Sanskara Hukum dan HAM
Vol. 3, No. 3, April 2025, hal. 118-124
ISSN: 2985-7775, DOI: 10.58812/shh.v3.i03

Regulasi Keamanan Siber dan Penegakan Hukum terhadap *Cybercrime* di Indonesia

Loso Judijanto[1], Budi Nugroho[2]
[1] IPOSS Jakarta, losojudijantobumn@gmail.com
[2] Politeknik Tunas Pemuda Tangerang, nbudi2406@gmail.com

Info Artikel

Article history:

Received Apr, 2025
Revised Apr, 2025
Accepted Apr, 2025

Kata Kunci:

Indonesia; Keamanan Siber; Kejahatan Siber; Penegakan Hukum

Keywords:

Cyber Crime; Cyber Security; Indonesia; Law Enforcement

ABSTRAK

Penelitian ini mengkaji peraturan keamanan siber dan mekanisme penegakan hukum di Indonesia dalam menangani kejahatan siber dengan menggunakan pendekatan yuridis normatif. Analisis ini menunjukkan adanya kemajuan yang signifikan, termasuk pemberlakuan Undang-undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-undang Perlindungan Data Pribadi (UU PDP). Namun, masih ada kesenjangan dalam menangani ancaman yang muncul, ambiguitas dalam ketentuan hukum, dan inefisiensi penegakan hukum karena sumber daya yang terbatas dan masalah koordinasi. Perbandingan dengan kerangka kerja internasional, seperti Konvensi Budapest dan inisiatif keamanan siber ASEAN, menyoroti bidang-bidang yang perlu ditingkatkan. Rekomendasi yang diberikan mencakup reformasi hukum, peningkatan kapasitas, kolaborasi internasional, dan peningkatan kemitraan publik-swasta untuk memperkuat ekosistem keamanan siber Indonesia dan memerangi lanskap ancaman siber yang terus berkembang.

ABSTRACT

This research examines Indonesia's cybersecurity regulations and law enforcement mechanisms in dealing with cybercrime using a normative juridical approach. The analysis shows significant progress, including the enactment of the Electronic Information and Transaction Law (ITE Law) and the Personal Data Protection Law (PDP Law). However, there are still gaps in addressing emerging threats, ambiguities in legal provisions, and inefficiencies in law enforcement due to limited resources and coordination issues. Comparisons with international frameworks, such as the Budapest Convention and ASEAN cybersecurity initiatives, highlight areas for improvement. Recommendations include legal reforms, capacity building, international collaboration, and enhanced public-private partnerships to strengthen Indonesia's cybersecurity ecosystem and combat the evolving cyber threat landscape.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta
Email: losojudijantobumn@gmail.com

1. PENDAHULUAN

Kemajuan teknologi yang pesat dan meningkatnya ketergantungan pada internet telah membawa kenyamanan dan efisiensi yang belum pernah terjadi sebelumnya ke berbagai sektor di Indonesia. Namun, transformasi digital ini juga membawa tantangan yang kompleks, terutama dalam bentuk kejahatan siber, yang meliputi peretasan, *phishing*, penipuan *online*, dan pembobolan data, yang menimbulkan ancaman signifikan bagi individu, bisnis, dan lembaga pemerintah, dengan dampak ekonomi dan sosial yang substansial (Putri et al., 2024; Syalendro et al., 2024). Meskipun telah memiliki kerangka hukum, seperti Undang-undang Informasi dan Transaksi Elektronik (ITE) yang telah diamandemen pada tahun 2016, dan dukungan dari Kitab Undang-undang Hukum Pidana (KUHP), masih terdapat tantangan dalam penegakan hukum, termasuk penerapan teknologi forensik digital dan perlunya kerja sama internasional yang lebih kuat (Fitri et al., 2024; Syalendro et al., 2024). Ancaman siber yang umum terjadi seperti serangan *malware*, *denial of service* (DoS), *distributed denial of service* (DDoS), dan *phishing*, terutama di sektor perbankan dengan banyaknya insiden penipuan dan penggunaan kartu kredit yang tidak sah, semakin menggarisbawahi urgensi untuk mengatasi masalah ini (Hapsari & Pambayun, 2023; Putri et al., 2024). Langkah-langkah pencegahan seperti memperkuat infrastruktur keamanan, mempromosikan literasi digital, dan mendorong kolaborasi internasional ditekankan oleh regulator dan pelaku usaha, di samping upaya pemerintah dan BSSN untuk membangun mekanisme pertahanan yang kuat dalam melindungi aset digital (Fahlevi et al., 2019; Fitri et al., 2024). Selain itu, kurangnya kesadaran dan pendidikan publik tentang keamanan siber memperburuk ancaman, sehingga perlu adanya peningkatan kampanye pendidikan publik untuk memberdayakan individu dalam menghadapi ancaman daring (Hapsari & Pambayun, 2023).

Menanggapi tantangan yang ditimbulkan oleh kejahatan siber, Indonesia telah menerapkan serangkaian peraturan keamanan siber dan mekanisme penegakan hukum yang mapan, dengan Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi kerangka kerja legislatif utama untuk memerangi kejahatan siber. Namun, penegakan hukum ini menghadapi banyak tantangan, termasuk keterbatasan teknis, kurangnya keahlian khusus, konflik yurisdiksi, dan kesenjangan dalam ketentuan hukum, yang menghambat penerapannya secara efektif dan membutuhkan perbaikan berkelanjutan untuk mengimbangi kemajuan teknologi dan sifat ancaman siber yang terus berkembang (Mahrina et al., 2022; Syalendro et al., 2024). Keterbatasan teknis utama, seperti penggunaan teknologi forensik digital yang tidak memadai, dan kurangnya keahlian khusus di antara petugas penegak hukum, berdampak pada kemampuan untuk menyelidiki kejahatan siber yang kompleks secara efektif (Mahrina et al., 2022). Selain itu, konflik yurisdiksi muncul karena sifat kejahatan siber yang lintas batas, sehingga mempersulit penegakan hukum dan menyoroti perlunya kerja sama internasional dan harmonisasi peraturan (Erikha & Saptomo, 2024). Meskipun UU ITE menyediakan kerangka hukum yang komprehensif, UU ini mengandung ambiguitas dan ketentuan yang sudah ketinggalan zaman sehingga tidak dapat sepenuhnya mengatasi ancaman siber modern, seperti yang ditimbulkan oleh kecerdasan buatan dan teknologi *blockchain* (Erikha & Saptomo, 2024). Selain itu, kurangnya infrastruktur siber yang memadai dan rendahnya literasi digital masyarakat semakin menghambat penegakan hukum keamanan siber, karena individu dan organisasi mungkin tidak melakukan tindakan pencegahan yang diperlukan untuk melindungi diri mereka sendiri dari ancaman siber (Mahrina et al., 2022; Syalendro et al., 2024).

Penelitian ini bertujuan untuk menganalisis efektivitas peraturan keamanan siber dan praktik penegakan hukum di Indonesia dalam menangani kejahatan siber melalui pendekatan yuridis normatif. Penelitian ini berupaya mengidentifikasi kekuatan dan kelemahan kerangka hukum yang ada dan mengeksplorasi tantangan operasional yang dihadapi oleh lembaga penegak hukum di ranah digital. Penelitian ini juga mengkaji kesesuaian kebijakan keamanan siber Indonesia dengan standar internasional, dengan menekankan perlunya strategi yang komprehensif dan kolaboratif.

2. TINJAUAN PUSTAKA

2.1 Kejahatan dunia maya: Definisi dan Implikasi

Kejahatan siber, sebagaimana didefinisikan oleh Brenner (2010), melibatkan pelanggaran yang menargetkan sistem komputer atau menggunakannya untuk melakukan kejahatan, dengan sifat digitalnya yang mempersulit penegakan hukum lintas batas. Masalah global ini, dengan biaya melebihi $1 triliun per tahun, memengaruhi individu, bisnis, dan pemerintah, dan sangat menantang di negara-negara berkembang seperti Indonesia karena terbatasnya kesadaran, sumber daya teknis, dan kerangka kerja hukum yang terpecah-pecah (AllahRakha, 2024). Kejahatan siber menyebabkan kerugian ekonomi yang signifikan, kerusakan reputasi, dan gangguan operasional, terutama dengan kegiatan seperti peretasan dan penipuan, yang sulit diatasi oleh penegak hukum karena keterbatasan teknis dan kurangnya pelaporan (Bregant & Bregant, 2014). Sifat kejahatan siber yang lintas batas membutuhkan kerja sama internasional dan langkah-langkah keamanan siber yang kuat (AllahRakha, 2024), sementara negara-negara berkembang menghadapi tantangan tambahan dari kesadaran yang terbatas dan kerangka kerja hukum yang lemah (Pandey & Kapoor, 2025). Kemajuan teknologi dalam keamanan siber, seperti AI dan pembelajaran mesin, di samping inisiatif pendidikan untuk meningkatkan literasi digital, sangat penting untuk memitigasi ancaman siber (Pandey & Kapoor, 2025). Terlepas dari upaya untuk menerapkan Undang-undang dan tindakan pencegahan, menghilangkan semua celah teknis tetap tidak mungkin dilakukan, menggarisbawahi perlunya peningkatan berkelanjutan dalam praktik keamanan siber (Maheswari, 2015).

2.2 Peraturan Keamanan Siber: Perspektif Global

Pendekatan global untuk memerangi kejahatan siber melibatkan kerangka kerja hukum, kemampuan teknis, dan kerja sama internasional. Elemen-elemen utama termasuk Peraturan Perlindungan Data Umum (GDPR) Uni Eropa dan Konvensi Budapest Dewan Eropa, yang menyelaraskan definisi dan penegakan hukum, yang menekankan respons hukum terpadu terhadap sifat ancaman digital yang tidak mengenal batas (Archick & Foreign Affairs and Trade Division, 2005) (Buçaj & Idrizaj, 2025). Efektivitas kerangka kerja ini bergantung pada kemampuan beradaptasi terhadap ancaman yang terus berkembang dan keseimbangan antara keamanan dan hak-hak individu. Meskipun Konvensi Budapest memainkan peran penting dalam kolaborasi internasional, dampaknya terbatas tanpa partisipasi dari negara-negara di mana penjahat siber beroperasi secara bebas (Archick & Foreign Affairs and Trade Division, 2005). Para kritikus juga mencatat bahwa peraturan yang terlalu ketat, seperti yang diungkapkan oleh Perry dkk. (2018), dapat menghambat inovasi dan melanggar privasi, sehingga menyoroti perlunya pendekatan yang seimbang (AllahRakha, 2024)Respons hukum global yang terpadu sangat penting, yang membutuhkan kerja sama yang lebih baik antara sektor publik dan swasta serta standar pembagian data yang etis untuk investigasi kejahatan siber yang efektif (Buçaj & Idrizaj, 2025). ("Kejahatan siber dan ancaman keamanan global: tantangan dalam hukum internasional", 2023).

2.3 Kerangka Kerja Keamanan Siber Indonesia

Undang-undang Informasi dan Transaksi Elektronik (UU ITE), yang disahkan pada tahun 2008 dan diamandemen pada tahun 2016, berfungsi sebagai kerangka kerja utama Indonesia untuk memerangi kejahatan siber, menangani pelanggaran seperti pencemaran nama baik, ujaran kebencian, dan penipuan elektronik. Namun, efektivitasnya terhambat oleh ambiguitas dalam pasal-pasal terkait pencemaran nama baik dan ujaran kebencian, yang menurut para kritikus digunakan untuk menekan perbedaan pendapat dan kebebasan berpendapat (Djarawula et al., 2023; Sidik, 2013). Celah hukum di bidang-bidang seperti *cyberporn*, perjudian daring, dan misinformasi semakin mempersulit penegakan hukum, yang menyebabkan penerapan yang tidak konsisten oleh penegak hukum (Djarawula et al., 2023). Keahlian teknis yang terbatas, kemampuan forensik digital yang tidak memadai, dan

infrastruktur yang tidak memadai memperparah tantangan penegakan hukum (Mahrina et al., 2022; Syalendro et al., 2024). Selain itu, koordinasi antar lembaga yang buruk dan rendahnya literasi digital masyarakat menghambat implementasi Undang-undang tersebut, sehingga menggarisbawahi perlunya peningkatan koordinasi dan kampanye kesadaran untuk meningkatkan efektivitasnya (Syalendro et al., 2024).

2.4 Penegakan Hukum dan Tantangan Operasional

Lembaga penegak hukum Indonesia menghadapi tantangan besar dalam memerangi kejahatan siber, termasuk pelatihan khusus yang tidak memadai, alat teknologi yang ketinggalan zaman, dan keterbatasan sumber daya. Kesulitan-kesulitan ini diperparah oleh konflik yurisdiksi dan sifat transnasional kejahatan siber, yang semakin diperparah dengan terbatasnya partisipasi Indonesia dalam kerangka kerja internasional seperti Konvensi Budapest (Bawono, 2019; Laksito et al., 2024; Putra, 2023). Kurangnya sumber daya manusia dan fasilitas canggih menghambat penanganan ancaman siber yang canggih, sementara yurisdiksi nasional Indonesia membatasi kemampuannya untuk menangani pelanggaran lintas batas (Laksito et al., 2024; Putra, 2023). Untuk meningkatkan respons terhadap kejahatan siber di Indonesia, diperlukan penyelarasan peraturan dengan standar internasional, meningkatkan kerja sama lintas batas, dan membangun kapasitas penegakan hukum melalui pelatihan khusus dan perangkat forensik digital yang canggih (Kasim, 2024; Putra, 2023). Selain itu, memperkuat literasi dan kesadaran digital masyarakat sangat penting untuk mengurangi kerentanan dan menumbuhkan ketahanan masyarakat (Kasim, 2024; Syalendro et al., 2024).

2.5 Kesenjangan dan Peluang Penelitian

Meskipun literatur yang ada saat ini secara ekstensif mengeksplorasi aspek regulasi dan penegakan keamanan siber, masih ada kesenjangan dalam memahami hubungan antara kerangka hukum, penegakan operasional, dan kolaborasi internasional di Indonesia. Selain itu, penelitian empiris mengenai efektivitas reformasi kebijakan baru-baru ini, seperti Undang-undang Perlindungan Data Pribadi, masih terbatas dalam menangani ancaman siber kontemporer.

Penelitian ini bertujuan untuk menjembatani kesenjangan tersebut dengan menganalisis secara kritis peraturan keamanan siber Indonesia dan mekanisme penegakan hukum dalam kerangka yuridis normatif. Temuan-temuan yang dihasilkan diharapkan dapat memberikan wawasan yang dapat ditindaklanjuti untuk meningkatkan pendekatan negara terhadap kejahatan siber sekaligus menyelaraskan kebijakannya dengan standar internasional.

3. METODE PENELITIAN

Penelitian ini menggunakan metodologi kualitatif, dengan fokus pada analisis bahan hukum primer dan sekunder. Sumber-sumber primer mencakup Undang-undang dan peraturan di Indonesia seperti Undang-undang Informasi dan Transaksi Elektronik (UU ITE), Undang-undang Perlindungan Data Pribadi, dan peraturan pemerintah terkait. Materi sekunder meliputi jurnal akademis, komentar hukum, laporan, dan studi kasus yang memberikan wawasan kontekstual dan kritis terhadap implementasi dan penegakan hukum keamanan siber di Indonesia. Metode pengumpulan data mencakup tinjauan dokumen atas teks legislatif, laporan pemerintah, dan konvensi internasional untuk menggambarkan ruang lingkup dan implikasi kerangka kerja keamanan siber Indonesia; tinjauan literatur atas karya-karya ilmiah untuk memahami dasar-dasar teoretis; dan studi kasus tentang insiden kejahatan siber serta respons penegak hukum untuk mengevaluasi penerapan praktis ketentuan hukum.

Analisis ini menggunakan analisis konten kualitatif untuk mengungkap pola, kesenjangan, dan ketidakkonsistenan dalam kerangka kerja dan penegakan hukum keamanan siber di Indonesia. Hal ini melibatkan analisis hukum untuk memeriksa koherensi dan cakupan hukum, termasuk tumpang tindih atau ambiguitas; analisis komparatif untuk membandingkan praktik-praktik di

Indonesia dengan standar internasional seperti Konvensi Budapest dan inisiatif keamanan siber ASEAN; dan evaluasi kasus untuk menilai efektivitas mekanisme penegakan hukum, proses peradilan, dan koordinasi antar lembaga dalam menangani kejahatan siber. Langkah-langkah ini bertujuan untuk memberikan pemahaman yang komprehensif tentang kekuatan dan kelemahan dalam pendekatan Indonesia terhadap tata kelola keamanan siber.

4. HASIL DAN PEMBAHASAN

4.1 Analisis Kerangka Hukum

Peraturan keamanan siber Indonesia, yang tertuang dalam Undang-undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-undang Perlindungan Data Pribadi (UU PDP), menjadi landasan hukum untuk menangani kejahatan siber. UU ITE menetapkan ketentuan yang jelas untuk menangani pelanggaran seperti penipuan elektronik, pencemaran nama baik, dan peretasan, sementara UU PDP meningkatkan perlindungan data dengan membebankan kewajiban kepada penangan data dan memperkenalkan hukuman atas pelanggaran, yang selaras dengan tren regulasi privasi global. Peraturan pendukung, seperti Peraturan Presiden No. 53 Tahun 2017, semakin memperkuat tata kelola keamanan siber dengan membentuk Badan Siber dan Sandi Negara (BSSN) untuk mengoordinasikan upaya lintas sektor.

Terlepas dari kekuatan-kekuatan ini, masih ada kelemahan yang signifikan. UU ITE sering dikritik karena ketentuannya yang luas dan ambigu, yang dapat menyebabkan interpretasi yang tidak konsisten dan potensi penyalahgunaan, terutama dalam kasus-kasus pencemaran nama baik dan kebebasan berekspresi. Selain itu, masih ada kesenjangan dalam menangani ancaman yang canggih dan terus berkembang, seperti *ransomware* dan ancaman persisten tingkat lanjut (APT), yang membutuhkan pembaruan legislatif yang lebih komprehensif. Penegakan hukum semakin terhambat oleh tumpang tindihnya tanggung jawab dan fragmentasi di antara badan-badan pengatur, yang mengakibatkan inefisiensi dan kurangnya tindakan yang terkoordinasi.

4.2 Tantangan Penegakan Hukum

Penegakan hukum memainkan peran penting dalam mengimplementasikan peraturan untuk memerangi kejahatan siber, tetapi efektivitasnya terhalang oleh tantangan yang signifikan. Sumber daya dan keahlian yang terbatas dalam lembaga penegak hukum sering kali membatasi kemampuan mereka untuk menyelidiki dan menuntut kejahatan siber yang kompleks secara efektif. Sifat transnasional dari kejahatan siber semakin memperumit penegakan hukum, karena para pelaku sering beroperasi melintasi batas negara, mengeksploitasi keterbatasan yurisdiksi. Keterlibatan Indonesia yang minim dalam kerangka kerja internasional seperti Konvensi Budapest membatasi kemampuannya untuk berkolaborasi dalam investigasi lintas batas. Selain itu, lemahnya koordinasi antar lembaga seperti Polri dan Badan Siber dan Sandi Negara (BSSN) mengakibatkan penundaan dan duplikasi upaya.

Terlepas dari tantangan-tantangan ini, beberapa inisiatif telah menunjukkan potensi untuk meningkatkan penegakan hukum. Unit kejahatan siber khusus di dalam Polri telah dibentuk untuk meningkatkan kemampuan investigasi. Selain itu, kemitraan dengan perusahaan keamanan siber swasta memberikan akses ke alat dan keahlian canggih, yang berkontribusi pada respons yang lebih efektif terhadap ancaman siber. Langkah-langkah ini merupakan langkah maju dalam mengatasi kompleksitas penegakan kejahatan siber di Indonesia.

4.3 Analisis Perbandingan dengan Standar Internasional

Kerangka kerja keamanan siber Indonesia menunjukkan kemajuan, tetapi menunjukkan ketidaksesuaian yang signifikan dengan praktik-praktik terbaik global, yang membutuhkan penyempurnaan lebih lanjut untuk meningkatkan efektivitasnya. Sebagai negara yang tidak menandatangani Konvensi Budapest, Indonesia tidak memiliki akses

terhadap kerangka kerja yang komprehensif untuk kerja sama internasional dan dukungan teknis, yang sangat penting untuk menangani kejahatan siber lintas batas secara efektif (Laksito et al., 2024). Meskipun Indonesia berpartisipasi dalam program keamanan siber ASEAN, seperti Strategi Kerja Sama Keamanan Siber ASEAN, integrasi penuh pedoman regional ini ke dalam kebijakan domestiknya masih belum lengkap, sehingga membatasi dampaknya (Nugroho & Chandrawulan, 2022). Undang-undang Perlindungan Data Pribadi (PDP) sebagian sejalan dengan GDPR Uni Eropa, tetapi tidak cukup untuk memastikan independensi otoritas perlindungan data dan cakupan hak-hak individu (Qudus, 2025)Kesenjangan ini menyoroti perlunya mengadopsi prinsip-prinsip privasi sesuai desain, meningkatkan harmonisasi peraturan, dan memperkuat kapasitas penegakan hukum untuk mengatasi tantangan kejahatan siber global secara efektif (Qudus, 2025). Rekomendasi yang diberikan termasuk menyelaraskan peraturan Indonesia dengan standar internasional dan membentuk unit khusus dalam penegakan hukum untuk manajemen kejahatan siber lintas batas yang lebih baik (Laksito et al., 2024).

4.4 Evaluasi Studi Kasus

Analisis terhadap kasus-kasus kejahatan siber yang terkenal di Indonesia mengungkapkan wawasan praktis tentang tantangan dan area untuk perbaikan dalam memerangi ancaman siber. Penipuan *online* dan penipuan *e-commerce* menekankan pentingnya kesadaran masyarakat dan tindakan pencegahan, karena penegak hukum sering kali baru turun tangan setelah insiden terjadi karena keterbatasan sumber daya. Sementara itu, pelanggaran data profil tinggi, termasuk yang melibatkan lembaga pemerintah, menyoroti kerentanan yang signifikan dalam keamanan siber institusional dan perlunya pemantauan kepatuhan yang lebih ketat. Kasus-kasus ini menggarisbawahi perlunya mengatasi masalah sistemik dengan meningkatkan mekanisme pelaporan, merampingkan proses peradilan, dan meningkatkan pelatihan teknis bagi para penyelidik untuk memperkuat pertahanan keamanan siber negara.

4.5 Rekomendasi untuk Perbaikan

Berdasarkan temuan-temuan tersebut, beberapa rekomendasi diusulkan untuk memperkuat kerangka kerja keamanan siber Indonesia. Pertama, ketentuan hukum seperti UU ITE harus diamandemen untuk mengatasi ambiguitas dan memperluas cakupan terhadap ancaman siber yang muncul. Kedua, meningkatkan kapasitas penegakan hukum melalui program pelatihan yang ditargetkan, alat forensik yang canggih, dan peningkatan koordinasi antar-lembaga sangat penting untuk efektivitas operasional. Ketiga, mempromosikan kolaborasi internasional dengan menandatangani dan mengadopsi kerangka kerja seperti Konvensi Budapest yang dapat memfasilitasi investigasi lintas batas dan pertukaran praktik terbaik. Keempat, meningkatkan kesadaran publik melalui kampanye nasional dapat mengedukasi masyarakat dan pelaku usaha tentang ancaman siber dan langkah-langkah pencegahan. Terakhir, meningkatkan kemitraan publik-swasta dapat mendorong kolaborasi dengan para ahli dari sektor swasta untuk mengembangkan solusi inovatif dan berbagi sumber daya untuk memerangi kejahatan siber secara efektif.

5. KESIMPULAN

Indonesia telah membuat kemajuan penting dalam membangun kerangka hukum untuk memerangi kejahatan siber melalui pemberlakuan UU ITE, UU PDP, dan pembentukan mekanisme kelembagaan seperti Badan Siber dan Sandi Negara (BSSN). Terlepas dari kemajuan-kemajuan ini, tantangan seperti ambiguitas legislatif, sumber daya penegakan hukum yang terbatas, dan koordinasi antar-lembaga yang lemah masih ada. Mengingat sifat global dari kejahatan siber, penyelarasan yang lebih besar dengan standar internasional dan peningkatan kolaborasi lintas batas menjadi sangat penting. Untuk memperkuat ekosistem keamanan sibernya, Indonesia harus fokus pada amandemen ketentuan hukum untuk mengatasi ancaman yang muncul, melengkapi penegak hukum dengan alat dan pelatihan canggih, dan meningkatkan kerja sama antar lembaga. Selain itu,

menandatangani kerangka kerja internasional seperti Konvensi Budapest dan membina kemitraan dengan entitas swasta dan organisasi regional sangat penting untuk membangun ketahanan. Dengan mengatasi tantangan-tantangan ini secara komprehensif, Indonesia dapat melindungi ekonomi digitalnya, melindungi data pribadi, dan mempertahankan kepercayaan publik di era transformasi digital.

DAFTAR PUSTAKA

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure, Policy and Development*, *8*(10).

Archick, K., & Foreign Affairs and Trade Division, D. (2005). *Cybercrime: The council of Europe convention*.

Bawono, B. T. (2019). Reformation of Law Enforcement of Cyber Crime in Indonesia. *Jurnal Pembaharuan Hukum*, *6*(3), 332–349.

Bregant, J., & Bregant, R. (2014). Cybercrime and computer crime. *The Encyclopedia of Criminology and Criminal Justice*, 1–5.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024.

Djarawula, M., Alfiani, N., & Mayasari, H. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah*, *2*(10), 3799–3806.

Erikha, A., & Saptomo, A. (2024). Dilemma of Legal Policy to Address Cybercrime in the Digital Era. *Asian Journal of Social and Humanities*, *3*(3), 499–507.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime business digital in Indonesia. *E3S Web of Conferences*, *125*, 21001.

Fitri, D., Soesanto, E., & Winny, W. (2024). Implementasi Nilai-Nilai Kebangsaan yang Bersumber UUD 1945 dan NKRI dalam Mengacu Peran Manajemen Sekuriti Menunjang Keamanan Data Nasabah di Era Digital pada PT Bank Rakyat Indonesia. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, *2*(2), 84–105.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, *5*(1), 1–17.

Kasim, Z. (2024). Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia. *Indragiri Law Review*, *2*(1), 18–24.

Laksito, J., Idris, M. F., & Waryanto, A. (2024). Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 774–790.

Maheswari, K. (2015). Global aspects of cyber crime. *Indian Social Science Journal*, *4*(1), 41.

Mahrina, M., Sasmito, J., & Zonyfar, C. (2022). The electronic and transactions law (EIT law) as the first cybercrime law in Indonesia: an introduction and its implementation. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *21*(2).

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, 1.

Pandey, P., & Kapoor, A. (2025). Cybercrime In The Digital Era: Impacts, Awareness, And Strategic Solutions For A Secure Future. *Sachetas*, *4*(1), 32–37.

Putra, J. S. A. A. M. (2023). hacking as a challenge for change and the development of cyber law in Indonesia. *Jurnal Ilmu Hukum Tambun Bungai*, *8*(2), 344–355.

Putri, K. D. E., Latbin, M. W., & Bunga, G. A. (2024). Phenomenom Cyber Crime in Indonesia in the Digitalization Era. *Journal of Digital Law and Policy*, *3*(2), 99–109.

Qudus, L. (2025). *Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges*.

Sidik, S. (2013). Dampak Undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat. *Jurnal Ilmiah Widya*, *1*(1), 1–7.

Syalendro, O., Lubis, A. F., & Putra, R. Y. A. E. (2024). Cyber Crime Crimes in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases. *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia*, *4*(1), 335–347.