

ANALISIS EFEKTIVITAS DAN TANTANGAN HUKUM INTERNASIONAL DALAM PENANGGULANGAN KEJAHATAN SIBER LINTAS NEGARA SECARA GLOBAL

Heryanto Kawisen, Rafael Agrerio Firera, Alpon Siyus, Pelagia Melati

Teknik Informatika, Universitas Bina Sarana Informatika

Jalan Abdul Rahman Saleh No.18, Bangka Belitung Laut, Kec. Pontianak Tenggara, Kota Pontianak

Heryantokawisen2003@gmail.com

ABSTRAK

Kemajuan teknologi informasi telah menghadirkan tantangan serius bagi sistem hukum internasional, khususnya dalam menghadapi kejahatan siber yang melintasi batas yurisdiksi negara. Hal ini menimbulkan permasalahan hukum karena pelaku dapat beroperasi melintasi batas negara tanpa terikat oleh aturan wilayah tertentu, sehingga menyulitkan proses penegakan hukum. Penelitian ini bertujuan untuk mengevaluasi efektivitas instrumen hukum internasional, seperti Konvensi Budapest, dalam menangani kejahatan siber lintas negara serta mengkaji hambatan-hambatan yang menghalangi implementasinya. Penelitian ini menggunakan pendekatan kualitatif dengan metode hukum normatif, melalui studi literatur terhadap regulasi nasional dan internasional yang relevan. Hasil temuan menunjukkan bahwa meskipun sudah terdapat upaya global dalam bentuk kerja sama internasional, efektivitas pelaksanaannya masih terbatas. Faktor-faktor seperti belum meratanya ratifikasi, ketimpangan teknologi antarnegara, dan perbedaan kepentingan nasional menjadi penghambat utama. Oleh karena itu, diperlukan penguatan kolaborasi antarnegara serta harmonisasi hukum yang disertai kesiapan infrastruktur dan sumber daya manusia agar sistem hukum internasional dapat merespons ancaman siber secara lebih optimal.

Kata kunci : *Hukum Internasional,Kejahatan Siber,Kolaborasi Global,Regulasi Digital,Teknologi Informasi*

1. PENDAHULUAN

Kemajuan dalam teknologi informasi dan komunikasi telah menyebabkan tantangan baru untuk sistem hukum, terutama ketika berhadapan dengan perubahan ruang digital. Cybercrime adalah ancaman global yang saat ini tidak dikenali oleh pembatasan teritorial. Peretas dapat mengambil tindakan dari mana saja dan dari mana saja dapat berurusan dengan sistem di negara lain tanpa bergerak secara fisik. Kondisi ini tidak hanya mempengaruhi aspek tanggung jawab negara, tetapi juga mengarah pada kompleksitas hukum, dan menguji sejauh mana efektivitas mekanisme hukum internasional dapat menanggapi hal ini.

Berbeda dengan bentuk kejahatan tradisional, kejahatan dunia maya membutuhkan pendekatan hukum yang dapat mengikuti dinamika pengembangan teknologi. Namun, sejauh ini, belum ada keseragaman standar hukum untuk formulasi dan pengobatan kejahatan dunia maya. Ketidaksetaraan ini sering kali merupakan hambatan bagi penegakan hukum internasional dan mencakup mekanisme ekstradisi pelaku kejahatan dunia maya lintas negara. Sebagai bentuk respons terhadap persoalan ini, hukum internasional telah memperkenalkan sejumlah instrumen, salah satunya adalah Konvensi Budapest mengenai Kejahatan Siber. Meski begitu, penerapan konvensi ini masih menghadapi tantangan, utamanya karena belum seluruh negara terutama negara-negara berkembang melakukan ratifikasi dan implementasi secara konsisten. Di sisi lain, kerja sama antarnegara dalam memberantas kejahatan siber pun belum optimal karena adanya hambatan teknis, perbedaan kepentingan politik, serta sensitivitas terhadap isu kedaulatan.

Penelitian ini bertujuan untuk menganalisis efektivitas kerangka hukum internasional dalam mengatasi kejahatan siber lintas negara, serta mengeksplorasi tantangan dalam implementasi dan penegakan hukum tersebut. Fokus penelitian mencakup kerja sama antarnegara, hambatan hukum dan politik, serta peluang penguatan sistem hukum internasional yang lebih responsif terhadap ancaman siber.

2. TINJAUAN PUSTAKA

2.1. Kejahatan Siber Lintas Negara

Kejahatan siber berkembang menjadi bentuk kriminalitas modern yang kompleks karena bergantung pada teknologi digital serta melibatkan interaksi antarjaringan lintas negara. Tidak seperti kejahatan konvensional, serangan siber dapat dilakukan lintas batas negara tanpa kehadiran fisik pelaku di lokasi kejadian. Perkembangan ini menghadirkan persoalan serius bagi sistem hukum yang berpijak pada batas wilayah negara. Peningkatan penetrasi internet di berbagai negara, termasuk Indonesia, turut memperbesar risiko kejahatan digital seperti peretasan data dan gangguan terhadap infrastruktur strategis.

2.2. Peran dan Tantangan Hukum Internasional

Hukum internasional telah mencoba merespons ancaman kejahatan siber melalui berbagai instrumen, seperti Konvensi Budapest tentang Kejahatan Siber yang menjadi acuan global dalam kerja sama penegakan hukum di dunia maya. Namun, efektivitas konvensi ini masih menjadi perdebatan karena belum semua negara melakukan ratifikasi, terutama negara-negara berkembang yang memiliki keterbatasan

sumber daya. Selain itu, perbedaan kepentingan nasional, sistem hukum, dan sensitivitas terhadap isu kedaulatan membuat kerja sama internasional dalam bidang ini berjalan kurang optimal.

2.3. Upaya Penanggulangan dan Regulasi Nasional

Di Indonesia, penanggulangan kejahatan siber telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengalami revisi pada tahun 2016. Undang-undang ini bertujuan melindungi masyarakat dari penyalahgunaan teknologi informasi, serta memberikan dasar hukum untuk menindak pelaku kejahatan digital. Meski demikian, regulasi ini masih menghadapi berbagai tantangan seperti multitafsir pada pasal-pasal tertentu dan keterbatasan dalam mekanisme penegakan hukum di dunia maya.

2.4. Pentingnya Kerja Sama Internasional

Para pakar hukum berpendapat bahwa penanggulangan kejahatan siber secara efektif hanya dapat dicapai melalui kerja sama internasional yang kuat, terstruktur, dan berkelanjutan. Bentuk kolaborasi ini meliputi pertukaran informasi intelijen, penyeragaman kerangka hukum antarnegara, serta pembentukan institusi penegakan hukum yang memiliki otoritas untuk beroperasi lintas yurisdiksi. Efektivitas dari upaya ini sangat bergantung pada kecanggihan infrastruktur teknologi serta kemampuan sumber daya manusia di setiap negara dalam menghadapi dinamika kejahatan siber.

3. METODE PENELITIAN

Penelitian ini mengaplikasikan pendekatan kualitatif dengan menggunakan metode penelitian hukum normatif. Metode kualitatif adalah pendekatan penelitian yang berfokus pada pemahaman fenomena sosial melalui pengumpulan data non-numerik, seperti wawancara, observasi, dan analisis dokumen. Pendekatan kualitatif dipilih karena memungkinkan peneliti untuk melakukan pendalaman terhadap fenomena hukum yang kompleks, terutama dalam konteks kejahatan siber yang melintasi batas negara. Pendekatan ini lebih menitikberatkan pada pemahaman terhadap norma-norma hukum dan praktik internasional yang relevan.

Metode hukum normatif diterapkan untuk mengevaluasi norma-norma yang berlaku dalam hukum nasional dan internasional yang berkaitan dengan penanggulangan kejahatan siber. Metode ini berfokus pada analisis terhadap peraturan perundang-undangan, konvensi internasional, doktrin hukum, serta keputusan-keputusan pengadilan yang relevan. Tujuan dari pendekatan ini adalah untuk menilai sejauh mana norma-norma hukum tersebut efektif dalam mengatasi tantangan yang ditimbulkan oleh kejahatan siber lintas negara.

Dengan mengintegrasikan metode pendekatan kualitatif dan kajian literatur review penelitian ini diharapkan dapat memberikan pemahaman yang lebih menyeluruh dan mendalam mengenai topik yang sedang dibahas. Kombinasi ini tidak hanya memungkinkan peneliti untuk menghasilkan analisis yang komprehensif, tetapi juga memberikan kontribusi yang berarti terhadap pengembangan ilmu pengetahuan di bidang yang relevan.

4. HASIL DAN PEMBAHASAN

4.1. Data Trend Penggunaan Internet Dan Media Sosial Pada Tahun 2023 Secara Global.



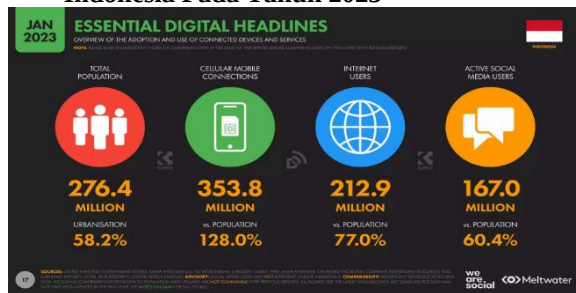
Gambar 1. Statistik Digital Dunia

Seiring dengan pesatnya perkembangan teknologi, pemanfaatan internet dan media sosial terlihat semakin meluas secara global pada tahun 2023. Platform-platform terkemuka seperti Facebook, Instagram, dan Twitter mencatat peningkatan jumlah pengguna aktif yang signifikan, menandai adanya pergeseran besar dalam pola komunikasi dan interaksi antarindividu. Akses internet yang semakin mudah dijangkau menjadi salah satu faktor utama yang mendorong perubahan ini. Dengan makin banyaknya orang yang terhubung ke internet, pola hubungan sosial menjadi lebih rumit, dinamis, serta melampaui batas geografis dan waktu.

Saat ini, cukup dengan beberapa sentuhan di layar, siapa pun dapat berkomunikasi dengan keluarga, teman, atau orang lain dari berbagai belahan dunia. Lebih jauh lagi, kehadiran internet telah membawa dampak besar dalam berbagai aspek kehidupan sosial, budaya, dan ekonomi di tingkat global. Berbagai aktivitas harian seperti berbelanja, belajar, bekerja, menikmati hiburan, hingga mengakses informasi kini semakin banyak dilakukan melalui platform digital. Hal ini memperlihatkan peran penting konektivitas digital dalam mendukung gaya hidup modern yang terus mengalami perubahan.

Visualisasi di bawah ini menyajikan data tentang tren serta perkembangan penggunaan internet, media sosial, dan berbagai aspek dunia digital di berbagai wilayah global sepanjang tahun 2023. Data tersebut menjadi bukti konkret dari transformasi digital yang tengah berlangsung pesat dan diperkirakan akan terus berkembang di masa depan.

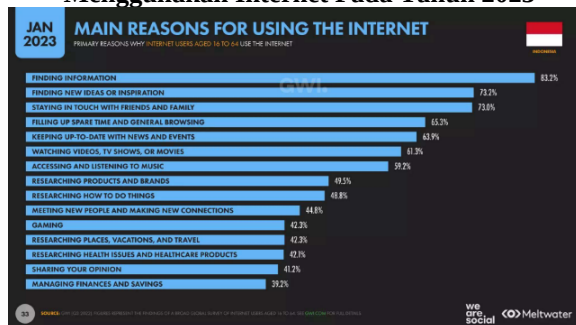
4.2. Tren Pengguna Internet Dan Media Sosial Di Indonesia Pada Tahun 2023



Gambar 2. Statistik Digital Indonesia

Berdasarkan laporan Indonesia Sosial Report 2023 yang dirilis oleh We Are Social bersama Meltwater, transformasi teknologi digital di Indonesia mengalami perkembangan yang pesat. Laporan ini memberikan informasi menyeluruh mengenai tingkat adopsi perangkat digital, akses internet, dan keterlibatan masyarakat dalam media sosial. Pada Januari 2023, jumlah penduduk Indonesia mencapai 276,4 juta jiwa. Jumlah koneksi perangkat seluler tercatat sebanyak 353,8 juta, yang berarti melebihi jumlah populasi dengan rasio 128%, mencerminkan kepemilikan beberapa perangkat oleh satu orang. Pengguna internet tercatat sebanyak 212,9 juta atau sekitar 77% dari total populasi, sedangkan pengguna aktif media sosial mencapai angka 167 juta jiwa atau 60,4%. Fakta ini menegaskan bahwa mayoritas masyarakat Indonesia telah terintegrasi dengan teknologi internet dan secara aktif menggunakan media sosial dalam aktivitas sehari-hari.

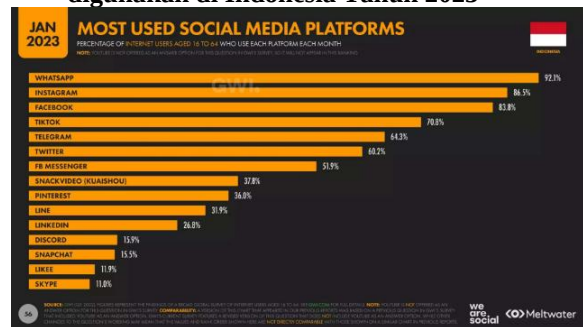
4.3. Alasan Utama Masyarakat Indonesia Menggunakan Internet Pada Tahun 2023



Gambar 3. Alasan Penggunaan Internet

Menurut data menurut Indonesian Sosial Report 2023, secara umum masyarakat Indonesia memanfaatkan internet untuk banyak sekali keperluan sehari-hari. Sekitar 83,2% pengguna berakibat internet menjadi wahana primer untuk mencari informasi. Sementara itu, 73,2% menggunakannya untuk mendapatkan inspirasi dan ide-ide baru. Serta, 73,% responden menggunakan internet untuk berkomunikasi dengan keluarga dan orang-orang terdekat sedangkan sisanya sekitar 65,3% menggunakannya sebagai media hiburan untuk mengisi waktu luang.

4.4. Platform Media Sosial yang Banyak digunakan di Indonesia Tahun 2023



Gambar 4. Platform Media Sosial Populer

Pada tahun 2023, penggunaan platform media sosial di Indonesia menunjukkan tren peningkatan yang signifikan. WhatsApp menduduki posisi teratas sebagai aplikasi yang paling banyak digunakan, dengan 92,1% dari total populasi pengguna, mengalami kenaikan dari 88,7% pada tahun sebelumnya. Instagram juga mencatatkan angka yang lebih tinggi, yaitu sekitar 86,5% pengguna, meningkat dari 84,8% pada tahun sebelumnya. Facebook mengalami sedikit kenaikan dari 81,3% menjadi 83,8%. sementara itu TikTok menunjukkan lonjakan pengguna yang mencolok, naik dari 63,1% menjadi 70,8% dari total populasi.

4.5. Jumlah Serangan Siber Di Indonesia (2019-2023)



Gambar 5. Jumlah Serangan Siber

Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa Indonesia mengalami ratusan juta serangan siber setiap tahunnya, dengan ancaman yang tidak hanya datang dari dalam negeri, tetapi juga dari luar negeri. Ada tahun sebelumnya, jumlah serangan siber yang ditujukan ke Indonesia mencapai 279,84 juta. Meskipun jumlah tersebut masih tinggi, angka ini menunjukkan penurunan sebesar 24,4% dibandingkan tahun sebelumnya yang mencatatkan 370,02 juta serangan. Sebagian besar serangan siber berasal dari Inggris, dengan total 59,73 juta serangan pada 2023, diikuti oleh Amerika Serikat yang mencatatkan 38,69

juta serangan. China berada di urutan berikutnya dengan total 20,56 juta serangan, sedangkan Prancis melancarkan sekitar 19,27 juta serangan ke Indonesia.

Di dalam negeri, Jakarta tercatat sebagai provinsi yang paling banyak menerima serangan siber pada 2023, dengan jumlah mencapai 100,98 juta atau sekitar 36,08% dari total serangan siber nasional. Riau berada di posisi kedua dengan 72,93 juta serangan, sementara Jawa Tengah juga tercatat mengalami jumlah serangan siber yang sama, yaitu 72,93 juta.

F. Undang-Undang Di Indonesia Yang Mengatur Tentang Siber Crime

Di Indonesia, regulasi mengenai kejahatan siber diatur secara komprehensif dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Undang-Undang ITE berperan sebagai dasar hukum yang mengatur penggunaan teknologi informasi dan aktivitas digital di Indonesia. Melalui regulasi ini, pemerintah berupaya membentuk kerangka hukum yang dapat melindungi masyarakat dari potensi penyalahgunaan teknologi serta mengatur interaksi elektronik secara tertib dan sah menurut hukum.

Regulasi ini menetapkan berbagai ketentuan untuk meniadakan aktivitas terlarang di dunia maya, termasuk tindakan merusak reputasi seseorang, menyebarkan konten yang bertentangan dengan hukum, serta melanggar hak privasi individu. Tujuan utamanya adalah membangun lingkungan digital yang aman dan tertib bagi seluruh pengguna.

Beberapa ketentuan penting dalam UU ITE antara lain:

- a. Pasal 27: Melarang pendistribusian, transmisi, atau penyediaan akses terhadap konten elektronik yang mengandung unsur penghinaan atau pencemaran nama baik, yang menjadi dasar penindakan terhadap tindak pidana serupa di internet.
- b. Pasal 28: Berisi ketentuan yang melarang penyebaran konten informasi yang bersifat manipulatif, menimbulkan kesalahpahaman, mengandung unsur intimidasi, atau berpotensi menciptakan ketakutan dan keresahan di tengah masyarakat.
- c. Pasal 29: Melarang setiap individu untuk masuk atau mengakses sistem elektronik milik pihak lain tanpa memperoleh izin terlebih dahulu, karena dianggap sebagai pelanggaran terhadap hak akses yang sah.
- d. Pasal 31: Mengatur mengenai kegiatan penyadapan komunikasi elektronik, termasuk pembatasan terhadap pelaksanaannya oleh pihak tertentu.
- e. Pasal 45 sampai Pasal 52: Mengatur ketentuan pidana bagi individu yang terbukti melakukan tindak kejahatan siber, dengan sanksi yang

beragam, mulai dari pemberian denda administratif hingga pidana penjara, tergantung pada tingkat pelanggaran yang dilakukan.

Revisi melalui UU No. 19 Tahun 2016 dilakukan untuk menyesuaikan sejumlah ketentuan dengan dinamika dan kemajuan teknologi. Perubahan signifikan tersebut mencakup:

- a. Pasal 27: Menegaskan bahwa pencemaran nama baik merupakan delik aduan, sehingga tindakan hukum hanya dapat dilakukan jika ada pengaduan dari korban.
- b. Pengurangan hukuman pidana, di mana beberapa pelanggaran seperti pencemaran nama baik mengalami penurunan ancaman hukuman penjara dari 6 tahun menjadi 4 tahun.
- c. Hak untuk dilupakan (Right to be Forgotten) mengizinkan seseorang untuk meminta penghapusan data atau informasi elektronik yang sudah tidak relevan atau berpotensi merugikan dirinya secara pribadi.
- d. Peningkatan kewenangan pemerintah, khususnya dalam mengendalikan dan memutus akses terhadap konten-konten yang dianggap melanggar hukum.

4.6. Tujuan Dan Ruang Lingkup Undang-Undang ITE

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016, bertujuan membangun pijakan hukum yang kokoh dalam pemanfaatan sistem informasi serta pelaksanaan aktivitas digital berbasis elektronik di Indonesia. Undang-undang ini dirancang untuk melindungi pengguna internet dari berbagai bentuk kejahatan siber, memberikan kepastian hukum dalam transaksi yang dilakukan secara elektronik, serta mengatur hak dan kewajiban para pihak yang UU ITE mengatur berbagai aspek dalam aktivitas digital, termasuk ketentuan mengenai pengelolaan informasi serta interaksi digital ruang elektronik, transaksi elektronik, serta tindakan pidana yang berkaitan dengan penyalahgunaan teknologi informasi.

Undang-undang ini juga memberikan perlindungan terhadap data pribadi dan informasi yang disimpan atau diproses melalui sistem elektronik. Oleh karena itu, UU ITE tidak semata-mata ditujukan untuk memberantas tindak kejahatan di ranah digital, UU ITE juga menjadi dasar dalam menciptakan ruang daring yang aman dan dapat diandalkan bagi masyarakat. Perubahan dalam undang-undang ini dilakukan sebagai respons terhadap dinamika kemajuan teknologi yang terus bertransformasi dan arus globalisasi, sehingga dapat menjawab kebutuhan hukum masyarakat di tengah kemajuan era digital.

4.7. Upaya Pencegahan Kejahatan Siber Lintas Negara

Dalam dunia digital yang terus berubah, ancaman kejahatan cyber lintas negara menjadi salah satu tantangan terbesar bagi keamanan cyber global. Serangan yang terorganisir membutuhkan langkah-langkah pencegahan untuk melindungi data dan sistem informasi. Langkah penting yang perlu dilakukan adalah meningkatkan kerja sama internasional antarnegara dalam berbagi informasi dan teknologi terkait keamanan cyber. Kerja sama ini tidak hanya melibatkan pertukaran data intelijen terkait berbagai ancaman, tetapi juga mencakup kolaborasi dalam pengembangan teknologi keamanan dan penegakan hukum, serta penyelenggaraan pendidikan dan pelatihan bagi para profesional di bidang teknologi informasi.

Menggunakan teknologi canggih seperti kecerdasan buatan (AI) dalam mendeteksi dan merespons ancaman adalah strategi yang efektif. AI mampu mendeteksi pola serangan, mengamati kejanggalan dalam lalu lintas jaringan, serta memberikan rekomendasi untuk memperbaiki pengelolaan sistem. Dengan kemampuannya untuk belajar dari data, AI akan membantu mendeteksi serangan yang belum pernah terjadi sebelumnya dan merespons insiden dengan cepat. Selain itu, pemerintah harus menetapkan undang-undang dan kebijakan yang sesuai untuk menjaga keamanan siber.

Memperkuat hukum terhadap kejahatan siber harus menjadi prioritas, begitu juga dengan menciptakan sistem hukum yang dapat menanggapi tantangan baru yang muncul dari perkembangan teknologi. Contoh Undang-Undang internasional yang penting adalah Konvensi Budapest tentang kejahatan siber, perjanjian internasional pertama yang secara komprehensif mengatur kejahatan siber. Perjanjian ini membentuk dasar untuk kerja sama dalam penyelidikan kejahatan dunia maya, serta secara bersamaan mempromosikan kepatuhan terhadap undang-undang domestik dan standar global.

Selain itu, beberapa negara telah menandatangani perjanjian bersama untuk mendukung pencegahan kejahatan siber serta pertukaran informasi. Contohnya, banyak negara anggota Uni Eropa aktif memperkuat kerja sama keamanan siber melalui berbagai inisiatif dan proyek kolaboratif. Dengan menggabungkan semua upaya ini kerja sama internasional, pendidikan dan pelatihan, penggunaan teknologi canggih seperti AI, serta regulasi yang kuat diharapkan kita dapat menciptakan lingkungan yang lebih aman dari ancaman kejahatan siber. Pendekatan terpadu ini tidak hanya akan memperkuat pertahanan siber di masing-masing negara, tetapi juga meningkatkan ketahanan global terhadap serangan siber yang semakin canggih serta dapat menjawab kebutuhan hukum masyarakat di tengah kemajuan era digital.

5. KESIMPULAN DAN SARAN

Upaya penegakan hukum dalam ranah kejahatan siber lintas negara masih menghadapi berbagai kendala seperti belum selarasnya proses adopsi hukum di setiap negara, adanya perbedaan prioritas nasional, dan hambatan teknis dalam membentuk kolaborasi internasional yang solid. Meski demikian, pemanfaatan teknologi seperti kecerdasan buatan, pembaruan regulasi nasional, dan kolaborasi global menjadi peluang penting untuk memperkuat sistem hukum yang adaptif dan responsif terhadap ancaman siber di era digital.

DAFTAR PUSTAKA

- [1] Azzahrah et al., (2024) Aini, N. and Lubis, F., 2024, Tantangan Pembuktian Dalam Kasus Kejahatan Siber, *Judge J. Huk.*, 05 (02), 55–63.
- [2] Pangestika, E.Q., Siregar, A., Sari, D.K., and Nurfajriani, Y.A., 2024, Penerapan Prinsip Hukum Internasional dalam Penegakan Hukum terhadap Kejahatan Siber dan Serangan Siber, *Rev. Pendidik. dan Pengajaran*, 9 (1), 75–84.
- [3] riyaningsih, S., Andrianto, A.A., Kusuma, A.S., and Prastyanti, R.A., 2023, Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia, *Justisia J. Ilmu Huk.*, 1 (1), 1–11.
- [4] Azzahra, N.S., Tambunan, A.M., Aulia, N.N., Binarsih, A., and Saepudin, T.H., 2024, Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan, *Humanit. J. Humaniora, Sos. dan Bisnis*, 2 (7), 692–700.
- [5] Azzahrah, B.T., Naufal, M., Hamdi, R., Raynee, R., and Layla, Z., 2024, Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi, *J. Pendidik. Tambusai*, 8 (2), 23934–23943.
- [6] Berlianti, D.F., Abid, A. Al, and Ruby, A.C., 2024, Penerapan Prinsip Hukum Internasional Dalam Penegakan Hukum Terhadap Kejahatan Siber Dan Serangan Siber, 7, 1861–1864.
- [7] Tobing, C.I., Surya, T.M., Selvias, L.R., and Ahmad, A., 2024, Globalisasi Digital dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas, *J. Hukum Sasana*, 10 (2), 112–124.
- [8] Dinda, A.L.S., 2024, Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia, *Al-Dalil J. Ilmu Sos. Polit. dan Huk.*, 2 (2), 65–72.
- [9] Habibi, M.R. and Liviani, I., 2020, Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia, *Al-Qanun J. Pemikir. dan Pembaharuan Huk. Islam*, 23 (2), 400–426.
- [10] Hapsari, R.D. and Pambayun, K.G., 2023, ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis, *J. Konstituen*, 5 (1), 1–17.

- [11] Alharun, S.J., 2025, Perbandingan Hukum Tindak Pidana Siber antara Indonesia dengan Singapura, *Causa J. Hukum dan Kewarganegaraan*, 11 (1), 55–63.
- [12] Zamayya, A.R.R., Wagiyanto, D.I., and Rahman, R.A., 2025, Kajian Teoritis Implikasi The United Nations Convention Against Cybercrime terhadap Pengaturan Tindak Pidana Siber Indonesia, *IKRA-ITH Humaniora*, 9 (2), 87–95.
- [13] Rusydi, M.T., 2025, Perbandingan Hukum Siber Indonesia dengan Negara ASEAN: Suatu Kajian Normatif, *J. Kolaboratif Sains*, 8 (1), 101–110