JPIM: Jurnal Penelitian Ilmiah Multidisipliner
Vol. 02, No. 02, Tahun 2025, Hal. 1295-1299 ISSN: 3089–0128 (online)

Kejahatan Siber dan Tantangan Penegakan Hukum di Indonesia

Abizar Al Ghiffari[1*]
[1]*Program Studi Hukum, Fakultas Hukum Universitas Bandar Lampung, Indonesia*
E-mail: abizaralqiffari@gmail.com[1]

Article Info

Article history:

Received Agust 04, 2025
Revised Agust 12, 2025
Accepted Agust 15, 2025

Keywords:

Cybercrime, Law Enforcement, Indonesia, Systematic Literature Review, Digital Security.

ABSTRACT

Cybercrime in Indonesia continues to increase in line with the development of digital technology, posing serious challenges for law enforcement agencies. This study aims to identify the dominant forms of cybercrime in Indonesia and analyze the obstacles to law enforcement, both in terms of regulation, agency capacity, and cross-border cooperation. The method used is a Systematic Literature Review (SLR) of five scientific articles published between 2020 and 2025, selected based on criteria of topic relevance, source credibility, and data recency. The findings indicate that cybercrime in Indonesia is dominated by phishing, hacking, misuse of personal data, and online fraud. The main challenges in law enforcement include delays in establishing data protection authorities, lack of harmonization of laws with international standards, limited technical expertise of law enforcement agencies, and insufficient cross-border cooperation. These findings indicate the need for more adaptive legal reforms, increased human resource capacity, and strengthened international cooperation in addressing cybercrime. This research contributes to the development of national policies that are responsive to the dynamics of cyber threats, while also serving as a reference for future researchers in examining law enforcement strategies in the digital age.

Article Info

Article history:

Received Agust 04, 2025
Revised Agust 12, 2025
Accepted Agust 15, 2025

Kata Kunci:

Kejahatan Siber, Penegakan Hukum, Indonesia, Systematic Literature Review, Keamanan Digital

ABSTRAK

Kejahatan siber di Indonesia terus mengalami peningkatan seiring perkembangan teknologi digital, yang menimbulkan tantangan serius bagi aparat penegak hukum. Penelitian ini bertujuan untuk mengidentifikasi bentuk-bentuk kejahatan siber yang dominan di Indonesia dan menganalisis hambatan penegakan hukum yang dihadapi, baik dari aspek regulasi, kapasitas aparat, maupun kerja sama lintas negara. Metode yang digunakan adalah Systematic Literature Review (SLR) terhadap lima artikel ilmiah terbitan 2020-2025, yang dipilih berdasarkan kriteria relevansi topik, kredibilitas sumber, dan keterkinian data. Hasil kajian menunjukkan bahwa kejahatan siber di Indonesia didominasi oleh phishing, peretasan, penyalahgunaan data pribadi, dan penipuan daring. Tantangan utama penegakan hukum meliputi keterlambatan pembentukan otoritas perlindungan data, kurangnya harmonisasi hukum dengan standar internasional, keterbatasan keahlian teknis aparat, serta minimnya kerja sama lintas batas negara. Temuan ini mengindikasikan perlunya reformasi hukum yang lebih adaptif, peningkatan kapasitas sumber daya manusia, dan penguatan kerja sama internasional dalam menangani kejahatan siber. Penelitian ini memberikan kontribusi bagi pengembangan kebijakan nasional yang responsif terhadap dinamika ancaman siber, sekaligus menjadi rujukan bagi peneliti selanjutnya dalam mengkaji strategi penegakan hukum di era digital.

Corresponding Author:

Abizar Al Ghiffari
Program Studi Hukum, Fakultas Hukum Universitas Bandar Lampung
E-mail: abizaralqiffari@gmail.com

Pendahuluan

Transformasi digital telah menjadi pendorong utama perubahan sosial, ekonomi, dan budaya di abad ke-21. Perkembangan teknologi informasi yang pesat membuka peluang ekonomi baru, namun sekaligus menciptakan ruang bagi berkembangnya kejahatan siber yang melampaui batas yurisdiksi negara, memanfaatkan anonimitas dan kerentanan sistem informasi (Hartono, W et al., 2024). Di Indonesia, peningkatan signifikan pada insiden kebocoran data, phishing, ransomware, serta penipuan daring menjadi indikasi nyata bahwa perangkat hukum dan kapasitas penegakan yang ada belum sepenuhnya mampu mengimbangi kecepatan inovasi modus kejahatan tersebut (Hartono, W et al., 2024).

Walaupun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya memberikan kerangka hukum formal bagi penindakan, tantangan praktis di lapangan masih besar. Pembuktian di pengadilan kerap terkendala oleh sifat bukti digital yang mudah dimodifikasi, hilang, atau rusak jika tidak ditangani dengan prosedur forensik yang tepat (Hartono, W et al., 2024). Rendahnya literasi digital aparat penegak hukum dan hakim dalam memahami kompleksitas bukti digital semakin memperlemah efektivitas penegakan hukum (Kusnadi, Efendi, & da Silva, 2025).

Di sisi perlindungan data pribadi, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) diharapkan menjadi tonggak penting dalam memperkuat rezim perlindungan privasi di Indonesia. Namun, penundaan pembentukan otoritas pengawas dan belum lengkapnya peraturan turunan menimbulkan ketidakpastian hukum, baik bagi pelaku usaha maupun aparat penegak hukum (Hernowo, 2025). Kekosongan ini berimplikasi pada lambannya proses penegakan administratif dan lemahnya koordinasi dengan penegakan pidana ketika kasus kebocoran data beririsan dengan tindak pidana siber (Hernowo, 2025).

Selain itu, sifat transnasional dari internet menimbulkan tantangan yurisdiksi yang kompleks. Perbedaan sistem hukum antarnegara, standar pembuktian, dan mekanisme bantuan hukum timbal balik (mutual legal assistance) sering menghambat proses investigasi dan penuntutan terhadap pelaku yang beroperasi dari luar negeri (Tekayadi et al., 2025). Ketiadaan harmonisasi hukum siber internasional juga berdampak pada sulitnya pengumpulan bukti lintas batas, terutama ketika infrastruktur serangan seperti server, domain, atau dompet aset kripto berada di berbagai negara (Tekayadi et al., 2025).

Di ranah sosial dan budaya digital, analisis wacana publik di media sosial menunjukkan bahwa masyarakat Indonesia sangat terpapar pada ancaman siber seperti judi daring, penipuan investasi, dan ujaran kebencian (Kusnadi et al., 2025). Data tersebut dapat menjadi indikator penting bagi aparat penegak hukum dalam menetapkan prioritas penindakan, sekaligus menjadi bahan perumusan kebijakan edukasi literasi digital yang lebih

sistemik. Kesadaran publik terhadap ancaman ini semakin penting mengingat modus kejahatan siber kini semakin terintegrasi dengan kehidupan sehari-hari.

Dalam konteks penegakan hukum, peningkatan kapasitas forensik digital merupakan kebutuhan mendesak. Tanpa laboratorium forensik yang memadai, prosedur chain of custody yang ketat, serta sumber daya manusia yang terlatih, proses pembuktian akan terus menghadapi hambatan signifikan (Hartono, W et al., 2024). Investasi dalam teknologi analisis bukti digital, baik untuk perangkat bergerak, cloud computing, maupun transaksi aset kripto, menjadi bagian integral dari strategi nasional penanggulangan kejahatan siber (Hartono, W et al., 2024).

Berdasarkan latar belakang tersebut, penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk menganalisis literatur terbitan 2020–2025 yang membahas kejahatan siber dan tantangan penegakan hukum di Indonesia. Tujuannya adalah untuk memetakan hambatan utama, mengevaluasi peran regulasi seperti UU ITE dan UU PDP, serta merumuskan rekomendasi kebijakan yang dapat memperkuat efektivitas penegakan hukum di era digital (Hernowo, 2025; Kusnadi et al., 2025; Tekayadi et al., 2025; Hartono, W et al., 2024).

Metode

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur ilmiah terbitan 2020–2025 yang relevan dengan topik kejahatan siber dan penegakan hukum di Indonesia. Pencarian dilakukan melalui Google Scholar, Portal Garuda, dan prosiding internasional EAI dengan kata kunci “cybercrime Indonesia”, “penegakan hukum siber”, “digital forensics Indonesia”, “UU ITE”, dan “Personal Data Protection Law Indonesia”. Kriteria inklusi mencakup: (1) fokus penelitian pada konteks Indonesia; (2) artikel ilmiah atau prosiding yang memuat pembahasan empiris atau normatif terkait penegakan hukum siber; (3) terbit pada periode 2020–2025; dan (4) dapat diakses secara full-text. Dari sekitar 120 temuan awal, proses seleksi judul dan abstrak menyisakan 18 artikel yang kemudian disaring lebih lanjut berdasarkan keterkaitan topik, kualitas metodologi, dan keterkinian regulasi yang dibahas.

Tahap evaluasi teks penuh menghasilkan lima artikel inti yang menjadi fokus SLR ini, yaitu: Hernowo (2025) yang membahas tantangan implementasi UU PDP; Kusnadi, Efendi, dan da Silva (2025) yang menganalisis wacana publik terkait kejahatan siber di Indonesia; Tekayadi, Sumerah, dan Efendi (2025) yang mengkaji tantangan penegakan hukum siber lintas negara; Hartono, W et al. (2024) yang memetakan hambatan investigasi kejahatan siber; serta Law Enforcement in Efforts to Combat Cyber Crime in Indonesia (2023) yang membahas kasus phishing dan tantangan pembuktiannya. Proses ekstraksi data dilakukan dengan mengidentifikasi tujuan penelitian, metode, temuan utama, dan rekomendasi dari masing-masing artikel, yang kemudian dianalisis secara tematik untuk menghasilkan sintesis menyeluruh (Hernowo, 2025; Kusnadi et al., 2025; Tekayadi et al., 2025; Hartono, W et al., 2024; Ardian, Y., et al., 2023).

Hasil dan Pembahasan

Hasil Systematic Literature Review terhadap lima artikel yang terbit antara tahun 2020–2025 menunjukkan bahwa kejahatan siber di Indonesia mengalami peningkatan signifikan, baik dari segi jumlah maupun kompleksitas modus operandi. Berdasarkan temuan Hartono, W et al. (2024), mayoritas insiden kejahatan siber di Indonesia meliputi phishing, malware, ransomware, dan penipuan berbasis media sosial. Modus ini memanfaatkan kerentanan perilaku pengguna dan lemahnya pengamanan sistem informasi pada lembaga

publik maupun swasta. Data dari Kusnadi, Efendi, & da Silva (2025) mengindikasikan bahwa kejahatan berbasis social engineering meningkat seiring rendahnya literasi digital di kalangan masyarakat, yang sering kali tidak menyadari risiko dari membagikan informasi pribadi secara daring.

Tantangan penegakan hukum menjadi isu utama yang diidentifikasi di seluruh literatur yang dianalisis. Hernowo (2025) mencatat bahwa meskipun UU PDP telah diberlakukan, proses penegakan masih terkendala karena belum terbentuknya lembaga otoritas perlindungan data yang berfungsi penuh. Kekosongan kelembagaan ini membuat koordinasi antara penegakan administratif dan pidana belum optimal. Selain itu, Tekayadi et al. (2025) menekankan bahwa sifat transnasional dari kejahatan siber menuntut adanya harmonisasi hukum internasional dan perjanjian ekstradisi yang lebih kuat. Tanpa mekanisme mutual legal assistance yang efektif, proses penuntutan terhadap pelaku lintas negara akan terus terhambat.

Aspek teknis pembuktian menjadi hambatan serius lainnya. Berdasarkan temuan Hartono, W et al. (2024), bukti digital memerlukan prosedur forensik yang sangat ketat untuk memastikan keabsahan di pengadilan. Kendala muncul ketika aparat penegak hukum tidak memiliki fasilitas laboratorium forensik yang memadai atau sumber daya manusia yang terlatih. Kasus-kasus yang melibatkan peretasan atau kebocoran data sering kali memerlukan digital evidence yang melibatkan log server, data cloud computing, atau transaksi aset kripto, yang penanganannya memerlukan keahlian dan teknologi canggih.

Selain hambatan regulasi dan teknis, penelitian juga menemukan bahwa dimensi sosial-budaya memainkan peran penting dalam eskalasi kejahatan siber. Menurut Kusnadi et al. (2025), budaya penggunaan internet di Indonesia masih didominasi oleh pola konsumtif dan hiburan, sementara kesadaran keamanan digital relatif rendah. Hal ini memberikan celah bagi pelaku kejahatan siber untuk menyasar korban melalui pendekatan yang memanipulasi kepercayaan, seperti penipuan investasi bodong atau phishing yang menyerupai pesan dari pihak berwenang. Tanpa upaya literasi digital yang sistemik, tingkat kerentanan ini akan tetap tinggi.

Upaya peningkatan kapasitas penegakan hukum sebenarnya telah dimulai melalui pelatihan forensik digital dan pengadaan perangkat analisis data oleh aparat kepolisian. Namun, Hernowo (2025) menilai bahwa langkah-langkah ini masih sporadis dan belum terintegrasi dalam strategi nasional penanggulangan kejahatan siber. Diperlukan pendekatan lintas sektoral yang melibatkan lembaga penegak hukum, regulator telekomunikasi, penyedia layanan internet, sektor swasta, dan organisasi masyarakat sipil. Kolaborasi ini penting mengingat serangan siber tidak hanya menimbulkan kerugian finansial, tetapi juga dapat mengancam keamanan nasional jika menyasar infrastruktur vital.

Dari perspektif kebijakan, harmonisasi antara UU ITE, UU PDP, dan regulasi teknis di sektor keuangan, telekomunikasi, dan pertahanan siber menjadi kunci untuk memperkuat efektivitas penegakan hukum. Tekayadi et al. (2025) mengusulkan pembentukan Cybersecurity Task Force nasional yang dilengkapi dengan kewenangan lintas sektor dan dukungan anggaran khusus untuk investigasi kejahatan siber. Langkah ini sejalan dengan tren global di mana banyak negara telah mengadopsi pendekatan terpadu dalam menghadapi ancaman siber.

Terakhir, penting untuk dicatat bahwa pemberantasan kejahatan siber tidak dapat hanya mengandalkan instrumen hukum dan teknologi, tetapi juga membutuhkan perubahan budaya keamanan di tingkat individu dan organisasi. Peningkatan literasi digital, kesadaran privasi, dan penerapan best practices keamanan informasi seperti multi-factor authentication

dan enkripsi data harus menjadi bagian dari strategi jangka panjang (Hartono, W et al., 2024; Kusnadi et al., 2025). Tanpa fondasi kesadaran publik yang kuat, penegakan hukum akan terus bersifat reaktif dan rentan tertinggal dari evolusi modus kejahatan siber.

Kesimpulan

Penegakan hukum terhadap kejahatan siber di Indonesia saat ini masih menghadapi tantangan kompleks yang melibatkan aspek regulasi, kelembagaan, kapasitas teknis, pembuktian di pengadilan, serta kerja sama lintas negara. Kesenjangan antara regulasi yang ada dengan implementasi di lapangan, keterbatasan sumber daya manusia dan teknologi forensik digital, serta rendahnya literasi digital di kalangan aparat menjadi faktor penghambat utama. Melalui tinjauan literatur sistematis, penelitian ini menegaskan perlunya reformasi kelembagaan, investasi dalam kapasitas forensik, penguatan mekanisme kerja sama internasional, dan penerapan pendekatan penegakan berbasis data yang terintegrasi dengan literasi digital publik. Kombinasi strategi ini diharapkan mampu meningkatkan efektivitas respons Indonesia terhadap kejahatan siber yang semakin canggih dan terorganisasi (Hernowo, 2025; Hartono, W et al., 2024; Tekayadi et al., 2025; Kusnadi et al., 2025; Ardian, Y., et al., 2023).

Daftar Pustaka

Ardian, Y., et al. (2023). Law enforcement in efforts to combat cyber crime in Indonesia (phishing case study). Riau Journal of Law.

Hartono, W et al. (2024). Challenges of criminal investigation cyber crime. Awang Long Law Review, 7(1), 11–19.

Hernowo, B. A. (2025). The challenges of implementing the Personal Data Protection Law in Indonesia: Delays in establishing a regulatory authority. In Proceedings of the EAI International Conference on Law.

Kusnadi, D., et al. (2025). Cybercrime and digital society in Indonesia: Legal challenges and public discourse. ADLIYA: Jurnal Hukum dan Kemanusiaan, 19(1), 39–56. https://doi.org/10.15575/adliya.v19i1.40404

Tekayadi, et al. (2025). Tantangan penegakan hukum siber di era lintas negara dan harmonisasi hukum internasional: Sebuah tinjauan hukum dan kebijakan