



INNOVATIVE: Journal Of Social Science Research

Volume 4 Nomor 6 Tahun 2024 Page 1179-1186

E-ISSN 2807-4238 and P-ISSN 2807-4246

Website: <https://j-innovative.org/index.php/Innovative>

Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional

Dyah Novita^{1✉}, Mulyono², Anis Retnowati³

Sekolah Tinggi Hukum Militer

Email: Dynov98@gmail.com^{1✉}

Abstrak

Tujuan dari penelitian ini adalah untuk menganalisis perkembangan hukum siber di Indonesia dalam konteks tantangan yang dihadapi akibat kemajuan teknologi informasi, serta untuk mengeksplorasi solusi yang dapat diimplementasikan untuk meningkatkan keamanan nasional. Penelitian ini menggunakan metode studi kepustakaan, yang menyajikan ringkasan penelitian terkait topik tertentu untuk menunjukkan pengetahuan yang sudah ada dan area yang perlu dieksplorasi lebih lanjut. Metode ini juga dapat menginspirasi ide penelitian baru. Sumber untuk studi literatur dapat berasal dari berbagai referensi, termasuk jurnal, buku, dokumentasi, internet, dan pustaka. Penelitian ini menganalisis perkembangan hukum siber di Indonesia dan tantangan terkait keamanan nasional di era digital. Meskipun hukum siber di Indonesia telah menunjukkan kemajuan, peraturan yang ada masih belum terintegrasi dengan baik, menyebabkan kerentanan terhadap kejahatan siber seperti peretasan dan penipuan online. Beberapa isu utama yang ditemukan antara lain ketidakjelasan definisi kejahatan siber, rendahnya kesadaran masyarakat terhadap risiko siber, dan kurangnya kolaborasi antara sektor publik, swasta, dan masyarakat sipil. Untuk mengatasi masalah ini, penelitian menyarankan pembaruan regulasi yang responsif, peningkatan edukasi keamanan siber, serta kolaborasi antar sektor untuk menciptakan sistem hukum siber yang lebih efektif dan melindungi keamanan nasional.

Kata Kunci: *Hukum Siber, Keamanan Nasional, Kejahatan Siber, Edukasi Keamanan*

Abstract

The aim of this research is to analyze the development of cyber law in Indonesia in the context of the challenges faced due to advances in information technology, as well as to explore solutions that can be implemented to improve national security. This research uses a literature study method, which presents a summary of research related to a particular topic to show existing knowledge and areas that need further exploration. This method can also inspire new research ideas. Sources for literature studies can come from various references, including journals, books, documentation, the internet, and libraries. This research analyzes the development of cyber law in Indonesia and challenges related to national security in the digital era. Although cyber law in Indonesia has shown progress, existing regulations are still not well integrated, causing vulnerability to cyber crimes such as hacking and online fraud. Some of the main issues found include unclear definitions of cyber crime, low public awareness of cyber risks, and a lack of collaboration between the public, private and civil society sectors. To overcome this problem, research suggests responsive regulatory updates, increased cyber security education, and collaboration between sectors to create a more effective cyber legal system and protect national security.

Keywords: *Cyber Law, National Security, Cyber Crime, Security Education*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah secara mendalam mengubah berbagai aspek kehidupan di Indonesia, menciptakan peluang sekaligus tantangan baru, terutama dalam bidang hukum siber (Himawan, 2022);(Fauzi, 2023). Dengan semakin meluasnya penggunaan internet dan platform digital, isu-isu terkait keamanan siber, seperti serangan digital, penyebaran informasi palsu, dan pelanggaran privasi, menjadi semakin krusial bagi stabilitas sosial dan politik negara (Gani, 2023). Oleh karena itu, pemahaman yang mendalam tentang perkembangan hukum siber, termasuk tantangan yang dihadapi dan solusi yang mungkin diterapkan, sangat penting untuk menjaga keamanan nasional dan mendorong pertumbuhan yang berkelanjutan di era digital ini.

Saat ini, telah muncul rezim hukum baru yang dikenal sebagai Hukum Siber, yang mencakup berbagai aspek hukum terkait pemanfaatan teknologi informasi. Istilah ini, yang juga dikenal sebagai Hukum Teknologi Informasi atau Hukum Dunia Maya, mencerminkan kompleksitas interaksi yang terjadi di dunia virtual (Akmal & Royal, 2019);(Setiawan, 2021). Hukum siber menghadapi tantangan unik, terutama dalam pembuktian masalah yang berhubungan dengan hal-hal yang tidak tampak dan bersifat semu, mengingat aktivitas di internet sering kali melibatkan elemen yang sulit ditangkap secara fisik (Maskun, 2022). Pemahaman yang mendalam tentang Hukum Siber penting untuk mengatasi persoalan-

persoalan yang muncul dalam konteks virtual ini, sehingga dapat melindungi hak-hak individu dan menjaga ketertiban di dunia maya.

Keamanan di dunia siber dapat dipertahankan melalui tiga pendekatan utama: teknologi, sosial budaya-etik, dan hukum, di mana pendekatan teknologi menjadi yang paling mendesak untuk mencegah penyusupan dan akses ilegal (Putra et al., 2023);(Soesanto, 2023). Dengan perkembangan teknologi yang sering disalahgunakan untuk kejahatan siber, penting untuk merumuskan kebijakan hukum yang efektif guna menangani kejahatan ini melalui hukum pidana (Ramadhan, 2020);(Najwa et al., 2024). Penegakan hukum harus mengikuti asas legalitas, di mana seseorang dapat dinyatakan bersalah berdasarkan peraturan yang ada, dengan pembuktian yang sah sebagai kunci untuk memastikan bahwa setiap pelanggaran dapat dipertanggungjawabkan secara hukum (Jainah, 2023);(Anwar, 2022).

Kegiatan siber, meskipun berlangsung di ruang virtual, dapat dikategorikan sebagai tindakan hukum yang nyata, sehingga pendekatan hukum konvensional tidak lagi memadai untuk mengatur perilaku ini (Nurwati, 2024). Pengabaian terhadap karakteristik unik dari kegiatan siber dapat menyebabkan banyak masalah yang tidak terjangkau oleh hukum. Dengan bukti elektronik yang mendasari tindakan ini, pelaku juga harus dianggap telah melakukan perbuatan hukum secara nyata. Oleh karena itu, penggunaan hukum pidana dalam mengatur masyarakat tidak hanya sekadar bagian dari regulasi, tetapi juga merupakan langkah kebijakan yang harus sejalan dengan tujuan pembangunan nasional. Hal ini menekankan pentingnya menciptakan kebijakan hukum yang terintegrasi, yang berfokus pada kesejahteraan masyarakat dan efektivitas penegakan hukum dalam menghadapi tantangan di dunia siber.

Bertolak dari dasar pembenaran yang telah diuraikan, perkembangan hukum siber di Indonesia menjadi krusial dalam menghadapi tantangan-tantangan yang muncul akibat kemajuan teknologi informasi. Dalam konteks ini, aktivitas siber yang bersifat virtual tidak dapat dipandang remeh, karena dampaknya yang nyata mempengaruhi keamanan nasional. Dengan meningkatnya jumlah kejahatan siber, seperti penipuan online, penyebaran informasi palsu, dan serangan siber, penting untuk mengembangkan regulasi yang sesuai dan efektif.

Tujuan dari penelitian ini adalah untuk menganalisis perkembangan hukum siber di Indonesia dalam konteks tantangan yang dihadapi akibat kemajuan teknologi informasi, serta untuk mengeksplorasi solusi yang dapat diimplementasikan untuk meningkatkan keamanan nasional.

METODE PENELITIAN

Penelitian ini menggunakan metode studi kepustakaan, yang menyajikan ringkasan penelitian terkait topik tertentu untuk menunjukkan pengetahuan yang sudah ada dan area yang perlu dieksplorasi lebih lanjut. Metode ini juga dapat menginspirasi ide penelitian baru. Sumber untuk studi literatur dapat berasal dari berbagai referensi, termasuk jurnal, buku, dokumentasi, internet, dan pustaka. Metode ini melibatkan serangkaian kegiatan yang terkait dengan pengumpulan data pustaka, membaca, mencatat, dan mengolah bahan untuk penulisan (Zed, 2014). Jenis penulisan yang digunakan adalah studi literatur review, yang fokus pada hasil penelitian yang relevan dengan topik atau variabel yang dibahas.

Secara sistematis, langkah-langkah dalam penulisan literatur review meliputi:

1. Penentuan Topik dan Pertanyaan Penelitian: Identifikasi topik spesifik yang ingin diteliti dan formulasi pertanyaan penelitian yang jelas.
2. Pengumpulan Sumber: Kumpulkan berbagai sumber informasi dari jurnal, buku, artikel, dan sumber online yang relevan dengan topik.
3. Evaluasi Sumber: Tinjau kualitas dan relevansi setiap sumber, pastikan bahwa informasi yang digunakan berasal dari sumber yang terpercaya dan valid.
4. Membaca dan Mencatat: Bacalah sumber-sumber tersebut dengan cermat dan buat catatan tentang temuan, argumen, dan kesimpulan yang dihasilkan.
5. Kategorisasi Informasi: Kelompokkan informasi yang diperoleh berdasarkan tema, subtopik, atau variabel yang relevan untuk memudahkan analisis.
6. Analisis dan Sintesis: Analisis hubungan antara berbagai sumber, identifikasi kesenjangan dalam penelitian yang ada, dan sintesis temuan untuk memberikan perspektif yang komprehensif.
7. Penulisan: Susun hasil analisis dalam bentuk tulisan yang sistematis, dengan pengantar, pembahasan, dan kesimpulan yang jelas.
8. Referensi: Cantumkan semua sumber yang digunakan dengan format yang sesuai untuk memberikan kredit dan memudahkan pembaca mencari informasi lebih lanjut.

HASIL DAN PEMBAHASAN

Perkembangan Hukum Siber di Indonesia

Analisis terhadap berbagai sumber mengenai perkembangan hukum siber di Indonesia mengungkapkan beberapa isu penting yang perlu diperhatikan. Pertama, penelitian oleh Hapsari, (2023) menunjukkan bahwa hukum siber di Indonesia masih dalam tahap perkembangan awal, dengan banyak peraturan yang belum terintegrasi secara

menyeluruh. Ini mengakibatkan kerentanan terhadap kejahatan siber yang semakin kompleks, seperti penipuan online dan peretasan data pribadi.

Sumber-sumber dari jurnal hukum siber, seperti yang diungkapkan oleh Faridi, (2018);Butarbutar, (2023), menggarisbawahi perlunya definisi yang lebih jelas mengenai kejahatan siber. Ketidakjelasan ini sering kali menjadi hambatan dalam penegakan hukum, di mana pelaku kejahatan dapat memanfaatkan ambiguitas dalam peraturan yang ada. Hal ini tercermin dalam meningkatnya jumlah kasus yang tidak dapat ditindaklanjuti karena ketidakjelasan dalam kategorisasi hukum.

Selain itu, studi yang dilakukan oleh Hafizh, (2023);Maulindar & Hartanti, (2023);Sussolaikah, (2023) menyoroti pentingnya kesadaran masyarakat terhadap risiko keamanan siber. Penelitian ini menunjukkan bahwa meskipun ada peningkatan penggunaan teknologi digital, tingkat pemahaman masyarakat tentang kejahatan siber dan cara melindungi diri mereka tetap rendah. Program pendidikan yang tidak mencukupi menyebabkan banyak individu dan organisasi menjadi target empuk bagi pelaku kejahatan siber.

Dalam konteks kerja sama antar sektor, analisis yang dipublikasikan dalam berbagai laporan pemerintah menunjukkan bahwa kolaborasi antara pemerintah, sektor swasta, dan masyarakat sipil merupakan faktor kunci dalam menciptakan ekosistem keamanan siber yang efektif. Kerja sama ini dapat mencakup berbagi informasi mengenai ancaman dan praktik terbaik, serta pengembangan strategi bersama untuk mengatasi kejahatan siber.

Sumber-sumber lain menekankan perlunya pembaruan regulasi yang lebih responsif terhadap perkembangan teknologi. Penelitian Tahir, (2023) menyarankan bahwa pembentukan undang-undang baru yang khusus menangani isu-isu siber sangat penting untuk menjaga relevansi hukum dalam menghadapi tantangan yang terus berubah. Ini mencakup perlindungan data pribadi, tanggung jawab platform digital, dan mekanisme penegakan hukum yang lebih kuat.

Secara keseluruhan, analisis dari berbagai sumber menunjukkan bahwa meskipun ada kemajuan dalam perkembangan hukum siber di Indonesia, tantangan signifikan masih ada. Oleh karena itu, langkah-langkah strategis yang mencakup peningkatan regulasi, edukasi masyarakat, dan kolaborasi multisektoral diperlukan untuk mengatasi masalah ini secara efektif. Hanya dengan pendekatan yang komprehensif, Indonesia dapat menciptakan sistem hukum siber yang kuat dan responsif, yang dapat melindungi keamanan nasional di era digital.

Tantangan dan Solusi Keamanan Nasional dalam Hukum Siber di Indonesia

Analisis terhadap tantangan yang dihadapi dalam konteks hukum siber di Indonesia menunjukkan bahwa kejahatan siber telah menjadi salah satu ancaman utama bagi keamanan nasional. Pertama, meningkatnya kompleksitas dan variasi jenis kejahatan siber, seperti peretasan, penipuan online, dan penyebaran informasi palsu, menciptakan tantangan besar bagi aparat penegak hukum.

Kedua, ketidakjelasan dan ketidaklengkapan regulasi siber menjadi penghalang utama dalam penegakan hukum. Sumber-sumber seperti studi oleh Pratama, (2024) menunjukkan bahwa definisi hukum mengenai kejahatan siber sering kali ambigu, membuatnya sulit untuk menuntut pelaku kejahatan. Ketidakpastian ini menyebabkan banyak kasus kejahatan siber tidak dapat ditindaklanjuti secara hukum, menciptakan impunitas bagi pelanggar.

Ketiga, kurangnya kesadaran masyarakat tentang keamanan siber juga menjadi tantangan signifikan. Banyak individu dan organisasi tidak sepenuhnya memahami risiko yang terkait dengan aktivitas online mereka, yang membuat mereka menjadi target empuk bagi pelaku kejahatan. Penelitian oleh Manurung et al., (2023) menegaskan perlunya program edukasi yang lebih luas untuk meningkatkan pemahaman masyarakat mengenai keamanan siber.

Sebagai solusi untuk mengatasi tantangan ini, pertama-tama perlu dilakukan pembaruan regulasi yang lebih responsif dan komprehensif. Pemerintah harus merumuskan undang-undang baru yang secara khusus menangani berbagai jenis kejahatan siber dan melindungi data pribadi. Ini termasuk menciptakan mekanisme penegakan hukum yang lebih kuat untuk menangkap dan menghukum pelaku kejahatan siber.

Kedua, edukasi dan kampanye kesadaran publik tentang keamanan siber harus ditingkatkan. Ini dapat dilakukan melalui program pendidikan formal di sekolah-sekolah, seminar, dan kampanye informasi yang lebih luas. Kesadaran yang tinggi di masyarakat dapat membantu mengurangi risiko dan mendorong individu untuk mengambil langkah-langkah preventif dalam melindungi diri mereka.

Ketiga, kolaborasi antara sektor publik, swasta, dan masyarakat sipil sangat penting untuk menciptakan lingkungan yang aman di dunia maya. Penelitian menunjukkan bahwa kerja sama ini dapat mencakup berbagi informasi tentang ancaman dan praktik terbaik, serta pengembangan strategi bersama untuk menghadapi tantangan keamanan siber.

Secara keseluruhan, meskipun Indonesia menghadapi tantangan signifikan dalam hukum siber dan keamanan nasional, langkah-langkah strategis yang terintegrasi dapat diambil untuk mengatasi masalah ini. Dengan pembaruan regulasi, edukasi masyarakat, dan kolaborasi multisektoral, diharapkan Indonesia dapat membangun sistem hukum siber yang

kuat dan responsif, serta meningkatkan keamanan nasional di era digital yang terus berkembang.

SIMPULAN

Hasil analisis menunjukkan bahwa perkembangan hukum siber di Indonesia menghadapi tantangan signifikan yang berkaitan dengan kompleksitas kejahatan siber dan ketidakjelasan regulasi. Kerangka hukum yang ada belum sepenuhnya terintegrasi dan jelas, sehingga banyak kasus kejahatan tidak dapat ditindaklanjuti. Selain itu, rendahnya kesadaran masyarakat tentang risiko keamanan siber memperburuk situasi, membuat individu dan organisasi menjadi target empuk bagi pelaku kejahatan. Sebagai solusi, penting untuk melakukan pembaruan regulasi yang komprehensif dan responsif, meningkatkan program edukasi publik tentang keamanan siber, serta mendorong kolaborasi antara sektor publik, swasta, dan masyarakat sipil. Pendekatan yang terintegrasi ini diharapkan dapat membangun sistem hukum siber yang lebih kuat, melindungi keamanan nasional, dan menghadapi tantangan di era digital yang terus berkembang.

DAFTAR PUSTAKA

- Akmal, A. D., & Royal, S. (2019). URGENSI PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA KEJAHATAN TEKNOLOGI INFORMASI Ari. *Journal of Science and Social Research*, 4307(1), 39–46.
- Anwar, M. C. (2022). PANDANGAN HUKUM PIDANA DALAM KEJAHATAN DUNIA MAYA. *Jurnal Hukum*, 5(1).
- Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya Fakultas Hukum Universitas Bung Karno. *Technology and Economics Law Journal*, 2(2).
- Faridi, M. K. (2018). KEJAHATAN SIBER DALAM BIDANG PERBANKAN. *CyberSecurity Dan Forensik Digital*, 1(2), 57–61.
- Fauzi. (2023). Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0 . In PT. Sonpedia Publishing Indonesia.
- Gani. (2023). Kedaulatan data digital untuk integritas bangsa. In Syiah Kuala University Press.
- Hafizh, F. (2023). PKM TENTANG BAHAYA CYBER CRIME DAN PENTINGNYA. *Abdi Jurnal Publikasi*, 2(2), 31–35.
- Hapsari. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. In *Jurnal Konstituen (Vol. 5)*.

- Himawan. (2022). Etika Profesi Teknologi Informasi Dan Komunikasi. In TOHAR MEDIA.
- Jainah, Z. O. (2023). Penegakan Hukum Tindak Pidana Tanpa Hak Dengan Sengaja Turut Serta Menawarkan Kepada Khalayak Umum Untuk Bermain Judi (Studi. SYARI'AH, 6(1).
- Manurung, J., Putra, A., Sihombing, E., & Pandiangan, B. (2023). Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, 2(1), 1–7.
- Maskun. (2022). Kejahatan Siber (Cyber Crime): Suatu Pengantar. In Prenada Media.
- Maulindar, J., & Hartanti, D. (2023). Pelatihan Perlindungan Data Pribadi dan Keamanan Siber Untuk Siswa SMK Negeri 2 Surakarta. *Madaniya*, 4(4), 1851–1856.
- Najwa, L., Hutagalung, V., Hukum, F. I., Studi, P., Hukum, I., Bengkulu, U., & Belakang, A. L. (2024). ASPEK HUKUM ACARA PIDANA DALAM PEMBUKTIAN TINDAK PIDANA CYBERCRIME DI INDONESIA. *Jurnal Hukum Dan Kewarganegaraan*, 6(6), 1–10.
- Nurwati. (2024). Hukum Teknologi Informasi & Komunikasi. In PENERBIT KBM INDONESIA.
- Pratama. (2024). Keamanan Data dan Informasi. In kaizen Media Publishing.
- Putra, R. G., Fauzi, A., Prasetyo, E. T., & Pratama, S. R. (2023). Pentingnya Manajemen Security di Era Digitalisasi. *JIM*, 2(1), 75–83.
- Ramadhan, M. (2020). Pencurian e-money pada e-commerce dalam Tindak Pidana Cybercrime sebagai Tindak Pidana Ekonomi. *Jurnal Reformasi Hukum*, 6(1), 169–188.
- Setiawan, N. (2021). Mengkritisi Undang-Undang ITE Pasal 27 Ayat (3) dilihat dari Sosio-Politik Hukum Pidana Indonesia. *DATIN LAW JURNAL*, 4(3).
- Soesanto, E. (2023). ImplementasiObjek Vital, Pengamanan File dan Pengamanan Cyber di PTPertamina. *IJM: Indonesian Journal of Multidisciplinary*, 1(1).
- Sussolaikah, K. (2023). Pelatihan Media Edukasi Kesadaran Keamanan Siber di SDN 01 Pandean Kota Madiun. *Jurnal Abdimas Tgd*, 3(2), 131–136.
- Tahir. (2023). METODOLOGI PENELITIAN BIDANG HUKUM: Suatu Pendekatan Teori Dan Praktik . In PT. Sonpedia Publishing Indonesia.
- Zed. (2014). Metode Penelitian Kepustakaan. In Jakarta:Yayasan Pustaka Obor Indonesia.