

Cybersecurity dan Pancasila: Harmonisasi Regulasi Hukum Internasional dengan Kepentingan Nasional

Ayman Hammam Abdurrohman¹, Cahyo Nurul Uzmawi², Ridhwan Khoiruddin³, Ahmad Muhamad Mustain Nasoha⁴, Ashfiya Nur Atqiya⁵

^{1,2,3,4} Universitas Islam Negeri Raden Mas Said Surakarta

⁵ Universitas Sebelas Maret Surakarta

Correspondence email; aymanhammam2004@gmail.com

Article history

Submitted: 2025/01/14;

Revised: 2025/02/23;

Accepted: 2025/03/30

Abstract

The purpose of this study is to comprehensively examine the challenges and opportunities in aligning international cybersecurity regulations with the Indonesian legal system based on Pancasila values. Using a literature review method, this study explores the dynamics of legal policy in the digital era. The results of the study indicate that cybersecurity has become a strategic issue in modern governance, especially with the increasing threat of hacking, data breaches, malware distribution, and ransomware attacks that can disrupt national stability, erode public trust, and weaken state sovereignty. At the international level, the 2001 Budapest Convention on Cybercrime is one of the main legal instruments that many countries refer to in building a cross-border digital crime protection system. However, the implementation of these international regulations in Indonesia cannot be directly adopted without considering the cultural aspects and ideals of the nation. Several strategic recommendations are proposed, including strengthening law enforcement capacity, formulating specific cybersecurity laws, and launching educational campaigns to raise public awareness of the importance of protecting personal data in the digital era.

Keywords

Cybersecurity, Data Protection, Digital Sovereignty, Indonesian Legal System.



© 2025 by the authors. This is an open-access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY SA) license, <https://creativecommons.org/licenses/by-sa/4.0/>.

PENDAHULUAN

Indonesia sebagai negara hukum lahir dari semangat besar rakyat yang ingin melepaskan diri dari penjajahan kolonial Belanda. Semangat kemerdekaan tersebut tergambar jelas dalam alinea kedua Pembukaan UUD 1945, yang menegaskan bahwa setiap bangsa berhak untuk merdeka dan bahwa penjajahan harus dihapuskan karena bertentangan dengan nilai-nilai kemanusiaan dan keadilan. Seiring waktu, konsep negara hukum di Indonesia berkembang dengan kekhasan tersendiri yang dipengaruhi oleh nilai-nilai lokal, budaya masyarakat, dan keragaman sosial yang menjadi bagian dari jati diri bangsa. Karena itu, penerapan hukum di Indonesia tidak bisa dilakukan secara kaku, melainkan harus adaptif terhadap kondisi sosial yang terus berubah dan realitas masyarakat yang dihadapi. Meski demikian, fleksibilitas tersebut tetap harus berpijak pada cita-cita Indonesia sebagai negara hukum modern yang menjunjung keadilan, kesejahteraan, serta perlindungan hak-hak warga negara (Ristanti, 2015).

Di sisi lain, tantangan besar dalam tata kelola negara modern saat ini adalah meningkatnya ancaman terhadap keamanan siber. Kejahatan digital seperti peretasan, pencurian informasi, hingga serangan ransomware semakin marak dan dapat mengganggu stabilitas nasional. Dampaknya tidak

hanya dirasakan oleh individu, tetapi juga oleh sektor pemerintahan dan dunia usaha (Sumantri, 2022). Oleh sebab itu, penegakan hukum yang tegas dan efektif sangat penting dalam menangani kejahatan siber. Perkembangan teknologi digital telah menjadikan data pribadi seperti identitas, informasi finansial, dan catatan medis sebagai aset yang sangat bernilai namun juga rentan terhadap pelanggaran. Situasi ini meningkatkan risiko penyalahgunaan dan pelanggaran privasi. Karena itu, perlindungan terhadap data pribadi merupakan bagian dari hak asasi manusia yang harus dijamin oleh negara (Nirwana et al., 2024). Secara global, penanggulangan kejahatan siber telah memperoleh dasar hukum yang kuat melalui Konvensi Budapest tentang Kejahatan Siber yang diresmikan pada tahun 2001. Konvensi ini hingga saat ini masih menjadi acuan utama dalam pengembangan kebijakan dan penegakan hukum siber di berbagai negara (Akbar & Putra, 2014). Meskipun demikian, dalam proses adaptasi dan penerapan ketentuan internasional tersebut ke dalam sistem hukum nasional, Indonesia perlu tetap berlandaskan pada nilai-nilai Pancasila yang berfungsi sebagai dasar normatif dalam pembentukan hukum di Indonesia (Risdiyani & Dewi, 2021).

Penelitian ini bertujuan untuk mengkaji secara komprehensif bagaimana regulasi keamanan siber internasional dapat disesuaikan dengan konteks hukum nasional Indonesia yang berpijak pada prinsip-prinsip Pancasila. Kajian ini memusatkan perhatian pada bagaimana prinsip kedaulatan negara dan perlindungan hak asasi manusia dapat diintegrasikan dalam kerangka hukum keamanan siber global (Kuntadi, 2022). Dengan meningkatnya ancaman di ruang digital, sangat penting bagi Indonesia untuk memiliki sistem hukum yang responsif, adil, dan mampu menjaga kepentingan nasional tanpa mengabaikan jaminan atas hak-hak asasi setiap individu.

METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi pustaka (library research) sebagai teknik utama pengumpulan data. Data yang dianalisis berasal dari sumber sekunder, antara lain peraturan perundang-undangan, konvensi internasional, artikel jurnal ilmiah, serta literatur akademik lainnya. Proses analisis dilakukan secara tematik-kualitatif dengan menelusuri isu-isu utama yang berkaitan dengan keamanan siber, hukum internasional, dan nilai-nilai Pancasila. Pendekatan ini memberikan ruang bagi peneliti untuk menelaah sejauh mana regulasi global terkait keamanan siber dapat selaras dengan Pancasila sebagai landasan hukum dan pandangan hidup bangsa Indonesia.

TEMUAN DAN PEMBAHASAN

Temuan

Cybersecurity dalam Perspektif Hukum Internasional

Keamanan Siber atau Cybersecurity memegang peranan penting di era digital saat ini, terutama dalam melindungi data, menjaga privasi, dan memastikan kelangsungan layanan yang krusial. Dengan semakin meningkatnya konektivitas dan ketergantungan pada teknologi, penerapan langkah-langkah keamanan siber yang kuat serta kewaspadaan terus-menerus menjadi sangat penting untuk menghadapi berbagai ancaman siber secara efektif (Madya et al., 2023).

Dalam ranah hukum internasional, terdapat dua prinsip utama yang menjadi dasar pengaturan hubungan global. Prinsip pertama berkaitan dengan ketentuan hukum yang mengatur peran, fungsi, dan kewenangan lembaga atau organisasi internasional, termasuk mekanisme kerja mereka, hubungan antarorganisasi, serta interaksi dengan negara-negara berdaulat maupun individu dalam konteks hukum dan politik. Sedangkan prinsip kedua menyoroti aspek hukum yang berkaitan dengan individu dan

entitas non-negara, khususnya mengenai hak dan kewajiban mereka yang memiliki relevansi dalam tatanan masyarakat internasional (Katiandagho, 2020).

Secara bertahap, hukum internasional telah merumuskan beragam regulasi dan kebijakan yang dirancang khusus untuk mengatasi ancaman siber yang melintasi batas negara, mengingat kejahatan digital tidak terbatas pada wilayah yurisdiksi satu negara saja. Salah satu instrumen hukum utama dalam konteks ini adalah Konvensi Budapest tahun 2001, yang dibuat untuk memperkuat kerja sama antarnegara dalam pencegahan, penanganan, dan penindakan berbagai jenis kejahatan siber yang terus berkembang. (Akbar & Putra, 2014). Namun, penerapan konvensi ini di Indonesia masih menemui sejumlah kendala yang kompleks, seperti perbedaan norma hukum antara sistem nasional dengan standar internasional yang ada dalam konvensi, tantangan teknis terkait kesiapan infrastruktur dan sumber daya penegakan hukum siber, serta isu terkait kedaulatan negara (Budi et al., 2021).

Di sisi lain, keberadaan regulasi internasional terkait keamanan siber harus disesuaikan dengan sistem hukum nasional Indonesia yang berlandaskan pada nilai-nilai Pancasila. Dalam kebijakan luar negerinya, Indonesia selalu menekankan pentingnya prinsip kedaulatan digital sebagai upaya menjaga kontrol penuh atas ruang siber nasional, sehingga aturan dan kebijakan yang diterapkan tidak hanya mengacu pada standar internasional, tetapi juga mengakomodasi kepentingan nasional (Purwaningsih, 2022). Selain itu, perlindungan hak-hak warga negara di era teknologi informasi menjadi bagian penting dalam pendekatan Indonesia terhadap hukum siber, di mana setiap kebijakan terkait regulasi digital harus mampu memastikan keamanan data, kebebasan berekspresi, dan hak privasi individu (Lestari & Finaldin, 2023).

Kelemahan sistem dunia siber di Indonesia juga dipengaruhi oleh kurangnya regulasi yang jelas mengenai isu-isu siber, yang menyebabkan kebingungan di masyarakat. Karena karakter dunia virtual yang melampaui batas negara, kepemilikan, hingga wilayah pribadi, hal ini sering menimbulkan konflik dan perselisihan di tengah masyarakat (Aji, 2023). Keamanan siber merupakan kombinasi dari konsep, teknologi, regulasi, kebijakan, pelatihan, praktik, jaminan, serta prosedur yang dirancang untuk melindungi perusahaan, aset, dan lingkungan digital para penggunanya. Dalam konteks ini, keamanan siber mencakup berbagai perangkat yang terintegrasi dengan infrastruktur, aplikasi, layanan komputasi, serta sistem informasi dan komunikasi yang menjadi bagian dari aset dan struktur organisasi. Oleh sebab itu, peran utama keamanan siber adalah menjaga serta memastikan perlindungan aset organisasi dan pengguna dari berbagai ancaman yang ada di ruang siber (Rahman Najwa, 2024).

Harmonisasi Regulasi Internasional dengan Pancasila

Negara Hukum Pancasila merupakan bentuk negara hukum yang didasarkan pada prinsip-prinsip, identitas, serta karakteristik yang terkandung dalam Pancasila. Sebagai dasar negara Indonesia, Pancasila memuat prinsip-prinsip fundamental yang wajib dijadikan pedoman dalam penyusunan regulasi keamanan siber. Prinsip-prinsip tersebut meliputi: 1) Ketuhanan Yang Maha Esa: Prinsip ini mengarahkan regulasi keamanan siber agar tetap sesuai dengan nilai-nilai etika dan moral. Etika dan moral yang berlandaskan keadilan dan martabat ini berakar pada moralitas yang tercantum dalam sila pertama Pancasila. Oleh karena itu, prinsip ini harus menjadi roh dalam setiap norma dan asas hukum yang diterapkan, menjadikan Pancasila sebagai sumber utama dalam sistem hukum nasional. Dalam perspektif sila pertama, semua lembaga hukum dipandang sebagai institusi yang menegakkan nilai-nilai etika dan moral serta selaras dengan ajaran agama. 2) Kemanusiaan yang Adil dan Beradab: Prinsip ini menekankan pentingnya keseimbangan antara penegakan hukum keamanan siber dan perlindungan hak asasi Manusia (Ashfiya Nur Atqiya et al., 2024). Setiap lembaga hukum harus berpegang pada sila kedua Pancasila yang mengutamakan penghormatan dan perlindungan HAM. Peran institusi hukum adalah

menjaga nilai-nilai ini dengan memberikan perlindungan tidak hanya kepada korban, tetapi juga kepada pelaku dan masyarakat secara keseluruhan. Masalah kebocoran data pribadi harus diselesaikan melalui mekanisme hukum yang berlandaskan keadilan bermartabat, di mana pelaku dikenai sanksi sesuai dengan tindakan mereka, sementara korban mendapatkan perlindungan dan keadilan. Selain itu, penyelenggara sistem elektronik juga berkewajiban meningkatkan keamanan untuk mencegah terulangnya insiden serupa di masa mendatang. 3) Persatuan Indonesia: Prinsip ini memastikan bahwa setiap kebijakan dan regulasi di bidang keamanan siber dirancang dan diterapkan secara strategis untuk memperkuat semangat persatuan serta menjaga integritas bangsa dalam menghadapi tantangan perkembangan teknologi yang terus berubah. 4) Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan: Prinsip ini menekankan pentingnya keterlibatan aktif seluruh lapisan masyarakat dalam proses penyusunan dan perumusan kebijakan keamanan siber. Dengan demikian, regulasi yang dihasilkan dapat merefleksikan kebutuhan serta kepentingan publik secara luas (Ariyani et al., 2020). Kebijakan keamanan siber harus dirancang dengan mempertimbangkan kepentingan masyarakat secara umum tanpa mengabaikan hak-hak dan kepentingan individu. 5) Keadilan Sosial bagi Seluruh Rakyat Indonesia: Prinsip ini menegaskan perlunya memastikan akses yang merata terhadap keamanan digital dan perlindungan data pribadi. Setiap warga negara harus memperoleh kesempatan yang sama untuk mengakses sistem keamanan digital yang dapat dipercaya serta perlindungan data yang memadai (Kurniawan, 2020).

Salah satu pendekatan yang dapat dilakukan Indonesia adalah dengan mengadaptasi regulasi internasional sambil mempertahankan unsur-unsur yang berlandaskan nilai-nilai Pancasila. Upaya ini termasuk memperkuat regulasi nasional, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), agar lebih tanggap terhadap ancaman siber berskala global (Akbar & Putra, 2014). Selain itu, dalam menghadapi ancaman siber di kawasan Asia Tenggara, negara-negara anggota ASEAN menjalin kerja sama. ASEAN Regional Forum (ARF), yang dibentuk oleh ASEAN pada tahun 1994, menjadi wadah diskusi mengenai isu politik dan keamanan di kawasan Asia Pasifik, termasuk keamanan digital.

Pada tahun 2008, pemerintah mengeluarkan UU ITE yang bertujuan melindungi pemanfaatan teknologi sekaligus mencegah penyalahgunaannya yang dapat merugikan individu, pelaku bisnis digital, maupun negara. Dalam bagian pendahuluan UU ITE 2008 dijelaskan bahwa perkembangan teknologi informasi, media, dan komunikasi telah mengubah perilaku masyarakat serta peradaban manusia secara global. Kemajuan ini memperluas hubungan antarnegara dan berdampak pada perubahan di bidang sosial, ekonomi, dan budaya.

Teknologi informasi membawa dampak yang bersifat ganda, yakni positif dan negatif. Di satu sisi, teknologi ini mendukung kemajuan peradaban dan peningkatan kesejahteraan masyarakat, namun di sisi lain, teknologi juga bisa digunakan sebagai alat untuk melakukan tindakan yang melanggar hukum. Dalam bagian kedua dari pendahuluan UU ITE, dijelaskan bahwa hukum siber (cyber law) merupakan aturan yang mengatur pemanfaatan teknologi informasi dan komunikasi, sedangkan hukum telematika adalah perpaduan dari hukum telekomunikasi, media, dan informatika. UU ITE tahun 2008 memperkenalkan kebijakan baru yang dikenal dengan istilah hukum siber atau hukum informatika.

Perlindungan Data Pribadi dalam Sistem Elektronik

Perkembangan teknologi komputer dan internet membawa kemudahan dalam kehidupan sehari-hari, namun juga menimbulkan tantangan baru, terutama dalam bentuk kejahatan siber. Di Indonesia, masalah seperti peretasan, pencurian identitas, dan penipuan daring semakin menjadi perhatian serius. Kejahatan siber ini memberikan dampak besar, mulai dari kerugian finansial hingga risiko terhadap privasi individu serta keamanan nasional (Arafat & Wirasto, 2024). Penanganan kebocoran data pribadi harus dilakukan melalui mekanisme hukum dengan prinsip keadilan yang bermartabat. Pelaku harus mendapat sanksi yang sesuai dengan tingkat pelanggaran, sedangkan korban berhak mendapatkan perlindungan dan keadilan. Selain itu, Indonesia memiliki Kitab Undang-Undang Hukum Acara Pidana (KUHA) yang bertujuan utama melindungi hak asasi manusia, termasuk hak kebebasan, kemerdekaan, kehormatan nama baik, dan kerahasiaan pribadi.

Penyelenggara sistem elektronik perlu meningkatkan keamanan demi mencegah terulangnya kasus serupa. Salah satu langkah penting dalam melindungi data pribadi adalah meningkatkan kesadaran masyarakat tentang pentingnya pemahaman teknologi di era digital. Edukasi ini bisa dilakukan dengan mengajarkan pentingnya penggunaan PIN atau metode pengamanan lain pada perangkat seperti ponsel dan laptop, serta menghindari penggunaan data pribadi seperti nama lengkap dan tanggal lahir saat membuat PIN atau kata sandi. Selain itu, masyarakat perlu dibimbing agar waspada dan menghindari mengakses situs web yang tidak jelas, tidak valid, atau mencurigakan guna mencegah kebocoran data.

Tantangan dalam Implementasi Regulasi Keamanan Siber di Indonesia

Di Indonesia, berbagai bentuk kejahatan siber telah diatur melalui sejumlah undang-undang dan peraturan yang dibuat untuk mengatasi berbagai tindak kriminal yang menggunakan media digital. Sejak awal tahun 2000-an, perkembangan teknologi informasi dan internet di Indonesia berlangsung sangat cepat, namun regulasi yang mengatur transaksi digital, perlindungan data pribadi, serta penegakan hukum terhadap kejahatan siber belum ada secara memadai (Tobing et al., 2024).

Menanggapi kebutuhan tersebut, pada tanggal 21 April 2008 disahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ini menjadi peraturan pertama di Indonesia yang secara khusus mengatur pemanfaatan teknologi informasi, termasuk transaksi elektronik, perlindungan data pribadi, dan ketentuan hukum untuk penanganan kejahatan siber. Sejak diberlakukan, UU ITE menjadi dasar hukum utama dalam penanganan kasus kejahatan siber di Indonesia.

Pembahasan

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 30 mengatur bahwa: 1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun. 2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. 3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk mendapatkan Dokumen Elektronik atau Informasi Elektronik.

Ada beberapa tantangan dalam menyelaraskan hukum nasional dengan standar internasional, yaitu: 1) Kesenjangan Regulasi: Beberapa jenis kejahatan siber seperti spamming dan serangan ransomware belum sepenuhnya diatur dalam UU ITE. 2) Tantangan Teknis dan Kelembagaan: Kapasitas penegakan hukum yang masih lemah dalam menghadapi serangan siber lintas negara. 3) Isu Kedaulatan Digital: Pengaruh regulasi global terhadap kebijakan domestik sering kali memunculkan dilema antara kepentingan nasional dan kewajiban internasional. 4) Kurangnya Kesadaran Masyarakat: Masih

rendahnya memahami pentingnya keamanan siber dan perlindungan data pribadi bagi masyarakat. 5) Ketidakadilan Sosial: Sejarah mengatakan bahwa perlawanan antar suku bangsa dalam satu negara terjadi, pun halnya terjadi di Negara Indonesia yang seringkali dipicu oleh ketidakadilan sosial. Karena itu bisa dikatakan bahwa permasalahan ini dapat melemahkan bahkan mematikan persatuan bangsa.

Pada tahun 2021, Indonesia mengalami sejumlah insiden kebocoran data yang melibatkan berbagai instansi pemerintah, lembaga pelayanan publik, serta sektor swasta yang menyimpan data pribadi warga. Salah satu serangan besar dilaporkan berasal dari kelompok peretas asal China bernama Mustang Panda, yang berhasil menembus sistem keamanan sekitar 10 kementerian/lembaga, termasuk Badan Intelijen Negara (BIN). Kelompok ini dikenal sering menargetkan negara-negara di Asia Tenggara, menurut laporan lembaga keamanan siber The Record dari Insikt Group (Pedrason, 2021).

Pendekatan pemerintah yang masih bersifat sektoral dinilai belum efektif dalam mengatasi kebocoran data. Oleh karena itu, dorongan kuat muncul untuk segera merumuskan undang-undang yang komprehensif, seperti Undang-Undang Keamanan dan Ketahanan Siber, yang dapat memberikan panduan jelas dalam penyusunan kebijakan siber dan memperkuat posisi Indonesia dalam kedaulatan data. Penanggulangan kejahatan siber juga memerlukan partisipasi aktif masyarakat agar aparat penegak hukum dapat menjalankan tugas sesuai ketentuan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi landasan hukum penanganan kejahatan digital (Panggabean & Jamba, 2020).

Selain itu, pusat data milik perusahaan swasta yang mengelola data pribadi warga harus rutin diperiksa dan berada dalam wilayah hukum Indonesia agar negara memiliki kontrol yuridis yang kuat terhadap data tersebut. Peningkatan kesadaran masyarakat mengenai keamanan data akan memperkuat kemampuan warga dalam melindungi data pribadinya. Mengingat data memiliki nilai strategis yang tinggi, perlindungan data harus menjadi prioritas utama. Jadi, penguatan kapasitas masyarakat akan berkontribusi besar terhadap pembentukan kedaulatan data dan keamanan siber nasional Indonesia.

SIMPULAN

Penelitian ini menegaskan pentingnya pengembangan regulasi keamanan siber yang tidak hanya mengacu pada standar internasional, tetapi juga berlandaskan nilai-nilai Pancasila sebagai dasar negara Indonesia. Dengan pesatnya perkembangan dunia digital dan meningkatnya ancaman kejahatan siber, Indonesia perlu memperkuat sistem hukum siber yang responsif terhadap ancaman global, sekaligus menjaga kepentingan nasional dan hak asasi manusia. Harmonisasi antara hukum nasional dan hukum internasional menjadi kunci utama dalam menghadapi tantangan keamanan siber saat ini. Untuk itu, beberapa rekomendasi yang dapat diambil untuk memperkuat regulasi dan penegakan hukum siber di Indonesia yaitu peningkatan Kapasitas Penegakan Hukum: Meningkatkan keterampilan dan kapabilitas aparat penegak hukum dalam menangani kejahatan siber, terutama yang bersifat lintas negara, agar penanganan kasus menjadi lebih efektif dan efisien.

REFERENSI

- Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13(2), 222–238. <https://doi.org/10.22212/jp.v13i2.3299>
- Akbar, O. :, & Putra, K. (2014). Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional. In *Jurnal Ilmu Hukum*.
- Arafat, M., & Wirasto, A. T. E. (2024). *Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus*

- di Indonesia. 1(2), 221–241. <https://doi.org/10.5281/Zenodo.4766614>
- Ariyani, N., Fauzi, A., & Umar, F. (2020). Model hubungan aktor pemangku kepentingan dalam pengembangan potensi pariwisata Kedung Ombo. *Jurnal Ekonomi Dan Bisnis*, 23(2), 357–378.
- Ashfiya Nur Atqiya, Ahmad Muhamad Mustain Nasoha, Cahya Juwanti Arum Sari, Nurmi Syahidah, & Rifky Azuan Syahlevi. (2024). Kewarganegaraan dan Hak Asasi Manusia : Perspektif Hukum Nasional dan Hukum Islam. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora*, 2(1), 28–52. <https://doi.org/10.62383/humif.v2i1.943>
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, 3, 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Katiandagho, F. G. O. (2020). Aspek Hukum Pengelolaan Pembangunan Wilayah Pesisir Dan Pulau-Pulau Kecil Terluar Menurut Undang-Undang Nomor 1 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 27 Tahun 2007 Tentang Pengelolaan Wilayah Pesisir Dan Pulau-Pulau Kecil. *Lex Et Societatis*, 8(1), 97–108. <https://doi.org/10.35796/les.v8i1.28476>
- Kuntadi, K. (2022). House of Restorative Justice as a Forum of Actualizing the Nation's Culture in Solving Criminal Cases. *Jurnal Dinamika Hukum*, 22(2), 323–333. <https://doi.org/10.20884/1.JDH.2022.22.2.3242>
- Kurniawan, R. (2020). Implementasi Kebijakan Keamanan Aset Tanah Milik Pemerintah Kota Semarang Berdasarkan PP No 27 Tahun 2014. *Syntax Literate; Jurnal Ilmiah Indonesia*, 5(5), 145. <https://doi.org/10.36418/syntax-literate.v5i5.1103>
- Lestari, M., & Finaldin, T. (2023). Kerja Sama Antara Indonesia Dan Negara-Negara Di Asia Tenggara Melalui Asean Regional Forum Dalam Bidang Keamanan Siber. *Global Mind*, 4(2), 27–42. <https://doi.org/10.53675/jgm.v4i2.987>
- Madya, A. D., Haryanto, B. D., Ningsih, D. P., & Sinlae, F. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *Indonesian Journal of Education And Computer Science*, 1(3), 127–135. <https://doi.org/10.60076/indotech.v1i3.236>
- Nirwana, D., Nurjannah, E., Marpaung, C. R. A., & Wijaya, H. A. (2024). Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital. *JiIP - Jurnal Ilmiah Ilmu Pendidikan*, 7(7), 7364–7373. <https://doi.org/10.54371/jiip.v7i7.4790>
- Panggabean, E., & Jamba, P. (2020). Kebijakan Hukum Pidana Terkait Sanksi Pidana Bagi Pelaku Kejahatan Siber Di Indonesia. 60–67.
- Pedrasan, R. P. R. (2021). *Tantangan Intelijen di Papua Menghadapi Evolusi Gerakan Papua Merdeka*. Jakad Media Publishing.
- Purwaningsih, M. R. (2022). Pelaksanaan Musrenbang Daerah Dalam Proses Perencanaan Dan Penganggaran Partisipatif. *Jurnal Litbang Sukowati : Media Penelitian Dan Pengembangan*, 6(1), 151–164. <https://doi.org/10.32630/sukowati.v6i1.346>
- Rahman Najwa, F. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum*, 2(1), 8–16. <https://doi.org/10.32520/albahts.v2i1.3044>
- Risdiany, H., & Dewi, D. A. (2021). Penguatan Karakter Bangsa Sebagai Implementasi Nilai-Nilai Pancasila. *Jurnal Pendidikan Indonesia*, 2(04), 696–711.
- Ristanti, Y. D. (2015). Undang-Undang Otonomi Daerah Dan Pembangunan Ekonomi Daerah. *Jurnal Riset Akutansi Keuangan*, 2(2), 115–122.
- Sumantri, I. (2022). Reorientasi reformasi birokrasi dan good governance dalam penyelenggaraan sektor publik di Indonesia. *PAPATUNG: Jurnal Ilmu Administrasi Publik, Pemerintahan Dan Politik*, 5(2), 63–72.
- Tobing, C. I., Surya, T. M., Selvias, L. R., Girsang, S. R., & Azzahra, P. B. (2024). *Globalisasi Digital Dan Cybercrime : Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas*. 10, 105–123.