Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
5 (3) 2025, Page: 36877-36884

Implementasi Regulasi Pidana Dalam Melawan Kejahatan Siber Pada Era Digital Di Indonesia

Della Abelia Hermawan, Siti Nuraisyah Putri, Asmak Ul Hosnah
Prodi Ilmu Hukum, Fakultas Hukum, Universitas Pakuan
E-mail : della@gmail.com

Published: December , 2025

ABSTRAK

Perkembangan teknologi informasi telah membuat keuntungan dan bahaya kejahatan siber semakin terlihat di Indonesia, seperti pencurian identitas dan serangan DDoS. Jumlah insiden meningkat dari tahun 2019 hingga 2022, tetapi menurun antara tahun 2022 dan 2023. Alasan utama untuk ini adalah penggunaan internet yang tinggi, kurangnya pengetahuan tentang teknologi digital, dan perlindungan data yang buruk. Penegak hukum menggunakan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang- Undang Hukum Pidana (KUHP), namun masih menghadapi banyak tantangan. Tujuan penelitian ini untuk menganalisis bagaimana hukum pidana digunakan untuk menangani kejahatan siber, memeriksa masalah yang ada, dan menyarankan cara mengatasinya. Studi ini menggunakan pendekatan hukum normatif, dengan fokus pada pengamatan aturan, prinsip, dan kasus tentang kejahatan siber di Indonesia. Sumber informasi utama adalah UU ITE, KUHP, dan peraturan terkait, sedangkan sumber sekunder meliputi artikel dan makalah akademis. Dokumen ini membahas tantangan dan solusi potensial untuk keamanan siber di negara tersebut. Meskipun teknologi informasi membawa banyak manfaat, teknologi ini juga menyebabkan lebih banyak kejahatan siber, seperti pencurian data dan penipuan online. Meskipun undang-undang seperti UU ITE dan KUHP telah diperbarui, penegakan hukum masih menghadapi tantangan di bidang teknis, sosial, budaya, dan hukum, serta masalah dalam pengumpulan bukti digital dan perbedaan peraturan internasional. Beberapa solusi yang disarankan termasuk pelatihan yang lebih baik untuk masyarakat, kerja sama internasional yang lebih kuat, peningkatan infrastruktur, dan lebih banyak kerja sama tim antar sektor yang berbeda untuk memperkuat keamanan digital di tingkat nasional.
Kata kunci : Hukum Pidana, Kejahatan Siber, Penegakan Hukum.

ABSTRACT

Developments in information technology have made both the advantages and dangers of cybercrime more noticeable in Indonesia, like identity theft and DDoS attacks. The number of incidents went up from 2019 to 2022 but went down between 2022 and 2023. The key reasons for this are high internet use, not much knowledge about digital tech, and poor data protection. Law enforcement uses the Electronic Information and Transaction Law (ITE Law) and the Criminal Code (KUHP) but still has many challenges. This study looks into how criminal law is used to deal with cybercrime, checks the existing problems, and suggests ways to solve them. The study uses a normative legal approach, focusing on looking at rules, principles, and cases about cybercrime in Indonesia. Main sources of information are the ITE Law, the Criminal Code, and related rules, while secondary sources include articles and academic papers. This document looks at the challenges and possible solutions for cybersecurity in the country. While information technology brings many benefits, it also leads to more cybercrime, such as data theft and online scams. Even though laws like the ITE Law and the Criminal Code have been updated, law enforcement still faces challenges in technical, social, cultural, and legal areas, as well as problems with collecting digital evidence and differences in international regulations. Some suggested solutions include better training for people, stronger international cooperation, improved infrastructure, and more teamwork between different sectors to make digital security stronger at the national level.
Keywords : *Criminal Law, Cybercrime, Law Enforcement.*

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Di zaman globalisasi sekarang ini, perkembangan dalam teknologi informasi dan komunikasi telah berjalan dengan cepat dan punya dampak besar pada berbagai aspek kehidupan manusia (Dinarti et al., 2024). Teknologi informasi digunakan oleh pemerintah, perusahaan swasta, dan lembaga lainnya

untuk mengelola, memproses, serta menganalisis data dengan tujuan untuk menghasilkan informasi yang akurat, cepat, jelas, dan tepat (Siregar & Nasution, 2020). Kemajuan dalam teknologi informasi sangat penting untuk masyarakat agar memenuhi kebutuhan sehari-hari mereka. Kenyamanan dan kualitas yang dihadirkan oleh inovasi teknologi informasi memberikan manfaat positif bagi masyarakat. Keuntungan dari kemajuan teknologi ini tidak hanya dirasakan oleh pengguna yang memakainya untuk kegiatan yang produktif. Namun, di sisi lain, ada juga pelaku kejahatan yang memanfaatkan teknologi informasi untuk melakukan tindakan yang merugikan. Ini terlihat dari meningkatnya jumlah kejahatan di internet, yang biasa disebut kejahatan siber (Ningrum & Robekha, 2023).

Kejahatan siber merupakan aktivitas kriminal yang dilakukan oleh individu-individu penjahat siber dengan mengeksploitasi kemajuan dalam teknologi informasi, di mana komputer dan perangkat elektronik lainnya berfungsi sebagai alat untuk melangsungkan aksi kejahatan mereka. Beragam bentuk tindakan ilegal termasuk dalam kejahatan siber, seperti pencurian identitas, penipuan lewat internet, peretasan, distribusi *malware*, serta serangan DDoS. Tindak kejahatan ini berpotensi merugikan individu maupun organisasi, serta mampu mengancam keamanan negara dan perekonomian suatu bangsa (Sitanggang et al., 2024). Perkembangan kejahatan siber di Indonesia terus mengalami peningkatan tajam dan menjadi tantangan utama di era digital. Tren tindak pidana siber di Indonesia menunjukkan dinamika yang sangat fluktuatif selama beberapa tahun terakhir, baik dari sisi jumlah kasus maupun dari kompleksitas serta kerugian yang ditimbulkan.

Pada periode 2019 hingga 2021, Indonesia mengalami tren peningkatan signifikan dalam jumlah serangan siber. Menurut data dari Badan Siber dan Sandi Negara (BSSN), laporan serangan siber meningkat dari sekitar 290 juta serangan pada tahun 2019 menjadi lebih dari 495 juta serangan pada tahun 2020. Memasuki periode 2021-2022, terjadi lonjakan luar biasa dalam jumlah kasus yang ditangani oleh Kepolisian Republik Indonesia (Polri), yakni dari 612 kasus pada tahun 2021 menjadi 8.831 kasus pada tahun 2022 menunjukkan kenaikan sekitar 14 kali lipat. Peningkatan ini didorong oleh pembentukan lebih banyak satuan siber di berbagai daerah. Namun, pada periode 2022-2023, jumlah kasus kejahatan siber yang ditangani Polri mengalami penurunan dari 4.860 kasus menjadi 3.758 kasus, turun sekitar 22%. Meskipun jumlah perkara menurun, BSSN melaporkan peningkatan serangan siber mengindikasikan bahwa ancaman tetap tinggi (Mursyid et al., 2025).

Peningkatan jumlah kasus ini menunjukkan bahwa kejahatan siber menjadi tantangan serius bagi sistem hukum pidana nasional. Bentuk kejahatan yang dilaporkan mencakup penipuan daring, ujaran kebencian, penyebaran hoaks, penghinaan di media sosial, serta penyalahgunaan data pribadi. Fenomena ini dipicu oleh meningkatnya penggunaan internet dan media sosial, minimnya literasi digital, serta lemahnya perlindungan data pribadi (Siagian & Alexander, 2025). Di Indonesia, sejumlah peraturan telah diterapkan untuk mengatasi kejahatan siber, Kejahatan siber diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) juga tetap digunakan untuk menjerat pelaku kejahatan siber yang memenuhi unsur-unsur delik umum (Siagian & Alexander, 2025). Meski demikian, penerapan hukum pidana yang ada masih memiliki banyak kelemahan, baik dalam aspek pembuktian, yurisdiksi, maupun penegakan hukum.

Berdasarkan permasalahan tersebut, tujuan dari penelitian ini adalah untuk menganalisis penerapan hukum pidana dalam mengatasi kejahatan siber, meninjau kendala yang dihadapi, serta memberikan solusi atas kendala tersebut. Oleh sebab itu, artikel ini merumuskan beberapa rumusan permasalahan sebagai berikut: Bagaimana regulasi pidana di Indonesia dalam mengatur kejahatan siber? dan Apa saja kendala dalam penerapan regulasi pidana tersebut?

METODE PENELITIAN

Studi ini menggunakan metode penelitian hukum normatif yang berfokus pada kajian terhadap ketentuan peraturan perundang-undangan, doktrin hukum, serta yurisprudensi yang relevan. Metode tersebut diterapkan guna mengkaji secara mendalam aturan hukum yang mengatur tindak pidana siber serta problematikanya dalam implementasi di Indonesia. Secara metodologis, riset ini dirancang sebagai studi literatur atau literature review. Pengumpulan bahan hukum dilakukan dengan memanfaatkan dua jenis sumber, yaitu data primer dan sekunder. Sumber primer meliputi dokumen hukum tertulis seperti

Undang-Undang Informasi dan Transaksi Elektronik beserta revisinya, Kitab Undang-Undang Hukum Pidana, peraturan pemerintah, produk hukum Badan Siber dan Sandi Negara, serta instrumen hukum yang dikeluarkan oleh Kepolisian. Adapun sumber sekunder diperoleh dari berbagai publikasi akademik, seperti artikel ilmiah, monograf di bidang hukum pidana, dan jurnal-jurnal yang mengkhususkan pembahasan pada topik keamanan dunia maya serta penanganan hukum atas kejahatan digital di Indonesia. Dengan kerangka metode ini, penelitian diharapkan mampu memberikan kontribusi pemahaman yang lebih komprehensif terkait dinamika kejahatan siber di Indonesia dan menghasilkan rekomendasi kebijakan yang konstruktif guna penguatan penegakan hukum di tengah kompleksitas tantangan yang dihadapi.

HASIL DAN PEMBAHASAN

Pentingnya Regulasi Pidana dalam Menghadapi Kejahatan Siber

Kemajuan dalam bidang teknologi informasi saat ini menjadi salah satu komponen paling penting dalam memenuhi kebutuhan sehari-hari masyarakat. Kemudahan serta keunggulan yang diberikan oleh inovasi teknologi dianggap sebagai nilai tambah positif di pandangan masyarakat. Manfaat dari kemajuan teknologi ini jelas tidak hanya dirasakan oleh individu yang memanfaatkannya untuk aktifitas yang konstruktif. Di sisi lain, keuntungan tersebut juga dimanfaatkan oleh pelaku kriminal yang menggunakan teknologi informasi untuk tindakan yang merugikan. Hal ini terlihat dari adanya peningkatan dalam aksi kejahatan yang dikenal dengan sebutan kejahatan siber. Dalam mengatasi ancaman yang semakin kompleks, tindakan penegakan hukum perlu diselaraskan dan ditingkatkan supaya dapat menjawab tantangan di dunia digital yang terus berubah (Sariani, 2024).

Di tengah kemajuan yang tak henti-hentinya dalam zaman digital, kejahatan dunia maya di Indonesia kini menjadi risiko yang signifikan, terutama dalam sektor ekonomi. Kejahatan di dunia maya seperti pengambilan informasi secara ilegal, penipuan di internet, perdagangan yang dilarang, dan serangan pada sistem keuangan menunjukkan peningkatan yang signifikan. Regulasi pidana dalam hal kejahatan siber memiliki peran penting sebagai alat untuk mengatur dan mengendalikan kegiatan di dunia maya yang terus berkembang. Dengan adanya aturan hukum yang jelas, tindakan kriminal di dunia maya bisa diketahui, dicegah, dan ditangani secara terorganisir. Hal ini menjadikan hukum sebagai pelindung keamanan digital yang menyeluruh. Peran hukum dalam ranah siber adalah menetapkan batasan dan mengklasifikasikan tindak pidana yang terjadi di dunia maya sebagai perbuatan kriminal. Selain itu, hukum juga membentuk landasan prosedural bagi upaya penindakan terhadap pelanggaran tersebut, sekaligus menjamin keselamatan serta kepentingan hukum baik bagi perorangan maupun korporasi (Fahmi & Tambunan, 2024).

Regulasi Pidana di Indonesia Terkait Kejahatan Siber

Penanggulangan kejahatan siber di Indonesia telah memiliki landasan hukum pidana melalui sejumlah regulasi, di antaranya Undang-Undang Informasi dan Transaksi Elektronik (ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) (Umami & Fithry, 2024). Upaya penyesuaian hukum pidana dengan kemajuan teknologi tercermin dari dikeluarkannya Undang-Undang Nomor 11 Tahun 2008 tentang ITE. Undang undang ini kemudian mengalami penyempurnaan dua kali untuk merespons kompleksitas ancaman kejahatan siber yang terus berkembang, yakni melalui revisi pertama dalam Undang-Undang Nomor 19 Tahun 2016 dan revisi kedua dalam Undang-Undang Nomor 1 Tahun 2024 (Judijanto, 2025).

Tindak pidana siber di dalam KUHP yang baru dapat dibagi menjadi beberapa kategori. Pertama, pelanggaran yang menyasar keamanan serta integritas sistem komputer yang diatur dalam Pasal 554 hingga 557. Kategori ini meliputi aktivitas seperti mengakses sistem komputer tanpa izin, merusak atau memodifikasi data digital, serta mengganggu fungsi sistem komputer. Kedua, kejahatan yang berkaitan dengan pemalsuan serta manipulasi data digital yang tertera dalam Pasal 558 hingga 562. Kelompok ini mencakup tindakan membuat dokumen elektronik palsu dan pemanfaatan dokumen elektronik palsu untuk tujuan tertentu. Ketiga, tindak pidana ekonomi yang berbasis teknologi yang diatur dalam Pasal 563 hingga 567, termasuk penipuan melalui sistem elektronik dan pencurian data dengan niat untuk mendapatkan keuntungan (Ganjar, 2025).

Dalam sistem hukum Indonesia, berbagai lembaga teknis menerbitkan aturan-aturan tambahan untuk menjelaskan dan memberi petunjuk pelaksanaan Undang-Undang. Instrumen-instrumen tersebut

meliputi Peraturan Pemerintah (PP), Peraturan Presiden (Perpres), Peraturan Menteri (Permen), Peraturan Kepolisian Negara Republik Indonesia (PERKAP), serta Surat Edaran (SE) dari instansi terkait. Keberadaan aturan turunan ini bertujuan memberikan arahan dalam menangani perkembangan bentuk kejahatan yang dinamis.

Meskipun demikian, dalam hierarki peraturan perundang-undangan, instrumen seperti PERKAP dan Surat Edaran tidak menempati kedudukan yang sederajat dengan undang-undang. Oleh karena itu, secara umum kedua jenis aturan ini berperan sebagai pedoman internal bagi instansi pelaksana, bukan sebagai dasar hukum yang dapat diajukan langsung dalam proses persidangan di pengadilan (Azis et al., 2025).

Implementasi Regulasi Pidana dalam Penanganan Kejahatan Siber

Mekanisme penegakan hukum menekankan peran serta tanggung jawab sejumlah lembaga yang berpartisipasi dalam melawan kejahatan siber. Kerjasama dan sinkronisasi antara lembaga-lembaga ini sangat perlu untuk penegakan hukum yang efektif (Mokombang et al., 2023). Urgensi dari rekonstruksi ini terlihat jelas melalui besarnya kerugian yang ditimbulkan oleh kejahatan siber, yang mencakup kerugian finansial yang signifikan, gangguan dalam operasi bisnis, serta risiko bagi keamanan nasional (Saputra et al., 2024).

Penegakan hukum terkait kejahatan siber di Indonesia dilaksanakan oleh beberapa institusi, di antaranya adalah Kepolisian Republik Indonesia (POLRI), Kejaksaan Agung, serta Komisi Pemberantasan Korupsi (KPK). POLRI memiliki divisi khusus yang bertanggung jawab untuk menangani masalah kejahatan di ranah maya, yaitu Direktorat Tindak Pidana Siber Bareskrim Polri. Di sisi lain, Kejaksaan Agung memainkan peran krusial dalam membawa para pelanggar kejahatan siber ke pengadilan (Saputra et al., 2024).

Kendala Penegakan Hukum terhadap Kejahatan Siber

Meskipun Indonesia memiliki regulasi yang dapat menjerat pelaku kejahatan siber, kenyataannya implementasi dari aturan tersebut masih jauh dari optimal. Terdapat sejumlah hambatan yang menghalangi penanganan kasus kejahatan di dunia maya. Berbagai rintangan itu dihadapi oleh pihak berwenang dalam usaha untuk memberantas aksi kejahatan siber. Rintangan-rintangan ini tentunya berpengaruh pada proses penegakan hukum terkait kejahatan siber, yang mengakibatkan penanganan tidak efektif. Rintangan-rintangan ini meliputi:

1. Kendala Teknis dalam Penegakan Hukum terhadap Kejahatan Siber

   Tantangan signifikan dalam penindakan hukum atas kejahatan siber adalah minimnya jumlah tenaga ahli dengan kompetensi mendalam di bidang forensik digital. Banyak penyidik menghadapi keterbatasan dalam pemahaman dan pengalaman teknis untuk menangani barang bukti elektronik, misalnya dalam menganalisis log aktivitas, melacak alamat IP, atau mengakses data terenkripsi. Pada banyak situasi, aparat penegak hukum dituntut memiliki keahlian tingkat tinggi guna membongkar metode kompleks yang dipakai pelaku, seperti jaringan terselubung *(anonymous networks)* atau transaksi menggunakan mata uang kripto yang sengaja dirancang untuk menghilangkan jejak.

   Selain keterbatasan sumber daya manusia, ketersediaan teknologi khusus kejahatan siber yang kurang memadai di banyak lembaga penegak hukum di Indonesia juga menjadi kendala yang cukup berarti bagi sarana dan prasarana yang dibutuhkan oleh penyidik untuk secara efektif memberantas kejahatan siber (Djabar et al., 2025). Keterbatasan teknologi ini menyebabkan lamanya waktu penyidikan untuk menangani kasus kejahatan siber. Selain itu, untuk mengembangkan infrastuktur teknologi yang diperlukan juga memerlukan pengeluaran yang tidak sedikit. Hal ini menjadi hambatan dalam memperbarui infrastruktur dan memperluas kapasitas penegak hukum dalam hal teknologi.

   Kendala yang ketiga yaitu, Proses pengumpulan dan verifikasi bukti digital. Berbeda dengan kejahatan tradisional yang meninggalkan tanda fisik, kejahatan siber sering kali tergantung pada data digital yang rentan untuk dihapus, dimodifikasi, atau disembunyikan. Bukti seperti tangkapan layar, rekaman obrolan, metadata, atau aktivitas internet pelaku perlu dikumpulkan dengan cara yang sah dan terjamin keandalannya agar bisa diterima di pengadilan. Prosedur ini memerlukan keterampilan forensik digital serta perangkat teknologi yang memadai, yang masih kurang tersedia di banyak instansi penegak hukum di Indonesia (Rahmiati et al., 2025).
2. Tantangan Sosial dan Budaya dalam Penegakan Hukum terhadap Kejahatan Siber

Kesadaran masyarakat di Indonesia tentang pentingnya perlindungan data pribadi masih sangat kurang karena tingkat literasi digital yang rendah, minimnya pendidikan, dan budaya penggunaan internet yang terlalu longgar. Banyak individu yang tanpa pikir panjang membagikan informasi pribadi tanpa menyadari risiko yang mungkin muncul. Kampanye yang dilakukan pemerintah atau platform digital belum sampai ke semua daerah, terutama di lokasi yang sulit dijangkau. Kebanyakan masyarakat percaya pada instutisi pemerintah, sehingga tidak banyak yang mempertanyakan cara pengelolaan data. Kurangnya konsekuensi langsung dan lemahnya hukum yang diterapkan juga membuat masyarakat tidak terlalu peka terhadap masalah privasi. Tanpa pendidikan dan perlindungan hukum yang baik, masyarakat tetap menjadi pengguna internet yang pasif dan rentan terhadap serangan siber (Sitorus et al., 2025).

Selain itu, masih ada sejumlah korban yang enggan untuk melaporkan tindakan kriminal yang mereka alami disebabkan oleh kurangnya pemahaman mengenai kejahatan yang telah terjadi. Tingginya angka ketidaklaporan ini berpengaruh pada lambannya proses hukum dan juga terbatasnya informasi yang bisa digunakan untuk menganalisis pola kejahatan. Kejahatan siber biasanya terjadi tanpa sepengetahuan korban, bahkan ketika tindakan kriminal tersebut berlangsung, tidak ada saksi yang melihat. Banyak korban baru menyadari setelah mengecek informasi yang mereka gunakan, di mana data tersebut tidak dapat diakses atau hilang sama sekali (Sadar et al., 2023).

3. Kendala Hukum dalam Penegakan Hukum terhadap Kejahatan Siber

Selain kendala teknis di atas, terdapat juga kendala berupa keterbatasan regulasi yang mengatur tindak pidana siber. UU ITE berperan sebagai dasar hukum utama untuk menangani kejahatan siber di Indonesia. Hukum ini dianggap belum sepenuhnya responsif terhadap kemajuan teknologi terkini seperti *blockchain, cryptocurrency*, dan kecerdasan buatan (AI) (Saputra et al., 2025). Akibatnya, banyak serangan siber tidak memiliki pengaturan yang jelas dalam regulasi yang berlaku, sehingga penegak hukum sering kali perlu menciptakan cara baru di luar regulasi yang ada. Selain itu, UU ITE tidak menjelaskan dengan rinci tentang prosedur teknis dalam menangani bukti elektronik. Hukum ini juga tidak menetapkan secara spesifik tentang norma pengumpulan, penyimpanan, serta penyelidikan bukti digital, yang dapat mengakibatkan bukti menjadi tidak valid atau susah dipakai di pengadilan (Wibowo et al., 2024).

Kendala hukum yang kedua yaitu, terdapat kesamaan antara KUHP 2023 dan UU ITE 2024 berkaitan dengan usaha menanggulangi kejahatan di dunia maya. Kesamaan dalam regulasi ini menyebabkan berbagai masalah operasional bagi aparat penegak hukum. Proses penyidikan mengalami kesusahan dalam menentukan landasan hukum yang tepat ketika memulai investigasi dan penyelidikan. Penegak hukum dihadapkan pada pilihan untuk menggunakan KUHP 2023 atau UU ITE 2024, keduanya memiliki prosedur dan ketentuan yang berbeda. Masalah juga timbul terkait pengumpulan dan penyajian bukti. KUHP 2023 menerapkan ketentuan umum mengenai alat bukti sebagaimana diatur dalam KUHAP, sedangkan UU ITE menetapkan ketentuan khusus mengenai bukti elektronik. Perbedaan dalam standar pembuktian ini dapat memengaruhi kualitas serta keabsahan proses peradilan (Ganjar, 2025).

Kejahatan siber umumnya melibatkan yang merugikan, pihak yang dirugikan, dan sistem yang tersebar di seluruh dunia, sehingga menimbulkan rintangan yang besar mengenai hukum terhadap penegak hukum di Indonesia. Masalah utama yang muncul adalah karena perbedaan aturan hukum di berbagai negara (Wibowo et al., 2024). Misalnya, di Indonesia, akses ke data secara ilegal dianggap melanggar hukum, tetapi di negara lain, hal tersebut mungkin tidak diatur sama sekali atau justru dianggap sah. Situasi ini menyebabkan investigator kesulitan dalam mendapatkan dukungan dari otoritas luar, karena lembaga penegak hukum di Indonesia tidak selalu memiliki wewenang atau akses hukum untuk melakukan pemblokiran, penyitaan data, atau menangkap pelaku di luar negeri (Yudhistira & Puspitosari, 2025). Ketidakadaan perjanjian kerjasama internasional yang memadai juga menjadi penghalang besar, sehingga kolaborasi lintas negara dalam mengumpulkan bukti, melacak identitas pelaku, serta membawa kasus ke pengadilan menjadi sangat kompleks dan memakan waktu.

Upaya atau Solusi Menangani Kejahatan Siber

Dalam mengatasi tantangan penegakan hukum terkait kejahatan siber di Indonesia, beberapa langkah yang bisa diambil untuk menangani masalah ini, antara lain:

Peningkatan sumber daya manusia dalam aspek keamanan siber mesti dijadikan fokus utama bangsa. Upaya ini bisa dilakukan melalui program pelatihan yang mendalam, pendidikan tinggi yang berorientasi pada teknologi informasi, dan sertifikasi profesional di sektor keamanan siber. Kerjasama antara institusi pendidikan, sektor industri, dan pemerintah sangatlah diperlukan untuk menghasilkan generasi ahli keamanan siber yang siap menghadapi ancaman di tingkat global (Syawaluddin et al., 2025). Upaya dalam peningkatan *cyber security* di Indonesia yaitu dengan cara meningkatkan pelatihan dan pemahaman sumber daya manusia (SDM), hal ini menjadi langkah penting dalam mengurangi risiko serangan siber.

Rendahnya tingkat kesiapan infrastruktur keamanan siber, baik pada sektor publik maupun privat, merupakan tantangan pokok dalam tata kelola keamanan digital di Indonesia (Dzaky & Edrisy, 2025). Sebagai respons, upaya strategis yang diperlukan meliputi peningkatan alokasi anggaran untuk pengembangan infrastruktur teknologi pendukung keamanan siber. Selain itu, pemerintah juga harus menjamin ketersediaan akses bagi aparat penegak hukum terhadap perangkat dan sistem teknologi mutakhir, guna memperkuat kapabilitas investigasi dan penindakan hukum atas berbagai modus kejahatan digital (Fahmi & Tambunan, 2024).

Selain itu, peningkatan pemahaman literasi di antara masyarakat dipandang sebagai solusi yang krusial. Dengan meningkatkan wawasan masyarakat mengenai kejahatan siber dan mengedukasi mereka tentang perilaku bertanggung jawab dalam dunia digital, diharapkan masyarakat dapat lebih waspada saat beraktivitas secara daring. Upaya ini dapat membantu menurunkan tingkat kerentanan masyarakat terhadap serangan siber serta meningkatkan kesadaran akan risiko yang mungkin muncul di ruang digital (Pamungkas et al., 2024).

Dalam proses penegakan hukum, penting adanya keselarasan antara berbagai peraturan hukum yang memiliki tingkat kesetaraan berbeda. Kesenjangan bisa terjadi antara undang-undang yang memiliki tingkat lebih tinggi dengan peraturan yang lebih rendah, serta antara undang-undang khusus dengan undang-undang umum. Hal-hal ini bisa menyebabkan masalah dalam penerapan hukum karena tujuan dari pembuatan peraturan adalah untuk memberikan rasa aman, manfaat, dan keadilan. Oleh karena itu, agar menghindari hal tersebut, harus diperhatikan asas dan tujuan dari setiap undang-undang itu sendiri (Januri et al., 2022).

Diperlukan tindakan nyata untuk menyelaraskan regulasi, termasuk strategi jangka panjang. Salah satu langkah strategis yang dapat ditempuh adalah menyusun dan memberlakukan suatu undang-undang pidana siber yang bersifat komprehensif, memuat segala aspek pengaturan dalam satu instrumen hukum yang utuh. Pendekatan penyatuan regulasi semacam ini telah diimplementasikan oleh berbagai yurisdiksi di dunia dan terbukti mampu memberikan dampak positif, terutama dalam membangun stabilitas kerangka hukum serta mendorong efisiensi proses penindakan terhadap tindak pidana di ruang siber. Penyusunan hukum ini dapat mengambil referensi dari praktik terbaik internasional, sambil tetap mempertimbangkan sifat-sifat khas dari sistem hukum di Indonesia (Ganjar, 2025).

Langkah yang sangat penting untuk mengatasi kejahatan siber adalah dengan melakukan perbaikan serta pembaruan pada ITE. Perubahan ini diharapkan dapat memperluas jangkauan regulasi dan menyesuaikan dengan kemajuan teknologi yang terus berkembang, sehingga kekurangan dalam hukum yang bisa dimanfaatkan oleh pelaku kejahatan siber bisa berkurang (Pamungkas et al., 2024).

Selain memperbaiki peraturan, kerja sama antar negara juga harus ditingkatkan agar bisa mengejar dan menindak pelaku kriminal yang beroperasi di luar wilayah hukum Indonesia. Cara untuk memperkuat kerja sama internasional adalah dengan meningkatkan kolaborasi dengan organisasi hukum internasional agar bisa bertukar informasi dan bekerja sama dalam penyelidikan serta penanganan ancaman kejahatan siber yang menyeberang batas negara (Fahmi & Tambunan, 2024). Selain itu, Indonesia juga diharapkan lebih terlibat dalam perjanjian atau konvensi yang terkait dengan penanganan ancaman siber. Dengan demikian, komunikasi dan koordinasi antar negara dalam menghadapi masalah ini bisa lebih lancar dan efektif (Febriawan & Marisa, 2024). Solusi terakhir dalam mengatasi kejahatan siber ialah kerjasama antara sektor publik, sektor swasta, dan masyarakat untuk

memperkuat keamanan siber. Sinergi ini sangat vital guna membangun lingkungan yang aman di dunia digital. Kerjasama ini bisa meliputi berbagai informasi mengenai ancaman dan praktik terbaik, serta merumuskan strategi bersama untuk menghadapi tantangan serangan siber (Novita et al., 2024).

KESIMPULAN

Implementasi hukum pidana untuk menghadapi kejahatan siber di Indonesia, menekankan pesatnya kemajuan teknologi informasi serta tantangan yang ada dalam penegakan hukum. Kasus kejahatan siber, seperti pencurian informasi dan penipuan daring, mengalami peningkatan drastis antara tahun 2019 dan 2022, yang mengakibatkan kerugian finansial yang terus meningkat. Aturan hukum yang relevan, termasuk UU ITE dan KUHP, telah diterapkan, tetapi terdapat masalah seperti minimnya tenaga ahli dan hambatan teknis yang mengganggu efektivitas penegakan hukum oleh kepolisian dan kejaksaan. Selanjutnya, berbagai penelitian menunjukkan tantangan sosial, budaya, dan regulasi yang harus diatasi melalui pengembangan sumber daya manusia, penyelarasan regulasi, serta kolaborasi internasional untuk memperkuat usaha melawan kejahatan siber di Indonesia.

DAFTAR PUSTAKA

Arisandy, Y. O. (2020). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1(3), 162-169.

Azis, M. A., Purwanda, S., Darwis, M., Kairuddin, K., & Tijjang, B. (2025). Tindak Pidana Judi Online Sebagai Kejahatan Siber: Analisis Normatif Terhadap Efektivitas Regulasi Di Indonesia. *Innovative: Journal of Social Science Research,* 5(4), 3912-3928.

Dinarti, N. S., Salsabila, S. R., & Herlambang, Y. T. (2024). Dilema Etika dan Moral dalam Era Digital: Pendekatan Aksiologi Teknologi terhadap Privasi Keamanan, dan Kejahatan Siber. *Daya Nasional: Jurnal Pendidikan Ilmu-Ilmu Sosial Dan Humaniora*, 2(1), 8-16.

Djabar, O., Ismail, D. E., & Mantali, A. R. Y. (2025). Cyber Phishing dan Penegakan Hukumnya: Peran Krusial Penyidik Menurut UU ITE. *RechtJiva*.

Dzaky, M. A. T., & Edrisy, I. F. (2025). Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital. *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora*, 4(2), 3614-3625.

Fahmi, M. H., & Tambunan, H. M. (2024). ANALISIS PERAN DAN EFEKTIVITAS HUKUM DALAM MELAWAN ANCAMAN CYBERCRIME DI INDONESIA. *JURNAL PANAH KEADILAN*, 3(2), 72- 80.

Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora,* 1(6), 8-20.

Febriawan, D., & Marisa, H. (2024). Understanding Indonesia's Cyber Security Policies: Opportunities and Challenges In The Digitalization Transformation Era. *JOELS: Journal of Election and Leadership*, 5(1), 13-21.

Ganjar, S.D. (2025). Urgensi Pembaruan Hukum Pidana dalam Menanggulangi Kejahatan Siber: Tinjauan Kritis Terhadap Kesesuaian KUHP Nasional dan Perubahan UU ITE. *Lucos Journal of Academic Literature Review*, 4(3), 197-208.

Januri, J., Melati, D. P., & Muhadi, M. (2022). Upaya kepolisian dalam penanggulangan kejahatan cyber terorganisir. *Audi Et AP: Jurnal Penelitian Hukum*, 1(02), 94-100.

Judijanto, L. (2025). Hukum Pidana dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital di Era Teknologi. *Indonesian Research Journal on Education*, 5(1), 968-972.

Kasim, Z. (2023). Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia. *Indragiri Law Review*, 2(1).

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum dan HAM Wara Sains,* 2(6), 517-525.

Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana di Indonesia. *Jurnal Tana Mana*, 6(2), 289-296.

Ningrum, D. P. S., & Robekha, J. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora*, 2(4), 765-776.

Novita, D., Mulyono, M., & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. *Innovative: Journal Of Social Science Research,* 4(6), 1179-1186.

Pamungkas, A. T., Muliyono, A., & Lahangatubun, N. (2024). Tracing Legal Regulations in Dealing with Cybercrime in Indonesia: Examining Obstacles and Solutions.

Prianto, Y., Fuzain, N. A., & Farhan, A. (2021). Kendala Penegakan Hukum Terhadap Cyber Crime Pada Masa Pandemi Covid-19. *Prosiding SENAPENMAS,* 1111-1118.

Rahmiati, R., Latukau, F., & Nadila, G. (2025). Kejahatan Seksual Berbasis Digital: Tantangan Penegakan Hukum di Era Media Sosial. *Jurnal Hukum Legalita*, 7(1), 10-17.

Sadar, A., Oner, B., & Almusawir, A. (2023). PELAKSANAA PENEGAKAN HUKUM TINDAK PIDANA CYBER CRIME TERHADAP PELAKU KEJAHATAN INFORMASI DATA PRIBADI. *Clavia,* 21(3), 382-390.

Sariani, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil: Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(2).

Saputra, A., Kristiawanto, K., & Ismed, M. (2024). Rekonstruksi Penegakan Hukum Tindak Pidana Siber di Indonesia. *SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum*, 3(1), 63-70.

Saputra, I. R., Sapada, R. R. A., Dzulqarnain, A., & Suprapto, S. (2025). Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber dan Tantangan Penegakan Hukum Pidana. *Jurnal Litigasi Amsir*, 12(3), 255-261.

Siagian, A., & Alexander, D. (2025). PENERAPAN HUKUM PIDANA TERHADAP PELAKU TINDAK PIDANA SIBER DI INDONESIA: ANALISIS PUTUSAN PENGADILAN. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, 4(9), 2641-2656.

Siregar, L. Y., & Nasution, M. I. P. (2020). Perkembangan teknologi informasi terhadap peningkatan bisnis online. *HIRARKI: Jurnal Ilmiah Manajemen Dan Bisnis*, 2(1), 71-75.

Sitanggang, A. S., Darmawan, F., & Manurung, D. S. (2024). Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber. *Jurnal Pendidikan Dan Teknologi Indonesia,* 4(3), 79-83.

Sitorus, R., Saragih, J. Z. F., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. *Locus: Jurnal Konsep Ilmu Hukum*, 5(1), 53-61.

Syawaluddin, A. S. (2025). CYBER SECURITY DAN KETAHANAN NASIONAL: TANTANGAN DAN SOLUSI DI ERA DIGITAL. *Jurnal Media Akademik (JMA),* 3(6).

Umami, S. H., & Fithry, A. (2023). Mekanisme Penyidikan Dan Penuntutan Tindak Pidana Cybercrime: Tinjauan Hukum Indonesia. *Prosiding SNAPP: Sosial Humaniora, Pertanian, Kesehatan dan Teknologi,* 2(1), 114-120.

Warouw, A.S. (2025). Peran Hukum Pidana dalam Perlindungan Data Pribadi dan Pencegahan Kejahataan Siber di Indonesia. *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*, 2(6), 65-71.

Wibowo, M. S. I., & Munawar, A. (2024). Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia. *Jurnal Hukum Lex Generalis*, 5(7).

Yudhistira, F. A., & Puspitosari, H. (2025). Penegakan Hukum terhadap Pelaku Pembuat Dapat Diaksesnya Website Bermuatan Asusila dan Pornografi Anak. *Jurnal Hukum Lex Generalis*, 6(7).