lembaga yang terlibat dalam keamanan siber. Koordinasi antara Kemenkominfo, *cyber* unit Polri dan lembaga keamanan lain mulai diarahkan pada model kolaborasi informasi, sehingga pelacakan pelaku dapat dilakukan lebih terstruktur. Selain itu, kerja sama dengan penyedia platform digital seperti media sosial dan layanan *e-commerce* mulai menjadi bagian dari strategi dari penanggulangan *cybercrime*, termasuk dalam menyediakan *log data*

⁴¹ Nugroho, *Tantangan Hukum dalam Penanganan Kejahatan Siber di Indonesia*, Jurnal Keamanan Digital, Vol.7, No.1 (2023), p.21–34.

⁴² Edmon Makarim, *Kompilasi Hukum Telematika*, Raja Grafindo Persada, Jakarta, 2003, p.210.

⁴³ Lawrence M. Friedman, *American Law: An Introduction*, W.W. Norton & Company, New York, 1984, p.6-7.

saat proses investigasi berlangsung. Sinergi ini diharapkan mampu mengurangi kesenjangan antara kecepatan inovasi teknologi dan kemampuan aparat dalam merespons ancaman digital.⁴⁴

Efektivitas penegakan hukum tetap bergantung pada kemampuan negara dalam membangun sistem pencegahan dan investigasi yang berorientasi pada teknologi masa depan. Kesiapan sumber daya manusia, modernisasi perangkat penyelidikan, percepatan reformasi pelatihan teknis dan perbaikan mekanisme kerja sama internasional menjadi langkah yang harus terus dijalankan. Tanpa perubahan yang progresif dan komprehensif, aparat penegak hukum akan tetap berada dalam posisi mengejar bayangan para pelaku kejahatan digital yang selalu selangkah lebih maju di ruang maya.⁴⁵

5. Implikasi Sosial dan Psikologis Kejahatan Siber Pada Korban

Kejahatan siber telah berkembang menjadi fenomena kriminal yang mampu menciptakan kerusakan multidimensional bagi korban. Dampak ekonomi yang timbul tidak hanya berkaitan dengan hilangnya dana akibat *phishing*, *social engineering*, atau penipuan investasi, tetapi juga mencakup kerugian tidak langsung seperti biaya pemulihan, konsultasi hukum, serta hilangnya kesempatan kerja. Laporan yang dikeluarkan *Internet Crime Complaint Center* mencatat lonjakan signifikan kerugian finansial korban dari tahun ke tahun, menunjukkan bahwa serangan digital terus menembus sistem keuangan pribadi secara masif.⁴⁶ Kerugian ekonomi ini seringkali membawa dampak lanjutan terhadap stabilitas rumah tangga, menimbulkan konflik internal dan merusak perencanaan keuangan jangka panjang keluarga.

Selain itu, reputasi dari korban juga turut menjadi sasaran kerusakan serius dalam kejahatan siber yang melibatkan penyebaran fitnah, *doxxing*, atau peretasan akun media sosial. Konten yang menyesatkan dapat menyebar sangat cepat melalui jejaring digital dan sekaligus menjadi rekam jejak permanen di internet, mengubah cara masyarakat dan lingkungan profesional memandang korban.⁴⁷

⁴⁴ A. Firmansyah, *Kesadaran Hukum Masyarakat dalam Menanggulangi Kejahatan Siber*.

⁴⁵ Ananda, *Penegakan Hukum Siber di Indonesia pada Era Transformasi Digital*, Jurnal Hukum Rekayasa Teknologi, Vol.8, No.1 (2025), p.14–29.

⁴⁶ FBI IC3, *Internet Crime Report*, U.S. Department of Justice, Washington, DC, 2024.

⁴⁷ D. Nugraha, *Tantangan Penegakan Hukum dalam Kejahatan Siber di Indonesia*, Jurnal Kriminalitas Digital, Vol.5, No.1 (2022), p.135-45.

Menegaskan bahwa serangan siber terhadap identitas digital dapat mengakibatkan hilangnya kepercayaan sosial, penurunan kredibilitas di tempat kerja, serta penarikan peluang ekonomi yang sebelumnya tersedia bagi korban. Proses untuk mengembalikan reputasi digital membutuhkan waktu lama, serta tidak selalu berhasil sepenuhnya.

Dalam aspek psikologis, kerusakan yang dialami korban bahkan sering lebih berat daripada dampak ekonomi maupun reputasi. Tekanan emosional seperti kecemasan, rasa malu, stres berat, hingga depresi merupakan gejala umum pada korban penipuan dan pelecehan berbasis digital.⁴⁸ Trauma psikologis yang dialami korban dapat berlangsung lama karena sifat ruang digital yang selalu menampilkan kembali konten yang melukai mereka, sehingga penyembuhan mental menjadi lebih sulit dibanding kasus kekerasan konvensional. Pada situasi ekstrem, korban isolasi digital dapat mengalami gangguan identitas, rasa tidak berdaya, bahkan muncul ide bunuh diri akibat tekanan psikologis berulang.

Lebih jauh lagi, kejahatan siber menghasilkan implikasi sosial yang meluas tidak hanya pada korban individu, tetapi juga mempengaruhi keluarga dan lingkungan sekitarnya. Keamanan digital rumah tangga terguncang saat keuangan dan privasi keluarga terlibat, terutama dalam kasus penipuan investasi yang menghabiskan tabungan masa depan.⁴⁹ Menunjukkan bahwa kehilangan aset akibat kejahatan digital memperburuk kualitas hidup keluarga, meningkatkan konflik internal dan membuat korban enggan kembali berinteraksi di ruang digital karena hilangnya rasa aman. Akibatnya, muncul fenomena *digital withdrawal* yang justru menurunkan literasi teknologi masyarakat secara keseluruhan.⁵⁰

Aspek lain yang sering terabaikan adalah ketidakpastian hukum yang memperburuk keadaan psikososial korban. Prosedur pelaporan yang panjang dan memerlukan pembuktian digital membuat banyak korban merasa tidak mendapatkan keadilan, sehingga kepercayaan mereka terhadap aparat hukum.⁵¹ Ketika pelaku tidak tertangkap atau bukti dinyatakan tidak sah, rasa aman korban

⁴⁸ A. Rahman, *Doxxing dan Dampaknya terhadap Reputasi Korban di Media Sosial*, Jurnal Hukum Siber Indonesia, Vol.5, No.3 (2023), p.101–15.

⁴⁹ L. Balcombe, *Psychological Impact of Scam Victimization in the Digital Era*, Journal of Cyber Behavior, Vol.12, No.2 (2025), p.44–59.

⁵⁰ R. Shalihah, *Dimensi Sosial Kejahatan Siber terhadap Rumah Tangga di Indonesia*, Jurnal Sosial Teknologik, Vol.9, No.1 (2024), p.55–70.

⁵¹ D. Nugraha, *Tantangan Penegakan Hukum dalam Kejahatan Siber di Indonesia*.

runtuh dan trauma emosional bertahan lebih lama. Proses hukum yang kurang sensitif terhadap kondisi korban juga memperbesar beban mental dan memunculkan rasa frustrasi terhadap institusi negara.

Untuk pulih, korban membutuhkan dukungan multidisiplin mulai dari layanan hukum, finansial, hingga psikoterapi. Intervensi pemulihan perlu dikembangkan dalam bentuk layanan terpadu yang menghubungkan antara aparat penegak hukum, konselor psikologi dan ahli keamanan digital. Model pemulihan terpadu ini telah terbukti dapat mempercepat stabilitas emosi dan pemulihan sosial korban.⁵² Namun, di banyak negara berkembang, termasuk Indonesia, akses terhadap layanan dukungan bagi korban kejahatan siber masih sangat terbatas dan belum terhubung langsung dengan mekanisme pelaporan kejahatan.

Dampak sosial dan psikologis kejahatan siber menjadi pengingat bahwa ancaman digital tidak hanya merusak perangkat atau akun, tetapi menghantam struktur kehidupan manusia secara mendalam. Oleh karena itu, diperlukan pendekatan holistik dalam perlindungan terhadap korban, yang tidak hanya fokus pada penangkapan pelaku tetapi juga memastikan pemulihan martabat, reputasi dan kesehatan mental masyarakat yang terdampak. Jika sistem perlindungan korban tidak diperkuat, maka ruang digital akan terus menciptakan korban yang menderita dalam senyap tanpa dukungan yang memadai untuk kembali bangkit.⁵³

C. PENUTUP

Peningkatan kejahatan siber di media sosial mencerminkan tantangan serius bagi sistem hukum, teknologi dan sosial di Indonesia. Regulasi yang tertinggal dari perkembangan teknologi, rendahnya literasi digital masyarakat, serta keterbatasan kapasitas penegakan hukum memperburuk kerentanan ruang siber nasional. Dampak yang ditimbulkan tidak hanya bersifat ekonomi, tetapi juga merusak psikologis dan sosial korban secara mendalam. Oleh karena itu, diperlukan langkah operasional terintegrasi untuk menanggulangi masalah ini. Pemerintah perlu mempercepat pembaruan regulasi dengan memasukkan modus

⁵² D. Yulianto, *Integrasi Dukungan Psikososial dalam Penanganan Korban Cybercrime*, Journal of Digital Security Studies, Vol.4, No.1 (2024), p.66–79.

⁵³ T. Wijaya, *Model Pemulihan Korban Cybercrime Berbasis Layanan Terpadu*, Hukum & Masyarakat Digital, Vol.6, No.2 (2024), p.90–104.

kejahatan baru seperti *deepfake*, *social engineering* dan pencurian identitas digital. Aparat penegak hukum harus diperkuat melalui pelatihan digital forensik, peningkatan infrastruktur investigasi dan mekanisme *mutual legal assistance* yang efisien. Selain itu, program literasi digital harus diperluas secara berkelanjutan dengan melibatkan sekolah, komunitas dan platform media sosial. Pembentukan pusat layanan terpadu bagi korban kejahatan siber yang mengintegrasikan bantuan hukum, psikologis dan keamanan digital juga menjadi kebutuhan mendesak. Sinergi lintas sektor inilah yang akan menentukan efektivitas negara dalam mewujudkan ruang digital yang aman, adil dan berkeadilan bagi seluruh warga.



DAFTAR PUSTAKA

Buku

- Arief, Barda Nawawi. 2014. *Tindak Pidana Mayantara: Perkembangan Cybercrime di Indonesia*. (Jakarta: Raja Grafindo Persada).
- BSSN. 2024. *Laporan Tahunan Keamanan Siber Indonesia*. (Jakarta: Kominfo Csirt).
- FBI IC3. 2024. *Internet Crime Report*. (Washington, DC: U.S. Department of Justice).
- Friedman, Lawrence M.. 1975. *The Legal System: A Social Science Perspective*. (New York: Russell Sage Foundation).
- Friedman, Lawrence M.. 1984. *American Law: An Introduction*. (New York: W.W. Norton & Company).
- Makarim, Edmon. 2003. *Kompilasi Hukum Telematika*. (Jakarta: Raja Grafindo Persada).
- Maras, Mary Helen. 2014. *Computer Forensics: Cybercriminals, Laws, and Evidence*. (New York: Jones & Bartlett Publishers).
- Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. (Jakarta: Tatanusa).
- Widodo. 2013. *Hukum Pidana di Bidang Teknologi Informasi*. (Yogyakarta: Aswaja Pressindo).

Publikasi

- Abdullah, Muhammad, dkk.. *Evolution Cybercrime - Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data*. Analytics. Vol.4. No.3 (September 2025).
- Ananda. *Penegakan Hukum Siber di Indonesia pada Era Transformasi Digital*. Jurnal Hukum Rekayasa Teknologi. Vol.8. No.1 (2025).
- Astari, L. D.. *Kebijakan Penegakan Hukum terhadap Kejahatan Siber di Indonesia*. Jurnal Kriminologi Indonesia. Vol.17. No.1 (2021).
- Balcombe, L.. *Psychological Impact of Scam Victimization in the Digital Era*. Journal of Cyber Behavior. Vol.12. No.2 (2025).
- Butar, R.. *Perilaku Siber dan Kejahatan Media Sosial*. Jurnal Kejahatan Siber Indonesia. Vol.2. No.1 (2025).
- Firdaus, Mohamad. *Analisa Yuridis terhadap Peningkatan Tindak Cybercrime Ditinjau dari Perspektif Hukum Pidana*. Multiple Journal of Global and Multidisciplinary. Vol.2. No.3 (Maret 2024).
- Firmansyah, A.. *Dampak Psikososial Korban Tindak Pidana Siber*. Jurnal Kriminologi Indonesia. Vol.2. No.2 (2024).
- H., Dinda A. dan Muhamad H. S.. *Perlindungan Hukum terhadap Serangan Siber: Tinjauan atas Kebijakan dan Regulasi Terbaru*. CAUSA: Jurnal Hukum dan Kewarganegaraan. Vol.1. No.5 (November 2023).
- Harahap, Rahma Hayati dan Muhammad Adfhol Zikri. *Online Identity and Cybercrime: Unmasking Threats in the Digital Age*. CONTENT: Journal of Communication Studies. Vol.3. No.1 (Mei 2025).

- Hukom, Rafli dan Martinus Hukmu Setiadi. *Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi*. Perkara : Jurnal Ilmu Hukum dan Politik. Vol.3. No.1 (Maret 2025).
- Hutajulu, Andreas Fransiskus dan Sri Endah Wahyuningsih. *Penegakan Hukum Pidana terhadap Cyber Crime di Indonesia*. Ensiklopedia of Journal Lembaga Penelitian dan Penerbitan Hasil Penelitian Ensiklopedia. Vol.7. No.3 (2025).
- Ismail, R. dan B. Nugroho. *Literasi Digital dan Keamanan Informasi Masyarakat Indonesia*. Jurnal Teknologi Informasi. Vol.11. No.2 (2023).
- Koto, Ismail. *Cyber Crime According to the ITE Law*. IJRS: International Journal Reglement & Society. Vol.2. No.2 (Mei-Agustus 2021).
- Kusnadi, D. dan G. N. Efendi. *Cybercrime and Digital Society in Indonesia: Legal Challenges and Public Discourse*. Adliya: Jurnal Hukum dan Kemanusiaan. Vol.19. No.1 (Juni 2025).
- Mulyadi, dkk.. *Analisis Penipuan Online Melalui Media Sosial dalam Perspektif Kriminologi*. Media Hukum Indonesia (MHI). Vol.2. No.2 (April-Juni 2024).
- Nugraha, D.. *Tantangan Penegakan Hukum dalam Kejahatan Siber di Indonesia*. Jurnal Kriminalitas Digital. Vol.5. No.1 (2022).
- Nugroho. *Tantangan Hukum dalam Penanganan Kejahatan Siber di Indonesia*, Jurnal Keamanan Digital. Vol.7. No.1 (2023).
- Prahassacitta, Vidya. *Kesiapan Kitab Undang-Undang Hukum Pidana Nasional dalam Menghadapi Kejahatan Siber di Masa Depan*. Jurnal Hukum & Pembangunan. Vol.53. No.4 (2023).
- Pribowo, A. S. dan M. N. Alhadi. *Cyber Crime Social Media Account Data Hacking in Indonesia*. TATOHI: Jurnal Ilmu Hukum. Vol.5. No.6 (Agustus 2025).
- Rahman, A.. *Doxxing dan Dampaknya terhadap Reputasi Korban di Media Sosial*. Jurnal Hukum Siber Indonesia. Vol.5. No.3 (2023).
- Revilia, Donna dan Irwansyah. *Social Media Literacy: Millenial's Perspective Of Security And Privacy Awareness*. Jurnal Penelitian Komunikasi dan Opini Publik. Vol.24. No.1 (Juli 2020).
- Shalihah, R.. *Dimensi Sosial Kejahatan Siber terhadap Rumah Tangga di Indonesia*. Jurnal Sosial Teknologik. Vol.9. No.1 (2024).
- Sherley, *Tantangan Hukum Pidana dalam Menghadapi Teknologi Deepfake di Indonesia*. Jurnal Hukum & Pembangunan. Vol.53. No.2 (2023).
- Sutanto, D.. *Digital Forensic Challenges in Cybercrime Investigation*. Indonesian Journal of Cyber Law. Vol.2. No.2 (2023).
- Syaputra, A. dan S. Malik. *Efektivitas UU ITE dalam Penanggulangan Cybercrime Berbasis Media Sosial di Indonesia*. Jurnal Hukum Digital Nusantara. Vol.6. No.4 (2024).
- Widiasari, H. dan N. Thalib. *Cybercrime Trends in Southeast Asia*. Jurnal Keamanan Digital ASEAN. Vol.3. No.2 (2024).
- Wijaya, T.. *Model Pemulihan Korban Cybercrime Berbasis Layanan Terpadu*. Hukum & Masyarakat Digital. Vol.6. No.2 (2024).
- Yulianto, D.. *Integrasi Dukungan Psikososial dalam Penanganan Korban Cybercrime*. Journal of Digital Security Studies. Vol.4. No.1 (2024).

Website

- Alinea.id. *Polisi Bongkar Penipuan Berkedok Chat WA Kurir Paket, 493 Orang Jadi korban*. diakses dari <https://www.alinea.id/nasional/polisi-bongkar-penipuan-berkedok-chat-wa-kurir-paket-b2hKs9JO8>. diakses pada 16 Januari 2026.
- Kemkomdigi. *Program Literasi Digital Nasional "Indonesia Makin Cakap Digital"*. diakses dari <https://literasidigital.id/profil>. diakses pada 16 Januari 2026.
- Kristiani, Livia. *Kemkomdigi Perkuat 4 Pilar Literasi Digital Jaga Ruang Siber Kondusif*. diakses dari <https://www.antaranews.com/berita/4879581/kemkomdigi-perkuat-4-pilar-literasi-digital-jaga-ruang-siber-kondusif>. diakses pada 16 Januari 2026.
- Nugraha, Farhan Arda. *BSSN Menggalakkan Kampanye SIAP #JagaRuangSiber*. diakses dari <https://www.antaranews.com/berita/3632217/bssn-menggalakkan-kampanye-siap-jagaruangsiber>. diakses pada 16 Januari 2026.
- Rizki, Mochamad Januar. *Pasal Karet dalam UU ITE Terbaru Masih Mengancam Masyarakat yang Kritis*. diakses dari <https://www.hukumonline.com/berita/a/pasal-karet-dalam-uu-ite-terbaru-masih-mengancam-masyarakat-yang-kritis-lt6597e40be9b8c>. diakses pada 16 Januari 2026.

Sumber Hukum

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.