Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 3, 2026
DOI: https://doi.org/10.61104/alz.v4i3.5679

Strategi Hukum dalam Penanggulangan Kejahatan Digital di Era Globalisasi untuk Masayarakat Indonesia

Muaidin Jaya Putra[1], Hartanto[2], Uyan Wiryadi[3]
Universitas Krisnadwipayana, Indonesia[1-3]
Email Korespondensi:: adingitu@gmail.com, doktorhartanto18@gmail.com2, uyanwiryadi01@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Maret 2026, Article published: 01 Mei 2026

***ABS*TRACT**
This study examines legal strategies in combating digital crime in the globalization era for Indonesian society. The development of information technology has provided major benefits in social, economic, and governmental sectors, but it has also created threats in the form of digital crimes such as hacking, data theft, online fraud, phishing, carding, and malware distribution. The purpose of this research is to analyze the implementation of the Electronic Information and Transactions Law and to identify obstacles and challenges faced by law enforcement agencies in handling digital crime. The research method used is normative juridical with statutory, conceptual, historical, and comparative approaches. Data sources were obtained from primary, secondary, and tertiary legal materials analyzed qualitatively. The results show that Indonesian regulations are relatively adequate through the Electronic Information and Transactions Law and the Personal Data Protection Law, yet their implementation still faces challenges such as limited human resources, inadequate digital forensic capabilities, low public digital literacy, and the transnational nature of cybercrime. The ideal legal strategy includes adaptive legal reform, strengthening law enforcement capacity, enhancing international cooperation, utilizing cybersecurity technology, and continuously educating the public. Therefore, combating digital crime requires synergy among the state, law enforcement agencies, private sectors, and society as a whole.
Keywords: *Legal Strategy, Digital Crime, Cybercrime, Globalization, Legal Protection.*

ABSTRAK
Penelitian ini membahas strategi hukum dalam penanggulangan kejahatan digital di era globalisasi untuk masyarakat Indonesia. Perkembangan teknologi informasi telah memberikan manfaat besar bagi kehidupan sosial, ekonomi, dan pemerintahan, namun di sisi lain menimbulkan ancaman berupa kejahatan digital seperti peretasan, pencurian data, penipuan daring, phishing, carding, dan penyebaran malware. Tujuan penelitian ini adalah menganalisis implementasi Undang-Undang Informasi dan Transaksi Elektronik serta mengidentifikasi hambatan dan tantangan aparat penegak hukum dalam menangani kejahatan digital. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, historis, dan perbandingan. Sumber data diperoleh dari bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa regulasi di Indonesia telah cukup memadai melalui Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi, namun

implementasinya masih menghadapi kendala berupa keterbatasan sumber daya manusia, minimnya kemampuan digital forensik, rendahnya literasi digital masyarakat, serta sifat kejahatan siber yang lintas negara. Strategi hukum yang ideal dilakukan melalui pembaruan regulasi yang adaptif, peningkatan kapasitas aparat penegak hukum, penguatan kerja sama internasional, pemanfaatan teknologi keamanan siber, serta edukasi masyarakat secara berkelanjutan. Dengan demikian, penanggulangan kejahatan digital memerlukan sinergi antara negara, aparat penegak hukum, sektor swasta, dan masyarakat luas.
Kata Kunci: *Strategi Hukum, Kejahatan Digital, Cybercrime, Globalisasi, Perlindungan Hukum*

PENDAHULUAN

Perkembangan teknologi digital menjadi fondasi utama dalam berbagai aspek kehidupan di era globalisasi, mulai dari sosial, ekonomi, hingga pemerintahan. Transformasi ini meningkatkan efisiensi sekaligus memperluas akses interaksi global, termasuk dalam aktivitas e-commerce sebagai bentuk transaksi komersial berbasis digital (Ding, 1999). Generasi digital native memiliki ketergantungan tinggi terhadap teknologi dalam mengakses informasi daring (Siregar, 2023). Generasi ini lahir dalam konteks perkembangan teknologi yang sangat pesat (Siregar, 2023). Oleh karena itu, diperlukan penguatan nilai moral dan budaya agar mampu menyaring dampak negatif digitalisasi (Siregar, 2023).

Di Indonesia, pertumbuhan pengguna internet yang pesat meningkatkan kompleksitas aktivitas digital sekaligus risiko kejahatan siber. Kejahatan seperti carding menunjukkan bagaimana sistem komputer dapat disusupi untuk memperoleh data secara ilegal (Prasetyo, 2020). Salah satu kasus nyata adalah pembobolan akun e-commerce yang menyebabkan kerugian finansial tanpa persetujuan pengguna (Rahman, 2016). Kejahatan siber juga telah menjangkau wilayah pedesaan dengan tingkat literasi digital yang masih rendah, seperti pencurian data, penipuan daring, peretasan sistem, *ransomware*, *cyberbullying*, dan kejahatan finansial digital (Maddatuang, 2025). Peningkatan ini dipengaruhi oleh tingginya penggunaan internet dan lemahnya sistem keamanan (Waranggani, 2022).

Meskipun Indonesia telah memiliki berbagai regulasi terkait kejahatan digital, implementasinya masih menghadapi kendala dalam penegakan hukum dan pembuktian digital (M. R. Arief, 2018). Keterbatasan sumber daya manusia juga menjadi hambatan dalam penanganan cybercrime (Hutajulu & Wahyuningsih, 2019). Oleh karena itu, kebijakan hukum pidana berperan penting dalam merespons kejahatan digital (B. N. Arief, 2021).

Indonesia juga menghadapi tantangan dalam pengelolaan data digital yang semakin masif seiring meningkatnya jumlah pengguna internet (Asosiasi Penyelenggara Jasa Internet Indonesia, 2025). Data penting seperti informasi kependudukan dan perbankan menjadi target utama kejahatan siber (Badan Siber dan Sandi Negara, 2022). Kurangnya pemahaman masyarakat terhadap risiko digital meningkatkan kerentanan terhadap serangan siber (Kasali, 2017). Selain itu, celah keamanan pada sistem turut memperbesar potensi kejahatan digital (Kasali, 2017). Arus data lintas negara yang semakin cepat juga memperumit karakter kejahatan

siber (Eechoud, 2015). Perkembangan ini mendorong meningkatnya kompleksitas kejahatan digital secara global (Wall, 2007).

Kasus pembobolan akun digital menunjukkan dampak nyata terhadap kepercayaan publik terhadap teknologi (Rahman, 2016). Kejahatan siber memiliki karakteristik tidak meninggalkan jejak fisik dan bersifat lintas negara (Maddatuang, 2025). Bentuk kejahatan yang umum terjadi meliputi pencurian data, peretasan, dan kejahatan finansial digital (Maddatuang, 2025). Peningkatan kejahatan ini juga dipengaruhi oleh rendahnya kesadaran keamanan digital. Selain itu, lemahnya implementasi regulasi turut memperparah kondisi tersebut. Tantangan ini semakin kompleks dengan karakter kejahatan siber yang terus berkembang (M. R. Arief, 2018).

METODE

Penelitian ini menggunakan pendekatan yuridis normatif yang berfokus pada norma hukum positif serta asas-asas hukum yang mengatur tata kelola digital. Pendekatan ini memandang hukum sebagai norma yang bersifat preskriptif, sehingga tidak hanya mendeskripsikan fenomena, tetapi juga menilai kesesuaian antara aturan hukum dan praktik kelembagaan. Dengan demikian, penelitian ini diarahkan untuk mengkaji efektivitas serta konsistensi regulasi dalam mendukung tata kelola digital di Indonesia. Pendekatan yang digunakan meliputi beberapa metode, yaitu pendekatan perundang-undangan (statute approach) melalui telaah terhadap berbagai regulasi seperti UU ITE, UU Cipta Kerja, dan UU Perlindungan Data Pribadi beserta peraturan turunannya. Selain itu, digunakan pendekatan konseptual (conceptual approach) dengan memanfaatkan teori kewenangan, perlindungan hukum, dan harmonisasi hukum sebagai dasar analisis normatif. Penelitian ini juga menggunakan pendekatan perbandingan (comparative approach) dengan mengkaji praktik tata kelola digital di beberapa negara, serta pendekatan historis (historical approach) untuk menelusuri perkembangan kelembagaan dan perubahan paradigma hukum dalam kebijakan digital nasional. Data yang digunakan merupakan data sekunder yang diperoleh melalui studi kepustakaan, yang meliputi bahan hukum primer, sekunder, dan tersier. Pengumpulan data dilakukan dengan cara menginventarisasi dan mengklasifikasikan berbagai sumber hukum seperti peraturan perundang-undangan, literatur ilmiah, dan dokumen pendukung lainnya. Data dianalisis menggunakan metode deskriptif-kualitatif dengan cara mengelompokkan, menafsirkan, dan menghubungkan antar norma secara sistematis dan logis. Hasil analisis tersebut digunakan untuk merumuskan model sinkronisasi kewenangan dan harmonisasi hukum digital sebagai dasar penguatan kelembagaan Komdigi.

HASIL DAN PEMBAHASAN

Analisis Yuridis-Kriminologis Terhadap Kasus Putusan Pengadilan Negeri Purwakarta No: 133/Pid.B/2024/PN.Pwk Tentang Sanksi Pidana Hacker Menurut UU No 1 Tahun 2024 Tentang Perubahan Kedua Atas UU Nomor 11 Tqahun 2008 Tentang ITE

Berdasarkan hasil penelitian, tindak pidana hacking dalam Putusan Pengadilan Negeri Purwakarta Nomor 133/Pid.B/2024/PN.Pwk dikualifikasikan sebagai perbuatan melawan hukum yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Perbuatan tersebut memenuhi unsur-unsur pidana sebagaimana diatur dalam Pasal 51 ayat (2) jo Pasal 36 jo Pasal 30 ayat (1), (2), (3) jo Pasal 32 ayat (2) jo Pasal 34 ayat (1) huruf b UU ITE.

Unsur-unsur tersebut mencakup adanya tindakan dengan sengaja dan tanpa hak dalam mengakses sistem elektronik milik orang lain, termasuk tindakan menerobos atau melampaui sistem pengamanan. Selain itu, terdapat pula perbuatan memindahkan atau mentransfer informasi elektronik kepada pihak yang tidak berhak, serta penggunaan sarana seperti kode akses yang ditujukan untuk memfasilitasi kejahatan. Perbuatan tersebut juga mengakibatkan kerugian bagi pihak lain dan dilakukan dengan kesadaran penuh oleh pelaku.

Dalam putusan tersebut, majelis hakim menjatuhkan pidana berupa penjara selama 5 (lima) tahun serta denda sebesar Rp100.000.000,00. Putusan ini didasarkan pada pertimbangan yuridis serta keadaan yang memberatkan dan meringankan terdakwa. Hal yang memberatkan antara lain karena perbuatan terdakwa menimbulkan kerugian bagi PT Telkomsel dan dilakukan oleh seseorang yang memiliki keahlian di bidang teknologi, sehingga seharusnya memahami batasan hukum. Selain itu, terdakwa juga melibatkan pihak lain dan melakukan lebih dari satu perbuatan pidana.

Di sisi lain, terdapat pula hal-hal yang meringankan, seperti sikap sopan terdakwa selama persidangan, belum pernah dihukum sebelumnya, serta adanya penyesalan atas perbuatan yang dilakukan. Meskipun demikian, hasil analisis menunjukkan bahwa putusan tersebut belum sepenuhnya mencerminkan rasa keadilan. Hal ini dikarenakan ancaman pidana dalam Pasal 51 ayat (2) UU ITE memungkinkan hukuman maksimal hingga 12 tahun penjara dan denda yang jauh lebih besar.

Dengan demikian, sanksi yang dijatuhkan tergolong relatif ringan jika dibandingkan dengan dampak yang ditimbulkan. Kondisi ini menunjukkan bahwa hakim masih mempertimbangkan aspek subjektif pelaku secara dominan dibandingkan efek jera dan perlindungan terhadap korban. Selain itu, penerapan asas legalitas yang ketat dalam hukum pidana menyebabkan hakim cenderung terbatas pada ketentuan normatif yang ada, sehingga belum mampu sepenuhnya menjawab perkembangan kejahatan berbasis teknologi.

Analisis Kriminologis terhadap Cybercrime

Berdasarkan hasil penelitian, perkembangan cybercrime tidak dapat dilepaskan dari kemajuan teknologi informasi. Sejarah menunjukkan bahwa aktivitas peretasan telah dimulai sejak tahun 1950-an oleh mahasiswa yang melakukan eksplorasi terhadap sistem komputer di Massachusetts Institute of Technology. Perkembangan ini kemudian berlanjut pada tahun 1988 ketika muncul virus komputer yang mampu mengganggu jaringan secara luas.

Pada dekade berikutnya, cybercrime mengalami peningkatan signifikan seiring dengan berkembangnya internet sebagai sarana komunikasi global. Kejahatan tidak hanya dilakukan untuk eksplorasi teknologi, tetapi juga untuk memperoleh keuntungan ekonomi maupun kepuasan pribadi (Ding, 1999). Perkembangan ini menunjukkan bahwa cybercrime merupakan fenomena yang terus berevolusi mengikuti kemajuan teknologi.

Dari perspektif kriminologi, faktor utama yang mendorong terjadinya cybercrime adalah kombinasi antara kemampuan teknis yang tinggi dan lemahnya kontrol moral. Individu yang memiliki kecerdasan dan kreativitas dalam bidang teknologi cenderung memiliki potensi untuk melakukan penyalahgunaan apabila tidak diimbangi dengan nilai etika yang kuat. Oleh karena itu, cybercrime tidak hanya dipengaruhi oleh faktor teknologi, tetapi juga oleh faktor kepribadian pelaku.

Faktor Penyebab Terjadinya Cybercrime

Hasil penelitian menunjukkan bahwa terdapat berbagai faktor yang menyebabkan terjadinya cybercrime, baik yang bersifat individu maupun struktural. Secara umum, faktor individu meliputi rasa ingin tahu yang tinggi, dorongan untuk mencoba hal baru, serta motivasi ekonomi dan keinginan untuk menunjukkan kemampuan diri. Selain itu, faktor emosional seperti sakit hati atau keinginan balas dendam juga dapat menjadi pemicu terjadinya kejahatan di dunia maya.

Dalam perspektif yang lebih luas, cybercrime juga dipengaruhi oleh faktor teknis dan sosioekonomi (Siregar, 2023). Dari sisi teknis, internet yang bersifat tanpa batas wilayah memungkinkan pelaku kejahatan untuk melakukan aksinya secara anonim dan lintas negara. Kondisi ini diperparah dengan adanya ketimpangan dalam sistem keamanan jaringan, sehingga membuka peluang bagi pelaku untuk mengeksploitasi kelemahan sistem.

Sementara itu, dari sisi sosioekonomi, cybercrime merupakan bagian dari dinamika ekonomi global yang berkaitan dengan keamanan jaringan. Keamanan sistem informasi menjadi komoditas yang memiliki nilai ekonomi tinggi, sehingga mendorong munculnya berbagai bentuk kejahatan berbasis teknologi. Selain itu, kemudahan akses internet, lemahnya sistem keamanan, serta kurangnya kesadaran masyarakat terhadap keamanan digital juga menjadi faktor penting yang mempercepat pertumbuhan cybercrime (Siregar, 2023).

Upaya Penanggulangan Cybercrime

Berdasarkan hasil penelitian, penanggulangan cybercrime dilakukan melalui pendekatan hukum dan non-hukum. Dalam aspek penegakan hukum, proses penyidikan cybercrime menghadapi berbagai kendala, terutama dalam hal identifikasi pelaku dan pengumpulan alat bukti. Hal ini disebabkan oleh sifat kejahatan yang anonim serta penggunaan teknologi yang memungkinkan pelaku untuk menyembunyikan identitasnya.

Selain itu, pembuktian dalam kasus cybercrime sering kali terkendala oleh keterbatasan alat bukti digital serta kurangnya pemahaman aparat penegak hukum

terhadap teknologi informasi. Oleh karena itu, peran ahli dalam bidang digital forensik menjadi sangat penting dalam proses pembuktian di persidangan.

Di sisi lain, upaya pencegahan cybercrime juga perlu dilakukan melalui peningkatan keamanan sistem teknologi informasi serta kesadaran masyarakat. Pengamanan sistem harus dilakukan secara menyeluruh untuk mencegah adanya celah yang dapat dimanfaatkan oleh pelaku kejahatan. Selain itu, diperlukan kerja sama internasional mengingat sifat cybercrime yang tidak mengenal batas wilayah.

Upaya lain yang tidak kalah penting adalah modernisasi hukum pidana serta peningkatan kapasitas aparat penegak hukum agar mampu menghadapi perkembangan teknologi yang semakin pesat (Siregar, 2023). Tanpa adanya pembaruan hukum, penanganan cybercrime akan terus mengalami keterbatasan.

Peran Hukum dalam Perkembangan Teknologi

Hasil analisis menunjukkan bahwa terdapat kesenjangan antara perkembangan teknologi dan hukum. Hukum sering kali tertinggal dalam mengatur fenomena baru yang muncul akibat kemajuan teknologi informasi. Kondisi ini menunjukkan bahwa keberadaan hukum dalam bidang teknologi merupakan suatu kebutuhan yang tidak dapat dihindari (M. R. Arief, 2018).

Perkembangan teknologi yang pesat menuntut adanya regulasi yang adaptif dan responsif terhadap perubahan. Hal ini penting untuk memastikan adanya kepastian hukum serta perlindungan terhadap masyarakat dari berbagai bentuk kejahatan berbasis teknologi (Hutajulu & Wahyuningsih, 2019). Tanpa adanya regulasi yang memadai, cybercrime akan semakin sulit dikendalikan.

Dalam konteks pertanggungjawaban pidana, cybercrime harus memenuhi unsur objektif dan subjektif. Pelaku harus terbukti melakukan perbuatan melawan hukum serta memiliki kesalahan yang dapat dipertanggungjawabkan secara pidana. Namun demikian, keterbatasan regulasi yang ada saat ini menyebabkan tidak semua bentuk cybercrime dapat dijangkau oleh hukum yang berlaku.

Berdasarkan keseluruhan hasil penelitian, dapat disimpulkan bahwa penegakan hukum terhadap cybercrime masih menghadapi berbagai tantangan yang kompleks. Putusan Pengadilan Negeri Purwakarta menunjukkan bahwa penerapan hukum terhadap kasus hacking telah dilakukan sesuai dengan ketentuan yang berlaku, namun belum sepenuhnya mencerminkan rasa keadilan.

Dari perspektif kriminologi, cybercrime merupakan kejahatan yang dipengaruhi oleh berbagai faktor, baik internal maupun eksternal. Oleh karena itu, penanggulangan cybercrime tidak dapat hanya mengandalkan pendekatan represif melalui penegakan hukum, tetapi juga harus didukung oleh upaya preventif.

Selain itu, diperlukan pembaruan hukum yang lebih adaptif terhadap perkembangan teknologi. Tanpa adanya pembaruan tersebut, hukum akan terus tertinggal dan tidak mampu memberikan perlindungan yang optimal bagi masyarakat.

SIMPULAN

Berdasarkan uraian di atas, dapat disimpulkan bahwa dasar pertimbangan hakim dalam Putusan Pengadilan Negeri Purwakarta Nomor 133/Pid.B/2024/PN.Pwk telah mengacu pada ketentuan hukum yang berlaku, khususnya Pasal 51 ayat (2) jo Pasal 36 jo Pasal 30 ayat (1), (2), (3) jo Pasal 32 ayat (2) jo Pasal 34 ayat (1) serta Pasal 55 ayat (1) ke-1 KUHP dalam kaitannya dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Berdasarkan ketentuan tersebut, majelis hakim menjatuhkan pidana berupa penjara selama 5 (lima) tahun dan denda sebesar Rp100.000.000,00 dengan ketentuan apabila denda tidak dibayar maka diganti dengan pidana kurungan selama 3 (tiga) bulan. Selain itu, masa penangkapan dan penahanan yang telah dijalani terdakwa diperhitungkan sebagai bagian dari pidana yang dijatuhkan serta terdakwa tetap berada dalam tahanan. Dari aspek kriminologis, perilaku kejahatan dalam dunia maya dapat dijelaskan melalui teori *Differential Association* yang dikemukakan oleh Edwin H. Sutherland. Teori ini menyatakan bahwa perilaku kriminal bukan merupakan sifat bawaan, melainkan hasil proses pembelajaran melalui interaksi sosial. Dalam konteks cybercrime, pelaku mempelajari teknik, motif, serta pembenaran atas tindakannya melalui lingkungan sosial yang mendukung perilaku tersebut, terutama dalam kelompok yang memiliki hubungan intens dan komunikasi yang berkelanjutan. Dengan demikian, tindak pidana hacking tidak hanya dipengaruhi oleh kemampuan teknis, tetapi juga oleh faktor lingkungan sosial yang membentuk pola pikir dan perilaku individu. Hal ini menunjukkan bahwa penanggulangan cybercrime tidak cukup hanya melalui pendekatan hukum semata, melainkan juga memerlukan upaya preventif melalui pendidikan, peningkatan kesadaran hukum, serta pembinaan moral agar dapat mengurangi potensi terjadinya kejahatan di dunia maya.

DAFTAR RUJUKAN

Arief, B. N. (2021). *Penegakan Hukum Pidana terhadap Cybercrime di Indonesia*. Citra Aditya Bakti.

Arief, M. R. (2018). *Keamanan Informasi dan Cybercrime*. Gramedia.

Asosiasi Penyelenggara Jasa Internet Indonesia. (2025). *Laporan Survei Internet Indonesia*.

Badan Siber dan Sandi Negara. (2022). *Strategi Keamanan Siber Nasional*. Badan Siber dan Sandi Negara.

Ding, J. (1999). *E-Commerce: Law and Practice*. Sweet & Maxwell.

Eechoud, M. van. (2015). *Hukum Hak Cipta dan Digitalisasi*. Kluwer Law International.

Hutajulu, A. F., & Wahyuningsih, S. E. (2019). *Penegakan Hukum Pidana terhadap Cybercrime di Indonesia*. Universitas Sultan Agung.

Kasali, R. (2017). *Disruption*. Gramedia.

Maddatuang. (2025, October 2). *Soslialisasi Cyber di Era Digital*. Matallo Digital Desa. https://mataallo.digitaldesa.id/berita/soslialisasi-cyber-di-era-digital

Prasetyo, D. (2020). *Cybercrime dan Penegakan Hukum di Indonesia*. Divisi Humas Polri.

Rahman, A. F. (2016). *Ini Cerita Korban Pembobolan Akun Lazada*. DetikInet. https://inet.detik.com/security/d-3184252/ini-cerita-korban-pembobolan-akun-lazada

Rahman, A. F. (2016). *Akun Lazada Dibobol, Kartu Kredit Pria Ini Jebol Jutaan Rupiah*. https://inet.detik.com/security/d-3183724/akun-lazada-dibobol-kartu-kredit-pria-ini-jebol-jutaan-rupiah

Siregar, R. S. (2023). INDONESIA ERA GLOBALISASI: PERAN DAN TANTANGAN GENERASI KEDUA DIGITAL NATIVE. *At Tawasul: Jurnal Komunikasi Dan Penyiaran Islam*, *2*(2), 101–109. http://jurnal.iuqibogor.ac.id

Wall, D. (2007). *Kejahatan Siber: Transformasi Kejahatan di Era Informasi*. Polity Press.

Waranggani, A. S. (2022). *Ini Penyebab Maraknya Insiden Kejahatan Siber di Indonesia*. Cloud Computing Indonesia. https://event.cloudcomputing.id/berita/ini-penyebab-maraknya-insiden-kejahatan-siber

