Journal of Law and Nation (JOLN)
Vol. 4 No. 4 (2026) hal. 424-439
e-ISSN: 2962-9675

PERTANGGUNGJAWABAN PIDANA DALAM KEJAHATAN SIBER (CYBERCRIME) DI ERA DIGITAL: KAJIAN PUSTAKA TERHADAP KETERBATASAN REGULASI HUKUM PIDANA INDONESIA

Gunawan Widjaja
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta,
widjaja_gunawan@yahoo.com

Abstract

The development of information and communication technology in the digital age has brought significant changes to various aspects of human life, including the emergence of a new form of technology-based crime: cybercrime. This study aims to analyze criminal liability in cybercrime and identify the limitations of Indonesian criminal law regulations in addressing cybercrime. The study employs a normative legal research method using a literature review approach. The findings indicate that although Indonesia has established a legal foundation for criminal liability through the Criminal Code (KUHP) and the Law on Information and Electronic Transactions (UU ITE), the effectiveness of law enforcement remains hindered by scattered regulatory limitations, the continued existence of legal gaps regarding certain forms of cybercrime, inconsistencies between the Criminal Code and the Electronic Information and Transactions Law, weaknesses in the regulation of electronic evidence, as well as limitations in human resources and digital forensic infrastructure. This study concludes that strengthening criminal liability for cybercrime requires a more comprehensive reform of criminal law, regulatory harmonization, enhanced technical capacity of law enforcement agencies, and strengthened international cooperation to address the transnational nature of cybercrime.

Keywords: *cybercrime, criminal liability, Indonesian criminal law, the Electronic Information and Transactions Law (ITE Law), regulatory limitations.*

Abstrak

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk munculnya bentuk kejahatan baru yang berbasis teknologi, yaitu cybercrime. Penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana dalam kejahatan siber serta mengidentifikasi keterbatasan regulasi hukum pidana Indonesia dalam menangani cybercrime. Penelitian menggunakan metode penelitian hukum normatif dengan pendekatan studi kepustakaan (library research). Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki dasar yuridis pertanggungjawaban pidana melalui KUHP dan Undang-Undang Informasi dan Transaksi Elektronik, efektivitas penegakan hukum masih terhambat oleh keterbatasan regulasi yang tersebar, masih adanya kekosongan hukum terhadap beberapa bentuk cybercrime, ketidakharmonisan antara KUHP dan UU ITE, kelemahan pengaturan pembuktian elektronik, serta keterbatasan sumber daya manusia dan infrastruktur forensik digital. Penelitian ini menyimpulkan bahwa penguatan pertanggungjawaban pidana dalam kejahatan siber memerlukan pembaruan hukum pidana yang lebih komprehensif, harmonisasi regulasi, peningkatan

kapasitas teknis aparat, dan penguatan kerja sama internasional untuk mengatasi sifat transnasional kejahatan siber.

Kata kunci: cybercrime, pertanggungjawaban pidana, hukum pidana Indonesia, UU ITE, keterbatasan regulasi

Pendahuluan

Kemudahan akses internet yang berkembang pesat di era digital membawa dampak positif bagi masyarakat, namun sekaligus membuka celah munculnya bentuk kejahatan baru yang berbasis digital. Kejahatan siber atau cybercrime telah menjadi ancaman serius bagi keamanan nasional dan stabilitas ekonomi Indonesia, mengingat perkembangan digital yang masif menciptakan ruang virtual tanpa batas geografis sehingga memudahkan pelaku kejahatan melakukan aksinya. Statistik menunjukkan peningkatan kasus cybercrime setiap tahunnya dengan modus operandi yang semakin canggih dan terorganisir, dengan kerugian material maupun immaterial yang ditimbulkan mencapai triliunan rupiah dan berdampak pada berbagai sektor kehidupan (Pansariadi & Soekorini, 2023).

Indonesia telah merespons ancaman cybercrime melalui pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menjadi payung hukum utama dalam mengatur dan menindak berbagai bentuk kejahatan di dunia maya. UU ITE kemudian mengalami revisi melalui UU Nomor 19 Tahun 2016 untuk menyempurnakan ketentuan yang dianggap multitafsir, dan perubahan terbaru melalui UU Nomor 1 Tahun 2024 semakin memperkuat landasan yuridis penanganan kejahatan siber di Indonesia (A. B. Putra, 2025). Keberadaan perangkat hukum ini menunjukkan keseriusan pemerintah dalam mengatasi persoalan cybercrime yang terus berkembang seiring transformasi teknologi informasi (Nurahman, 2019).

Namun, implementasi UU ITE dalam praktik penegakan hukum menghadapi berbagai tantangan yang kompleks dan multidimensional, terutama keterbatasan sumber daya manusia yang memiliki kompetensi di bidang teknologi informasi. Aparat penegak hukum seringkali kesulitan mengumpulkan dan menganalisis bukti digital yang bersifat teknis dan memerlukan keahlian khusus, sementara minimnya infrastruktur forensik digital di berbagai daerah mempersulit upaya penanganan kasus cybercrime secara optimal (Pansariadi & Soekorini, 2023). Karakteristik kejahatan siber yang bersifat lintas yurisdiksi menimbulkan persoalan dalam penetapan locus delicti atau tempat terjadinya kejahatan, dan koordinasi antar lembaga penegak hukum masih belum berjalan dengan baik dan terintegrasi (Singer & Friedman, 2013).

Berbagai bentuk kejahatan siber terus bermunculan dengan modus yang semakin canggih mengikuti perkembangan teknologi digital terkini, mulai dari hacking dan cracking sistem informasi yang menjadi ancaman serius bagi keamanan data pribadi maupun data institusi pemerintah. Phishing dan social engineering memanfaatkan kelengahan korban untuk mencuri informasi sensitif seperti password dan data

perbankan, sementara carding atau pencurian data kartu kredit mengakibatkan kerugian finansial yang sangat besar bagi para korban (Pierucci, 2025). Penyebaran konten ilegal seperti pornografi dan ujaran kebencian merusak tatanan sosial dan moral masyarakat Indonesia, dan penipuan online melalui marketplace palsu atau investasi bodong semakin marak terjadi di platform media sosial (Pansariadi & Soekorini, 2023).

Penegakan hukum terhadap cybercrime memerlukan pendekatan khusus yang berbeda dengan penanganan kejahatan konvensional pada umumnya, mengingat sifat virtual dari ruang siber membuat pelaku dapat dengan mudah menghilangkan jejak digital atau berada di luar yurisdiksi. Pembuktian dalam kasus cybercrime sangat bergantung pada kemampuan mengamankan dan menganalisis barang bukti elektronik dengan prosedur yang tepat, dan aparat penegak hukum harus memahami teknologi enkripsi, protokol internet, dan berbagai aplikasi yang digunakan dalam kejahatan siber. Keterlambatan dalam pengamanan bukti digital dapat mengakibatkan hilangnya data penting yang diperlukan dalam proses penuntutan, sehingga kerjasama dengan penyedia layanan internet dan platform digital menjadi krusial dalam proses penyidikan kasus cybercrime (Singer & Friedman, 2013).

Upaya penanggulangan cybercrime di Indonesia dilakukan melalui pendekatan preventif dan represif secara bersamaan dan saling melengkapi, dimulai dari kepolisian yang melakukan patroli siber untuk memantau aktivitas mencurigakan di ruang digital dan mengidentifikasi potensi kejahatan (U. I. P. Sari, 2021). Edukasi kepada masyarakat tentang literasi digital dan cara melindungi diri dari ancaman cybercrime terus dilakukan secara masif, dan program sosialisasi hukum terkait UU ITE diselenggarakan untuk meningkatkan kesadaran masyarakat tentang konsekuensi hukum kejahatan siber. Namun, pendekatan represif melalui penegakan hukum pidana tetap menjadi ultimum remidium ketika upaya preventif tidak memberikan hasil yang diharapkan (R. P. Sari, 2025).

Urgensi penelitian ini semakin kuat mengingat prediksi bahwa kejahatan siber akan terus meningkat seiring digitalisasi yang semakin masif, dengan penggunaan artificial intelligence dan big data oleh pelaku kejahatan menciptakan ancaman baru yang lebih sophisticated dan sulit dideteksi. Perlindungan data pribadi menjadi isu krusial setelah berlakunya UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan integrasi antara regulasi perlindungan data dengan UU ITE perlu dikaji untuk memastikan tidak ada tumpang tindih atau kekosongan hukum (A. B. Putra, 2025). Peran sektor swasta dan masyarakat sipil dalam ekosistem keamanan siber juga perlu mendapat perhatian dalam kajian penegakan hukum, karena membangun budaya keamanan siber yang kuat memerlukan sinergi antara pemerintah, sektor bisnis, akademisi, dan masyarakat umum (Nurahman, 2019).

Cybercrime atau kejahatan dunia maya merupakan fenomena baru yang mulai muncul seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, dan kejahatan ini berbeda dengan kejahatan konvensional karena dilakukan melalui

media elektronik dan jaringan internet sehingga menimbulkan tantangan baru bagi sistem hukum di berbagai negara, termasuk Indonesia. Kejahatan dunia maya meliputi berbagai tindakan kriminal yang memanfaatkan teknologi digital, seperti penipuan online, pencurian data, peretasan sistem, penyebaran konten ilegal, hingga kejahatan siber yang lebih kompleks seperti cyberterrorism dan cyber espionage. Keberadaan cybercrime yang terus berkembang ini memaksa para ahli hukum dan pembuat kebijakan untuk berpikir ulang tentang bagaimana sistem hukum pidana yang ada dapat mengakomodasi dan mengatasi jenis kejahatan baru tersebut (Nurahman, 2019).

Pengaturan cybercrime dalam hukum positif Indonesia terdapat ketentuan yang tersebar baik di dalam KUHP maupun di luar KUHP, misalnya Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi yang hadir sebagai pelengkap KUHP. Namun, dalam pengaturan kejahatan dunia maya muncul beberapa persoalan karena beberapa bentuk kejahatan dunia maya dapat dikenai sanksi berdasarkan hukum Indonesia, sementara bentuk lain belum dapat dijangkau oleh hukum yang ada. Contohnya, jika suatu tindak pidana memiliki unsur delik yang tercantum dalam KUHP tetapi tidak memenuhi syarat yang ada, seperti kasus peretasan, maka terjadi kekosongan hukum (vacuum legis) yang menjadi tantangan serius bagi penegakan hukum (Mayeke, 2025).

Kekurangan KUHP dalam menangani kejahatan dunia maya sangat terlihat jelas karena KUHP yang bersumber dari sistem hukum kontinental Eropa, khususnya Belanda, dibentuk pada masa sebelum munculnya teknologi digital modern. Struktur dan isi KUHP pada dasarnya dirancang untuk menangani tindak pidana konvensional yang terjadi di dunia nyata, sehingga ketika menghadapi kejahatan yang terjadi di dunia maya, KUHP masih menjadi rujukan utama penegakan hukum pidana karena belum adanya aturan yang secara spesifik mengatur tindak pidana yang dilakukan dengan media teknologi informasi dan internet. Penegak hukum masih berusaha menggunakan pasal-pasal dalam KUHP yang dianggap atipikal atau relevan untuk mengatasi kejahatan yang muncul di ranah dunia maya (Marune & Hartanto, 2021).

Permasalahan utama yang muncul adalah kenyataan bahwa kemajuan teknologi berlangsung jauh lebih cepat dibandingkan kemampuan hukum positif untuk menyesuaikan diri, sehingga menimbulkan kekhawatiran bahwa regulasi yang ada akan selalu tertinggal di belakang laju perkembangan teknologi. Hukum pidana positif Indonesia dianggap kurang mampu menjangkau seluruh bentuk kejahatan dunia maya yang semakin kompleks karena karakteristik unik dari cybercrime yang sifatnya lintas wilayah dan menggunakan teknologi canggih, sehingga sulit untuk disikapi dengan aturan pidana konvensional. Definisi dan unsur tindak pidana yang tercantum dalam KUHP sering kali tidak secara eksplisit mencakup modus operandi yang terjadi di dunia digital, sehingga penegakan hukum atas cybercrime menggunakan KUHP menjadi terbatas dan terkadang tidak efektif (Khan & Ahmed, 2024).

Dengan demikian, kajian tentang penegakan hukum cybercrime menjadi sangat penting mengingat dampaknya yang luas terhadap berbagai aspek kehidupan

masyarakat, dan penelitian ini berupaya menganalisis implementasi UU ITE dalam praktik penegakan hukum pidana terhadap kejahatan siber di Indonesia. Identifikasi terhadap hambatan dan tantangan yang dihadapi aparat penegak hukum menjadi fokus utama dalam kajian ini, dengan evaluasi terhadap efektivitas regulasi yang ada serta kesesuaiannya dengan perkembangan teknologi yang akan dibahas secara mendalam dan komprehensif. Penelitian ini diharapkan dapat memberikan pemahaman komprehensif tentang penegakan hukum cybercrime di Indonesia serta memberikan rekomendasi untuk penguatan sistem hukum pidana dalam menghadapi ancaman kejahatan siber di era digital.

Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan studi kepustakaan (library research) yang bersumber pada data sekunder berupa bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang terkait dengan kejahatan siber seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, Kitab Undang-Undang Hukum Pidana (KUHP), serta UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Walliman & Walliman, 2021). Bahan hukum sekunder terdiri dari buku, jurnal nasional dan internasional dan dokumen lainnya yang terkait dengan penelitian. Teknik pengumpulan data dilakukan dengan menghimpun, mencatat, dan mengolah data dari berbagai sumber literatur yang relevan, kemudian dianalisis secara kualitatif dengan metode deskriptif analitis untuk memberikan gambaran komprehensif tentang keterbatasan regulasi hukum pidana Indonesia dalam menangani kejahatan siber di era digital (Eliyah & Aslan, 2025).

Hasil dan Pembahasan

Pertanggungjawaban Pidana dalam Kejahatan Siber

Pertanggungjawaban pidana dalam kejahatan siber pada dasarnya merupakan konsekuensi hukum yang dibebankan kepada pelaku atas perbuatan yang memenuhi unsur tindak pidana dan dilakukan dengan kesalahan yang dapat dicela menurut hukum pidana. Dalam konteks cybercrime, konsep ini tidak berbeda secara prinsipil dari tindak pidana konvensional, sebab pertanggungjawaban pidana tetap mensyaratkan adanya perbuatan pidana, kemampuan bertanggung jawab, bentuk kesalahan, serta tidak adanya alasan pembenar atau pemaaf. Namun demikian, karakter digital dari kejahatan siber menyebabkan penerapan unsur-unsur tersebut menjadi lebih kompleks karena perbuatannya dilakukan melalui sistem elektronik, jaringan internet, atau perangkat digital yang sering kali melintasi batas teritorial negara (Sunaryo et al., 2026). Oleh sebab itu, pertanggungjawaban pidana dalam cybercrime harus dipahami sebagai penerapan

asas-asas umum hukum pidana terhadap bentuk kejahatan baru yang menggunakan media teknologi informasi sebagai sarana, objek, atau lingkungan terjadinya tindak.

Secara normatif, dasar hukum pertanggungjawaban pidana dalam kejahatan siber di Indonesia terutama bertumpu pada Kitab Undang-Undang Hukum Pidana dan Undang-Undang Informasi dan Transaksi Elektronik. KUHP masih digunakan untuk menjangkau perbuatan yang unsur-unsurnya dapat disesuaikan dengan delik konvensional, sedangkan UU ITE berfungsi sebagai lex specialis yang mengatur sejumlah perbuatan yang secara khusus terjadi dalam ranah elektronik, seperti akses ilegal, intersepsi tanpa hak, manipulasi data elektronik, dan distribusi muatan tertentu yang dilarang (Wibowo et al., 2026). Dengan demikian, sistem hukum pidana Indonesia membangun pertanggungjawaban pidana cybercrime melalui kombinasi antara hukum pidana umum dan hukum pidana khusus, meskipun dalam praktik masih sering muncul persoalan harmonisasi norma, interpretasi unsur delik, dan pembuktian elektronik. Kondisi ini menunjukkan bahwa pertanggungjawaban pidana pelaku cybercrime tidak berdiri pada satu rezim hukum tunggal, melainkan pada konstruksi regulatif yang tersebar namun saling berkaitan (Sunaryo et al., 2026).

Dalam hukum pidana, seseorang baru dapat dimintai pertanggungjawaban apabila terbukti melakukan perbuatan pidana dengan kesalahan, baik dalam bentuk kesengajaan maupun kealpaan, sesuai rumusan delik yang berlaku. Dalam kejahatan siber, unsur kesengajaan menjadi sangat penting karena mayoritas delik siber dilakukan secara sadar, terencana, dan menggunakan pengetahuan teknis tertentu, misalnya ketika pelaku sengaja mengakses sistem elektronik milik orang lain tanpa hak atau memanipulasi data untuk memperoleh keuntungan. UU ITE sendiri menempatkan frasa "dengan sengaja dan tanpa hak atau melawan hukum" sebagai unsur sentral dalam sejumlah ketentuan pidana, yang berarti penuntut umum harus membuktikan tidak hanya adanya perbuatan teknis digital, tetapi juga adanya kehendak sadar dari pelaku untuk melakukan perbuatan tersebut. Karena itu, pertanggungjawaban pidana dalam cybercrime sangat bergantung pada pembuktian relasi antara tindakan digital, pengetahuan pelaku, dan akibat hukum yang ditimbulkan (Rasiwan, 2024).

Salah satu bentuk cybercrime yang paling jelas menunjukkan konstruksi pertanggungjawaban pidana adalah peretasan atau akses ilegal terhadap komputer dan sistem elektronik. Pasal 30 ayat (1) UU ITE menegaskan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun dapat dipidana, dan norma ini menjadi dasar penting untuk menjerat pelaku hacking. Dengan adanya ketentuan tersebut, negara mengakui bahwa tindakan memasuki sistem elektronik tanpa otorisasi bukan sekadar pelanggaran etika digital, tetapi merupakan tindak pidana yang dapat dimintai pertanggungjawaban secara penuh. Dalam praktiknya, penerapan pasal ini sering dikaitkan dengan Pasal 46 UU ITE sebagai ketentuan sanksi, sehingga bentuk

pertanggungjawaban pidana pelaku akses ilegal menjadi lebih tegas dan terukur dalam sistem hukum positif Indonesia (Lubis et al., 2025).

Selain pelaku perseorangan, perkembangan kejahatan siber juga membuka kemungkinan pertanggungjawaban pidana terhadap korporasi atau badan hukum. Hal ini penting karena banyak serangan siber, pelanggaran data, atau distribusi konten ilegal dilakukan dalam konteks organisasi bisnis, platform digital, atau perusahaan yang memperoleh keuntungan dari aktivitas elektronik tertentu. Literatur hukum menunjukkan bahwa pelaku tindak pidana cyber tidak selalu terbatas pada individu, tetapi dapat pula berupa badan hukum yang bertindak melalui organ, pengurus, atau pihak yang bekerja untuk dan atas nama korporasi (Sutopo & Panjaitan, 2025). Dalam konteks ini, hukum menerapkan doktrin pertanggungjawaban yang ketat dan pertanggungjawaban pengganti untuk menilai sejauh mana tindakan dalam lingkungan korporasi dapat dibebankan sebagai kesalahan pidana kepada entitas hukum maupun pengurusnya. Dengan demikian, pertanggungjawaban pidana dalam cybercrime berkembang menuju model yang tidak lagi berfokus hanya pada pelaku fisik, tetapi juga pada struktur organisasi yang memungkinkan atau memperoleh manfaat dari tindak pidana tersebut.

Masalah penting lain dalam pertanggungjawaban pidana cybercrime adalah pembuktian. Tidak seperti kejahatan konvensional yang sering bertumpu pada barang bukti fisik dan saksi langsung, perkara cybercrime sangat bergantung pada barang bukti elektronik, log sistem, metadata, rekam jejak digital, serta hasil analisis forensik digital. Karena itu, keberhasilan membebankan pertanggungjawaban pidana kepada pelaku sangat ditentukan oleh kemampuan penyidik dan penuntut dalam menjaga keaslian, integritas, dan keterhubungan bukti elektronik dengan perbuatan terdakwa (Puspitasari, 2018). Sejumlah kajian menegaskan bahwa bukti elektronik memiliki peran sentral dalam kasus cybercrime, tetapi pada saat yang sama memunculkan tantangan karena dapat dengan mudah diubah, dihapus, disamarkan, atau diakses dari berbagai lokasi. Oleh sebab itu, pertanggungjawaban pidana dalam kejahatan siber pada praktiknya tidak hanya berbicara mengenai rumusan delik, melainkan juga tentang kapasitas sistem peradilan pidana untuk membuktikan keterlibatan pelaku secara sah dan meyakinkan (Ridwansyah et al., 2025).

Pembahasan pertanggungjawaban pidana cybercrime juga tidak dapat dilepaskan dari persoalan locus delicti dan yurisdiksi. Cybercrime sering dilakukan melalui jaringan lintas negara, server asing, akun anonim, dan perangkat yang dapat dipindahkan dengan cepat, sehingga penentuan tempat terjadinya tindak pidana menjadi lebih sulit dibandingkan delik biasa. Implikasi dari kondisi ini ialah proses pembebanan pertanggungjawaban pidana dapat terhambat sejak tahap awal, karena aparat penegak hukum harus terlebih dahulu memastikan hubungan hukum antara peristiwa pidana, pelaku, korban, dan wilayah hukum Indonesia (Maharani et al., 2024). Kajian yuridis tentang cybercrime menunjukkan bahwa yurisdiksi kriminal nasional

sering menghadapi keterbatasan ketika kejahatan dilakukan di ruang siber yang tidak tunduk pada batas fisik tradisional. Karena itu, pertanggungjawaban pidana pelaku cybercrime menuntut pendekatan hukum yang lebih adaptif, termasuk kerja sama lintas lembaga dan, dalam kasus tertentu, kerja sama internasional (Wiranata et al., 2024).

Dalam tataran doktrinal, pertanggungjawaban pidana pelaku cybercrime tetap memerlukan pembuktian adanya hubungan antara pelaku dan alat yang digunakan untuk melakukan kejahatan. Ini menjadi penting karena dalam kejahatan siber sering muncul kemungkinan penggunaan identitas palsu, akun pinjaman, VPN, malware otomatis, bot, atau perangkat pihak ketiga yang menyamarkan pelaku utama. Oleh karena itu, penyidik tidak cukup hanya membuktikan bahwa tindak pidana terjadi di suatu sistem elektronik, tetapi juga harus mengaitkan tindakan tersebut dengan subjek hukum tertentu yang dapat dimintai pertanggungjawaban. Kelemahan dalam menghubungkan identitas digital dengan identitas hukum pelaku dapat menyebabkan pertanggungjawaban pidana menjadi lemah atau bahkan gagal dibuktikan di pengadilan (Berlian, 2025). Hal ini menunjukkan bahwa cybercrime menuntut pembacaan ulang terhadap konsep klasik "siapa yang berbuat" dalam hukum pidana, karena pelaku tidak selalu hadir secara fisik di tempat terjadinya peristiwa pidana.

Dari sisi teori kesalahan, mayoritas tindak pidana siber lebih sering dilakukan dalam bentuk dolus atau kesengajaan daripada culpa atau kealpaan. Pelaku umumnya memiliki tujuan tertentu, seperti memperoleh keuntungan ekonomi, mengambil data korban, merusak sistem, menyebarkan konten terlarang, atau menyerang reputasi pihak lain melalui media elektronik. Unsur kesengajaan ini dapat terlihat dari persiapan teknis, penggunaan software tertentu, pola komunikasi digital, serta langkah-langkah pelaku untuk menyamarkan identitas atau menghindari pelacakan (Ar et al., 2024). Semakin tinggi kompleksitas perbuatan dan semakin jelas tujuan yang hendak dicapai, semakin kuat pula dasar untuk membebankan pertanggungjawaban pidana kepada pelaku. Dengan demikian, dalam banyak kasus cybercrime, unsur mens rea justru dapat terlihat lebih sistematis daripada pada beberapa kejahatan konvensional, meskipun tetap memerlukan pembuktian teknis yang cermat (T. W. Putra et al., 2023).

Namun, penerapan pertanggungjawaban pidana dalam cybercrime di Indonesia masih menghadapi kendala normatif karena tidak semua bentuk kejahatan digital telah dirumuskan secara memadai dalam peraturan perundang-undangan. Beberapa studi menilai bahwa regulasi yang ada belum mengakomodasi seluruh tindak pidana siber, sehingga masih terdapat perbuatan yang merugikan masyarakat dan negara tetapi belum dapat dijangkau secara optimal oleh hukum pidana nasional. Kondisi ini menimbulkan ruang kosong hukum atau setidaknya area abu-abu interpretatif yang dapat melemahkan upaya pembebanan pertanggungjawaban pidana terhadap pelaku (Sumadiyasa et al., 2021). Dalam situasi demikian, aparat penegak hukum sering berupaya menafsirkan pasal-pasal yang ada secara ekstensif, tetapi langkah ini juga berpotensi menimbulkan perdebatan mengenai kepastian hukum dan asas legalitas.

Karena itu, efektivitas pertanggungjawaban pidana cybercrime sangat dipengaruhi oleh kualitas perumusan delik dalam regulasi nasional.

Permasalahan lain yang turut memengaruhi pertanggungjawaban pidana adalah keterbatasan aparat dan sarana pendukung penegakan hukum. Sejumlah penelitian menunjukkan bahwa penanggulangan cybercrime di Indonesia masih menghadapi hambatan berupa keterbatasan sumber daya manusia, kurangnya fasilitas pendukung, dan keterbatasan anggaran. Hambatan tersebut berdampak langsung pada kemampuan negara untuk menelusuri pelaku, mengumpulkan alat bukti elektronik, melakukan digital forensics, serta menyusun pembuktian yang kuat di persidangan (Ali et al., 2025). Akibatnya, secara teoritis pertanggungjawaban pidana mungkin dapat dibebankan, tetapi secara praktis proses penegakannya menjadi tidak maksimal. Dengan kata lain, pembahasan pertanggungjawaban pidana cybercrime tidak dapat berhenti pada aspek norma, melainkan harus pula menilai kesiapan kelembagaan yang menjalankan norma tersebut (Budiyanto, 2025).

Dalam sejumlah kasus, pertanggungjawaban pidana juga berkaitan dengan kemungkinan penerapan delik-delik dalam KUHP terhadap perbuatan yang dilakukan melalui media digital. Hukumonline menjelaskan bahwa dalam arti luas, tindak pidana siber dapat mencakup semua tindak pidana yang menggunakan sarana atau bantuan sistem elektronik, sehingga tindak pidana konvensional tertentu dapat masuk ke ranah cybercrime apabila dilakukan dengan medium elektronik. Pendekatan ini penting karena tidak semua kejahatan digital merupakan delik murni siber; sebagian hanya merupakan transformasi medium dari tindak pidana yang telah lama dikenal, seperti penipuan, pencemaran nama baik, pemerasan, atau pengancaman (Calo, 2015). Dengan demikian, pertanggungjawaban pidana dapat dibangun baik melalui ketentuan khusus dalam UU ITE maupun melalui ketentuan umum dalam KUHP sepanjang unsur deliknya terpenuhi. Pendekatan gabungan ini memperlihatkan bahwa sistem hukum pidana Indonesia masih mengandalkan fleksibilitas interpretasi untuk menjangkau dinamika cybercrime yang terus berubah (Khan & Ahmed, 2024).

Perkembangan praktik penegakan hukum juga menunjukkan bahwa pertanggungjawaban pidana dalam cybercrime harus mempertimbangkan keseimbangan antara perlindungan kepentingan hukum masyarakat dan jaminan hak-hak tersangka atau terdakwa. Hal ini penting karena dalam perkara siber, penegak hukum memiliki akses pada data pribadi, komunikasi digital, dan perangkat elektronik yang bersifat sangat privat, sehingga proses pembuktian harus tetap tunduk pada prinsip due process of law. Kesalahan dalam penyitaan perangkat, pengambilan data, atau pemeriksaan sistem elektronik dapat menimbulkan persoalan legalitas alat bukti dan mengganggu validitas pertanggungjawaban pidana yang hendak dibangun (Marune & Hartanto, 2021). Oleh sebab itu, penggunaan instrumen pidana terhadap pelaku cybercrime harus selalu dibarengi dengan prosedur yang akuntabel, proporsional, dan sesuai standar pembuktian hukum acara pidana. Dalam konteks ini,

pertanggungjawaban pidana bukan hanya soal menghukum pelaku, tetapi juga menjaga agar penghukuman itu dibangun melalui proses yang sah dan adil.

Apabila ditinjau dari perspektif kebijakan hukum pidana, pertanggungjawaban pidana dalam kejahatan siber seharusnya tidak hanya dipahami sebagai reaksi represif setelah kejahatan terjadi, tetapi juga sebagai bagian dari strategi kriminal yang lebih luas untuk menciptakan efek pencegahan. Kejelasan rumusan tindak pidana, konsistensi penegakan hukum, dan kepastian mengenai siapa yang dapat dimintai pertanggungjawaban akan memperkuat fungsi preventif hukum pidana dalam ruang digital (Mayeke, 2025). Sebaliknya, jika norma kabur, aparat terbatas, dan pembuktian elektronik lemah, maka efek jera terhadap pelaku cybercrime menjadi berkurang. Sejumlah kajian bahkan mendorong pembentukan regulasi yang lebih komprehensif agar seluruh bentuk tindak pidana siber dapat ditangani dengan dasar hukum yang pasti. Dengan demikian, penguatan pertanggungjawaban pidana tidak hanya memerlukan penjatuhan pidana, tetapi juga pembenahan desain regulasi nasional di bidang kejahatan siber (Nurahman, 2019).

Pada akhirnya, pertanggungjawaban pidana dalam kejahatan siber di Indonesia menunjukkan bahwa asas-asas klasik hukum pidana masih relevan, tetapi penerapannya menuntut penyesuaian yang serius terhadap realitas digital. Pelaku cybercrime pada prinsipnya dapat dimintai pertanggungjawaban apabila memenuhi unsur delik, memiliki kesalahan, mampu bertanggung jawab, dan perbuatannya dapat dibuktikan melalui mekanisme hukum yang sah. Akan tetapi, efektivitas pembebanan pertanggungjawaban pidana masih dipengaruhi oleh keterbatasan regulasi, masalah yurisdiksi, kesulitan identifikasi pelaku, dan kelemahan kapasitas kelembagaan penegak hukum. Oleh karena itu, penguatan rezim pertanggungjawaban pidana cybercrime di Indonesia memerlukan harmonisasi antara KUHP, UU ITE, sistem pembuktian elektronik, dan peningkatan kemampuan aparat agar hukum pidana benar-benar mampu menjawab tantangan kejahatan di era digital.

Keterbatasan Regulasi Hukum Pidana Indonesia dalam Menangani Cybercrime

Keterbatasan regulasi hukum pidana Indonesia dalam menangani cybercrime pada dasarnya berangkat dari kenyataan bahwa perkembangan teknologi informasi berlangsung jauh lebih cepat daripada pembentukan dan penyesuaian norma hukum pidana. Hukum pidana positif yang selama ini dibangun untuk merespons kejahatan konvensional sering kali mengalami keterlambatan ketika harus berhadapan dengan bentuk-bentuk serangan digital yang dinamis, anonim, otomatis, dan lintas sistem. Dalam konteks ini, regulasi tidak selalu gagal karena tidak ada aturan sama sekali, tetapi sering kali gagal karena rumusan yang tersedia tidak cukup rinci, tidak cukup adaptif, atau tidak cukup harmonis dengan karakteristik kejahatan siber. Akibatnya, hukum pidana Indonesia kerap berada dalam posisi reaktif, yakni baru menyesuaikan diri

setelah muncul modus kejahatan baru yang telah lebih dahulu berkembang di masyarakat digital (YOGI OKTAFIAN ARISANDY, 2021).

Salah satu keterbatasan paling mendasar adalah tersebarnya pengaturan cybercrime di berbagai instrumen hukum, baik di dalam KUHP maupun di luar KUHP, tanpa integrasi normatif yang benar-benar solid. Arisandy menegaskan bahwa ketentuan mengenai kejahatan dunia maya tidak terkodifikasi secara utuh dalam satu rezim hukum, melainkan tersebar dalam KUHP, UU ITE, dan peraturan sektoral lainnya seperti Undang-Undang Telekomunikasi, sehingga menimbulkan persoalan dalam konsistensi penerapan norma pidana (YOGI OKTAFIAN ARISANDY, 2021). Fragmentasi seperti ini membuat aparat penegak hukum harus menafsirkan hubungan antarketentuan secara berlapis, terutama ketika satu perbuatan dapat disentuh oleh delik umum dan delik khusus sekaligus. Dalam praktik, kondisi tersebut berpotensi memunculkan ketidakpastian hukum, perbedaan pendekatan penyidikan, serta perdebatan mengenai penggunaan asas lex specialis, lex posterior, dan lex superior dalam penanganan perkara cybercrime (Nurahman, 2019).

Keterbatasan berikutnya tampak pada masih adanya kekosongan hukum atau setidaknya ruang abu-abu normatif terhadap beberapa bentuk cybercrime yang terus berkembang. Arisandy menjelaskan bahwa sebagian bentuk kejahatan dunia maya memang dapat dikenai sanksi berdasarkan hukum Indonesia, tetapi sebagian lainnya belum sepenuhnya dapat dijangkau oleh hukum yang ada, terutama apabila unsur-unsur deliknya tidak cocok sepenuhnya dengan formulasi delik yang sudah berlaku (YOGI OKTAFIAN ARISANDY, 2021). Contoh yang paling sering dikemukakan adalah kasus peretasan, di mana suatu perbuatan dapat secara substansial dianggap menyerang sistem elektronik, tetapi mengalami hambatan ketika harus dicocokkan secara ketat dengan rumusan delik klasik yang lahir sebelum era digital. Situasi ini memperlihatkan bahwa asas legalitas yang menuntut rumusan tindak pidana secara jelas kadang justru menjadi penghalang ketika hukum belum berhasil memperbarui diri secara memadai terhadap perkembangan teknologi (Singgi et al., 2020).

KUHP sebagai fondasi utama hukum pidana Indonesia juga memiliki keterbatasan historis dan struktural karena dibentuk dalam tradisi hukum kontinental yang dirancang untuk menghadapi tindak pidana di dunia fisik, bukan di ruang siber. Singgi menegaskan bahwa struktur dan isi KUHP pada dasarnya dirancang untuk menangani tindak pidana konvensional yang terjadi di dunia nyata, sehingga ketika kejahatan dilakukan melalui jaringan internet atau sistem elektronik, penegak hukum kerap dipaksa menggunakan pasal-pasal yang bersifat atipikal atau analogis secara argumentatif (Singgi et al., 2020). Padahal, hukum pidana tidak membuka ruang analogi secara bebas karena hal itu dapat bertentangan dengan asas legalitas dan kepastian hukum. Oleh karena itu, meskipun beberapa perbuatan cybercrime bisa dipaksakan masuk ke dalam pasal penipuan, pencemaran nama baik, atau penggelapan,

pendekatan seperti ini tetap menyisakan problem doktrinal dan risiko inkonsistensi putusan (U. I. P. Sari, 2021).

Meskipun UU ITE hadir sebagai lex specialis untuk merespons perkembangan dunia digital, regulasi ini pun belum sepenuhnya mampu menjawab kompleksitas cybercrime yang terus berubah. Arafat dan Wirasto menunjukkan bahwa Indonesia memang telah memiliki UU ITE dan UU Pelindungan Data Pribadi sebagai kerangka hukum penting, tetapi tantangan tetap besar pada level implementasi, adaptasi teknologi, dan harmonisasi dengan kebutuhan keamanan siber modern ((Arafat & Wirasto, 2024). Ini berarti persoalan hukum cybercrime di Indonesia bukan hanya soal "ada atau tidak ada undang-undang", melainkan juga soal kualitas desain regulasi dan kemampuan regulasi itu untuk bergerak seiring perubahan modus kejahatan. Ketika ancaman seperti ransomware, pencurian identitas digital, dan serangan terhadap infrastruktur kritis berkembang sangat cepat, regulasi yang lambat beradaptasi akan selalu tertinggal satu langkah dari pelaku kejahatan siber (U. I. P. Sari, 2021).

Aspek lain yang memperlihatkan keterbatasan regulasi ialah lemahnya harmonisasi antara hukum nasional dengan kerangka hukum internasional. Menurut Arafat dan Wirasto, salah satu kendala utama penanganan cybercrime di Indonesia adalah sifat kejahatan siber yang lintas batas, yang mengaburkan yurisdiksi hukum tradisional dan mempersulit proses penegakan hukum terhadap pelaku yang berada di luar negeri (Arafat & Wirasto, 2024). Dalam kasus seperti ini, keberadaan aturan pidana nasional yang kuat sekalipun tidak selalu cukup apabila tidak didukung oleh mekanisme kerja sama internasional, pertukaran informasi, dan bantuan hukum timbal balik yang efektif. Keterbatasan harmonisasi tersebut membuat regulasi nasional sering kali hanya efektif untuk kasus domestik, sementara banyak serangan siber justru beroperasi melalui server, akun, atau jaringan lintas negara yang tidak mudah dijangkau oleh yurisdiksi pidana Indonesia (Budiyanto, 2025).

Keterbatasan regulasi juga terlihat dari belum optimalnya pengaturan mengenai pembuktian digital dalam kerangka hukum pidana nasional. Kejahatan siber sangat bergantung pada data elektronik, log sistem, metadata, rekam jejak digital, dan hasil forensik siber, tetapi sistem pembuktian pidana Indonesia pada awalnya dibangun di atas paradigma alat bukti yang lebih konvensional. Arafat dan Wirasto mencatat bahwa sistem pembuktian digital di Indonesia masih menghadapi keterbatasan, sehingga proses hukum terhadap pelaku cybercrime menjadi lebih rumit dan tidak selalu efektif, terutama ketika bukti bersifat mudah dihapus, dipindahkan, dimanipulasi, atau berada pada infrastruktur pihak ketiga (Arafat & Wirasto, 2024). Dengan demikian, persoalan regulasi tidak berhenti pada rumusan delik, tetapi juga menyangkut apakah hukum acara dan kebijakan pembuktian sudah cukup kuat untuk menopang pertanggungjawaban pidana dalam perkara siber yang kompleks.

Lebih jauh, keterbatasan regulasi pidana Indonesia juga tampak pada belum menyatunya pendekatan penal dan non-penal dalam desain kebijakan kriminal

cybercrime. Budiyanto, (2025) menekankan bahwa keamanan siber yang efektif tidak cukup dibangun hanya dengan ancaman pidana, tetapi juga memerlukan edukasi publik, peningkatan literasi digital, penguatan kapasitas teknis aparat, kolaborasi dengan sektor swasta, serta jaringan pertukaran informasi siber yang responsif). Jika regulasi pidana hanya berorientasi pada penghukuman setelah kejahatan terjadi, sementara aspek pencegahan tidak diatur dan diinstitusionalisasikan secara kuat, maka hukum akan selalu bekerja terlambat. Dalam cybercrime, keterlambatan respons berarti kerugian dapat menyebar sangat luas dalam waktu singkat, sehingga regulasi pidana yang efektif semestinya dirancang sebagai bagian dari ekosistem perlindungan digital yang lebih menyeluruh, bukan sekadar instrumen represif (U. I. P. Sari, 2021).

Kendala regulasi juga bertaut erat dengan kapasitas penegakan hukum, karena regulasi yang baik sekalipun tidak akan efektif apabila tidak disertai kesiapan teknis aparat dan kelembagaan. Arafat dan Wirasto menyebut adanya kesenjangan dalam penegakan hukum siber di Indonesia, termasuk kurangnya kapasitas teknis aparat, rendahnya kesadaran masyarakat mengenai keamanan digital, serta keterbatasan kerja sama internasional untuk menangani kejahatan lintas batas (Arafat & Wirasto, 2024). Dari sudut pandang hukum pidana, kondisi ini menunjukkan bahwa keterbatasan regulasi bersifat ganda: pertama, pada tataran substansi norma; dan kedua, pada tataran implementasi institusional. Artinya, pembaruan hukum cybercrime tidak dapat berhenti pada revisi pasal-pasal pidana saja, tetapi harus diikuti pembangunan kapasitas penyidik, jaksa, hakim, laboratorium forensik digital, serta koordinasi lintas lembaga yang benar-benar operasional (Singgi et al., 2020).

Pada akhirnya, keterbatasan regulasi hukum pidana Indonesia dalam menangani cybercrime menunjukkan adanya kebutuhan mendesak untuk melakukan pembaruan hukum secara lebih komprehensif, sistematis, dan berorientasi ke depan. Nurahman, (2019) secara tegas menyatakan bahwa KUHP dan UU ITE harus sejalan dalam menerapkan norma-norma tindak pidana siber sebagai bagian dari kebijakan kriminalisasi ke depan atau ius constituendum, sedangkan Arafat dan Wirasto menekankan perlunya penguatan UU ITE dan UU PDP, peningkatan kompetensi aparat, literasi digital publik, kerja sama internasional, serta pembentukan jaringan pertukaran informasi siber. Dengan demikian, agenda pembaruan hukum pidana siber di Indonesia harus bergerak dari sekadar respons terhadap kasus menuju desain regulasi yang antisipatif, harmonis, dan adaptif terhadap perkembangan teknologi. Tanpa langkah tersebut, hukum pidana Indonesia akan terus menghadapi kesulitan untuk menjangkau, membuktikan, dan menanggulangi cybercrime secara efektif di era digital yang berubah sangat cepat

Kesimpulan

Pertanggungjawaban pidana dalam kejahatan siber di era digital pada prinsipnya tetap bertumpu pada asas-asas umum hukum pidana, yaitu adanya perbuatan pidana,

kesalahan, kemampuan bertanggung jawab, serta tidak adanya alasan pembenar atau pemaaf. Dalam konteks Indonesia, dasar yuridis pertanggungjawaban pidana terhadap pelaku cybercrime telah tersedia melalui KUHP dan Undang-Undang Informasi dan Transaksi Elektronik, sehingga pelaku kejahatan siber pada dasarnya dapat dimintai pertanggungjawaban secara pidana baik sebagai individu maupun, dalam kondisi tertentu, sebagai badan hukum atau korporasi. Namun, karakter cybercrime yang anonim, lintas batas, dan sangat bergantung pada bukti elektronik menyebabkan penerapan pertanggungjawaban pidana menjadi jauh lebih kompleks dibandingkan tindak pidana konvensional, khususnya dalam aspek identifikasi pelaku, pembuktian kesalahan, dan penegakan yurisdiksi.

Di sisi lain, bahwa keterbatasan utama regulasi hukum pidana Indonesia dalam menangani cybercrime terletak pada belum optimalnya harmonisasi antara KUHP, UU ITE, dan perangkat hukum lain yang terkait dengan sistem elektronik dan perlindungan data. Sebagian bentuk cybercrime memang telah dapat dijangkau oleh hukum positif, tetapi masih terdapat ruang abu-abu normatif, rumusan pasal yang multitafsir, kelemahan pengaturan pembuktian elektronik, serta ketidakseimbangan antara beratnya akibat kejahatan dengan efektivitas sanksi yang tersedia. Selain itu, kendala implementasi berupa keterbatasan sumber daya manusia, fasilitas forensik digital, anggaran, dan literasi digital masyarakat memperlihatkan bahwa persoalan cybercrime bukan hanya masalah norma, tetapi juga masalah kelembagaan dan kapasitas penegakan hukum.

Oleh karena itu, penguatan pertanggungjawaban pidana dalam kejahatan siber harus dilakukan melalui pembaruan hukum pidana yang lebih komprehensif, adaptif, dan terintegrasi dengan dinamika teknologi digital. Reformasi tersebut perlu diarahkan pada penyempurnaan rumusan delik cybercrime, penguatan legitimasi alat bukti elektronik, peningkatan kapasitas teknis aparat penegak hukum, serta pengembangan kerja sama nasional dan internasional untuk mengatasi sifat transnasional kejahatan siber. Dengan demikian, efektivitas pertanggungjawaban pidana terhadap pelaku cybercrime tidak cukup hanya mengandalkan keberadaan aturan tertulis, tetapi harus didukung oleh kebijakan hukum pidana yang responsif, kepastian hukum yang kuat, dan kesiapan institusional agar sistem hukum Indonesia mampu menjawab tantangan kejahatan di era digital.

References

Ali, S., Wang, J., & Leung, V. C. M. (2025). AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms– A comprehensive review. *Information Fusion*, *118*, 102922. https://doi.org/10.1016/j.inffus.2024.102922

Ar, A. M., Wirda, W., Rusbandi, A. S., Zulhendra, M., Bahri, S., & Fajri, D. (2024). Peran Niat (Mens rea) dalam Pertanggungjawaban Pidana di Indonesia. *Jimmi: Jurnal*

Ilmiah Mahasiswa Multidisiplin, *1*(3), 240–252. https://doi.org/10.71153/jimmi.v1i3.140

Arafat, M., & Wirasto, A. T. E. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia. *Equality : Journal of Law and Justice*, *1*(2), 220–241. https://doi.org/10.69836/equality-jlj.v1i2.170

Berlian, C. (2025). PERTANGGUNGJAWABAN PIDANA PELAKU KEJAHATAN SIBER MENGGUNAKAN ARTIFICIAL INTELLIGENCE. *Universitas Jambi*. https://repository.unja.ac.id/82076/

Budiyanto. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Calo, R. (2015). Robotics and the Lessons of Cyberlaw. *California Law Review*, *103*(3), 513–563.

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Khan, M. N. I., & Ahmed, I. (2024). A SYSTEMATIC REVIEW OF JUDICIAL REFORMS AND LEGAL ACCESS STRATEGIES IN THE AGE OF CYBERCRIME AND DIGITAL EVIDENCE. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 01–29. https://doi.org/10.63125/96ex9767

Lubis, J., Hidayat, E. F., Efendi, S., Rasiwan, I., Ishaq, F. M., Trisista, R. G. M., Minabari, A., Kartono, K., Nggeboe, F., & Wibowo, D. E. (2025). *Pengantar Hukum Pidana*. PT Adikara Cipta Aksa. https://doi.org/10.70565/617674

Maharani, P., Hafrida, H., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia. *PAMPAS: Journal of Criminal Law*, *5*(2), 242–252. https://doi.org/10.22437/pampas.v5i2.33291

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*, *2*(4), 143–152. https://doi.org/10.46336/ijbesd.v2i4.170

Mayeke, N. R. (2025). *Evaluating the Cost-Benefit Dynamics of Cybersecurity Compliance Investments: A Multi-Sectoral Analysis Across Financial, Educational, and Ecommerce Industries</p>* (SSRN Scholarly Paper No. 5593290). Social Science Research Network. https://papers.ssrn.com/abstract=5593290

Nurahman, D. (2019). Kebijakan Penegakan Hukum Cybercrime dan Pembuktian Yuridis dalam Sistem Hukum Pidana Nasional. *Keadilan*, *17*(2), 145–157.

Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum*, *12*(2), 287–298. https://doi.org/10.37893/jbh.v12i2.605

Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, *4*(1), 27. https://doi.org/10.1007/s44206-025-00189-4

Puspitasari, I. (2018). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif Di Indonesia. *Hukum Dan Masyarakat Madani*, *8*(1), 1–14. https://doi.org/10.26623/humani.v8i1.1383

Putra, A. B. (2025). Analisis Yuridis Normatif terhadap Pemanfaatan dan Pertanggungjawaban Hukum Artificial Intelligence dalam Aspek Cybercrime di Indonesia. *IKRA-ITH HUMANIORA : Jurnal Sosial Dan Humaniora*, *9*(2), 946–955.

Putra, T. W., Abdurrachman, H., & Hamzani, A. I. (2023). *Pertanggungjawaban Pidana terhadap Kejahatan Hacking*. Penerbit NEM.

Rasiwan, I. (2024). Suatu Pengantar Hukum Pembuktian Tindak Pidana. *AMU Press*, 1–246.

Ridwansyah, M. R., Naja, F., Aisah, S., & Saputra, D. N. (2025). Pertanggungjawaban Pidana Influencer atas Endorse Judi Online: Kajian Kejahatan Siber di Indonesia. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.1173

Sari, R. P. (2025). *Ancaman Digital 2025: 133, 4 Juta Serangan Siber Terjadi di RI. Cyberhub. Id*.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Journal of Studia Legalia*, *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339. https://doi.org/10.22225/jkh.1.2.2553.334-339

Sumadiyasa, I. K. A., Sugiartha, I. N. G., & Widyantara, I. M. M. (2021). Pertanggungjawaban Pidana Pelaku Cyber Crime Dengan Konten Pornogafi. *Jurnal Interpretasi Hukum*, *2*(2), 372–377. https://doi.org/10.22225/juinhum.2.2.3443.372-377

Sunaryo, S., Purnamawati, S. A., & Arifin, R. (2026). The Dialectics of TheoLogis and TheoLegis in the Meaning of Justice. *Legality : Jurnal Ilmiah Hukum*, *34*(1), 210–228. https://doi.org/10.22219/ljih.v34i1.44016

Sutopo, R. B. P., & Panjaitan, H. (2025). A Juridical Demarcation: Reconstructing the Proof of Mens Rea to Differentiate Policy and Corruption by Public Officials. *SIGn Jurnal Hukum*, *7*(2), 765–784. https://doi.org/10.37276/sjh.v7i2.525

Walliman, N., & Walliman, N. (2021). *Research Methods: The Basics* (3rd ed.). Routledge. https://doi.org/10.4324/9781003141693

Wibowo, B., Khowarizmi, M., Maulana, H., & Badi, A. (2026). Mens Rea and Juvenile Criminal Liability in Infanticide Cases: A Comparative Analysis of Indonesian Criminal Law and Fiqh Jinayat. *Jurnal Kajian Ilmu Hukum*, *5*(1), 25–37. https://doi.org/10.55583/jkih.v5i1.1687

Wiranata, G. A., Ucuk, Y., Subekti, & Sidarta, D. D. (2024). PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PHISHING. *COURT REVIEW: Jurnal Penelitian Hukum (e-ISSN: 2776-1916)*, *4*(02), 13–25. (Indonesia). https://doi.org/10.69957/cr.v4i02.1503

YOGI OKTAFIAN ARISANDY. (2021). *PENEGAKAN HUKUM PIDANA TERHADAP CYBER CRIME HACKER* [S1, Universitas Muhammadiyah Yogyakarta]. https://etd.umy.ac.id/id/eprint/3466/