Syntax Admiration: p-ISSN 2722-7782 | e-ISSN 2722-5356 Vol. 6, No. 1, Januari 2025

Transformasi Politik Hukum dalam Penguatan Regulasi *Cyber Law* di Indonesia

Muhenri Sihotang[1*], Zainal Arifin Hoessein[2]
Universitas Borobudur, Indonesia
Email: Muhenri.sihotang@yahoo.com, zainal.arifin@umj.ac.id

Abstrak

Perkembangan pesat teknologi informasi di Indonesia telah mendorong kebutuhan akan regulasi yang komprehensif dalam bidang cyber law. Penelitian ini bertujuan menganalisis transformasi politik hukum dalam penguatan regulasi cyber law di Indonesia, dengan fokus pada perubahan peraturan perundang-undangan terbaru. Metode yang digunakan adalah yuridis normatif, melalui analisis terhadap Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Kitab Undang-Undang Hukum Pidana (KUHP) baru yang mengatur tindak pidana siber Pembahasan mencakup dinamika politik hukum yang melatarbelakangi perubahan regulasi tersebut, termasuk peran pemerintah dan legislatif dalam merespons tantangan keamanan siber. Hasil penelitian menunjukkan bahwa transformasi politik hukum di Indonesia telah menghasilkan penguatan regulasi cyber law melalui pembaruan undang-undang yang lebih adaptif terhadap perkembangan teknologi dan ancaman siber. Kesimpulannya, perubahan peraturan perundang-undangan ini mencerminkan komitmen Indonesia dalam meningkatkan keamanan siber dan perlindungan data, meskipun tantangan dalam implementasinya masih memerlukan perhatian lebih lanjut. Implikasi penelitian ini adalah sebagai acuan bagi pembuat kebijakan dalam memperkuat regulasi cyber law yang adaptif, responsif, dan relevan dengan perkembangan teknologi informasi, guna menciptakan ekosistem digital yang aman dan kondusif bagi pembangunan nasional.

Kata Kunci: *cyber law*; Indonesia; keamanan siber; politik hukum; regulasi

Abstract

The rapid development of information technology in Indonesia has prompted the need for comprehensive regulations in the field of cyber law. This study aims to analyze the political transformation of law in strengthening cyber law regulations in Indonesia, with a focus on the latest changes in laws and regulations. The method used is normative juridical, through an analysis of Law Number 1 of 2024 concerning the

Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as the new Criminal Code (KUHP) which regulates cyber crime The discussion includes the legal and political dynamics behind the regulatory changes, including the role of the government and legislature in responding to cybersecurity challenges. The results of the study show that the transformation of legal politics in Indonesia has resulted in the strengthening of cyber law regulations through legal updates that are more adaptive to technological developments and cyber threats. In conclusion, these changes in laws and regulations reflect Indonesia's commitment to improving cybersecurity and data protection, although the challenges in its implementation still require further attention. The implications of this study are as a reference for policymakers in strengthening cyber law regulations that are adaptive, responsive, and relevant to the development of information technology, in order to create a safe and conducive digital ecosystem for national development.

Keywords: *cyber law; Indonesia; keamanan siber; politik hukum; regulasi*

Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK) di Indonesia telah mengalami peningkatan signifikan dalam beberapa tahun terakhir. Menurut Badan Pusat Statistik (BPS) Indeks Pembangunan TIK (IP-TIK) Indonesia pada tahun 2023 mencapai angka 5,90, meningkat dari 5,85 pada tahun 2022 (Nuryartono & Pasaribu, 2023)(Prayoga et al., 2024). Peningkatan ini mencerminkan akses yang lebih luas terhadap teknologi digital di berbagai wilayah, termasuk daerah terpencil.. Namun, perlu dicatat bahwa meskipun ada peningkatan, IP-TIK Indonesia masih tergolong moderat, dengan nilai yang tetap berada di kisaran 5 dari skala 0-10.

Seiring dengan kemajuan TIK, Indonesia menghadapi tantangan serius terkait kejahatan siber. Kejahatan seperti peretasan, pencurian data pribadi, dan penyebaran malware semakin marak terjadi. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa insiden kejahatan siber meningkat seiring dengan pertumbuhan pengguna internet (Ariyaningsih et al., 2023). Kondisi ini menuntut adanya regulasi yang efektif untuk melindungi masyarakat dan infrastruktur digital nasional.

Saat ini, Indonesia memiliki beberapa regulasi yang mengatur aktivitas di dunia maya, salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun, UU ITE sering dianggap belum mampu mengakomodasi seluruh aspek kejahatan siber yang terus berkembang. Beberapa pasal dalam UU ITE, seperti Pasal 27 ayat (3) tentang penghinaan dan/atau pencemaran nama baik, kerap menimbulkan interpretasi yang beragam dan dianggap kurang spesifik dalam menangani kejahatan siber yang kompleks (Handoyo et al., 2024).

Dinamika politik hukum dalam pembentukan regulasi siber di Indonesia menunjukkan adanya tarik-menarik kepentingan antara berbagai pemangku kepentingan. Proses legislasi sering kali dipengaruhi oleh pertimbangan politik, ekonomi, dan sosial yang kompleks. Hal ini berdampak pada efektivitas regulasi yang dihasilkan dalam menghadapi ancaman siber yang semakin canggih (Dinda, 2024). Selain itu, perbedaan kepentingan antara pemerintah, sektor swasta, dan masyarakat sipil sering kali mempengaruhi arah kebijakan yang diambil.

Urgensi transformasi regulasi cyber law di Indonesia menjadi semakin nyata dengan meningkatnya intensitas dan kompleksitas kejahatan siber. Tanpa regulasi yang adaptif dan komprehensif, Indonesia berisiko menjadi sasaran empuk bagi pelaku kejahatan siber, yang dapat merugikan perekonomian dan keamanan nasional. Oleh karena itu, diperlukan pembaruan regulasi yang mampu mengantisipasi perkembangan teknologi dan modus operandi kejahatan siber (Wahid, 2023).

Salah satu langkah penting dalam transformasi regulasi cyber law adalah harmonisasi dengan standar internasional (Pangestika et al., 2024). Beberapa negara, seperti Uni Eropa dengan General Data Protection Regulation (GDPR), telah memiliki regulasi komprehensif terkait perlindungan data pribadi (Riyanto, 2020). Selain itu, peningkatan kapasitas penegak hukum dalam menangani kejahatan siber menjadi krusial. Tanpa dukungan sumber daya manusia yang kompeten, regulasi yang baik pun tidak akan efektif. Pelatihan dan pendidikan khusus di bidang forensik digital dan keamanan siber perlu ditingkatkan untuk memastikan penegakan hukum yang optimal.

Partisipasi aktif masyarakat dalam menjaga keamanan siber juga tidak kalah penting. Kesadaran akan pentingnya perlindungan data pribadi dan praktik keamanan digital harus ditingkatkan melalui edukasi dan sosialisasi yang masif. Dengan demikian, masyarakat dapat menjadi garda terdepan dalam mencegah kejahatan siber. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat sipil menjadi kunci dalam penguatan regulasi cyber law. Pendekatan multipihak ini akan memastikan bahwa regulasi yang dihasilkan dapat diterima dan dilaksanakan oleh semua pihak, serta mampu menjawab tantangan yang ada. Selain itu, evaluasi dan revisi regulasi secara berkala perlu dilakukan untuk menyesuaikan dengan dinamika perkembangan teknologi dan ancaman siber. Regulasi yang stagnan akan cepat usang dan tidak relevan dalam menghadapi tantangan yang terus berubah.

Penerapan sanksi yang tegas dan proporsional terhadap pelaku kejahatan siber akan memberikan efek jera dan meningkatkan kepercayaan masyarakat terhadap sistem hokum (Husain, 2024). Namun, sanksi harus disertai dengan upaya rehabilitasi dan edukasi agar pelaku dapat kembali berkontribusi positif dalam masyarakat. Pengembangan infrastruktur keamanan siber nasional, seperti pusat respons insiden siber, akan memperkuat kemampuan deteksi dan respons terhadap

ancaman siber. Infrastruktur ini harus didukung dengan teknologi terkini dan sumber daya manusia yang kompeten. Terakhir, integrasi aspek keamanan siber dalam kurikulum pendidikan formal akan membekali generasi muda dengan pengetahuan dan keterampilan yang diperlukan untuk menghadapi tantangan di era digital. Pendidikan sejak dini akan membentuk budaya keamanan siber yang kuat di masyarakat.

Dengan demikian, transformasi politik hukum dalam penguatan regulasi cyber law di Indonesia merupakan kebutuhan mendesak yang harus segera diwujudkan. Hanya dengan regulasi yang adaptif, komprehensif, dan didukung oleh semua pemangku kepentingan, Indonesia dapat menghadapi tantangan kejahatan siber dan memanfaatkan potensi TIK untuk kemajuan bangsa.

Tujuan penelitian ini untuk mengetahui transformasi politik hukum diperlukan dalam penguatan regulasi cyber law di Indonesia untuk menghadapi perkembangan teknologi dan meningkatnya ancaman kejahatan siber dan mengetahui bagaimana peran politik hukum dalam membentuk dan mengimplementasikan regulasi cyber law yang efektif dan adaptif terhadap dinamika teknologi informasi di Indonesia.

Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum yuridis normatif yang berfokus pada analisis terhadap norma dan peraturan hukum yang berlaku. Pendekatan ini dilakukan melalui telaah sistematis terhadap peraturan perundang-undangan terkait cyber law, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dalam Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024. Selain itu, penelitian ini juga mengkaji kebijakan publik yang berkaitan dengan penguatan regulasi keamanan siber di Indonesia. Pendekatan konseptual digunakan untuk memahami konsep politik hukum dan relevansinya dalam membentuk regulasi cyber law yang efektif.

Sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer dan sekunder. Bahan hukum primer meliputi peraturan perundang-undangan, peraturan pemerintah, dan kebijakan terkait keamanan siber di Indonesia. Bahan hukum sekunder diperoleh dari literatur akademik, seperti jurnal ilmiah bereputasi yang terindeks Scopus, buku-buku hukum, hasil penelitian terdahulu, serta pendapat ahli hukum yang relevan. Pengumpulan bahan hukum dilakukan melalui studi pustaka dan penelusuran sumber ilmiah dari database jurnal internasional. Selain itu, wawancara dengan pakar hukum dan praktisi di bidang cyber law turut dilakukan untuk memperoleh perspektif empiris yang mendukung analisis.

Teknis analisis bahan hukum dilakukan dengan menggunakan metode deskriptif-analitis, yaitu menguraikan dan menganalisis peraturan yang berlaku dan

relevansinya terhadap perkembangan kejahatan siber di Indonesia. Penelitian ini juga membandingkan regulasi cyber law di Indonesia dengan standar internasional untuk mengidentifikasi kelemahan dan peluang perbaikan regulasi. Analisis dilakukan secara komprehensif dengan mengaitkan teori politik hukum dan kebijakan publik untuk menghasilkan rekomendasi yang aplikatif dalam penguatan regulasi cyber law di Indonesia. Pendekatan ini diharapkan dapat memberikan kontribusi ilmiah yang signifikan dalam pengembangan hukum siber di Indonesia.

Hasil dan Pembahasan

Transformasi politik hukum penting untuk memperkuat regulasi cyber law di Indonesia guna menghadapi perkembangan teknologi dan ancaman kejahatan siber

Transformasi politik hukum di Indonesia menjadi elemen krusial dalam memperkuat regulasi *cyber law* untuk menghadapi perkembangan teknologi dan meningkatnya ancaman kejahatan siber. Perkembangan pesat teknologi informasi telah mendorong Indonesia untuk segera menyesuaikan regulasi hukum guna melindungi masyarakat dan infrastruktur digital. Seiring dengan meningkatnya akses internet, muncul berbagai bentuk kejahatan siber seperti pencurian data, peretasan sistem, dan penyebaran malware. Kondisi ini menuntut peran aktif politik hukum dalam membentuk kerangka regulasi yang adaptif dan efektif (Putra et al., 2024).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, menjadi dasar hukum utama dalam mengatur aktivitas di dunia digital. UU ITE, khususnya Pasal 27 hingga Pasal 29, mengatur tentang larangan penyebaran konten negatif, pencemaran nama baik, dan tindakan peretasan. Namun, regulasi ini dinilai masih memiliki celah hukum yang tidak mampu mengantisipasi bentuk-bentuk kejahatan siber yang lebih kompleks dan dinamis.

Selain UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam perlindungan data di era digital. UU PDP, khususnya pada Pasal 4 dan Pasal 22, mengatur hak pemilik data pribadi dan kewajiban pengendali data dalam menjaga keamanan informasi. Pengaturan ini merupakan respons terhadap meningkatnya insiden kebocoran data yang menimbulkan kerugian besar bagi masyarakat.

Namun, penerapan regulasi tersebut menghadapi tantangan dalam penegakan hukum, terutama terkait kapasitas aparat penegak hukum dalam memahami dan mengimplementasikan aturan yang kompleks di bidang siber. Keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan

siber dan forensik digital menjadi hambatan signifikan dalam optimalisasi penegakan hukum di Indonesia.

Dalam konteks politik hukum, pembentukan regulasi *cyber law* sering kali dipengaruhi oleh dinamika politik dan kepentingan ekonomi (Akbar et al., 2025). Proses legislasi menghadapi tantangan dalam menyelaraskan kebutuhan pengaturan dengan kepentingan berbagai pemangku kepentingan. Akibatnya, kebijakan yang dihasilkan sering kali belum optimal dalam menghadapi perkembangan teknologi dan modus kejahatan siber yang terus berubah.

Indonesia juga berupaya menyesuaikan regulasi *cyber law* dengan standar internasional. Pengadopsian prinsip-prinsip dalam General Data Protection Regulation (GDPR) Uni Eropa menjadi salah satu referensi penting dalam pembentukan UU PDP. Penyesuaian ini bertujuan agar regulasi nasional dapat diakui secara global dan mendukung kerja sama internasional dalam penanganan kejahatan siber lintas negara.

Selain itu, peraturan teknis terkait pengamanan sistem elektronik diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Pasal 14 dan Pasal 15 dalam peraturan ini mengatur kewajiban penyelenggara sistem elektronik untuk menerapkan standar keamanan yang memadai guna melindungi data dan informasi yang dikelola.

Upaya penguatan regulasi *cyber law* juga melibatkan pembentukan lembaga yang berperan dalam menjaga keamanan siber nasional, seperti Badan Siber dan Sandi Negara (BSSN). BSSN memiliki kewenangan strategis dalam merumuskan kebijakan teknis dan melakukan pengawasan terhadap keamanan infrastruktur digital di Indonesia sesuai dengan Peraturan Presiden Nomor 28 Tahun 2021.

Di sisi lain, partisipasi sektor swasta dalam mendukung penguatan regulasi *cyber law* menjadi hal yang penting (Farhan et al., 2023). Sektor industri teknologi informasi perlu berkolaborasi dengan pemerintah dalam penerapan standar keamanan siber dan kepatuhan terhadap regulasi yang berlaku. Sinergi ini diharapkan dapat meningkatkan ketahanan siber nasional.

Selain penguatan regulasi, edukasi dan peningkatan kesadaran masyarakat terkait keamanan siber menjadi strategi penting dalam mencegah kejahatan siber. Program literasi digital yang diinisiasi oleh Kementerian Komunikasi dan Informatika bertujuan untuk meningkatkan pemahaman masyarakat tentang risiko dan perlindungan di dunia digital (Zahwani & Nasution, 2024).

Pengawasan dan penegakan hukum juga harus diperkuat melalui kerja sama lintas sektor dan lintas negara. Kerja sama ini mencakup pertukaran informasi, pelatihan, dan pengembangan teknologi untuk mendeteksi dan menangani kejahatan siber secara efektif. Pengembangan regulasi *cyber law* yang adaptif membutuhkan pembaruan secara berkala agar tetap relevan dengan perkembangan

teknologi. Proses revisi dan evaluasi regulasi perlu didasarkan pada analisis menyeluruh terhadap tren kejahatan siber dan dampaknya terhadap masyarakat serta ekonomi nasional. Transformasi politik hukum yang berkelanjutan di Indonesia diharapkan dapat menciptakan ekosistem digital yang aman dan kondusif. Penguatan regulasi *cyber law* yang komprehensif dan responsif menjadi fondasi penting dalam mendukung pertumbuhan ekonomi digital serta melindungi kepentingan nasional di era globalisasi.

Peran politik hukum dalam merumuskan dan menerapkan regulasi *cyber law* yang efektif dan adaptif terhadap dinamika teknologi di Indonesia.

Transformasi politik hukum di Indonesia menjadi elemen krusial dalam memperkuat regulasi *cyber law* untuk menghadapi perkembangan teknologi dan meningkatnya ancaman kejahatan siber (Napitupulu, 2017). Perkembangan pesat teknologi informasi telah mendorong Indonesia untuk segera menyesuaikan regulasi hukum guna melindungi masyarakat dan infrastruktur digital. Seiring dengan meningkatnya akses internet, muncul berbagai bentuk kejahatan siber seperti pencurian data, peretasan sistem, dan penyebaran malware. Kondisi ini menuntut peran aktif politik hukum dalam membentuk kerangka regulasi yang adaptif dan efektif.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, menjadi dasar hukum utama dalam mengatur aktivitas di dunia digital. UU ITE, khususnya Pasal 27 hingga Pasal 29, mengatur tentang larangan penyebaran konten negatif, pencemaran nama baik, dan tindakan peretasan. Namun, regulasi ini dinilai masih memiliki celah hukum yang tidak mampu mengantisipasi bentuk-bentuk kejahatan siber yang lebih kompleks dan dinamis (Aini & Lubis, 2024).

Selain UU ITE, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam perlindungan data di era digital. UU PDP, khususnya pada Pasal 4 dan Pasal 22, mengatur hak pemilik data pribadi dan kewajiban pengendali data dalam menjaga keamanan informasi. Pengaturan ini merupakan respons terhadap meningkatnya insiden kebocoran data yang menimbulkan kerugian besar bagi masyarakat (Soleh & Tjenreng, 2025).

Namun, penerapan regulasi tersebut menghadapi tantangan dalam penegakan hukum, terutama terkait kapasitas aparat penegak hukum dalam memahami dan mengimplementasikan aturan yang kompleks di bidang siber. Keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan siber dan forensik digital menjadi hambatan signifikan dalam optimalisasi penegakan hukum di Indonesia (Darmawan, 2024).

Dalam konteks politik hukum, pembentukan regulasi *cyber law* sering kali dipengaruhi oleh dinamika politik dan kepentingan ekonomi. Proses legislasi menghadapi tantangan dalam menyelaraskan kebutuhan pengaturan dengan kepentingan berbagai pemangku kepentingan. Akibatnya, kebijakan yang dihasilkan sering kali belum optimal dalam menghadapi perkembangan teknologi dan modus kejahatan siber yang terus berubah (Munajat & Yusuf, 2024).

Indonesia juga berupaya menyesuaikan regulasi *cyber law* dengan standar internasional. Pengadopsian prinsip-prinsip dalam General Data Protection Regulation (GDPR) Uni Eropa menjadi salah satu referensi penting dalam pembentukan UU PDP. Penyesuaian ini bertujuan agar regulasi nasional dapat diakui secara global dan mendukung kerja sama internasional dalam penanganan kejahatan siber lintas negara (Nabila et al., 2024).

Selain itu, peraturan teknis terkait pengamanan sistem elektronik diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Pasal 14 dan Pasal 15 dalam peraturan ini mengatur kewajiban penyelenggara sistem elektronik untuk menerapkan standar keamanan yang memadai guna melindungi data dan informasi yang dikelola. Upaya penguatan regulasi *cyber law* juga melibatkan pembentukan lembaga yang berperan dalam menjaga keamanan siber nasional, seperti Badan Siber dan Sandi Negara (BSSN). BSSN memiliki kewenangan strategis dalam merumuskan kebijakan teknis dan melakukan pengawasan terhadap keamanan infrastruktur digital di Indonesia sesuai dengan Peraturan Presiden Nomor 28 Tahun 2021.

Di sisi lain, partisipasi sektor swasta dalam mendukung penguatan regulasi *cyber law* menjadi hal yang penting. Sektor industri teknologi informasi perlu berkolaborasi dengan pemerintah dalam penerapan standar keamanan siber dan kepatuhan terhadap regulasi yang berlaku. Sinergi ini diharapkan dapat meningkatkan ketahanan siber nasional. Selain penguatan regulasi, edukasi dan peningkatan kesadaran masyarakat terkait keamanan siber menjadi strategi penting dalam mencegah kejahatan siber. Program literasi digital yang diinisiasi oleh Kementerian Komunikasi dan Informatika bertujuan untuk meningkatkan pemahaman masyarakat tentang risiko dan perlindungan di dunia digital.

Pengawasan dan penegakan hukum juga harus diperkuat melalui kerja sama lintas sektor dan lintas negara. Kerja sama ini mencakup pertukaran informasi, pelatihan, dan pengembangan teknologi untuk mendeteksi dan menangani kejahatan siber secara efektif (Sitanggang et al., 2024). Pengembangan regulasi *cyber law* yang adaptif membutuhkan pembaruan secara berkala agar tetap relevan dengan perkembangan teknologi. Proses revisi dan evaluasi regulasi perlu didasarkan pada analisis menyeluruh terhadap tren kejahatan siber dan dampaknya terhadap masyarakat serta ekonomi nasional. Transformasi politik hukum yang

berkelanjutan di Indonesia diharapkan dapat menciptakan ekosistem digital yang aman dan kondusif. Penguatan regulasi *cyber law* yang komprehensif dan responsif menjadi fondasi penting dalam mendukung pertumbuhan ekonomi digital serta melindungi kepentingan nasional di era globalisasi.

Kesimpulan

Transformasi politik hukum dalam penguatan regulasi cyber law di Indonesia merupakan langkah strategis dan mendesak untuk menghadapi perkembangan teknologi informasi dan meningkatnya ancaman kejahatan siber. Regulasi yang telah ada, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), menunjukkan adanya upaya pemerintah dalam memperkuat kerangka hukum di bidang keamanan siber. Namun, masih terdapat berbagai tantangan dalam implementasi dan penegakan hukum yang memerlukan pembaruan regulasi yang lebih adaptif, komprehensif, dan selaras dengan standar internasional. Transformasi ini penting untuk menciptakan perlindungan hukum yang efektif terhadap ancaman siber dan mendukung pembangunan ekonomi digital yang aman dan berkelanjutan. Temuan penelitian ini mengindikasikan perlunya sinergi antara pemerintah, sektor swasta, dan masyarakat dalam memperkuat ekosistem keamanan siber di Indonesia. Peningkatan kapasitas aparat penegak hukum, pengembangan infrastruktur keamanan digital, dan harmonisasi regulasi dengan standar global menjadi strategi utama dalam mewujudkan regulasi cyber law yang efektif. Selain itu, implementasi regulasi harus diimbangi dengan edukasi publik mengenai literasi digital dan perlindungan data pribadi. Hasil penelitian ini dapat dijadikan referensi bagi pembuat kebijakan dalam merumuskan dan menyempurnakan regulasi cyber law yang adaptif dan responsif terhadap perkembangan teknologi serta tantangan kejahatan siber di masa depan.

BIBLIOGRAFI

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. Judge: Jurnal Hukum, 5(02), 55–63.

Akbar, V., Dirkareshza, N. P., & Syahuri, T. (2025). Tugas Dan Sifat Politik Hukum Terhadap Sistem Hukum Di Indonesia. Intellektika: Jurnal Ilmiah Mahasiswa, 3(1), 85–100. **Https://Doi.Org/10.59841/Intellektika.V3i1.2033**

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber Dengan Percepatan Digitalisasi Di Indonesia. Justisia: Jurnal Ilmu Hukum, 1(1), 1–11.

Darmawan, K. S. (2024). Implementasi Peran Bareskrim Dalam Melindungi Masyarakat Pada Era Society 5.0. Jurnal Salam Presisi, 2(01), 49–61.

Dinda, A. L. S. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia. Al-Dalil: Jurnal Ilmu Sosial, Politik, Dan Hukum, 2(2), 69–77.

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.

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. Maqasidi: Jurnal Syariah Dan Hukum, 40–55.

Husain, W. R. A.-F. (2024). Hukum Pidana Judi Online Perspektif Indonesia Dan Perkembangan Aspek Legalitas. Journal Of Human And Education (Jahe), 4(6), 1297–1304.

Munajat, A. A., & Yusuf, H. (2024). Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital. Jurnal Intelek Insan Cendikia, 1(9), 4853–4865.

Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional. Indonesian Journal Of Law, 1(1), 26–37.

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. Deviance Jurnal Kriminologi, 1(1), 100–113.

Nuryartono, N., & Pasaribu, S. H. (2023). Dampak Teknologi Informasi Dan Komunikasi Terhadap Pertumbuhan Ekonomi Kawasan Barat Dan Timur Indonesia. Jurnal Ekonomi Dan Kebijakan Pembangunan, 12(2).

Pangestika, E. Q., Suningrat, N., Herwantono, H., Andriyani, W., & Rahardian, R. L. (2024). Penerapan Prinsip Hukum Internasional Dalam Penegakan Hukum Terhadap Kejahatan Siber Dan Serangan Siber. Jurnal Review Pendidikan Dan Pengajaran (Jrpp), 7(2), 5782–5788.

Prayoga, A., Simanjuntak, D. G. F., Seda, F. T. A., & Parhusip, J. (2024). Analisis Perbedaan Rata-Rata Pembangunan Teknologi Informasi Dan Komunikasi Di Indonesia Mempengaruhi Tingkat Ekonomi (Studi Kasus: Perbandingan Pembangunan Wilayah Barat Dan Timur Indonesia). Informatech: Jurnal Ilmiah Informatika Dan Komputer, 1(2), 163–169.

Putra, N. R., Triadi, I., Setiadi, W., Achmad, M. M., & Supriyadi, M. W. (2024). Politik Hukum Teknologi Blockchain Indonesia Menuju Kerangka Hukum Yang Implementasi Inovasi Dan Adaptasi. Hukum Dinamika Ekselensia, 6(4). **Https://Journalpedia.Com/1/Index.Php/Hde/Index**

Riyanto, H. R. B. (2020). Pembaruan Hukum Nasional Era 4.0. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 9(2), 161.

Sitanggang, A. S., Darmawan, F., & Saputra, D. (2024). Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber. Jurnal Pendidikan Dan Teknologi Indonesia, 4(3), 79–83. **Https://Doi.Org/10.52436/1.Jpti.409**

Soleh, M., & Tjenreng, Z. (2025). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. Jurnal Kajian Pemerintah: Journal Of Government, Social And Politics, 11(1), 1–10.

Wahid, A. (2023). Policy Formulation Of Fraud Offenses In The New Penal Code Concept For Combating Technology-Related Crimes. Rechtsidee, 11(2), 10–21070. **Https://Doi.Org/10.21070/Jihr.V12i2.1008**

Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi Di Era Digital. Journal Of Sharia Economics Scholar (Joses), 2(2). **Https://Doi.Org/10.5281/Zenodo.12608751**