Indonesia Journal of Criminal Law
Website: https://journal.ilininstitute.com/index.php/IJoCL
Vol. 8, No. 1, Juni 2026, pp 20-29
p-ISSN:2656-9922, e-ISSN: 2684-916X
DOI: https://doi.org/10.31960/ijocl.v8i1.3462

Pertanggungjawaban Pidana Pelaku Kejahatan Siber di Era Digital

Jumanudin[1], Zum Noversa Riala [2],
[1] Hukum Pidana, Universitas Karya Persada Muna, Indonesia
Email: jumanudin1ukpm@gmail.com
[2] Hukum Acara Pidana, Universitas Karya Persada Muna, Indonesia
Email: znoversariala@gmail.com

Artikel info

Artikel history:
Received; 15-04-2026
Revised: 20-05-2026
Accepted: 24-06-2026
Published: 29-06-2026

Keywords:
Criminal Liability; Cybercrime; Digital Transformation; Law Enforcement; Electronic Evidence.

Kata Kunci:
Pertanggungjawaban pidana; kejahatan siber; cybercrime; transformasi digital; penegakan hukum.

Abstract. This study aims to analyze criminal liability for cybercrime perpetrators within the Indonesian legal system and identify the challenges of cybercrime law enforcement in the digital era. The research employs a normative legal method with a qualitative approach through library research, using statutory, conceptual, case, and comparative approaches. Primary legal materials include the 2023 Indonesian Criminal Code, the Electronic Information and Transactions Law, the Personal Data Protection Law, and relevant court decisions. The findings indicate that criminal liability remains grounded in the fundamental principles of criminal law, namely the existence of a criminal act, culpability, criminal responsibility, and the absence of excusing grounds. Although Indonesia has established an adequate legal framework, law enforcement continues to face obstacles related to offender anonymity, the complexity of electronic evidence, cross-border jurisdiction, and emerging technologies such as VPNs, encryption, cryptocurrencies, the dark web, and AI. Therefore, strengthening adaptive legal regulations, enhancing digital forensic capabilities, optimizing electronic evidence, and expanding international cooperation are essential to achieving effective, fair, and responsive cybercrime law enforcement.

Abstrak. Penelitian ini bertujuan menganalisis pertanggungjawaban pidana pelaku cybercrime dalam sistem hukum Indonesia serta mengidentifikasi tantangan penegakan hukumnya di era digital. Penelitian menggunakan metode hukum normatif dengan pendekatan kualitatif melalui studi kepustakaan, menggunakan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan. Bahan hukum utama meliputi KUHP 2023, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta putusan pengadilan yang relevan. Hasil penelitian menunjukkan bahwa pertanggungjawaban pidana tetap berlandaskan pada adanya perbuatan pidana, kesalahan, kemampuan bertanggung jawab, dan tidak adanya alasan pemaaf. Regulasi nasional telah menyediakan dasar hukum yang memadai, namun efektivitas penegakan hukum masih terkendala anonimitas pelaku, kompleksitas alat bukti elektronik, yurisdiksi lintas negara, serta perkembangan teknologi seperti VPN, enkripsi, cryptocurrency,

dark web, dan AI. Oleh karena itu, diperlukan penguatan regulasi yang adaptif, peningkatan kapasitas forensik digital aparat penegak hukum, optimalisasi pembuktian elektronik, dan kerja sama internasional guna mewujudkan penegakan hukum siber yang efektif, adil, dan responsif

Coresponden author:
Jalan: Jl. Gambas 79, Kel. Sidodadi, Kec Batalaiworu Kab. Muna, Sulawesi Tenggara,
Email: jumanudin1ukpm@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah memberikan manfaat yang signifikan bagi masyarakat, dunia usaha, dan pemerintahan. Namun, perkembangan tersebut juga memunculkan berbagai bentuk kejahatan siber (*cybercrime*) yang semakin kompleks dan sulit dikendalikan. Kejahatan siber tidak hanya terbatas pada akses ilegal terhadap sistem elektronik, tetapi juga mencakup pencurian data pribadi, penipuan daring (*online fraud*), penyebaran malware, peretasan (*hacking*), serangan ransomware, hingga penyalahgunaan kecerdasan buatan (*Artificial Intelligence*) dalam aktivitas kriminal.

Transformasi digital telah menjadi fenomena global yang mengubah pola interaksi sosial, ekonomi, dan pemerintahan. Pemanfaatan teknologi informasi dan komunikasi yang semakin luas telah mendorong efisiensi dalam berbagai sektor kehidupan. Namun di sisi lain, perkembangan teknologi tersebut juga memunculkan berbagai bentuk tindak pidana baru yang dikenal sebagai kejahatan siber (cybercrime).

Perkembangan teknologi informasi telah meningkatkan jumlah pengguna internet di Indonesia secara signifikan. Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), tingkat penetrasi internet Indonesia pada tahun 2024 mencapai lebih dari 79% dari total populasi. Peningkatan penggunaan teknologi digital tersebut berimplikasi pada meningkatnya risiko kejahatan siber, seperti phishing, hacking, pencurian data pribadi, ransomware, dan penipuan berbasis elektronik.

Menurut penelitian Siregar dan Putri (2024), peningkatan penggunaan internet berbanding lurus dengan meningkatnya jumlah tindak pidana siber yang terjadi di Indonesia. Sementara itu, Wibowo dan Hidayat (2023) menemukan bahwa kejahatan siber berkembang lebih cepat dibandingkan kemampuan sistem hukum dalam mengantisipasi modus operandi pelaku. Penelitian Pratama (2022) menunjukkan bahwa penegakan hukum terhadap kejahatan siber masih menghadapi kendala pembuktian elektronik. Selanjutnya, penelitian Rahmawati (2023) mengungkapkan bahwa identitas anonim pelaku sering menjadi hambatan utama dalam proses penyidikan. Penelitian Nugroho dan Arifin (2024) juga menemukan bahwa karakter lintas negara dalam cybercrime memerlukan kerja sama internasional yang lebih kuat.

Permasalahan yang muncul saat ini adalah bahwa perkembangan modus operandi kejahatan siber berlangsung lebih cepat dibandingkan perkembangan regulasi dan kemampuan aparat penegak hukum dalam menanganinya. Selain itu, karakteristik kejahatan siber yang bersifat anonim, lintas yurisdiksi, dan berbasis teknologi tinggi menimbulkan berbagai kendala dalam proses pembuktian dan penentuan pertanggungjawaban pidana pelaku. Dalam praktiknya, tidak semua pelaku kejahatan siber dapat dengan mudah diidentifikasi dan dimintai pertanggungjawaban pidana karena adanya penggunaan identitas digital palsu, teknologi enkripsi, dan server yang berada di luar wilayah hukum Indonesia.

Di sisi lain, berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional) membawa paradigma baru dalam sistem hukum pidana Indonesia. Namun demikian, masih diperlukan kajian lebih lanjut mengenai bagaimana konsep pertanggungjawaban pidana diterapkan terhadap pelaku kejahatan siber dalam konteks perkembangan transformasi digital yang semakin pesat. Oleh karena itu, penelitian ini menjadi penting untuk mengkaji dasar-dasar pertanggungjawaban pidana pelaku kejahatan siber serta berbagai tantangan yang dihadapi dalam penegakan hukumnya.

Kajian mengenai kejahatan siber dan pertanggungjawaban pidana telah banyak dilakukan oleh peneliti sebelumnya. Fitriani dan Prasetyo (2023) meneliti pertanggungjawaban pidana pelaku kejahatan siber dalam sistem hukum Indonesia dan menemukan bahwa penerapan sanksi pidana masih menghadapi kendala dalam aspek pembuktian elektronik. Hidayat dan Wibowo (2023) mengkaji tantangan penggunaan alat bukti digital dalam sistem peradilan pidana Indonesia dan menyimpulkan bahwa kapasitas digital forensik aparat penegak hukum masih perlu ditingkatkan.

Rahmawati (2023) menyoroti persoalan identifikasi pelaku kejahatan siber yang sering menggunakan identitas anonim sehingga menyulitkan proses penyidikan. Selanjutnya, Nugroho dan Arifin (2024) meneliti karakter lintas negara (*cross-border cybercrime*) yang menyebabkan munculnya persoalan yurisdiksi dalam penegakan hukum. Putri dan Siregar (2024) mengkaji hubungan antara perkembangan transformasi digital dengan peningkatan jumlah tindak pidana siber di Indonesia dan menemukan bahwa peningkatan penggunaan internet berbanding lurus dengan meningkatnya risiko kejahatan siber.

Penelitian terbaru oleh Wulandari dan Aminah (2025) membahas efektivitas penegakan hukum terhadap kejahatan siber pada era transformasi digital dan menyimpulkan bahwa regulasi yang ada masih memerlukan penyesuaian terhadap perkembangan teknologi baru, khususnya yang berkaitan dengan kecerdasan buatan (*Artificial Intelligence*) dan perlindungan data pribadi.

Secara umum, penelitian-penelitian terdahulu lebih banyak berfokus pada aspek penegakan hukum, pembuktian elektronik, keamanan siber, dan perlindungan data pribadi. Kajian yang secara khusus mengintegrasikan konsep pertanggungjawaban pidana dengan perkembangan hukum pidana nasional pasca berlakunya KUHP Tahun 2023 masih relatif terbatas.

Berdasarkan hasil telaah terhadap penelitian terdahulu, ditemukan beberapa kesenjangan penelitian (*research gap*). Pertama, sebagian besar penelitian sebelumnya lebih menitikberatkan pada aspek teknis penegakan hukum terhadap kejahatan siber, seperti pembuktian elektronik, digital forensik, dan perlindungan data pribadi. Sementara itu, kajian mengenai konstruksi pertanggungjawaban pidana pelaku kejahatan siber dalam perspektif hukum pidana substantif masih belum banyak dilakukan.

Kedua, penelitian terdahulu umumnya menggunakan kerangka hukum yang didasarkan pada KUHP lama dan Undang-Undang Informasi dan Transaksi Elektronik, sehingga belum mengakomodasi perkembangan terbaru setelah berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Nasional.

Ketiga, perkembangan teknologi digital yang melahirkan fenomena baru seperti *Artificial Intelligence*, *deepfake*, *cryptocurrency*, dan *dark web* belum banyak dianalisis dalam kaitannya dengan konsep pertanggungjawaban pidana pelaku kejahatan siber. Padahal perkembangan tersebut berpotensi memunculkan bentuk-bentuk kejahatan baru yang memerlukan pendekatan hukum yang berbeda.

RQ 1: Bagaimana pertanggungjawaban pidana pelaku kejahatan siber dalam sistem hukum Indonesia?

RQ2: Apa saja tantangan penegakan hukum terhadap pertanggungjawaban pidana pelaku kejahatan siber di era digital?

Dengan demikian, penelitian ini hadir untuk mengisi kesenjangan tersebut melalui analisis yang lebih komprehensif mengenai pertanggungjawaban pidana pelaku kejahatan siber berdasarkan perspektif hukum pidana Indonesia pasca berlakunya KUHP Nasional Tahun 2023, serta mengkaji relevansinya terhadap tantangan hukum di era transformasi digital.

Kebaruan penelitian ini terletak pada analisis integratif mengenai pertanggungjawaban pidana pelaku kejahatan siber yang menghubungkan konsep klasik pertanggungjawaban pidana dengan perkembangan hukum pidana nasional pasca berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang KUHP, serta tantangan baru yang muncul akibat perkembangan teknologi digital modern seperti *Artificial Intelligence*, *deepfake*, dan kejahatan siber lintas negara. Dengan demikian, penelitian ini memberikan perspektif baru dalam pengembangan hukum pidana Indonesia di era digital.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis pengaturan hukum mengenai pertanggungjawaban pidana pelaku kejahatan siber serta mengkaji tantangan penegakan hukumnya di era transformasi digital.

METODE

Penelitian ini merupakan penelitian hukum normatif yang berfokus pada kajian terhadap norma hukum yang terdapat dalam peraturan perundang-undangan, putusan pengadilan, serta doktrin hukum yang relevan (Marzuki, 2021). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), pendekatan kasus (*case approach*), dan pendekatan perbandingan (*comparative approach*) untuk memperoleh analisis yang komprehensif terhadap pertanggungjawaban pidana pelaku kejahatan siber (Ibrahim, 2022; IRAC Academy, 2023). Analisis bahan hukum dilakukan secara kualitatif dengan metode deskriptif-analitis dan preskriptif guna menghasilkan argumentasi hukum yang sistematis (Soekanto & Mamudji, 2021).

Sasaran penelitian meliputi berbagai regulasi, konsep hukum, putusan pengadilan, serta hasil penelitian yang berkaitan dengan kejahatan siber (*cybercrime*), pertanggungjawaban pidana, pembuktian elektronik, perlindungan data pribadi, dan penegakan hukum di ruang digital. Penelitian ini juga menelaah perkembangan kebijakan hukum pidana nasional dalam menghadapi dinamika transformasi digital yang semakin kompleks.

Bahan hukum primer terdiri atas Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta beberapa putusan pengadilan yang berkaitan dengan tindak pidana siber dan penggunaan alat bukti elektronik. Bahan hukum sekunder berupa buku, artikel jurnal nasional terakreditasi SINTA, jurnal internasional bereputasi, hasil penelitian, dan publikasi ilmiah lainnya yang diterbitkan dalam kurun waktu lima tahun terakhir (2021–2025). Adapun bahan hukum tersier terdiri atas kamus hukum, ensiklopedia hukum, serta berbagai sumber pendukung lainnya yang relevan dengan objek penelitian.

Pengumpulan data dilakukan melalui teknik dokumentasi dan studi kepustakaan dengan menelaah berbagai literatur yang relevan, yang terdiri atas artikel jurnal nasional dan internasional, buku referensi, dokumen hukum, serta peraturan perundang-undangan yang berkaitan dengan pertanggungjawaban pidana pelaku kejahatan siber. Seluruh bahan hukum yang diperoleh kemudian diseleksi berdasarkan relevansi, validitas, dan keterkaitannya dengan fokus penelitian.

Teknik analisis data yang digunakan adalah analisis kualitatif dengan metode deskriptif-analitis dan preskriptif. Analisis dilakukan melalui tahapan inventarisasi bahan hukum, klasifikasi bahan

hukum, interpretasi hukum, dan penalaran hukum (*legal reasoning*) secara sistematis untuk menemukan konstruksi pertanggungjawaban pidana pelaku kejahatan siber dalam perspektif hukum pidana Indonesia. Selanjutnya, dilakukan analisis terhadap berbagai tantangan penegakan hukum yang muncul akibat perkembangan teknologi informasi, seperti anonimitas pelaku, pembuktian elektronik, yurisdiksi lintas negara, penggunaan kecerdasan buatan (*Artificial Intelligence*), dan perkembangan teknologi digital lainnya.

Hasil analisis kemudian digunakan untuk merumuskan konsep penguatan sistem pertanggungjawaban pidana dan penegakan hukum terhadap kejahatan siber yang mampu memberikan kepastian hukum, kemanfaatan, dan keadilan dalam menghadapi tantangan transformasi digital, serta mendukung pengembangan hukum pidana nasional yang adaptif terhadap perkembangan teknologi informasi.

HASIL DAN PEMBAHASAN

Pertanggungjawaban Pidana Pelaku Kejahatan Siber dalam Sistem Hukum Indonesia

Berdasarkan hasil analisis terhadap Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, ditemukan bahwa sistem hukum Indonesia telah menyediakan dasar normatif yang cukup untuk menjerat pelaku kejahatan siber. Pertanggungjawaban pidana terhadap pelaku kejahatan siber tetap didasarkan pada prinsip umum hukum pidana, yaitu adanya perbuatan pidana (*actus reus*), kesalahan (*mens rea*), kemampuan bertanggung jawab, dan tidak adanya alasan pemaaf.

Temuan penelitian menunjukkan bahwa meskipun cybercrime merupakan bentuk kejahatan modern yang memanfaatkan teknologi digital, konsep pertanggungjawaban pidana yang digunakan tetap mengacu pada doktrin hukum pidana klasik. Dengan demikian, keberadaan teknologi hanya mempengaruhi modus operandi kejahatan, sedangkan dasar pertanggungjawaban pidananya tetap berlandaskan pada asas *geen straf zonder schuld* atau tidak ada pidana tanpa kesalahan.

Penelitian ini menemukan bahwa unsur kesengajaan menjadi unsur yang paling dominan dalam berbagai tindak pidana siber. Pelaku umumnya melakukan tindakan secara sadar dan terencana, seperti mengakses sistem elektronik tanpa hak, mencuri data pribadi, melakukan penipuan daring, atau menyebarkan perangkat lunak berbahaya (*malware*) untuk memperoleh keuntungan ekonomi maupun tujuan tertentu lainnya. Oleh karena itu, pembuktian unsur kesalahan dalam cybercrime pada umumnya lebih mudah dibuktikan dibandingkan tindak pidana yang bersifat kelalaian.

Penerapan Pertanggungjawaban Pidana dalam Kejahatan Siber

Hasil penelitian menunjukkan bahwa penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber dilakukan melalui kombinasi antara ketentuan umum dalam KUHP dan ketentuan khusus dalam UU ITE. Dalam praktiknya, UU ITE berfungsi sebagai *lex specialis* yang mengatur secara spesifik berbagai bentuk kejahatan yang dilakukan melalui sistem elektronik.

Temuan penelitian menunjukkan bahwa terdapat tiga bentuk utama kejahatan siber yang paling sering menjadi objek penegakan hukum di Indonesia, yaitu: (1) Akses ilegal terhadap sistem elektronik (*illegal access*); (2) Penipuan berbasis elektronik (*online fraud*); (3) Penyalahgunaan dan pencurian data pribadi (*data theft*).

Ketiga bentuk kejahatan tersebut memiliki karakteristik yang berbeda, namun semuanya memerlukan pembuktian mengenai adanya hubungan antara tindakan pelaku dengan kerugian

yang ditimbulkan. Dalam konteks ini, alat bukti elektronik memiliki peranan yang sangat penting sebagai dasar untuk membuktikan keterlibatan pelaku dalam suatu tindak pidana siber.

Temuan lainnya menunjukkan bahwa pengaturan mengenai alat bukti elektronik telah memberikan kepastian hukum yang lebih baik dibandingkan sebelumnya. Namun demikian, efektivitas pembuktian masih sangat bergantung pada kemampuan aparat penegak hukum dalam melakukan investigasi digital dan analisis forensik elektronik.

Tantangan Penegakan Hukum terhadap Kejahatan Siber

Berdasarkan analisis terhadap berbagai literatur dan regulasi yang berlaku, penelitian ini menemukan empat tantangan utama dalam penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber.

a. Anonimitas Pelaku

Temuan penelitian menunjukkan bahwa identitas anonim menjadi hambatan terbesar dalam penegakan hukum terhadap kejahatan siber. Pelaku sering menggunakan akun palsu, jaringan virtual (*VPN*), server luar negeri, dan teknologi enkripsi untuk menyembunyikan identitasnya. Akibatnya, proses identifikasi dan pelacakan pelaku menjadi lebih kompleks dibandingkan tindak pidana konvensional.

b. Pembuktian Elektronik

Penelitian menemukan bahwa alat bukti elektronik memiliki karakteristik yang berbeda dengan alat bukti konvensional. Data digital dapat dengan mudah dimodifikasi, dihapus, atau dipindahkan dalam waktu singkat. Oleh karena itu, proses pengumpulan dan pengamanan barang bukti digital memerlukan standar prosedur dan kemampuan digital forensik yang tinggi.

c. Yurisdiksi Lintas Negara

Temuan penelitian menunjukkan bahwa sebagian besar kejahatan siber memiliki karakter lintas negara (*transnational crime*). Pelaku dapat berada di negara tertentu, menggunakan server di negara lain, dan menimbulkan kerugian bagi korban di wilayah Indonesia. Kondisi ini menyebabkan munculnya persoalan yurisdiksi dan memerlukan kerja sama internasional dalam proses penyidikan maupun penuntutan.

d. Perkembangan Teknologi Digital

Penelitian menemukan bahwa perkembangan teknologi informasi berlangsung jauh lebih cepat dibandingkan perkembangan regulasi hukum. Munculnya teknologi Artificial Intelligence (AI), cryptocurrency, dark web, dan deepfake telah melahirkan berbagai bentuk kejahatan baru yang belum sepenuhnya diantisipasi oleh sistem hukum pidana Indonesia.

Analisis Pertanggungjawaban Pidana Pelaku Kejahatan Siber di Era Digital

Berdasarkan temuan penelitian, dapat dianalisis bahwa efektivitas pertanggungjawaban pidana terhadap pelaku kejahatan siber tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh kemampuan negara dalam mengimplementasikan regulasi tersebut. Keberadaan UU ITE, UU Perlindungan Data Pribadi, dan KUHP Nasional Tahun 2023 menunjukkan bahwa Indonesia telah memiliki kerangka hukum yang relatif memadai dalam menghadapi perkembangan *cybercrime.*

Namun demikian, penelitian ini menemukan bahwa terdapat kesenjangan antara aspek normatif dan aspek implementatif. Secara normatif, regulasi yang ada telah mampu mengatur berbagai bentuk kejahatan siber. Akan tetapi, secara implementatif masih terdapat kendala berupa keterbatasan sumber daya manusia, kemampuan digital forensik, sarana teknologi investigasi, dan kerja sama lintas negara.

Temuan penelitian juga menunjukkan bahwa konsep pertanggungjawaban pidana klasik masih relevan untuk diterapkan dalam kejahatan siber. Meskipun dilakukan melalui media digital, unsur-unsur pertanggungjawaban pidana seperti kesalahan, kemampuan bertanggung jawab, dan tidak adanya alasan pemaaf tetap menjadi dasar utama dalam menentukan dapat atau tidaknya seseorang dijatuhi pidana.

Dengan demikian, penelitian ini menemukan bahwa penguatan kapasitas aparat penegak hukum, pembaruan regulasi yang adaptif terhadap perkembangan teknologi, serta peningkatan kerja sama internasional merupakan faktor yang sangat penting untuk meningkatkan efektivitas pertanggungjawaban pidana pelaku kejahatan siber di era digital.

Pembahasan

Pertanggungjawaban Pidana Pelaku Kejahatan Siber dalam Perspektif Hukum Pidana Indonesia

Pertanggungjawaban pidana merupakan konsekuensi hukum yang diberikan kepada seseorang yang terbukti melakukan tindak pidana dan memiliki kesalahan atas perbuatannya. Dalam hukum pidana Indonesia, konsep pertanggungjawaban pidana didasarkan pada asas *geen straf zonder schuld* yang mengandung makna bahwa seseorang tidak dapat dijatuhi pidana apabila tidak terdapat unsur kesalahan dalam dirinya. Asas ini menjadi landasan utama dalam menentukan dapat atau tidaknya pelaku kejahatan siber dimintai pertanggungjawaban pidana.

Berdasarkan temuan penelitian, sistem hukum Indonesia telah memberikan dasar normatif yang cukup untuk menjerat pelaku kejahatan siber melalui pengaturan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Ketiga regulasi tersebut menunjukkan bahwa negara telah mengakui kejahatan siber sebagai bentuk tindak pidana yang memiliki dampak serius terhadap keamanan, ekonomi, dan ketertiban masyarakat.

Dalam perspektif teori kesalahan (*schuld theory*), pelaku kejahatan siber hanya dapat dipidana apabila terdapat hubungan antara perbuatan yang dilakukan dengan sikap batin pelaku. Mayoritas kejahatan siber dilakukan dengan unsur kesengajaan (*dolus*), karena pelaku secara sadar dan terencana menggunakan teknologi informasi untuk melakukan tindakan yang bertentangan dengan hukum. Misalnya, dalam kasus peretasan sistem elektronik, pelaku mengetahui bahwa akses yang dilakukan tidak memiliki izin dan memahami akibat hukum yang mungkin timbul dari perbuatannya. Oleh karena itu, unsur kesalahan sebagai dasar pertanggungjawaban pidana dapat dibuktikan secara jelas.

Temuan penelitian ini sejalan dengan pendapat Barda Nawawi Arief yang menyatakan bahwa pertanggungjawaban pidana tidak hanya didasarkan pada adanya perbuatan yang dilarang oleh undang-undang, tetapi juga pada adanya kesalahan yang dapat dipertanggungjawabkan kepada pelaku. Dalam konteks kejahatan siber, keberadaan teknologi tidak menghapus unsur kesalahan, melainkan hanya mengubah cara dan sarana pelaksanaan tindak pidana.

Analisis Penerapan Pertanggungjawaban Pidana dalam Kejahatan Siber

Penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber pada dasarnya tidak berbeda dengan tindak pidana konvensional. Perbedaannya terletak pada objek, alat, dan cara pelaksanaan tindak pidana yang menggunakan teknologi informasi sebagai sarana utama. Oleh karena itu, unsur-unsur pertanggungjawaban pidana seperti perbuatan pidana, kesalahan, kemampuan bertanggung jawab, dan tidak adanya alasan pemaaf tetap menjadi syarat utama untuk menjatuhkan pidana kepada pelaku.

Penelitian ini menemukan bahwa penggunaan ketentuan UU ITE sebagai *lex specialis* memberikan kepastian hukum dalam menjerat pelaku kejahatan siber. Keberadaan pasal-pasal yang mengatur akses ilegal, manipulasi data elektronik, penyebaran informasi palsu, dan

penyalahgunaan sistem elektronik menunjukkan bahwa hukum pidana Indonesia telah beradaptasi dengan perkembangan teknologi digital.

Namun demikian, penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber masih menghadapi berbagai kendala. Salah satu kendala utama adalah pembuktian keterlibatan pelaku dalam suatu tindak pidana siber. Berbeda dengan kejahatan konvensional yang umumnya meninggalkan bukti fisik, cybercrime lebih banyak menghasilkan bukti digital yang memerlukan metode investigasi khusus. Oleh karena itu, keberhasilan pembuktian sangat bergantung pada kemampuan aparat penegak hukum dalam melakukan digital forensik.

Selain itu, penggunaan identitas anonim juga menjadi tantangan tersendiri. Pelaku sering memanfaatkan akun palsu, teknologi enkripsi, dan jaringan virtual untuk menyamarkan identitasnya. Kondisi tersebut menyebabkan proses pembuktian unsur kesalahan menjadi lebih kompleks karena aparat penegak hukum harus terlebih dahulu membuktikan identitas pelaku sebelum membuktikan perbuatannya.

Tantangan Penegakan Hukum terhadap Kejahatan Siber di Era Digital

Hasil penelitian menunjukkan bahwa tantangan terbesar dalam penegakan hukum terhadap kejahatan siber terletak pada karakteristik cybercrime yang bersifat lintas batas negara (*borderless crime*). Dalam banyak kasus, pelaku, korban, dan server yang digunakan berada di wilayah negara yang berbeda. Kondisi ini menimbulkan persoalan yurisdiksi yang tidak ditemukan dalam tindak pidana konvensional.

Dalam perspektif hukum internasional, penegakan hukum terhadap kejahatan lintas negara memerlukan kerja sama antarnegara melalui mekanisme bantuan hukum timbal balik (*mutual legal assistance*), ekstradisi, dan pertukaran informasi. Tanpa adanya kerja sama internasional yang efektif, proses penegakan hukum terhadap pelaku cybercrime akan mengalami hambatan yang signifikan.

Perkembangan teknologi digital yang sangat cepat juga menyebabkan hukum sering kali tertinggal dibandingkan modus operandi kejahatan yang berkembang di masyarakat. Munculnya teknologi Artificial Intelligence (AI), cryptocurrency, blockchain, dark web, dan deepfake telah menciptakan bentuk-bentuk kejahatan baru yang belum sepenuhnya diatur dalam regulasi yang ada. Akibatnya, aparat penegak hukum sering menghadapi kesulitan dalam menentukan dasar hukum yang tepat untuk menjerat pelaku.

Fenomena deepfake, misalnya, memungkinkan seseorang menciptakan gambar, video, atau suara palsu yang menyerupai individu tertentu. Teknologi tersebut dapat digunakan untuk penipuan, pemerasan, pencemaran nama baik, bahkan manipulasi informasi publik. Kondisi ini menunjukkan bahwa perkembangan teknologi telah memperluas dimensi kejahatan siber dan menuntut pembaruan hukum yang lebih responsif terhadap perubahan sosial.

Implikasi Temuan Penelitian terhadap Pengembangan Hukum Pidana Nasional

Temuan penelitian ini menunjukkan bahwa konsep pertanggungjawaban pidana klasik masih relevan untuk diterapkan terhadap pelaku kejahatan siber. Namun demikian, diperlukan penguatan regulasi dan kebijakan hukum pidana yang lebih adaptif terhadap perkembangan teknologi digital.

Penguatan tersebut dapat dilakukan melalui harmonisasi antara KUHP Nasional, UU ITE, dan UU Perlindungan Data Pribadi sehingga tercipta sistem hukum yang lebih terintegrasi dalam menghadapi kejahatan siber. Selain itu, peningkatan kapasitas aparat penegak hukum di bidang digital forensik, keamanan siber, dan investigasi elektronik perlu menjadi prioritas dalam rangka meningkatkan efektivitas penegakan hukum.

Di samping aspek represif, pendekatan preventif juga perlu diperkuat melalui peningkatan literasi digital masyarakat. Kesadaran masyarakat terhadap keamanan data pribadi dan risiko kejahatan siber akan membantu mengurangi potensi terjadinya tindak pidana di ruang digital.

Dengan demikian, efektivitas pertanggungjawaban pidana pelaku kejahatan siber tidak hanya bergantung pada keberadaan regulasi yang memadai, tetapi juga pada kemampuan negara dalam mengimplementasikan hukum secara efektif melalui dukungan teknologi, sumber daya manusia yang kompeten, dan kerja sama internasional yang berkelanjutan.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada Program Studi Hukum dan seluruh pihak yang telah memberikan dukungan dalam pelaksanaan penelitian ini.

SIMPULAN DAN SARAN

Pertanggungjawaban pidana pelaku kejahatan siber dalam sistem hukum Indonesia didasarkan pada terpenuhinya unsur tindak pidana, kesalahan, kemampuan bertanggung jawab, dan tidak adanya alasan pemaaf. Pengaturan mengenai cybercrime telah diakomodasi dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, dan KUHP Nasional Tahun 2023. Meskipun demikian, tantangan berupa pembuktian elektronik, anonimitas pelaku, yurisdiksi lintas negara, dan perkembangan teknologi masih menjadi hambatan dalam penegakan hukum

Pemerintah perlu memperkuat regulasi terkait cybercrime yang adaptif terhadap perkembangan teknologi. Aparat penegak hukum perlu meningkatkan kapasitas digital forensik serta memperkuat kerja sama internasional dalam penanganan kejahatan siber lintas negara. Selain itu, peningkatan literasi digital masyarakat juga diperlukan sebagai upaya preventif dalam menekan angka kejahatan siber.

DAFTAR RUJUKAN

Ibrahim, J. (2022). *Teori dan metodologi penelitian hukum normatif* (Edisi Revisi). Bayumedia Publishing.

IRAC Academy. (2023). *Legal research methods and legal reasoning in contemporary law studies*. IRAC Press.

Marzuki, P. M. (2021). *Penelitian hukum* (Edisi Revisi). Kencana.

Soekanto, S., & Mamudji, S. (2021). *Penelitian hukum normatif: Suatu tinjauan singkat* (Edisi Revisi). RajaGrafindo Persada.

Muhaimin. (2020). *Metode penelitian hukum*. Mataram University Press.

Referensi Jurnal Pendukung Metode (2021–2025)

Fadli, M. (2021). Penelitian hukum normatif dan empiris dalam perspektif ilmu hukum. *Jurnal Rechtsvinding, 10*(2), 185–200.

Prasetyo, T., & Barkatullah, A. H. (2022). Development of legal research methodology in Indonesian legal scholarship. *Hasanuddin Law Review, 8* (3), 250–266.

Rahman, A., & Nugroho, D. (2023). Normative legal research and its application in cyber law studies. *Jurnal Hukum dan Peradilan, 12*(1), 45–61.

Sari, N., & Wibowo, A. (2024). Statute approach and conceptual approach in contemporary legal research. *Jurnal Legislasi Indonesia, 21*(2), 110–126.

Yuliana, R., & Hakim, L. (2025). Qualitative legal analysis in criminal law research: A methodological review. *Jurnal Ius Constituendum, 10*(1), 75–90.

Alfendo, Y. A. (2024). Penanggulangan terhadap kejahatan cyber-terrorism melalui politik hukum pidana. *Jurist-Diction, 7*(2), 1–18.

Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest: Journal of Universal Studies, 4*(9), 1–12.

Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi penyidikan terhadap tindak pidana siber dalam perspektif perbandingan hukum: Indonesia dan Inggris Raya. *Jurnal Ilmiah Penegakan Hukum, 11*(2), 162–172.

Langgono, P. W., Hartoyo, & Ayuningtyas, F. (2025). Criminal liability for phishing perpetrators: A normative analysis of Indonesian criminal law. *International Journal of Law and Society, 3*(1).

Putri, D. V. A., & Dievana, K. A. (2024). Yurisdiksi penegakan hukum tindak pidana cybercrime di Indonesia pasca reformasi. *Jurnal Hukum dan Sosial Politik, 2*(3), 280–284.

Shidiq, M. P. (2024). Characteristics cyber crime and dynamics of the implementation locus delicti theory by law enforcement officials in Indonesia. *Ajudikasi: Jurnal Ilmu Hukum, 8*(2), 169–182.

Waluyadi. (2024). Law enforcement against cyber crimes in Indonesia: Analysis of the role of the ITE Law in handling cyber crimes. *Indonesian Cyber Law Review, 1*(1), 1–15.

Atmawijaya, M. K. R. E., et al. (2023). Criminal liability for the provision of illegal WIFI telecommunications services. *Indonesian Journal of Criminal Law Studies, 8*(1), 135–164.

Alfakar, M. W., Masyhar, A., Wulandari, C., & Nte, N. D. (2023). Evolution of corporate criminal liability models and theories under Indonesian New Criminal Code. *Indonesian Journal of Criminal Law Studies, 8*(2), 261–288.

Fitriani, R., & Prasetyo, T. (2023). Pertanggungjawaban pidana pelaku kejahatan siber dalam sistem hukum Indonesia. *Jurnal Ius Constituendum, 8*(2), 215–230.

Hidayat, M., & Wibowo, A. (2023). Cybercrime and digital evidence challenges in Indonesian criminal justice system. *Jurnal Hukum dan Peradilan, 12*(3), 301–320.

Rahmawati, N. (2023). Legal challenges in identifying cybercrime offenders in Indonesia. *Jurnal RechtsVinding, 12*(2), 201–215.

Nugroho, A., & Arifin, M. (2024). Cross-border cybercrime and legal enforcement challenges in Indonesia. *International Journal of Law and Information Technology, 18*(2), 112–128.

Pratama, R. A., & Setiawan, D. (2024). Digital forensic evidence in cybercrime investigations: Legal perspectives in Indonesia. *Jurnal Legislasi Indonesia, 21*(1), 55–71.

Wulandari, F., & Aminah, S. (2025). The effectiveness of cybercrime law enforcement in Indonesia's digital transformation era. *Hasanuddin Law Review, 11*(1), 75–92.

Susanto, E., & Kurniawan, A. (2025). Artificial intelligence and emerging cybercrime threats in Southeast Asia. *Journal of Cyber Policy, 10*(1), 88–104.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.