Jurnal Hukum dan HAM Wara Sains
Vol. 5, No. 02, Juni 2026, pp. 391-410

Kejahatan Dunia Maya pada Platform Media Sosial: Analisis Yuridis dan Sosial

Jason Indrakusuma[1], Rae Bennett Celeste Saragih[2], Glen Brilliant[3]
[1] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan jasonindrakusuma@gmail.com
[2] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan rae.saragih@gmail.com
[3] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan glenbrt01@gmail.com

Article Info

Article history:

Received Jun, 2026
Revised Jun, 2026
Accepted Jun, 2026

Kata Kunci:

Kejahatan Dunia Maya, Media Sosial, Penegakan Hukum, Literasi Digital, Indonesia

Keywords:

Cybercrime, Social Media, Law Enforcement, Digital Literacy, Indonesia

ABSTRAK

Maraknya kejahatan dunia maya di platform media sosial seperti penipuan online, perundungan siber, ujaran kebencian, dan kebocoran data pribadi telah menimbulkan kerugian finansial sekaligus gangguan psikologis dan sosial bagi masyarakat. Penelitian ini bertujuan menganalisis pengaturan hukum di Indonesia dalam menanggulangi kejahatan tersebut, mengidentifikasi bentuk dan dampak sosialnya, serta merumuskan model kolaborasi ideal antara negara, platform media sosial, dan masyarakat. Metode yang digunakan adalah studi literatur dengan sumber data sekunder yang terdiri dari bahan hukum primer (UU ITE, UU PDP, KUHP), bahan hukum sekunder (lima jurnal ilmiah terdahulu, buku teks, artikel jurnal), serta bahan hukum tersier (kamus hukum dan artikel berita terpercaya). Data dikumpulkan melalui penelusuran sistematis dengan kata kunci relevan, kemudian dianalisis secara kualitatif-deskriptif untuk mengidentifikasi pola, hambatan, dan sintesis teoretis. Hasil penelitian menunjukkan bahwa secara normatif UU ITE dan UU PDP telah membangun kerangka regulasi komprehensif, namun implementasinya terkendala keterbatasan kapasitas digital forensik, lemahnya koordinasi lintas lembaga, dan multitafsir pasal. Bentuk kejahatan yang dominan meliputi penipuan dengan social engineering, cyberbullying, hate speech, dan hoaks, yang berdampak multidimensional. Kebaruan penelitian ini terletak pada penguatan aplikasi Space Transition Theory dalam konteks Indonesia serta perumusan model kolaborasi multipihak yang mengintegrasikan pendekatan penal, non-penal, dan internasional. Implikasi penelitian mencakup rekomendasi penguatan kapasitas aparat, harmonisasi regulasi, perluasan literasi digital nasional, penguatan kerja sama internasional, serta peningkatan akuntabilitas platform media sosial.

ABSTRACT

The rise of cybercrimes on social media platforms, such as online fraud, cyberbullying, hate speech, and personal data leaks, has caused financial losses as well as psychological and social disruption to society. This study aims to analyze legal regulations in Indonesia in addressing these crimes, identify their forms and social impacts, and formulate an ideal collaboration model between the state, social media platforms, and society. The method used is a literature study with secondary data sources consisting of primary legal materials (the ITE Law, the PDP Law, the Criminal Code), secondary legal materials (five previous scientific journals, textbooks, journal articles), and tertiary legal materials (legal dictionaries and reliable news articles). Data were

collected through systematic searches with relevant keywords, then analyzed qualitatively and descriptively to identify patterns, obstacles, and theoretical synthesis. The results of the study indicate that normatively, the ITE Law and the PDP Law have established a comprehensive regulatory framework, but its implementation is hampered by limited digital forensic capacity, weak cross-agency coordination, and multiple interpretations of articles. The dominant forms of crime include fraud through social engineering, cyberbullying, hate speech, and hoaxes, which have multidimensional impacts. The novelty of this research lies in strengthening the application of Space Transition Theory in the Indonesian context and formulating a multi-stakeholder collaboration model that integrates penal, non-penal, and international approaches. Implications of the research include recommendations for strengthening the capacity of law enforcement officers, harmonizing regulations, expanding national digital literacy, strengthening international cooperation, and enhancing the accountability of social media platforms.

Corresponding Author:

Name: Jason Indrakusuma
Institution: Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan
Email: jasonindrakusuma@gmail.com

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat dalam dua dekade terakhir telah membawa perubahan besar terhadap cara manusia berinteraksi, bekerja, dan mendapatkan informasi. Media sosial sebagai salah satu produk revolusi digital telah menjadi bagian tak terpisahkan dari kehidupan sosial modern. Menurut berbagai survei internasional, lebih dari setengah populasi dunia kini aktif menggunakan platform media sosial untuk berkomunikasi, berinteraksi, berbisnis, dan berekspresi secara daring. Penggunaan media sosial mencapai skala global yang belum pernah terjadi sebelumnya, dengan tingkat adopsi yang terus meningkat setiap tahunnya. Namun, di balik dampak positifnya seperti kemudahan komunikasi, peningkatan akses informasi, dan peluang ekonomi digital media sosial juga menciptakan ruang baru bagi aktivitas kriminal yang disebut kejahatan dunia maya (cybercrime) (Purboningsih et al., 2023). Kejahatan ini dilakukan melalui atau berdampak pada sistem digital, jaringan, atau perangkat elektronik, dan sering memanfaatkan kelemahan teknologi serta perilaku sosial pengguna untuk mencapai tujuan jahatnya. Media sosial, dengan jumlah pengguna yang masif dan data pribadi yang terpusat, telah menjadi medan subur bagi para pelaku kejahatan dunia maya untuk melakukan berbagai tindak pidana, termasuk penipuan online, pencurian identitas, penyebaran konten ilegal, dan penyalahgunaan data pribadi (Liviani, 2020).

Secara global, dampak kejahatan dunia maya sangatlah luas dan merugikan secara finansial maupun sosial. Laporan FBI *Internet Crime Complaint Center (IC3)* menyatakan bahwa kerugian akibat cybercrime pada tahun 2024 mencapai lebih dari USD 16 miliar, meningkat sekitar sepertiga dibanding tahun sebelumnya, meskipun angka ini sebagian kecil dari kerugian nyata karena banyak kasus tidak dilaporkan (Reuters, 2025). Selain itu, berbagai institusi riset melaporkan bahwa jutaan

akun media sosial diretas setiap tahunnya. Diperkirakan pada tahun 2025, lebih dari 429 juta akun media sosial menjadi korban peretasan, dengan peningkatan tren yang terus berlanjut (Franetic, 2025). Di Indonesia sendiri, fenomena kejahatan dunia maya juga menunjukkan kecenderungan peningkatan yang signifikan. Data dari aplikasi pengaduan kriminal nasional melaporkan bahwa pada tahun 2022 terdapat 8.636 kasus kejahatan siber yang ditangani oleh aparat penegak hukum, dan jumlah ini melonjak drastis menjadi lebih dari 32.000 laporan hingga Januari 2025, dengan hampir 29.000 korban teridentifikasi. Jenis tindak pidana yang tercatat sangat beragam, mulai dari penipuan online hingga pencemaran nama baik dan ancaman kekerasan digital (Mustopa & Dewi, 2026). Sementara itu, survei dan penelitian lokal juga menunjukkan bahwa media sosial seperti WhatsApp, Instagram, dan Facebook menjadi platform utama yang sering dimanfaatkan oleh pelaku kejahatan untuk melakukan penipuan, penyebaran hoaks, dan tindakan kriminal lainnya.

Kejahatan dunia maya melalui media sosial bukan hanya sekedar masalah kriminal biasa, tetapi memiliki dimensi hukum (yuridis) dan sosial yang kompleks. Secara yuridis, negara-negara telah mencoba merespon fenomena ini dengan membentuk regulasi dan kerangka hukum yang relevan. Di Indonesia, undang-undang dan peraturan mengenai Sistem Elektronik dan Informasi, Perlindungan Data Pribadi, serta tindak pidana terkait penyalahgunaan teknologi telah mengalami perkembangan sebagai respons terhadap ancaman yang terus meningkat. Namun demikian, implementasi hukum sering kali menghadapi tantangan besar mulai dari kurangnya literasi digital masyarakat, kesulitan dalam penegakan hukum lintas batas negara, hingga kompleksitas teknologi yang berkembang cepat. Secara sosial, dampak kejahatan dunia maya juga sangat meresahkan. Selain kerugian finansial, para korban sering mengalami gangguan psikologis akibat pencemaran nama baik, penipuan emosional, serta intimidasi berbasis daring. Penelitian akademik menunjukkan bahwa kurangnya kesadaran dan literasi digital di kalangan pengguna merupakan salah satu faktor utama meningkatnya kerentanan terhadap serangan siber dan eksploitasi kriminal di media sosial. Algoritma platform sendiri yang mendukung personalisasi konten berdasarkan preferensi pengguna tanpa memperhatikan aspek keamanan sering memperkuat penyebaran informasi manipulatif atau berbahaya.

Berdasarkan fenomena tersebut, dapat dikatakan bahwa media sosial telah berubah dari sekedar ruang interaksi sosial menjadi medan pertempuran digital yang kompleks, di mana ancaman kejahatan dunia maya terus berubah dalam bentuk, modus, dan dampaknya. Penjahat dunia maya memanfaatkan celah teknologi, perilaku sosial, serta kurangnya pengaturan hukum yang komprehensif untuk mencapai tujuan mereka, sehingga memerlukan pendekatan yang lebih mendalam dalam kajian akademik, khususnya dari perspektif yuridis dan sosial. Kajian yuridis terhadap kejahatan dunia maya pada platform media sosial mendasarkan diri pada analisis norma hukum positif yang berlaku serta interpretasi hukum dalam konteks dinamika digital. Hal ini mencakup studi terhadap undang-undang dan peraturan nasional, putusan pengadilan, serta perbandingan hukum internasional dalam menangani kejahatan siber. Pendekatan ini penting untuk menunjukkan seberapa efektif kerangka peraturan yang ada dalam menangkap fenomena kejahatan yang bersifat lintas negara dan sering memanfaatkan celah regulasi. Selain itu, kajian yuridis juga mempertimbangkan aspek sanksi pidana, prosedur penegakan hukum, serta kesesuaian prinsip hukum dengan hak-hak asasi manusia dalam konteks kebebasan berekspresi dan privasi di dunia digital.

Sementara itu, kajian sosial berupaya menganalisis dampak kejahatan dunia maya dari sudut pandang masyarakat. Pendekatan ini mencakup studi tentang perilaku pengguna media

sosial, tingkat literasi digital masyarakat, efek psikologis terhadap korban, serta persepsi publik terhadap keamanan siber. Aspek sosial juga mengeksplorasi bagaimana media sosial membentuk wacana publik, memengaruhi opini, dan berkontribusi terhadap dinamika sosial baik positif maupun negatif. Dalam konteks ini, kejahatan dunia maya sering mencerminkan ketimpangan sosial dan ekonomi, di mana kelompok rentan cenderung menjadi sasaran utama penipuan dan eksploitasi digital. Dalam praktiknya, fenomena kejahatan dunia maya di media sosial juga menimbulkan tantangan tersendiri bagi penegak hukum dan pembuat kebijakan (Pramudita et al., 2025). Perkembangan teknologi yang sangat cepat menuntut regulasi yang adaptif, sementara sifat lintas batas internet menyulitkan koordinasi antarnegara dalam penyidikan dan penindakan. Selain itu, isolasi hukum nasional sering kali menghadapi batasan ketika harus menangani pelaku yang berada di luar yurisdiksi nasional. Oleh karena itu, muncul kebutuhan untuk memperkuat kerja sama internasional, harmonisasi regulasi, dan adopsi teknologi penegakan hukum yang canggih.

Kejahatan dunia maya yang beraksi melalui media sosial merupakan fenomena multidimensi yang membutuhkan perhatian serius dari berbagai pihak bukan hanya akademisi, tetapi juga pembuat kebijakan, penegak hukum, platform teknologi, dan masyarakat umum. Pendekatan yuridis dan sosial dalam penelitian ini diharapkan dapat memberikan gambaran komprehensif mengenai karakteristik kejahatan siber di platform media sosial, serta menawarkan rekomendasi strategis dalam upaya pencegahan, penanganan, dan penegakan hukum yang lebih efektif (Idris et al., 2024). Kebutuhan untuk meningkatkan literasi digital, memperkuat kerangka hukum, serta mengembangkan teknologi pertahanan siber yang inovatif merupakan bagian integral dari solusi terhadap ancaman kejahatan dunia maya di era digital yang semakin kompleks.

2. TINJAUAN PUSTAKA

2.1 Konsep Kejahatan Dunia Maya (Cybercrime)

Konsep kejahatan dunia maya atau *cybercrime* merupakan fenomena kompleks yang telah berkembang seiring pesatnya transformasi digital global. Pada dasarnya, tidak ada satu definisi tunggal yang diterima secara universal untuk menjelaskan kejahatan dunia maya. Namun, para ahli dan lembaga internasional telah merumuskan pemahaman konseptual yang mencakup elemen-elemen esensial dari fenomena ini. Secara sederhana, kejahatan dunia maya dapat diartikan sebagai segala aktivitas melanggar hukum yang memanfaatkan teknologi informasi dan komunikasi (TIK), baik sebagai sasaran kejahatan maupun sebagai alat untuk melakukan kejahatan (UNODC, 2020). Konsep ini membedakannya dari kejahatan konvensional karena sifatnya yang tidak mengenal batas fisik atau geografis, dapat dilakukan dengan upaya yang lebih ringan, serta kecepatan dan jangkauannya yang luar biasa.

Untuk memahami konsep ini lebih dalam, para kriminolog dan penegak hukum mengkategorikan kejahatan dunia maya ke dalam beberapa tipologi. David S. Wall, seorang ahli kriminologi terkemuka, mengajukan tipologi yang komprehensif dengan membagi *cybercrime* ke dalam empat kategori utama. Pertama adalah cybertrespass, yang merujuk pada pelanggaran batas kepemilikan digital, seperti peretasan (*hacking*) untuk memasuki sistem orang lain tanpa izin. Kedua, cyberdeception and theft, yang mencakup berbagai bentuk pencurian dan penipuan di dunia maya seperti pembajakan digital (*digital piracy*), penipuan, dan pencurian identitas. Ketiga, cyberporn and obscenity, yang meliputi konten-konten seksual yang menyimpang atau terlarang,

termasuk pornografi anak. Keempat adalah cyberviolence, yang merepresentasikan penyebaran materi berbahaya atau merugikan secara *online*, seperti penguntitan maya (*online stalking*), perundungan maya (*cyberbullying*), hingga terorisme (Perkins, 2024).

Pendekatan lain yang lebih sederhana dan banyak digunakan oleh lembaga penegak hukum seperti Europol dan BKA (Bundeskriminalamt, Jerman) adalah dengan membagi *cybercrime* menjadi dua kelompok besar berdasarkan peran teknologi. Kelompok pertama adalah cyber-dependent crimes, yaitu kejahatan yang hanya dapat dilakukan dengan menggunakan komputer, jaringan komputer, atau TIK lainnya. Dengan kata lain, kejahatan ini tidak akan ada tanpa teknologi digital. Contohnya termasuk penyebaran *malware* (perangkat lunak berbahaya), serangan *ransomware* yang mengenkripsi data korban dan meminta tebusan, serta serangan DDoS (*Distributed Denial of Service*) yang membuat sebuah layanan *online* menjadi tidak tersedia dengan membanjiri lalu lintas palsu. Kelompok kedua adalah cyber-enabled crimes, yaitu kejahatan tradisional yang keberadaannya sudah ada sebelum internet, namun kini difasilitasi dan ditingkatkan jangkauannya oleh teknologi digital (Alawida et al., 2020). Contohnya adalah penipuan, pencurian identitas, perdagangan narkoba, atau prostitusi *online* yang kini dapat dilakukan secara lintas batas dengan lebih mudah dan anonim.

Konsep *cybercrime* juga tidak terlepas dari dampaknya yang sangat luas dan merusak, yang telah melampaui sekadar kerugian finansial. Serangan siber kini dianggap sebagai ancaman serius terhadap perekonomian global, keamanan nasional, hingga keselamatan jiwa manusia. Sebuah laporan memproyeksikan bahwa kerugian global akibat kejahatan dunia maya pada tahun 2025 mencapai angka yang mencengangkan, yaitu 10,5 triliun dolar AS. Lebih dari itu, serangan terhadap infrastruktur kritis seperti rumah sakit dapat berakibat fatal. Contohnya, serangan *ransomware* pada Juni 2024 terhadap layanan kesehatan nasional di Inggris Raya tidak hanya menyebabkan kerugian finansial tetapi juga mengganggu lebih dari 10.000 janji temu medis dan setidaknya menyebabkan satu pasien meninggal dunia akibat tertundanya perawatan (TTXVN, 2025). Hal ini menunjukkan bahwa dampak kejahatan dunia maya bersifat nyata dan dapat mengancam nyawa.

Selain kerugian fisik dan ekonomi, kejahatan dunia maya juga meninggalkan luka psikologis yang mendalam bagi para korbannya. Perkembangan kecerdasan buatan atau *artificial intelligence* (AI) semakin memperparah situasi ini dengan mengaburkan batas antara realitas dan kepalsuan. Serangan yang menggunakan teknologi *deepfake* untuk memalsukan identitas meningkat lebih dari 700% pada tahun 2023. Di Amerika Serikat, dilaporkan bahwa 16% korban pencurian identitas pernah memiliki pikiran untuk bunuh diri, yang mencerminkan konsekuensi kesehatan mental yang parah dari kejahatan ini (TTXVN, 2025). Jenis kejahatan seperti perundungan maya, *sextortion*, dan eksploitasi *deepfake* sangat rentan menimpa kelompok wanita dan anak-anak, sehingga diperlukan sistem dukungan korban yang lebih baik dan respons cepat untuk menurunkan konten negatif.

Dalam perkembangannya, lanskap kejahatan dunia maya telah bertransformasi menjadi sebuah ekosistem ekonomi bawah tanah yang sangat terorganisir dan profesional, sering disebut sebagai "Cybercrime-as-a-Service" (CaaS). Konsep ini mirip

dengan model bisnis legal, di mana para pelaku kejahatan tidak perlu lagi memiliki keahlian teknis yang tinggi. Mereka dapat membeli "layanan" kejahatan di pasar gelap (*darknet*), seperti membeli kit *ransomware*, alat *phishing*, atau layanan peretasan dari penjual lain (Communications Security Establishment Canada, 2024). Model bisnis ini menurunkan barrier to entry bagi calon penjahat dunia maya dan membuat siklus kejahatan menjadi lebih sulit diberantas karena sifatnya yang modular dan anonim. Uang kripto seperti Bitcoin sering digunakan untuk mencuci hasil kejahatan dalam ekosistem ini, mempersulit pelacakan oleh otoritas.

Menghadapi kompleksitas dan sifat kejahatan dunia maya yang tanpa batas, respons yang efektif tidak dapat dilakukan oleh satu negara atau entitas saja. Diperlukan pendekatan kolaboratif dan strategis yang melibatkan banyak pemangku kepentingan. Kerja sama internasional menjadi kunci utama, di mana lembaga seperti INTERPOL, Europol, dan kepolisian nasional dari berbagai negara harus bertukar informasi dan melakukan operasi bersama secara real-time. Selain itu, kemitraan publik-swasta juga krusial (Sarkar & Shukla, 2023). Perusahaan teknologi dan penyedia layanan internet berada di garis depan dan memiliki data serta kapabilitas untuk mendeteksi serta mencegah kejahatan sejak dini. Pendekatan pertahanan sistemik yang komprehensif mencakup tiga pilar: pencegahan dengan memperkuat keamanan infrastruktur digital, perlindungan dengan merancang produk digital yang aman secara bawaan, dan mitigasi dengan berbagi sinyal ancaman secara cepat untuk merespons serangan.

2.2 Media Sosial sebagai Ruang Kriminogenik

Media sosial dalam perkembangan masyarakat digital modern tidak lagi sekadar berfungsi sebagai sarana komunikasi dan berbagi informasi, tetapi telah berkembang menjadi ruang sosial virtual yang memiliki karakteristik kompleks dan dinamis. Dalam perspektif kriminologi, media sosial dapat dipahami sebagai *ruang kriminogenik*, yakni lingkungan yang secara struktural dan situasional berpotensi memfasilitasi terjadinya tindak kejahatan. Istilah kriminogenik merujuk pada kondisi atau faktor yang mendorong atau memungkinkan timbulnya perilaku kriminal. Media sosial memiliki sejumlah karakteristik yang membuatnya rentan terhadap eksploitasi oleh pelaku kejahatan, mulai dari keterbukaan akses, anonimitas pengguna, hingga masifnya distribusi informasi tanpa batas geografis (Tanaka et al., 2025).

Salah satu faktor utama yang menjadikan media sosial bersifat kriminogenik adalah tingkat keterbukaan informasi pribadi yang tinggi. Platform seperti Facebook, Instagram, TikTok, dan X memungkinkan pengguna membagikan data pribadi secara sukarela, termasuk identitas, lokasi, aktivitas harian, hingga preferensi pribadi. Informasi ini sering kali digunakan oleh pelaku kejahatan untuk melakukan penipuan, pencurian identitas, *social engineering*, atau bahkan pemerasan digital. Dalam konteks ini, media sosial menyediakan target yang sesuai (suitable target) sebagaimana dijelaskan dalam *Routine Activity Theory* yang dikemukakan oleh Lawrence E. Cohen dan Marcus Felson. Teori tersebut menyatakan bahwa kejahatan terjadi ketika terdapat tiga elemen utama: pelaku yang termotivasi, target yang rentan, dan ketiadaan pengawasan yang efektif (Leukfeldt, 2014). Media sosial secara inheren menghadirkan ketiga elemen tersebut dalam satu ekosistem digital.

Selain keterbukaan informasi, anonimitas dan kemudahan pembuatan akun juga memperkuat sifat kriminogenik media sosial. Pelaku dapat dengan mudah menciptakan identitas palsu atau akun anonim untuk menyamarkan diri, sehingga memperkecil risiko terdeteksi. Identitas digital yang fleksibel ini memungkinkan terjadinya berbagai bentuk kejahatan seperti penipuan daring, penyebaran ujaran kebencian, perundungan siber (*cyberbullying*), hingga penyebaran konten ilegal. Anonimitas menurunkan hambatan psikologis (psychological barriers) untuk melakukan tindakan menyimpang karena pelaku merasa tidak terikat oleh norma sosial yang biasanya berlaku dalam interaksi tatap muka. Fenomena ini dikenal sebagai *online disinhibition effect*, yaitu kecenderungan individu untuk bertindak lebih agresif atau tidak etis di dunia maya dibandingkan di dunia nyata.

Karakteristik algoritmik media sosial juga turut berkontribusi terhadap terciptanya ruang kriminogenik. Platform digital menggunakan algoritma berbasis keterlibatan (*engagement-based algorithm*) yang dirancang untuk memaksimalkan interaksi pengguna. Konten yang bersifat provokatif, sensasional, atau emosional cenderung mendapatkan distribusi lebih luas dibandingkan konten informatif yang netral (Gunawan, 2026). Kondisi ini membuka peluang bagi penyebaran hoaks, disinformasi, propaganda, serta konten manipulatif yang dapat menimbulkan dampak sosial serius. Dalam banyak kasus, pelaku kejahatan memanfaatkan mekanisme algoritma tersebut untuk memperluas jangkauan tindakannya secara cepat dan masif.

Dari perspektif teori pembelajaran sosial (*Social Learning Theory*) yang dikembangkan oleh Albert Bandura, media sosial juga menjadi ruang di mana perilaku menyimpang dapat dipelajari dan direplikasi melalui observasi. Individu yang terpapar pada konten kekerasan, ujaran kebencian, atau praktik penipuan tertentu dapat terdorong untuk meniru perilaku tersebut, terutama apabila tidak terdapat konsekuensi hukum yang terlihat secara langsung (Saputra & Karsiwan, 2024). Media sosial dengan demikian tidak hanya menjadi sarana kejahatan, tetapi juga medium transmisi nilai-nilai menyimpang.

Aspek lain yang menjadikan media sosial sebagai ruang kriminogenik adalah sifatnya yang lintas batas (borderless). Internet tidak mengenal batas teritorial negara, sehingga pelaku kejahatan dapat beroperasi dari yurisdiksi yang berbeda dengan korban (Idul et al., 2026). Kondisi ini menyulitkan penegakan hukum karena adanya perbedaan sistem hukum, keterbatasan kerja sama internasional, serta kompleksitas pembuktian digital. Situasi tersebut memperbesar peluang pelaku untuk memanfaatkan celah regulasi (regulatory gaps) dan kelemahan koordinasi antarnegara. Dari sudut pandang sosial, media sosial juga mencerminkan ketimpangan literasi digital di masyarakat. Kelompok dengan tingkat literasi digital rendah lebih rentan terhadap manipulasi informasi dan penipuan daring. Kurangnya pemahaman mengenai keamanan siber, privasi digital, dan verifikasi informasi menjadikan sebagian pengguna sebagai sasaran empuk pelaku kejahatan (Parwitasari et al., 2025). Di sisi lain, perkembangan teknologi yang cepat sering kali tidak diimbangi dengan peningkatan kapasitas pengawasan dan edukasi masyarakat, sehingga risiko sosial semakin meningkat.

Konsep *risk society* yang diperkenalkan oleh Ulrich Beck relevan untuk menjelaskan fenomena ini. Beck menyatakan bahwa masyarakat modern menghasilkan risiko-risiko baru sebagai konsekuensi dari modernisasi itu sendiri. Media sosial sebagai produk modernitas digital menghadirkan risiko sistemik yang tidak selalu dapat dikendalikan melalui mekanisme tradisional (Anugrah et al., 2023). Risiko tersebut bersifat global, tidak kasat mata, dan dapat berdampak luas dalam waktu singkat.

2.3 Bentuk-Bentuk Kejahatan Dunia Maya di Media Sosial

Salah satu bentuk yang paling dominan adalah penipuan daring (online fraud). Penipuan di media sosial umumnya dilakukan melalui teknik *social engineering*, yaitu manipulasi psikologis untuk memperoleh informasi atau keuntungan tertentu. Modus yang sering digunakan meliputi penipuan investasi palsu, undian berhadiah fiktif, toko online palsu, hingga penyamaran sebagai institusi resmi. Pelaku memanfaatkan kepercayaan sosial dan kedekatan emosional yang dibangun melalui interaksi digital untuk meyakinkan korban (Sahara & Kuswandi, 2025). Dalam banyak kasus, pelaku menggunakan akun palsu atau meretas akun korban lain untuk meningkatkan kredibilitas. Variasi lain dari penipuan daring adalah *romance scam*, di mana pelaku membangun hubungan emosional dengan korban sebelum meminta sejumlah uang dengan alasan darurat. Bentuk ini sering menimbulkan kerugian finansial sekaligus trauma psikologis.

Bentuk kedua adalah phishing dan pencurian identitas (identity theft). Phishing dilakukan dengan cara mengirimkan tautan atau pesan palsu yang menyerupai situs resmi untuk memperoleh data pribadi seperti kata sandi, nomor kartu kredit, atau kode OTP. Media sosial sering menjadi sarana distribusi tautan phishing karena tingkat interaksi pengguna yang tinggi. Data pribadi yang berhasil diperoleh kemudian digunakan untuk mengambil alih akun korban atau melakukan transaksi illegal (Iskandar, 2024). Pencurian identitas juga dapat terjadi ketika pelaku membuat akun palsu dengan menggunakan foto dan informasi pribadi milik orang lain. Tindakan ini dapat digunakan untuk penipuan, pencemaran nama baik, maupun aktivitas kriminal lainnya.

Selanjutnya adalah perundungan siber (cyberbullying) dan ujaran kebencian (hate speech). Cyberbullying terjadi ketika seseorang secara berulang kali menjadi sasaran penghinaan, ancaman, atau pelecehan melalui media sosial. Bentuknya dapat berupa komentar merendahkan, penyebaran rumor, hingga doxing (penyebaran data pribadi tanpa izin). Dampaknya sangat serius, terutama bagi remaja dan kelompok rentan, karena dapat menyebabkan gangguan psikologis seperti kecemasan, depresi, bahkan kecenderungan bunuh diri (Syahid et al., 2022). Ujaran kebencian di media sosial juga menjadi persoalan serius karena berpotensi memicu konflik sosial berbasis suku, agama, ras, dan antargolongan. Penyebaran konten bermuatan kebencian sering diperkuat oleh algoritma platform yang memprioritaskan konten dengan tingkat keterlibatan tinggi.

Bentuk kejahatan lain yang marak adalah penyebaran hoaks dan disinformasi. Media sosial memungkinkan informasi menyebar secara viral dalam waktu singkat tanpa proses verifikasi yang memadai. Pelaku dapat menyebarkan berita palsu untuk tujuan politik, ekonomi, maupun ideologis. Disinformasi sering dirancang secara

sistematis dengan memanfaatkan bot atau akun palsu untuk menciptakan ilusi dukungan publik (Aïmeur et al., 2023). Dampaknya tidak hanya merugikan individu, tetapi juga dapat mengganggu stabilitas sosial dan demokrasi.

Selain itu, terdapat pula pemerasan dan eksploitasi seksual berbasis digital, seperti *sextortion*. Dalam modus ini, pelaku memperoleh foto atau video pribadi korban melalui tipu daya atau peretasan, kemudian mengancam akan menyebarkannya jika korban tidak memberikan sejumlah uang. Kejahatan ini semakin meningkat dengan tingginya penggunaan media sosial berbasis visual. Eksploitasi seksual terhadap anak melalui media sosial juga menjadi perhatian serius karena melibatkan jaringan lintas negara dan memanfaatkan anonimitas digital (Ray & Henry, 2025).

Tidak hanya individu, entitas bisnis dan figur publik juga menjadi target kejahatan dunia maya di media sosial. Serangan terhadap akun resmi perusahaan dapat merusak reputasi dan menimbulkan kerugian finansial besar. Selain itu, manipulasi opini publik melalui kampanye digital terkoordinasi dapat memengaruhi persepsi masyarakat terhadap isu tertentu.

Dari perspektif hukum, berbagai bentuk kejahatan tersebut di Indonesia diatur dalam Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, serta diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Regulasi tersebut mencakup larangan akses ilegal, manipulasi data elektronik, distribusi konten melanggar hukum, hingga penyalahgunaan data pribadi. Namun demikian, tantangan penegakan hukum tetap besar karena sifat kejahatan yang lintas batas dan cepat berubah.

2.4 Penelitian Terdahulu

Penelitian oleh Nai & Hoesein (2026) yang berjudul "Analisis Yuridis Terhadap Perlindungan Hukum Bagi Korban Kejahatan Siber di Indonesia" menyoroti isu krusial mengenai efektivitas perlindungan korban di tengah maraknya kejahatan siber. Meskipun Indonesia telah memiliki instrumen hukum seperti UU ITE dan UU Perlindungan Saksi dan Korban, studi yuridis normatif ini menemukan bahwa implementasi perlindungan bagi korban masih jauh dari optimal. Hambatan utama teridentifikasi dalam tiga aspek: substansi hukum yang belum sepenuhnya mengakomodasi dinamika kejahatan siber, struktur kelembagaan yang lemah dalam koordinasi antar aparat penegak hukum, dan budaya hukum masyarakat yang masih rendah. Penelitian ini menawarkan solusi melalui pendekatan hukum responsif, yang menekankan pada model perlindungan yang adaptif terhadap perkembangan teknologi, partisipatif dengan melibatkan berbagai pemangku kepentingan, serta berorientasi pada keadilan substantif bagi korban, terutama melalui penguatan mekanisme restitusi dan kompensasi yang selama ini belum efektif.

Sementara itu, penelitian oleh Ayman & Nurhadiyanto (2025) dalam "Analisis Kejahatan Siber Sniffing pada Media Sosial WhatsApp" secara spesifik mengkaji modus kejahatan sniffing yang marak terjadi. Dengan menggunakan metode kualitatif dan wawancara dengan pihak Bareskrim, penelitian ini menemukan bahwa karakteristik ruang siber menjadi faktor kriminogenik utama. Konsep aksesibilitas, anonimitas, dan fleksibilitas identitas yang dijelaskan dalam Space Transition Theory memungkinkan pelaku untuk melakukan penyadapan data dengan risiko rendah dan sulit dilacak.

Studi ini memaparkan modus operandi yang umum, seperti pengiriman file APK berkedok kurir paket, serta mengkaji pertanggungjawaban hukum pelaku. Menariknya, penelitian ini menyimpulkan adanya tumpang tindih norma antara UU ITE dan UU PDP, dan berdasarkan asas lex specialis derogat legi generalis, ketentuan dalam UU PDP dinilai lebih relevan untuk menjerat pelaku sniffing karena fokusnya pada perlindungan data pribadi, meskipun ancaman hukumannya lebih rendah.

Dari perspektif yang lebih umum, penelitian Putri et al. (2024) berjudul "Analisis Yuridis Terhadap Penegakan dan Pengaturan Hukum Kejahatan Dunia Maya (Cybercrime) di Indonesia" mengkaji upaya penegakan hukum melalui dua jalur utama, yaitu penal dan non-penal. Penelitian normatif ini menegaskan bahwa secara penal, UU ITE beserta perubahannya menjadi landasan utama untuk mengkriminalisasi berbagai tindak pidana siber, termasuk yang diatur dalam undang-undang sektoral lainnya. Namun, penelitian ini juga menyoroti keterbatasan hukum pidana sebagai "ultimum remedium" yang hanya bersifat simptomatik dan tidak mampu menjangkau akar masalah. Oleh karena itu, pendekatan non-penal melalui edukasi masyarakat, peningkatan kapasitas aparat penegak hukum, serta penguatan kerja sama internasional menjadi sangat krusial. Penelitian ini menyimpulkan bahwa efektivitas penegakan hukum siber membutuhkan modernisasi regulasi dan peningkatan keahlian aparat, mengingat sifat kejahatan siber yang dinamis dan transnasional.

Fokus pada sektor perbankan diangkat oleh Ningrum & Robekha (2022) dalam "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia". Penelitian kualitatif dengan pendekatan studi kasus ini menganalisis rentetan serangan siber yang menimpa bank-bank di Indonesia, seperti Bank Indonesia, BRI, dan Bank Syariah Indonesia. Temuan utama penelitian ini menyoroti ironi antara gencarnya promosi layanan digital banking oleh pemerintah dan industri perbankan dengan lemahnya sistem keamanan siber yang ada. Kasus peretasan dan kebocoran data nasabah dalam jumlah besar menjadi bukti nyata kerentanan tersebut. Lebih jauh, penelitian ini mengkritisi ketiadaan payung hukum yang jelas mengenai pertanggungjawaban penyedia jasa (bank) atas kelalaian dalam menjaga data nasabah. UU ITE selama ini lebih berfokus pada penghukuman pelaku, sementara perlindungan dan mekanisme ganti rugi bagi nasabah yang dirugikan akibat lemahnya sistem keamanan perbankan belum diatur secara tegas.

Terakhir, penelitian oleh (Sihombing et al., 2025) yang berjudul "Analisis Yuridis Peningkatan Kejahatan Digital Berbasis Media Sosial (Studi Penelitian Polda Kepulauan Riau)" memberikan perspektif empiris dari praktik penegakan hukum di tingkat kewilayahan. Dengan melakukan wawancara di Polda Kepri, penelitian ini menemukan bahwa implementasi UU ITE dalam menangani kejahatan seperti judi online dan penipuan telah berjalan cukup efektif, salah satunya dibuktikan dengan keberhasilan pengungkapan kasus promosi judi online. Namun, studi ini juga mengidentifikasi sejumlah kendala signifikan, seperti pasal-pasal dalam UU ITE yang masih multitafsir (misalnya tentang "kesusilaan") sehingga menyulitkan penyidik, serta terbatasnya yurisdiksi untuk menindak pelaku yang menggunakan server di luar negeri. Penelitian ini merekomendasikan pembaruan regulasi yang lebih adaptif,

peningkatan kapasitas sumber daya manusia dan teknologi forensik di kepolisian, serta penguatan literasi digital masyarakat sebagai solusi komprehensif.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur (library research) untuk menganalisis kejahatan dunia maya pada platform media sosial dari perspektif yuridis dan sosial. Objek yang diteliti mencakup dua aspek utama: pertama, aspek yuridis yang mengkaji pengaturan hukum kejahatan siber di media sosial berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan terkait lainnya; kedua, aspek sosial yang menganalisis faktor-faktor kriminogenik seperti anonimitas dan aksesibilitas yang menjadikan media sosial sebagai ruang subur bagi kejahatan, serta dampaknya terhadap korban dan masyarakat. Sumber data penelitian seluruhnya berasal dari data sekunder, yang terdiri dari bahan hukum primer (peraturan perundang-undangan), bahan hukum sekunder (lima jurnal ilmiah terdahulu yang telah diulas, buku teks, dan artikel jurnal lainnya), serta bahan hukum tersier (kamus hukum dan artikel berita terpercaya). Data diperoleh melalui proses penelusuran sistematis dengan kata kunci relevan, kemudian dikategorisasi dan dianalisis berdasarkan topik yuridis dan sosial. Sebagai penelitian kualitatif, pengukuran tidak dilakukan secara statistik melainkan melalui telah mendalam terhadap konsistensi norma dan identifikasi hambatan implementasi untuk aspek yuridis, serta analisis faktor kerentanan dan dampak sosial untuk aspek sosial. Keunggulan metode studi literatur ini terletak pada kemampuannya memberikan analisis komprehensif melalui sintesis berbagai sumber berkualitas. Dengan menggabungkan temuan dari lima jurnal terdahulu yang memiliki fokus beragam—mulai dari perlindungan korban, analisis modus operandi sniffing, penegakan hukum, hingga studi kasus perbankan dan kewilayahan—penelitian ini mampu mengidentifikasi benang merah dan kesenjangan penelitian (research gap) yang belum terungkap dalam studi-studi sebelumnya. Pendekatan ini menawarkan cakupan yang lebih luas dan perspektif yang lebih general dibandingkan penelitian lapangan yang terbatas pada lokasi atau kasus tertentu, sekaligus menghubungkan secara simultan dimensi yuridis dan sosial dalam memahami fenomena kejahatan dunia maya di media sosial.

4. HASIL DAN PEMBAHASAN

Maraknya kasus penipuan online, perundungan siber (cyberbullying), ujaran kebencian, hingga kebocoran data pribadi menunjukkan bahwa media sosial yang awalnya dirancang sebagai ruang interaksi positif telah bertransformasi menjadi ladang subur bagi berbagai aktivitas kriminal. Fenomena ini menuntut pemahaman yang holistik, tidak hanya dari perspektif hukum yang mengatur larangan dan sanksi, tetapi juga dari perspektif sosial yang menjelaskan mengapa ruang digital begitu rentan disalahgunakan serta bagaimana dampaknya terhadap kehidupan bermasyarakat. Oleh karena itu, pembahasan dalam penelitian ini akan diuraikan secara sistematis untuk menjawab tiga rumusan masalah utama. Pertama, akan dikaji secara mendalam mengenai pengaturan hukum di Indonesia, khususnya melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan terkait lainnya, dalam upaya menanggulangi kejahatan dunia maya yang terjadi di platform media sosial, termasuk identifikasi berbagai hambatan dalam implementasinya (Syahid et al., 2022). Kedua, analisis akan beralih pada bentuk-bentuk konkret

kejahatan siber yang marak terjadi di media sosial serta dampaknya yang multidimensional terhadap individu dan masyarakat dari perspektif sosial, dengan menggunakan teori kriminologi untuk memahami faktor-faktor kriminogenik yang melekat pada ruang siber. Ketiga, sebagai sintesis dari kedua pembahasan sebelumnya, penelitian ini akan merumuskan model kolaborasi ideal yang melibatkan peran negara, platform media sosial, dan masyarakat dalam upaya pencegahan serta penanggulangan kejahatan dunia maya, karena penegakan hukum semata tidak akan cukup tanpa dukungan literasi digital dan tanggung jawab kolektif seluruh pemangku kepentingan (Sarkar & Shukla, 2023).

2.2 Pengaturan Hukum Kejahatan Siber di Media Sosial

Pengaturan hukum di Indonesia dalam menanggulangi kejahatan dunia maya pada platform media sosial bertumpu pada kerangka hukum nasional yang terus berkembang mengikuti dinamika teknologi digital. Fondasi utama regulasi tersebut adalah Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Revisi tahun 2024 dilakukan sebagai respons atas kritik publik terhadap sejumlah pasal yang dinilai multitafsir sekaligus untuk memperjelas batasan delik dalam ruang digital, termasuk aktivitas pada media sosial (Munir, 2024). UU ITE berfungsi sebagai *lex specialis* yang mengatur perbuatan pidana berbasis sistem elektronik, termasuk distribusi konten, akses ilegal, manipulasi data, dan gangguan terhadap sistem elektronik.

Dalam konteks media sosial, ketentuan yang paling relevan adalah pengaturan mengenai muatan yang dilarang. Pasal 27 ayat (1) UU ITE mengatur larangan mendistribusikan atau mentransmisikan informasi elektronik yang memiliki muatan melanggar kesusilaan. Ketentuan ini kerap digunakan untuk menindak penyebaran konten pornografi atau konten asusila melalui platform seperti Instagram atau X. Pasal 27 ayat (2) mengatur larangan muatan perjudian, yang relevan dengan maraknya promosi judi daring melalui akun media sosial dan fitur siaran langsung (Al-Ayoubi & Suharto, 2025). Sementara itu, perubahan signifikan dalam UU ITE 2024 adalah pemisahan delik pencemaran nama baik menjadi Pasal 27A dan Pasal 27B. Pasal 27A secara tegas mengatur penghinaan atau pencemaran nama baik berbasis elektronik sebagai delik aduan, sedangkan Pasal 27B mengatur pemerasan dan/atau pengancaman melalui sistem elektronik (Wahyuni, 2024). Pemisahan ini dimaksudkan untuk memberikan kejelasan norma dan menghindari kriminalisasi berlebihan terhadap ekspresi di ruang digital.

Pasal 28 ayat (1) UU ITE mengatur larangan penyebaran berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik, sedangkan Pasal 28 ayat (2) mengatur larangan penyebaran informasi yang menimbulkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan antargolongan (SARA). Ketentuan ini menjadi dasar hukum penindakan terhadap penyebaran hoaks dan ujaran kebencian di media sosial seperti Facebook dan TikTok. Ancaman pidana terhadap pelanggaran pasal-pasal tersebut diatur dalam Pasal 45 dan pasal turunannya, dengan sanksi pidana penjara dan/atau denda yang signifikan, sehingga menunjukkan keseriusan negara dalam mengendalikan konten ilegal di ruang digital (Hasanah, 2018).

Selain UU ITE, penanggulangan kejahatan dunia maya juga didukung oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini menjadi tonggak penting dalam perlindungan hak privasi di Indonesia, terutama dalam konteks kebocoran dan penyalahgunaan data pribadi di media sosial. UU PDP mengatur kewajiban pengendali dan pemroses data untuk menjaga keamanan data pribadi serta memberikan sanksi administratif dan

pidana terhadap pelanggaran. Dalam praktiknya, kebocoran data pengguna media sosial yang berujung pada penipuan atau pencurian identitas dapat dijerat melalui ketentuan pidana dalam UU PDP, sehingga melengkapi rezim pengaturan yang sebelumnya lebih berfokus pada aspek distribusi konten (Arief & Purwanto, 2025).

Keterkaitan dengan hukum pidana umum juga tidak dapat diabaikan. Kitab Undang-Undang Hukum Pidana (KUHP), khususnya KUHP baru yang disahkan melalui Undang-Undang Nomor 1 Tahun 2023, tetap relevan untuk menjerat kejahatan konvensional yang bermigrasi ke ranah daring. Misalnya, tindak pidana penipuan, pemerasan, atau ancaman kekerasan yang dilakukan melalui media sosial tetap dapat dijerat menggunakan ketentuan KUHP apabila memenuhi unsur delik umum (Yasin, 2026). Dengan demikian, sistem hukum Indonesia menerapkan pendekatan komplementer antara UU ITE sebagai lex specialis dan KUHP sebagai lex generalis.

Dari sisi kelembagaan, penegakan hukum terhadap kejahatan dunia maya dilakukan oleh Kepolisian Negara Republik Indonesia melalui Direktorat Tindak Pidana Siber Bareskrim Polri, dengan dukungan Kementerian Komunikasi dan Informatika dalam aspek pemutusan akses (take down) konten ilegal. Mekanisme pemblokiran situs atau akun media sosial yang melanggar hukum didasarkan pada kewenangan administratif pemerintah untuk menjaga ketertiban ruang digital. Selain itu, kerja sama internasional juga menjadi elemen penting mengingat karakter lintas batas dari media sosial.

Meskipun kerangka normatif telah relatif komprehensif, implementasi hukum menghadapi sejumlah hambatan struktural dan kultural. Secara struktural, keterbatasan kapasitas aparat dalam bidang digital forensik menjadi tantangan utama. Pembuktian kejahatan siber memerlukan keahlian khusus dalam pelacakan jejak digital, pengamanan barang bukti elektronik, serta pemenuhan standar pembuktian di pengadilan. Kurangnya sumber daya manusia yang terlatih dan infrastruktur teknologi yang memadai sering kali memperlambat proses penyidikan. Koordinasi antar lembaga, baik antara kepolisian, kejaksaan, pengadilan, maupun otoritas administrasi seperti Kominfo, juga belum sepenuhnya optimal, terutama dalam penanganan kasus yang melibatkan pelaku atau server di luar negeri.

Secara kultural, persoalan multitafsir pasal masih menjadi perdebatan. Beberapa kalangan menilai bahwa rumusan pasal terkait pencemaran nama baik dan ujaran kebencian berpotensi menimbulkan ketidakpastian hukum jika tidak diinterpretasikan secara hati-hati. Revisi UU ITE tahun 2024 berupaya menjawab kritik tersebut dengan memperjelas unsur delik dan menegaskan sifat delik aduan untuk penghinaan, namun efektivitasnya sangat bergantung pada konsistensi penegakan hukum. Selain itu, rendahnya literasi digital masyarakat turut memengaruhi efektivitas regulasi, karena banyak pelanggaran terjadi akibat ketidaktahuan pengguna mengenai batasan hukum dalam bermedia sosial (Tompunu et al., 2025).

Dengan demikian, pengaturan hukum di Indonesia dalam menanggulangi kejahatan dunia maya pada platform media sosial telah memiliki dasar normatif yang kuat melalui UU ITE, UU PDP, dan KUHP. Namun, efektivitasnya tidak hanya ditentukan oleh keberadaan norma hukum, melainkan juga oleh kapasitas institusional, koordinasi antar lembaga, serta kesadaran hukum masyarakat. Tantangan ke depan adalah memastikan bahwa regulasi yang ada mampu beradaptasi dengan perkembangan teknologi sekaligus menjamin perlindungan hak asasi manusia dalam ruang digital yang semakin kompleks.

4.1 Bentuk dan Dampak Sosial Kejahatan di Media Sosial

Perkembangan pesat penggunaan media sosial di Indonesia membawa konsekuensi sosial yang kompleks. Dengan tingkat penetrasi internet nasional yang telah melampaui 70% populasi dan mayoritas pengguna aktif di platform seperti Facebook, Instagram, TikTok, dan X, ruang digital menjadi arena interaksi sosial utama Masyarakat (APJII, 2024). Namun, ruang ini juga menjadi medium dominan terjadinya kejahatan siber, khususnya yang bersifat *cyber-enabled crime*, yaitu kejahatan konvensional yang difasilitasi oleh teknologi digital. Secara empiris, laporan penegak hukum menunjukkan peningkatan signifikan kasus penipuan daring, pencemaran nama baik, peretasan akun, hingga penyebaran konten bermuatan kebencian yang sebagian besar bermula dari interaksi di media sosial.

Salah satu bentuk kejahatan paling dominan adalah penipuan online yang memanfaatkan teknik *social engineering*. Modus ini bekerja dengan mengeksploitasi psikologi korban melalui manipulasi emosional atau penciptaan situasi darurat palsu. Pelaku sering menyamar sebagai kerabat, pejabat, atau institusi resmi dan menghubungi korban melalui pesan langsung atau aplikasi perpesanan yang terintegrasi dengan media sosial. Variasi lain adalah *phishing*, yakni pengiriman tautan palsu yang menyerupai situs resmi untuk mencuri data pribadi seperti kata sandi dan kode OTP (Krey & Senandi, 2024). Selain itu, terdapat praktik *sniffing* atau penyadapan data melalui jaringan tidak aman yang memungkinkan pelaku memperoleh kredensial akun korban. Kejahatan ini berdampak langsung pada kerugian finansial, dan dalam banyak kasus melibatkan kebocoran data pribadi yang kemudian disalahgunakan untuk tindak pidana lanjutan.

Bentuk lain yang signifikan adalah perundungan siber (cyberbullying). Perundungan daring terjadi ketika seseorang secara berulang menjadi sasaran hinaan, ancaman, atau pelecehan melalui komentar, unggahan, maupun pesan pribadi. Berbeda dengan perundungan konvensional, cyberbullying bersifat persisten dan memiliki jangkauan luas karena konten dapat disebarluaskan secara viral (United Nations Office for Disaster Risk Reduction, 2025). Dampaknya tidak hanya bersifat sosial tetapi juga psikologis, seperti depresi, kecemasan, kehilangan rasa percaya diri, bahkan kecenderungan menyakiti diri sendiri. Anak-anak dan remaja menjadi kelompok paling rentan karena tingginya intensitas penggunaan media sosial di kalangan ini.

Selanjutnya adalah ujaran kebencian (hate speech) dan penyebaran disinformasi. Konten yang menyerang identitas berbasis suku, agama, ras, dan antargolongan berpotensi memicu konflik sosial yang lebih luas. Dalam konteks hukum Indonesia, perbuatan tersebut dapat dijerat melalui ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 yang merevisi Undang-Undang Nomor 11 Tahun 2008, khususnya Pasal 28 ayat (2) mengenai penyebaran informasi yang menimbulkan kebencian atau permusuhan berbasis SARA. Selain itu, penyebaran berita bohong yang merugikan konsumen dalam transaksi elektronik diatur dalam Pasal 28 ayat (1). Fenomena ini menunjukkan bahwa media sosial tidak hanya menjadi ruang interaksi pribadi, tetapi juga arena kontestasi opini publik yang rentan dimanipulasi (Arifin et al., 2025).

Untuk memahami mengapa media sosial menjadi ruang kriminogenik, *Space Transition Theory* yang dikemukakan oleh K. Jaishankar memberikan kerangka analitis yang relevan. Teori ini menjelaskan bahwa individu yang dalam kehidupan nyata mungkin tidak menunjukkan perilaku menyimpang dapat melakukan kejahatan ketika berada di ruang siber karena adanya perubahan karakteristik ruang (Waruwu & Srihadiati, 2023). Faktor anonimitas, fleksibilitas identitas, dan lemahnya kontrol sosial formal maupun informal menciptakan kondisi yang memungkinkan pelaku bertindak tanpa rasa takut terhadap konsekuensi langsung. Dalam ruang siber, identitas dapat

dimodifikasi atau disembunyikan, sehingga norma sosial yang berlaku di dunia nyata menjadi kurang efektif. Selain itu, interaksi daring yang tidak melibatkan kontak fisik mengurangi empati pelaku terhadap korban, sehingga tindakan agresif atau manipulatif lebih mudah dilakukan.

Dampak sosial dari kejahatan dunia maya di media sosial sangat luas dan tidak terbatas pada kerugian materiil. Kerugian finansial akibat penipuan online memang signifikan, tetapi kerugian immateriil sering kali lebih mendalam. Korban dapat mengalami trauma psikologis, gangguan kecemasan, hingga kehilangan kepercayaan terhadap interaksi digital. Dalam kasus pencemaran nama baik atau penyebaran konten pribadi tanpa izin, reputasi sosial korban dapat rusak secara permanen karena jejak digital sulit dihapus sepenuhnya. Reputasi yang tercemar dapat berdampak pada relasi sosial, kesempatan kerja, dan kehidupan pribadi korban.

Selain itu, maraknya hoaks dan ujaran kebencian di media sosial berdampak pada melemahnya kohesi sosial. Informasi palsu yang disebarluaskan secara masif dapat memicu polarisasi dan konflik horizontal di masyarakat. Ketika masyarakat terpapar konten yang memecah belah secara terus-menerus, rasa saling percaya (social trust) menurun dan solidaritas sosial terganggu. Dalam jangka panjang, kondisi ini dapat mengancam stabilitas sosial dan demokrasi.

Dari perspektif viktimologi, kelompok tertentu memiliki tingkat kerentanan lebih tinggi. Perempuan sering menjadi target kekerasan berbasis gender daring, termasuk pelecehan seksual dan *sextortion*. Anak-anak dan remaja rentan terhadap eksploitasi seksual dan perundungan siber karena kurangnya literasi digital dan kontrol orang tua. Lansia juga menjadi sasaran empuk penipuan daring karena keterbatasan pemahaman teknologi (Mármol et al., 2025). Perlindungan terhadap kelompok rentan ini diperkuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur kewajiban perlindungan data pribadi serta sanksi pidana bagi penyalahgunaan data, serta ketentuan dalam Kitab Undang-Undang Hukum Pidana yang tetap relevan untuk menjerat tindak pidana umum yang dilakukan melalui media sosial.

Dengan demikian, bentuk-bentuk kejahatan dunia maya pada platform media sosial mencerminkan pergeseran pola kriminalitas dari ruang fisik ke ruang digital. Perspektif sosial menunjukkan bahwa dampaknya jauh melampaui kerugian finansial, menyentuh aspek psikologis, reputasi, keamanan sosial, hingga kohesi masyarakat. Analisis berbasis *Space Transition Theory* menegaskan bahwa karakteristik ruang siber—anonimitas, fleksibilitas identitas, dan lemahnya kontrol—menjadi faktor kunci yang mendorong terjadinya kejahatan tersebut. Oleh karena itu, penanggulangan tidak cukup hanya mengandalkan pendekatan hukum, tetapi juga memerlukan penguatan literasi digital, edukasi etika bermedia sosial, serta peningkatan kesadaran kolektif untuk menciptakan ruang digital yang aman dan berkeadilan sosial.

4.2 Peran Negara, Platform, dan Masyarakat dalam Penanggulangan

Penanggulangan kejahatan dunia maya pada platform media sosial tidak dapat diserahkan hanya kepada satu aktor. Karakteristik kejahatan siber yang lintas batas, anonim, dan berbasis teknologi menuntut model kolaborasi multipihak antara negara, penyelenggara platform, dan masyarakat sebagai pengguna. Pendekatan ini sejalan dengan konsep *multi-stakeholder governance* dalam tata kelola internet, yang menekankan bahwa keamanan ruang digital merupakan tanggung jawab bersama. Dalam konteks Indonesia, kerangka hukum yang telah dibangun melalui Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 1 Tahun 2023 memberikan dasar normatif, namun efektivitasnya sangat bergantung pada sinergi implementatif (Tanaka et al., 2025).

Peran negara dapat dianalisis melalui tiga pendekatan utama: penal, non-penal, dan internasional. Dalam pendekatan penal, negara berkewajiban mengoptimalkan penegakan hukum terhadap pelaku kejahatan siber. Penegakan hukum dilakukan oleh Kepolisian Negara Republik Indonesia, khususnya Direktorat Tindak Pidana Siber Bareskrim Polri, yang memiliki kewenangan penyidikan berdasarkan hukum acara pidana dan ketentuan khusus UU ITE. Optimalisasi pendekatan penal memerlukan penguatan kapasitas aparat melalui pelatihan digital forensik, peningkatan kemampuan analisis *big data*, serta penyediaan infrastruktur laboratorium forensik digital yang memadai. Mengingat banyaknya kasus yang bermula dari interaksi di platform seperti Facebook, Instagram, dan TikTok, aparat penegak hukum perlu memiliki kemampuan teknis untuk menelusuri jejak digital lintas platform dan lintas yurisdiksi. Selain itu, pembentukan unit siber khusus di tingkat kepolisian daerah menjadi penting agar respons terhadap laporan masyarakat dapat dilakukan secara cepat dan terdesentralisasi.

Pendekatan penal juga mencakup penerapan sanksi yang proporsional dan konsisten. Dalam UU ITE, berbagai tindak pidana seperti distribusi konten melanggar kesusilaan, pemerasan, pengancaman, serta penyebaran berita bohong memiliki ancaman pidana penjara dan/atau denda yang signifikan. Namun, efektivitasnya tidak hanya ditentukan oleh beratnya sanksi, melainkan juga kepastian dan konsistensi penegakan hukum (Yulianto & Titiek, 2022). Oleh karena itu, koordinasi antara kepolisian, kejaksaan, dan pengadilan harus diperkuat untuk memastikan bahwa proses pembuktian berbasis alat bukti elektronik memenuhi standar hukum acara sebagaimana diakui dalam sistem peradilan pidana Indonesia.

Di sisi lain, pendekatan non-penal menjadi elemen preventif yang sama pentingnya. Negara melalui kementerian terkait, termasuk Kementerian Komunikasi dan Informatika, memiliki peran strategis dalam menyelenggarakan kampanye literasi digital nasional. Program literasi digital bertujuan meningkatkan kemampuan masyarakat dalam mengenali modus penipuan, memahami risiko penyebaran data pribadi, serta menyaring informasi sebelum membagikannya. Upaya ini relevan mengingat tingginya angka pengguna internet dan media sosial di Indonesia, yang sebagian besar mengakses internet melalui perangkat seluler. Kebijakan preventif juga mencakup pembaruan regulasi secara adaptif terhadap perkembangan teknologi, termasuk penguatan perlindungan data pribadi sebagaimana diatur dalam UU PDP. Dalam konteks ini, pengawasan terhadap pengendali dan pemroses data pribadi menjadi penting untuk mencegah kebocoran data yang dapat dimanfaatkan untuk penipuan daring.

Pendekatan internasional tidak kalah krusial karena kejahatan siber sering kali bersifat transnasional. Pelaku dapat beroperasi dari luar wilayah Indonesia dengan memanfaatkan server atau infrastruktur digital di negara lain. Oleh karena itu, kerja sama internasional melalui mekanisme *mutual legal assistance*, pertukaran informasi intelijen siber, dan kolaborasi dengan organisasi internasional menjadi kebutuhan mendesak. Harmonisasi standar penanganan kejahatan siber serta partisipasi aktif dalam forum global akan memperkuat posisi Indonesia dalam mengejar pelaku lintas negara.

Selain negara, platform media sosial memiliki tanggung jawab langsung sebagai penyelenggara sistem elektronik. Berdasarkan rezim hukum Indonesia, penyelenggara sistem elektronik wajib menjamin keamanan dan keandalan sistemnya serta memberikan akses kepada aparat penegak hukum sesuai prosedur yang berlaku. Platform seperti X dan Facebook harus menyediakan mekanisme pelaporan (reporting mechanism) yang mudah diakses dan responsif terhadap aduan pengguna. Transparansi dalam moderasi konten menjadi aspek penting untuk

menjaga keseimbangan antara kebebasan berekspresi dan perlindungan dari konten berbahaya. Laporan transparansi berkala mengenai jumlah konten yang dihapus, akun yang ditangguhkan, serta permintaan data oleh pemerintah dapat meningkatkan akuntabilitas platform.

Platform juga memiliki peran preventif melalui penguatan sistem keamanan, seperti verifikasi dua langkah, deteksi otomatis terhadap aktivitas mencurigakan, serta penggunaan kecerdasan buatan untuk mengidentifikasi ujaran kebencian dan konten ilegal. Kolaborasi aktif dengan aparat penegak hukum diperlukan dalam hal pengamanan barang bukti elektronik dan pelacakan pelaku, tentu dengan tetap memperhatikan prinsip perlindungan data dan hak asasi manusia (Sihombing et al., 2025). Sinergi ini penting agar proses penegakan hukum tidak terhambat oleh kendala teknis atau birokratis.

Adapun masyarakat sebagai pengguna memiliki peran fundamental dalam menciptakan ekosistem digital yang aman. Pertama, peningkatan kesadaran dan literasi digital individu menjadi benteng utama pencegahan. Pengguna perlu memahami pentingnya menjaga kerahasiaan data pribadi, tidak mudah membagikan kode OTP, serta melakukan verifikasi terhadap informasi sebelum menyebarkannya. Kedua, partisipasi aktif dalam membangun norma sosial digital yang positif sangat menentukan kualitas ruang publik daring. Tindakan sederhana seperti tidak menyebarkan hoaks, tidak terlibat dalam ujaran kebencian, dan berani melaporkan konten berbahaya dapat memperkuat kontrol sosial informal di media sosial.

Dari perspektif sosiologis, norma sosial yang terbentuk di ruang digital akan memengaruhi perilaku kolektif pengguna. Ketika mayoritas masyarakat menolak dan melaporkan konten berbahaya, maka ruang digital akan menjadi kurang kondusif bagi pelaku kejahatan. Sebaliknya, jika budaya permisif terhadap penyebaran informasi palsu atau konten merugikan terus berkembang, maka upaya penegakan hukum akan menghadapi hambatan kultural.

Dengan demikian, pencegahan dan penanggulangan kejahatan dunia maya pada platform media sosial hanya akan efektif apabila dilakukan secara sinergis dan berkelanjutan. Negara berperan melalui pendekatan penal, non-penal, dan internasional; platform media sosial bertanggung jawab dalam penguatan sistem keamanan dan moderasi konten; sementara masyarakat menjadi aktor kunci dalam membangun budaya digital yang sehat. Kolaborasi multipihak ini merupakan prasyarat utama untuk menciptakan ekosistem digital yang aman, adil, dan berkelanjutan di tengah dinamika perkembangan teknologi informasi yang terus berubah.

5. KESIMPULAN

Penelitian ini menghasilkan tiga temuan utama yang memberikan kontribusi signifikan bagi pengembangan kajian kejahatan dunia maya pada platform media sosial dari perspektif yuridis dan sosial. Pertama, dari aspek yuridis, ditemukan bahwa pengaturan hukum di Indonesia melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) secara normatif telah membangun kerangka regulasi yang komprehensif. Namun, efektivitasnya masih terkendala oleh hambatan struktural berupa keterbatasan kapasitas aparat dalam digital forensik dan lemahnya koordinasi antar lembaga, serta hambatan kultural berupa multitafsir pasal dan rendahnya literasi hukum masyarakat. Temuan ini berkontribusi pada pemetaan kesenjangan antara desain regulasi dan implementasinya, sekaligus mengidentifikasi titik-titik kritis yang perlu menjadi prioritas pembenahan sistem hukum siber nasional. Kedua, dari perspektif sosial, penelitian ini berhasil

mengidentifikasi ragam bentuk kejahatan di media sosial—mulai dari penipuan online dengan teknik social engineering, perundungan siber (cyberbullying), ujaran kebencian (hate speech), hingga penyebaran hoaks—serta dampaknya yang multidimensional, mencakup kerugian finansial, trauma psikologis, rusaknya reputasi sosial, hingga melemahnya kohesi masyarakat. Kontribusi teoretis yang signifikan dari temuan ini adalah penguatan aplikasi Space Transition Theory dalam konteks Indonesia, yang menjelaskan bahwa karakteristik ruang siber seperti anonimitas, fleksibilitas identitas, dan lemahnya kontrol sosial menjadi faktor kriminogenik utama yang mendorong terjadinya kejahatan. Ketiga, penelitian ini merumuskan model kolaborasi multipihak yang melibatkan peran sinergis negara, platform media sosial, dan masyarakat. Negara berperan melalui pendekatan penal, non-penal, dan internasional; platform bertanggung jawab dalam penyediaan mekanisme pelaporan yang responsif dan penguatan sistem keamanan; sementara masyarakat berperan sebagai garda terdepan pencegahan melalui peningkatan literasi digital dan partisipasi aktif dalam membangun norma sosial digital yang positif.

Temuan-temuan ini memiliki implikasi penting baik secara teoretis maupun praktis. Secara teoretis, penelitian ini memperkuat dan mengkontekstualisasikan Space Transition Theory dalam realitas kejahatan siber di Indonesia. Secara praktis, implikasi kebijakan mencakup perlunya penguatan kapasitas institusional aparat penegak hukum, harmonisasi regulasi, perluasan program literasi digital nasional, penguatan kerja sama internasional, serta pengembangan mekanisme akuntabilitas platform media sosial. Penelitian ini memiliki keterbatasan yang perlu diakui, yaitu penggunaan metode studi literatur yang sepenuhnya bergantung pada data sekunder tanpa pengumpulan data empiris langsung, cakupan penelitian yang bersifat umum dan nasional sehingga belum mampu menangkap variasi konteks lokal, serta perkembangan teknologi dan modus kejahatan siber yang sangat cepat menjadikan beberapa temuan mungkin perlu diperbarui. Oleh karena itu, penelitian lanjutan dengan pendekatan empiris, cakupan lokal yang lebih spesifik, serta kolaborasi interdisipliner yang melibatkan ahli teknologi informasi sangat diperlukan untuk melengkapi dan memperdalam temuan-temuan dalam penelitian ini.

DAFTAR PUSTAKA

Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news , disinformation and misinformation in social media : a review. *Social Network Analysis and Mining*, *13*(30), 1–36. https://doi.org/10.1007/s13278-023-01028-5

Al-Ayoubi, S. J., & Suharto, M. A. (2025). Pemidanaan Kepada Pelaku Konten Pornografi Menggunakan Aplikasi Deepfake Pada Peraturan Perundang-Undangan di Indonesia. *Unes Law Review*, *8*(1), 163–173.

Alawida, M., Esther, A., Isaac, O., & Al-rajab, M. (2020). Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID- 19 . The COVID-19 resource centre is hosted on Elsevier Connect , the company ' s public news and information. *Journal of King Saud University – Computer and Information Sciences*, *34*(January). https://pmc.ncbi.nlm.nih.gov/articles/PMC9367180/pdf/main.pdf

Anugrah, A. H. A., Laurent, C., & Zabrina, H. C. Z. (2023). Fenomena Permasalahan Masyarakat Modern Dalam Masyarakat Risiko. *Al YAZIDIY: Ilmu Sosial, Humaniora, Dan Pendidikan*, *5*(1), 34–52.

APJII. (2024). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Arief, L. S., & Purwanto, R. (2025). Tinjauan Yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam Menangani Kebocoran Data Pelanggan E-Commerce. *Pemuliaan Keadilan*, *2*(3).

Arifin, Z., Fernando, Z. J., & Handayani, E. P. (2025). Implikasi Hukum Perubahan Kedua Undang-Undang Informasi dan Transaksi Elektronik : Menyeimbangkan Kebebasan Berpendapat dan Partisipasi Publik dalam Demokrasi Digital. *Jurnal LITIGASI*, *26*(1), 192–227.

Ayman, D. N., & Nurhadiyanto, L. (2025). Analisis Kejahatan Siber Sniffing pada Media Sosial WhatsApp.

JURNAL ANOMIE, *7*(April), 35–49.

Communications Security Establishment Canada. (2024). *National Cyber Threat Assessment 2025-2026*. Communications Security Establishment Canada. https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

Franetic. (2025). *Hacking Stats by Type, Country, Cost & Social Media (2025)*. Franetic. https://franetic.com/hacking-stats-by-type-country-cost-social-media-2025/?utm_source=chatgpt.com

Gunawan, A. (2026). Algoritma sebagai Mimbar : Analisis Personalisasi Konten Keagamaan pada Media Sosial terhadap Moderasi Beragama. *IKHBAR: Jurnal Ilmu Dakwah Dan Komunikasi*, *1*(2), 101–111. https://doi.org/10.65823/ikhbar

Hasanah, S. (2018). *Arti Berita Bohong dan Menyesatkan dalam UU ITE*. Hukum Online. https://www.hukumonline.com/klinik/a/arti-berita-bohong-dan-menyesatkan-dalam-uu-ite-lt4eef8233871f5/

Idris, M., Aprita, S., & Nurlani, M. (2024). PENGATURAN DAN PENEGAKAN HUKUM KEJAHATAN DUNIA MAYA (CYEBER CRIME) : HARMONISASI REVISI UNDANG-UNDANG ITE DAN KUHP. *Lex Lata: Jurnal Ilmiah Ilmu Hukum*, *6*(3), 396–411. https://doi.org/10.28946/lexl.v6i3.4266

Idul, L., Deninta, D. D., Fatimah, Z. S., Aliandi, D., Muliawan, A. A., & Pranadita, N. (2026). Cybercrime dan Tantangan Perlindungan Individu dalam Kerangka Sistem Hukum di Indonesia. *JUSTITIABLE - Jurnal Hukum*, *8*(2). https://doi.org/10.56071/justitiable.v8i2.1755

Iskandar, O. (2024). Analisis kejahatan online phishing pada masyarakat. *Leuser: Jurnal Hukum Nusantara*, *1*(2), 32–36.

Krey, T. H. M. Y., & Senandi, W. A. A. (2024). EDUKASI BAHAYA MODUS KEJAHATAN SOCIAL ENGINEERING. *Jurnal PengabdianPapua*, *8*(3), 167–173.

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING*, *17*(8).

Liviani, M. R. H. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qānūn*, *23*(2).

Mármol, C. J., Luna, A., & Legaz, I. (2025). Disproportionate Cybersexual Victimization of Women from Adolescence into Midlife in Spain : Implications for Targeted Protection and Prevention. *MDPI*, *15*(11). https://doi.org/https://doi.org/10.3390/bs15111571

Munir. (2024). Kajian Pasal 27 A UU No . 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 8 Tahun 2008 Tentang ITE. *FUNDAMENTAL: JURNAL ILMIAH HUKUM*, *13*(2), 1–12.

Mustopa, D. H., & Dewi, D. D. (2026). *Generasi Z dan Keamanan Siber dalam Perspektif Revolusi Industri 5.0*. DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK. https://dkis.cirebonkota.go.id/artikel/generasi-z-dan-keamanan-siber-dalam-perspektif-revolusi-industri-50?utm_source=chatgpt.com

Nai, M. A., & Hoesein, Z. A. (2026). Analisis Yuridis Terhadap Perlindungan Hukum Bagi Korban Kejahatan Siber di Indonesia. *Journal of Innovative and Creativity*, *6*(1), 1637–1644.

Ningrum, D. P. S., & Robekha, J. (2022). ANALISA YURIDIS DALAM KASUS KEJAHATAN SIBER TERHADAP INTERNET BANKING DI INDONESIA. *Journal Evidence Of Law*, *1*(1), 112–128.

Parwitasari, T. A., Ismunarno, Supanto, Fitriono, R. A., Ginting, R., & Sulistyanta. (2025). Urgensi Kehati-Hatian Dalam Penggunaan Media Sosial Dalam Perspektif Hukum Di Era Digital. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(6), 10112–10130.

Perkins, R. C. (2024). Book Review: Cybercrime and digital deviance. *Sage Journals*, *49*(1). https://doi.org/https://doi.org/10.1177/0734016820988322

Pramudita, N., Rafa, N., Utomo, P., Hussein, K., & Ayu, K. (2025). Dampak Penggunaan Media Sosial terhadap Tingkat Perilaku Kenakalan Remaja di Era Digital Saat Ini. *Dialogika : Jurnal Penelitian Komunikasi Dan Sosialisasi*, *1*(3), 231–244.

Purboningsih, E. R., Massar, K., Hinduan, Z. R., & Agustiani, H. (2023). Perception and use of social media by Indonesian adolescents and parents : A qualitative study. *Frontiers in Psychology*, *5*(13), 1–18. https://doi.org/10.3389/fpsyg.2022.985112

Putri, E. H. A. D., Kasim, R., & Nurmala, L. D. (2024). Analisis Yuridis Terhadap Penegakan dan Pengaturan Hukum Kejahatan Dunia Maya (Cyebercrime) di Indonesia. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *2*(3).

Ray, A., & Henry, N. (2025). Sextortion : A Scoping Review. *Sage Journals*, *26*(1). https://doi.org/10.1177/15248380241277271

Reuters. (2025). *FBI says cybercrime costs rose to at least $16 billion in 2024*. Reuters. https://www.reuters.com/world/us/fbi-says-cybercrime-costs-rose-least-16-billion-2024-2025-04-

23/?utm_source=chatgpt.com

Sahara, A., & Kuswandi. (2025). Penipuan Online sebagai Bentuk Kejahatan Siber dalam Perspektif Kriminologi. *Parlementer : Jurnal Studi Hukum Dan Administrasi Publik*, *2*(4).

Saputra, B. R., & Karsiwan. (2024). Analisis Perilaku Sosial Siswa Berlandaskan Perspektif Teori Bandura. *SOSIAL HORIZON Jurnal Pendidikan Sosial*, *11*(3). https://doi.org/10.31571/sosial.v11i3.8145

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime_ Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*(September), 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Sihombing, A. C., Fadjriani, L., & Lubis, I. H. (2025). ANALISIS YURIDIS PENINGKATAN KEJAHATAN DIGITAL BERBASIS MEDIA SOSIAL(STUDI PENELITIAN POLDA KEPULAUAN RIAU). *Zona Keadilan : Program Studi Ilmu Hukum (S1) Universitas Batam*, *15*(3), 165–185.

Syahid, A., Sudana, D., & Bachari, A. D. (2022). PENISTAAN AGAMA DI MEDIA SOSIAL YANG BERDAMPAK HUKUM : KAJIAN LINGUISTIK FORENSIK. *Semantik*, *11*(1), 17–32. https://doi.org/10.22460/semantik.v11i1.p17-32

Tanaka, V., Chandra, J., & Banke, R. (2025). Kriminalitas Di Era Digital : Kajian Kriminologi Terhadap Kejahatan Online. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, *4*(4), 6095–6100.

Tompunu, N. I. N., Tampongangoy, G. H., & Roeroe, S. D. L. (2025). TINJAUAN YURIDIS TERHADAP PENCEMARAN NAMA BAIK DALAM KONTEKS PASAL 45 AYAT (4) UNDANGUNDANG NOMOR 1 TAHUN 2024 TENTANG INFOMRASI DAN TRANSAKSI ELEKTRONIK (STUDI PUTUSAN: 1909K/PID.SUS/2021. *Jurnal Fakultas Hukum*, *14*(2), 1–13.

TTXVN. (2025). *The silent war: When virtual attacks inflict real-world devastation*. TTXVN. https://happyvietnam.vnanet.vn/en/the-silent-war-when-virtual-attacks-inflict-real-world-devastation/47387.html

United Nations Office for Disaster Risk Reduction. (2025). *Cyberbullying atau Perundungan Siber - Pengertian dan Fakta-faktanya*. United Nations Office for Disaster Risk Reduction. https://indonesia.un.org/id/305496-cyberbullying-atau-perundungan-siber-pengertian-dan-fakta-faktanya

UNODC. (2020). *Cybercrime in brief*. United Nation Office on Drugs and Crime. https://www.unodc.org/cld/fr/education/tertiary/cybercrime/module-1/key-issues/cybercrime-in-brief.html

Wahyuni, W. (2024). *Perubahan Penting Soal Pencemaran Nama Baik di UU ITE Baru*. Hukum Online. https://www.hukumonline.com/berita/a/perubahan-penting-soal-pencemaran-nama-baik-di-uu-ite-baru-lt65a90c5004886/

Waruwu, S., & Srihadiati, T. (2023). Space Transition Theory dalam Cyber-Sexual Harassment terhadap Konten Kreator Wanita di Platform TikTok. *Journal of Feminism and Gender Studies*, *5*(2), 12–25.

Yasin, M. (2026). *Ini 12 Ketentuan KUHP Baru yang Potensial Timbulkan Masalah*. Hukum Online. https://www.hukumonline.com/berita/a/ini-12-ketentuan-kuhp-baru-yang-potensial-timbulkan-masalah-lt6967ccec2b9d2/

Yulianto, M., & Titiek, G. (2022). Penegakan Hukum Terhadap Tindak Pidana Perjudian Online Ditinjau dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Jurnal Kewarganegaraan*, *6*(2), 3281–3287. https://journal.upy.ac.id/index.php/pkn/article/download/3334/pdf/8333