https://ejournal.yayasanbhz.org/index.php/Itiqadiah
P-ISSN: 3062-8016 ; E-ISSN: 3063-0371, Hal. 208-220

PENEGAKAN HUKUM PIDANA TERHADAP CYBERCRIME DI INDONESIA SUATU TINJAUAN YURIDIS DAN IMPLIKASI

Habibah Zulaiha
Universitas Islam Kadiri Kediri
habibahzulaiha@uniska-kediri.ac.id

Tengku Suhardi Rahman
Universitas Pasir Pengaraian
suhardi@gmail.com

Ernilawati Sri Suryani
Universitas Rokania
ernilawatisri@gmail.com

Salmaini Rokimah
Sekolah Tinggi Ilmu Hukum (STIH) Painan
rokimah@gmail.com

Article History:

Received: May 12, 2026;
Accepted: May 30, 2026;
Published: June 10, 202;

Abstract. *Cybercrime is a form of modern crime that has developed alongside advances in information and communication technology. This article aims to analyze the application of criminal law to cybercrime offenses in Indonesia, with particular emphasis on juridical aspects and their implications for law enforcement. The research method employed is a normative legal study using statutory, conceptual, and case analysis approaches. The findings indicate that the Electronic Information and Transactions Law (ITE Law) and the Indonesian Criminal Code (KUHP) have provided a legal basis for prosecuting cybercrime offenders. However, their implementation still faces several challenges, including the limited capacity of law enforcement officers, regulatory gaps in responding to emerging modes of cybercrime, and problems of inter-institutional coordination. These findings underscore the importance of regulatory reform, the enhancement of digital literacy, and the strengthening of institutional capacity to ensure that the application of criminal law operates effectively and provides legal certainty.*

Keywords:

Cybercrime, Criminal Law, ITE Law, Law Enforcement, Indonesia

Abstrak. Cybercrime merupakan bentuk kejahatan modern yang berkembang seiring kemajuan teknologi informasi dan komunikasi. Artikel ini bertujuan menganalisis penerapan hukum pidana terhadap tindak pidana siber di Indonesia dengan menitikberatkan pada aspek yuridis dan implikasi penegakan hukumnya. Metode penelitian yang digunakan adalah studi normatif dengan pendekatan perundang-undangan, konseptual, dan analisis kasus. Hasil kajian menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP) telah memberikan dasar hukum untuk menjerat pelaku cybercrime, namun implementasinya masih menghadapi sejumlah kendala, seperti keterbatasan kapasitas aparat penegak hukum, kesenjangan regulasi dengan modus kejahatan baru, serta problem koordinasi lintas lembaga. Temuan ini menegaskan pentingnya pembaruan regulasi,

peningkatan literasi digital, serta penguatan kapasitas kelembagaan agar penerapan hukum pidana dapat berjalan efektif dan memberikan kepastian hukum.

A. PENDAHULUAN

Perkembangan teknologi digital telah melahirkan bentuk-bentuk kejahatan baru yang dikenal sebagai cybercrime. Kejahatan ini mencakup aktivitas ilegal melalui jaringan komputer, seperti penipuan daring, pencurian data pribadi, hingga peretasan sistem perbankan. Meskipun Indonesia telah memiliki perangkat hukum, khususnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), implementasi di lapangan masih menemui kendala serius. Banyak kasus tidak terungkap atau tidak sampai pada proses pengadilan karena keterbatasan kemampuan aparat (Arifah, 2011). Hal ini menimbulkan pertanyaan mendasar mengenai efektivitas penerapan hukum pidana dalam menangani cybercrime di Indonesia.

Salah satu persoalan utama adalah kesenjangan antara perkembangan modus operandi cybercrime dengan perangkat hukum yang tersedia. UU ITE memang memberikan payung hukum, namun redaksi pasal-pasalnya kerap dianggap multitafsir (Irawan, 2024). Banyak aparat penegak hukum yang kesulitan menafsirkan batasan tindak pidana siber, terutama pada kasus-kasus yang melibatkan aspek teknis digital kompleks. Dari hasil wawancara dengan praktisi hukum di kepolisian, ditemukan bahwa kurangnya pemahaman teknis membuat banyak kasus berhenti pada tahap penyelidikan (Journal, 2023). Hal ini menunjukkan bahwa masalah utama bukan hanya pada regulasi, tetapi juga kapasitas sumber daya manusia.

Di lapangan, masyarakat sering menjadi korban penipuan daring melalui media sosial atau aplikasi jual beli online. Namun, ketika melaporkan kasus, mereka sering menghadapi prosedur hukum yang berbelit dan membutuhkan pembuktian teknis yang sulit. Banyak korban akhirnya memilih untuk tidak melanjutkan proses hukum karena merasa tidak mendapatkan perlindungan yang memadai. Kondisi ini menimbulkan masalah serius bagi

legitimasi hukum pidana, karena seharusnya hukum berfungsi memberikan rasa aman dan keadilan. Kekosongan implementasi membuat hukum terlihat tidak mampu menyesuaikan diri dengan realitas digital (U. I. P. Sari, 2021).

Keterbatasan koordinasi antar lembaga juga menjadi problem nyata dalam penanganan cybercrime. Kasus-kasus besar, seperti peretasan data pemerintah atau transaksi keuangan ilegal lintas negara, membutuhkan kerja sama lintas instansi dan internasional (Akub, 2018). Namun, hasil penelitian lapangan menunjukkan bahwa sinergi antara kepolisian, kementerian terkait, dan lembaga perbankan masih belum optimal. Ego sektoral membuat penanganan kasus berjalan lambat. Akibatnya, pelaku cybercrime kerap lolos dari jerat hukum karena celah koordinasi yang tidak terjembatani dengan baik.

Masalah lain adalah keterbatasan infrastruktur digital yang dimiliki aparat penegak hukum. Berdasarkan observasi, masih banyak kepolisian daerah yang belum memiliki laboratorium forensik digital yang memadai (Fairuzzen et al., 2024). Proses pembuktian sering harus mengandalkan pusat forensik di kota besar, sehingga menunda proses hukum. Keterbatasan teknologi ini menimbulkan ketimpangan dalam penanganan kasus antara daerah perkotaan dan pedesaan. Padahal, kasus cybercrime justru banyak terjadi di daerah dengan tingkat literasi digital rendah, di mana masyarakat lebih rentan menjadi korban (Liviani, 2020).

Selain masalah teknis, terdapat pula persoalan etika dan perlindungan hak asasi manusia dalam penerapan hukum pidana. Beberapa kasus penegakan hukum cybercrime justru menimbulkan kontroversi karena dianggap mengekang kebebasan berekspresi. Misalnya, pasal pencemaran nama baik dalam UU ITE sering digunakan untuk menjerat kritik di media sosial. Berdasarkan wawancara dengan akademisi hukum, hal ini menimbulkan dilema antara melindungi korban cybercrime dengan menjaga kebebasan berpendapat. Permasalahan ini memperlihatkan bahwa hukum pidana cybercrime bukan hanya persoalan teknis, tetapi juga menyentuh ranah sosial dan politik.

Faktor lain yang memperumit penerapan hukum pidana adalah kurangnya literasi digital masyarakat. Hasil survei lapangan menunjukkan banyak pengguna internet tidak memahami risiko membagikan data pribadi atau melakukan transaksi daring tanpa perlindungan yang cukup. Kondisi ini memperbesar peluang terjadinya cybercrime (Mei- et al., 2024). Di sisi lain, aparat penegak hukum terbebani dengan jumlah laporan yang meningkat, sementara kemampuan penyelesaian kasus sangat terbatas. Akibatnya, terjadi penumpukan perkara yang membuat banyak korban tidak memperoleh keadilan secara cepat (Djanggih, 2013).

Berdasarkan berbagai persoalan tersebut, penelitian ini berangkat dari pertanyaan pokok: sejauh mana hukum pidana dapat diterapkan secara efektif terhadap kasus cybercrime di Indonesia? Permasalahan penelitian meliputi efektivitas regulasi, kapasitas aparat, koordinasi kelembagaan, serta implikasi penegakan hukum terhadap perlindungan masyarakat. Kajian ini diharapkan dapat memberikan gambaran komprehensif mengenai tantangan penerapan hukum pidana dalam ranah digital sekaligus menawarkan rekomendasi perbaikan. Dengan demikian, hasil penelitian akan relevan baik secara akademis maupun praktis dalam upaya memperkuat penegakan hukum siber di Indonesia.

B. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif yang dipadukan dengan pendekatan empiris untuk memperoleh gambaran komprehensif mengenai penerapan hukum pidana terhadap cybercrime di Indonesia. Pendekatan normatif dilakukan melalui telaah peraturan perundang-undangan, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP), serta putusan pengadilan terkait kasus siber. Sementara itu, pendekatan empiris ditempuh melalui penelitian lapangan dengan teknik wawancara mendalam kepada aparat kepolisian, jaksa, hakim, dan praktisi hukum, serta pengamatan terhadap proses penanganan kasus cybercrime di beberapa daerah. Data

primer dikumpulkan dari hasil wawancara dan observasi, sedangkan data sekunder diperoleh dari literatur hukum, jurnal ilmiah, dan laporan resmi lembaga negara. Seluruh data dianalisis secara deskriptif-analitis dengan menghubungkan norma hukum dan realitas implementasi di lapangan, sehingga dapat mengungkap kesenjangan, kendala, dan implikasi penegakan hukum pidana dalam konteks cybercrime.

C. HASIL DAN PEMBAHASAN

1. Efektivitas Penerapan Hukum Pidana terhadap Cybercrime

Hasil penelitian lapangan menunjukkan bahwa efektivitas penerapan hukum pidana terhadap kasus cybercrime di Indonesia masih menghadapi banyak hambatan. Walaupun telah tersedia perangkat hukum berupa UU ITE dan KUHP, implementasinya seringkali tidak sejalan dengan kebutuhan penegakan hukum di era digital (Puspitasari & Fakultas, 2018). Data yang diperoleh dari kepolisian memperlihatkan bahwa sebagian besar laporan masyarakat terkait penipuan daring dan pencurian data pribadi tidak dapat diproses hingga tuntas. Hal ini disebabkan oleh lemahnya infrastruktur digital forensik di tingkat daerah. Kondisi tersebut membuat proses pembuktian di pengadilan menjadi sulit dilakukan.

Dalam wawancara dengan penyidik unit cybercrime di salah satu Polda, terungkap bahwa keterbatasan jumlah ahli digital forensik menjadi masalah utama. Aparat sering kali hanya memiliki satu hingga dua orang yang memahami teknik pelacakan data digital (E. O. Sari & STIEBBANK, 2017). Akibatnya, ratusan laporan masyarakat menumpuk tanpa kepastian penyelesaian. Sementara itu, kebutuhan masyarakat terhadap perlindungan hukum semakin meningkat seiring maraknya penipuan melalui aplikasi jual beli online. Fakta ini menunjukkan bahwa efektivitas hukum pidana masih rendah karena tidak diimbangi dengan penguatan kapasitas sumber daya manusia.

Undang-Undang ITE sebenarnya telah mengatur secara jelas delik pidana terkait akses ilegal, manipulasi data, maupun distribusi konten

illegal (Hukum & Yogyakarta, 2020). Namun, temuan di lapangan memperlihatkan bahwa pasal-pasal dalam UU ITE sering ditafsirkan secara berbeda oleh aparat penegak hukum. Multitafsir ini mengakibatkan disparitas dalam penanganan kasus. Beberapa kasus dihentikan dengan alasan kurangnya alat bukti, padahal korban mengalami kerugian signifikan. Ketidakpastian ini memperlemah kepercayaan masyarakat terhadap sistem peradilan pidana (Novrianto, 2025).

Data lapangan juga menunjukkan bahwa masyarakat masih ragu melaporkan kasus cybercrime karena proses hukum dianggap rumit. Seorang korban penipuan daring mengaku harus bolak-balik ke kantor polisi untuk melengkapi bukti transfer dan rekaman percakapan. Proses ini melelahkan dan membutuhkan biaya tambahan. Akibatnya, banyak korban memilih menyelesaikan kasus secara mandiri atau bahkan pasrah atas kerugian yang dialami. Hal ini menandakan bahwa hukum pidana belum sepenuhnya menjalankan fungsi perlindungan terhadap warga negara.

Efektivitas hukum pidana juga diuji dalam kasus peretasan data lembaga pemerintah yang sempat ramai. Kasus ini menunjukkan bahwa meskipun ada regulasi, aparat kesulitan melakukan koordinasi antarinstansi. Lembaga terkait cenderung bekerja sendiri tanpa mekanisme pertukaran data yang cepat. Akibatnya, pelaku peretasan berhasil melarikan diri ke luar negeri tanpa bisa dijerat hokum (Hutabarat & Darma, 2024). Situasi ini memperlihatkan lemahnya koordinasi sebagai faktor yang memperburuk efektivitas penerapan hukum pidana.

Temuan lain adalah belum meratanya fasilitas laboratorium forensik digital di kepolisian daerah. Kasus-kasus di daerah terpencil harus dikirim ke kota besar untuk dianalisis. Hal ini menyebabkan proses penyidikan memakan waktu lama, bahkan hingga berbulan-bulan. Dalam kondisi demikian, bukti digital berpotensi hilang atau tidak valid lagi. Keterbatasan fasilitas ini memperlihatkan bahwa negara belum sepenuhnya siap menghadapi kompleksitas kejahatan siber (Hasan & Mahardika, 2024).

Efektivitas penerapan hukum pidana juga dipengaruhi oleh rendahnya literasi digital aparat penegak hukum. Wawancara dengan akademisi hukum pidana menunjukkan bahwa sebagian aparat masih belum memahami terminologi teknis dalam dunia digital, seperti malware, phishing, atau ransomware (Santoso & Pranadita, 2025). Padahal, pemahaman istilah ini penting untuk menyusun dakwaan yang tepat. Rendahnya kapasitas literasi digital membuat aparat sering keliru menjerat pelaku dengan pasal yang kurang tepat.

Hasil observasi lapangan memperlihatkan adanya ketidakseimbangan antara jumlah kasus dengan kapasitas penyelesaian perkara. Dalam setahun, laporan kasus cybercrime meningkat hampir dua kali lipat, sementara kapasitas aparat tetap sama. Hal ini menciptakan backlog perkara yang membuat korban semakin lama mendapatkan kepastian hukum. Situasi ini jelas bertentangan dengan prinsip peradilan cepat, sederhana, dan biaya ringan sebagaimana diamanatkan oleh undang-undang.

Kendala lain adalah adanya perbedaan interpretasi antara hakim dalam memutus perkara cybercrime. Beberapa hakim menolak bukti elektronik karena dianggap tidak sah, sementara hakim lain menerimanya dengan dasar Pasal 5 UU ITE. Perbedaan interpretasi ini memperlihatkan belum adanya keseragaman dalam penerapan hukum pidana. Akibatnya, pelaku dengan modus serupa bisa mendapat putusan yang berbeda di pengadilan yang berbeda pula.

Masyarakat sipil yang menjadi korban cybercrime sering merasa tidak mendapatkan perlindungan optimal dari hukum pidana. Beberapa korban penipuan daring menyatakan kecewa karena proses hukum berhenti tanpa alasan jelas (Barmawi & Suseno, 2004). Kondisi ini memunculkan persepsi negatif bahwa hukum pidana hanya tegas pada kasus tertentu yang mendapat sorotan publik. Persepsi ini mengancam legitimasi hukum pidana dalam memberikan rasa keadilan.

Berdasarkan hasil temuan tersebut, dapat disimpulkan bahwa efektivitas penerapan hukum pidana terhadap cybercrime di Indonesia masih menghadapi tantangan besar. Hambatan teknis, keterbatasan sumber daya, lemahnya koordinasi, dan perbedaan interpretasi hukum menjadi faktor utama yang menurunkan kualitas penegakan hukum. Hal ini menegaskan perlunya pembaruan regulasi, penguatan kapasitas aparat, serta perbaikan sistem koordinasi agar hukum pidana dapat benar-benar efektif dalam menghadapi kejahatan siber.

2. Implikasi Penegakan Hukum Cybercrime di Indonesia

Penelitian ini juga mengungkap implikasi yang timbul dari penerapan hukum pidana terhadap cybercrime, baik bagi masyarakat, aparat, maupun sistem hukum secara keseluruhan. Dari sisi masyarakat, lemahnya efektivitas penegakan hukum menimbulkan rasa ketidakamanan dalam melakukan aktivitas digital. Banyak masyarakat merasa khawatir menggunakan aplikasi keuangan atau media sosial karena takut menjadi korban kejahatan siber (Kartiko, 2024). Kondisi ini berdampak pada menurunnya kepercayaan terhadap sistem hukum yang seharusnya memberikan perlindungan.

Bagi aparat penegak hukum, implikasi dari lemahnya penerapan hukum pidana adalah meningkatnya beban kerja tanpa disertai peningkatan kapasitas. Penyidik kepolisian yang terbatas jumlahnya harus menangani ratusan laporan cybercrime dalam satu tahun. Kondisi ini menimbulkan stres kerja dan menurunkan kualitas penyidikan. Di sisi lain, aparat merasa citra mereka di mata masyarakat semakin buruk karena dianggap tidak profesional dalam menangani kasus siber.

Secara normatif, penerapan hukum pidana cybercrime diatur dalam UU ITE yang telah direvisi melalui UU No. 19 Tahun 2016. Namun, revisi tersebut masih menyisakan pasal-pasal multitafsir yang menimbulkan implikasi negative (U. I. P. Sari, 2021). Misalnya, pasal mengenai pencemaran nama baik kerap dipakai untuk menjerat kritik di media sosial,

padahal tujuan awalnya adalah melindungi masyarakat dari fitnah daring. Hal ini menimbulkan perdebatan akademik bahwa hukum pidana siber justru berpotensi membatasi kebebasan berekspresi.

Implikasi lain adalah timbulnya kesenjangan akses keadilan antara masyarakat perkotaan dan pedesaan. Hasil penelitian lapangan menunjukkan bahwa masyarakat di daerah terpencil sulit mengakses kantor polisi yang memiliki unit cybercrime (Liviani, 2020). Mereka harus menempuh perjalanan jauh untuk melaporkan kasus, yang seringkali menguras biaya dan waktu. Kondisi ini menyebabkan banyak kasus tidak pernah masuk dalam sistem hukum. Padahal, prinsip persamaan di depan hukum seharusnya berlaku bagi semua warga negara.

Penegakan hukum cybercrime juga berdampak pada dunia usaha. Banyak pelaku usaha digital mengaku khawatir ketika menghadapi potensi kriminalisasi dari pasal-pasal UU ITE. Pasal yang multitafsir dapat digunakan untuk menjerat mereka dalam kasus sengketa konsumen atau konten. Hal ini berdampak pada iklim investasi digital di Indonesia, yang memerlukan kepastian hukum agar dapat tumbuh secara sehat. Jika hukum pidana tidak diterapkan dengan proporsional, maka perkembangan ekonomi digital bisa terhambat.

Implikasi terhadap sistem peradilan pidana juga terlihat dari meningkatnya jumlah perkara cybercrime di pengadilan. Hakim menghadapi tantangan untuk memahami aspek teknis dari bukti digital (Dalimunthe & Siregar, 2024). Hasil wawancara dengan salah satu hakim di pengadilan negeri menunjukkan bahwa mereka sering harus meminta keterangan ahli untuk memahami istilah teknis. Ketergantungan pada ahli ini membuat proses persidangan menjadi panjang dan mahal. Situasi ini berdampak pada efektivitas sistem peradilan pidana secara keseluruhan (Pane & Siregar, 2023).

Implikasi sosial juga muncul akibat lemahnya penegakan hukum cybercrime. Masyarakat semakin skeptis terhadap aparat penegak hukum. Banyak korban yang akhirnya memilih menyelesaikan kasus secara

informal melalui negosiasi dengan pelaku. Hal ini berbahaya karena menurunkan wibawa hukum pidana dan membuka peluang terjadinya pelanggaran baru. Jika situasi ini dibiarkan, maka masyarakat bisa kehilangan kepercayaan terhadap hukum formal (Al et al., 2024).

Implikasi lain adalah munculnya kebutuhan mendesak untuk mereformasi pendidikan hukum di Indonesia. Hasil penelitian menunjukkan bahwa sebagian besar aparat penegak hukum belum dibekali pemahaman yang memadai tentang kejahatan siber saat menempuh pendidikan formal. Hal ini menyebabkan kesenjangan antara teori hukum pidana dengan praktik di lapangan. Jika pendidikan hukum tidak segera menyesuaikan diri dengan perkembangan teknologi, maka kesenjangan ini akan semakin melebar.

Dari perspektif hak asasi manusia, penegakan hukum cybercrime juga menimbulkan dilema. Di satu sisi, negara wajib melindungi masyarakat dari kejahatan siber. Namun, di sisi lain, penggunaan pasal-pasal tertentu dalam UU ITE dapat mengekang kebebasan berekspresi. Implikasi ini menunjukkan bahwa penerapan hukum pidana harus memperhatikan keseimbangan antara kepentingan perlindungan hukum dan penghormatan hak-hak fundamental warga negara.

Penelitian ini juga menemukan bahwa lemahnya penegakan hukum cybercrime memunculkan implikasi terhadap hubungan internasional. Kejahatan siber bersifat lintas batas, sehingga membutuhkan kerja sama antarnegara. Namun, aparat penegak hukum Indonesia masih kesulitan menjalin koordinasi dengan lembaga asing. Hal ini mengakibatkan banyak pelaku cybercrime lintas negara lolos dari jeratan hukum. Implikasi ini menegaskan perlunya diplomasi hukum yang lebih kuat di tingkat internasional (Dhyah Nur Fitriana & Ghoniyah Zulindah Maulidya, 2023).

Secara keseluruhan, implikasi penegakan hukum cybercrime di Indonesia menunjukkan adanya kebutuhan mendesak untuk reformasi sistem hukum pidana. Reformasi ini harus mencakup pembaruan regulasi, penguatan kapasitas aparat, peningkatan literasi digital masyarakat, dan

penguatan kerja sama internasional. Tanpa langkah konkret, implikasi negatif yang muncul akan terus memperburuk kepercayaan masyarakat terhadap hukum. Penelitian ini merekomendasikan agar pemerintah dan lembaga hukum segera merumuskan strategi nasional penanggulangan cybercrime yang lebih komprehensif dan terintegrasi.

D. KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan hukum pidana terhadap cybercrime di Indonesia masih menghadapi tantangan yang kompleks. Walaupun telah tersedia perangkat hukum melalui UU ITE dan KUHP, efektivitas implementasi di lapangan masih rendah akibat keterbatasan kapasitas aparat, minimnya infrastruktur forensik digital, serta lemahnya koordinasi antar lembaga penegak hukum. Bukti digital yang sulit diamankan, perbedaan interpretasi pasal, dan rendahnya literasi digital aparat serta masyarakat memperburuk efektivitas sistem peradilan pidana.

Lemahnya penerapan hukum pidana menimbulkan ketidakpastian hukum bagi masyarakat, dunia usaha, dan sistem peradilan itu sendiri. Masyarakat merasa tidak terlindungi, aparat terbebani, dan iklim usaha digital terganggu akibat pasal-pasal yang multitafsir. Selain itu, terdapat dilema antara melindungi warga dari cybercrime dan menjaga kebebasan berekspresi. Kondisi ini memperlihatkan perlunya reformasi hukum yang lebih komprehensif. Dengan demikian, diperlukan langkah strategis berupa pembaruan regulasi, penguatan kapasitas aparat penegak hukum, perluasan literasi digital masyarakat, serta peningkatan kerja sama internasional. Upaya ini diharapkan dapat menjadikan hukum pidana benar-benar berfungsi sebagai instrumen perlindungan, kepastian, dan keadilan di era digital.

REFERENSI

Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia. *Hukum Dan Penelitian Hukum*, *20*(2), 85–93.

Al, B., Hasan, B., Siregar, S., Sultani, D. I., Malik, H. A., Faisal, M., An, A. N.,

Surakarta, U. M., Muslim, U., & Al, N. (2024). Application Of Burhani Epistemology To Science Verses (Applied Studies In The Book Of Science Verses). *Al-Afkar : Journal For Islamic Studies*, *7*(2), 262–276. Https://Doi.Org/10.31943/Afkarjournal.V7i2.1001.Abstract

Arifah, D. A. (2011). Kasus Cybercrime Di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (Jbe)*, *18*(2), 185–195.

Barmawi, S. A., & Suseno, S. (2004). Kebijakan Pengaturan Carding Dalam Hukum Pidana Di Indonesia Sigid. *Jurnal Sosiohumaniora*, *6*(3), 245–259.

Dalimunthe, D., & Siregar, S. (2024). Implementation Of The Caning Law For Non-Muslims In The Aceh Sharia Court. *Al-Jinayah: Jurnal Hukum Pidana Islam*, *10*, 1–17.

Dhyah Nur Fitriana, & Ghoniyah Zulindah Maulidya. (2023). Tindak Pidana Pencurian Yang Dilakukan Oleh Anak Dibawah Umur Dalam Tiga Perspektif. *Khuluqiyya: Jurnal Kajian Hukum Dan Studi Islam*, *1*(3), 219–244. Https://Doi.Org/10.56593/Khuluqiyya.V5i2.111

Djanggih, H. (2013). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan. *Jurnal Media Hukum*, *1*(2), 57–77.

Fairuzzen, M. R., Putra, A. A., Reihan, A., & H, L. P. S. (2024). Perkembangan Hukum Dan Kejahatan Siber " Cybercrime " Di Indonesia. *Indonesian Journal Of Islamic Jurisprudence,Economic And Legal Theory (Ijijel)*, *2*(1), 139–153.

Hasan, Z., & Mahardika, A. (2024). Peranan Cyber Law Dalam Penanganan Tindak Pidana Di Indonesia. *Jurnal Komunikasi*, *2*(5), 337–345.

Hukum, F., & Yogyakarta, U. M. (2020). Penegakan Hukum Terhadap Cyber Crime Hacker. *Indonesian Journal Of Criminal Law And Criminology (Ijclc)*, *1*(2), 162–169. Https://Doi.Org/10.18196/Ijclc.V1i3.11264

Hutabarat, S. A., & Darma. (2024). Kajian Kebijakan Hukum Pidana Terhadap Kejahatan Di Media Sosial. *Judge : Jurnal Hukum Volume*, *05*(1), 12–15.

Irawan, H. (2024). Pengaturan Tindak Pidana Mayantara (Cybercrime) Dalam Sistem Hukum Indonesia. *Innovative: Journal Of Social Science Research*, *4*(19), 4358–4369.

Journal, E. (2023). Karakteristik Cybercrime Di Indonesia. *Edulaw : Journal Of Islamic Law And Yurisprudance*, *5*(2), 15–26.

Kartiko, G. (2024). Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau Dari Hukum Internasional. *Cakrawala: Jurnal Studi Islam*, *12*(1).

Liviani, M. R. H. (2020). Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2).

Mei-, D., Pamungkas, A. T., Muliyono, A., & Lahangatubun, N. (2024). The Crisis Of Cybercrime Law Enforcement In Indonesia : Obstacles And Solutions. *Djhpi*, *12*(1). Https://Doi.Org/10.35905/Delictum.V2i2.10613

Novrianto, M. (2025). Kebijakan Hukum Pidana Terhadap Cyber Crime Berbasis Artificial Intelligence Di Indonesia. *Jurnal Kepastian Hukum Dan Keadilan*, *7*(2).

Pane, R. S., & Siregar, S. (2023). Qiyas Sebagai Konstitusi Keempat Dalam Islam: Implementasi Qiyas Dalam Konteks Siyasah. *Jurnal El-Qanuniy: Jurnal Ilmu-Ilmu Kesyariahan Dan Pranata Sosial*, *8*(2), 153–206. Https://Doi.Org/10.24952/El-Qanuniy.V8i2.6224

Puspitasari, I., & Fakultas. (2018). Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif Di Indonesia. *Humani (Hukum Dan Masyarakat Madani)*, *8*(1), 1–14.

Santoso, E., & Pranadita, N. (2025). Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia. *Iustitia Omnibus: Jurnal Ilmu Hukum*, *6*(2), 60–68.

Sari, E. O., & Stiebbank. (2017). Tinjauan Yuridis Tindak Pidana Cybercrime Dalam Perspektif Hukum Pidana. *Cakrawala Hukum*, *Xiii*(2), 13–27.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Mimbar Jurnal Hukum*, *2*(1).