HAKIM
Jurnal Ilmu Hukum dan Sosial

LPPM Universitas Sains dan Teknologi Komputer
Vol. 3 No. 4 November 2025, Hal. 1471-1481
E-ISSN: 2987-7539; P-ISSN: 2987-6737
https://journal.stekom.ac.id/index.php/Hakim

International Norms on Cross-Border Data Protection in the Era of Global Cyber Threats

Maulana Fahmi Idris*[1]
[1] *Fakultas Studi Akademik, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia*
E-mail: Maulana@gmail.com

Article Info

Keywords:
Data Protection
Cross-Border Data Flows International Norms Cyber Threats
Regulatory Harmonization

Abstract

The rising volume of international data transfers in the modern digital era has created new cybersecurity threats that require improved legal frameworks for data protection. This study evaluates international norms by examining how global cyber threats operate in the present world. The research uses a normative juridical framework to analyze 32 international legal instruments and 45 scholarly articles published between 2018 and 2025 through both normative and comparative analytical methods. The study demonstrates that current regulatory systems are divided into separate parts, which are mostly controlled by non-binding rules that do not have standardized methods for enforcement and thus depend on each country's ability to enforce them, while international enforcement remains inadequate. The situation develops into a more severe problem because cyber threats now develop more advanced systems than existing rules can match. The research demonstrates the critical need for countries to establish uniform regulations while developing stronger compliance methods and building faster international partnership systems. The research presents a framework that connects international law and cybersecurity through a more extensive analytical approach.

DOI: *https://doi.org/10.51903/mypsh616*
Submitted: August 2025, Reviewed: September 2025, Accepted: October 2025
**Corresponding Author*

I. PENDAHULUAN

Perkembangan teknologi digital telah mendorong intensifikasi arus data lintas negara yang melampaui batas yurisdiksi teritorial, menjadikan data pribadi sebagai aset strategis yang sekaligus rentan terhadap ancaman siber seperti kebocoran dan penyalahgunaan informasi (Laksito et al., 2024; Putra et al., 2025). Peningkatan insiden pelanggaran data global dalam beberapa tahun terakhir menunjukkan dampak yang tidak hanya bersifat ekonomi, tetapi juga berkaitan dengan kedaulatan negara dan perlindungan hak asasi manusia, sehingga menuntut adanya kepastian hukum dalam tata kelola data lintas negara (Khan, 2025). Fenomena ini semakin kompleks seiring berkembangnya serangan siber yang bersifat terorganisir dan lintas yurisdiksi, sementara ketimpangan kapasitas keamanan digital antarnegara memperlemah efektivitas respons kolektif (Jampani, 2025). Kondisi tersebut menunjukkan bahwa norma internasional yang ada belum sepenuhnya mampu menjawab kebutuhan perlindungan data secara adaptif dalam lanskap ancaman global yang dinamis (Coche et al., 2024).

Sejumlah kajian telah membahas upaya harmonisasi regulasi perlindungan data melalui pendekatan regional dan internasional, termasuk peran instrumen hukum dan organisasi global dalam membentuk standar bersama (Xia et al., 2024). Literatur juga menyoroti kendala implementasi yang dipengaruhi oleh perbedaan sistem hukum, kepentingan nasional, serta tingkat kesiapan teknologi antarnegara, yang pada akhirnya menghasilkan tata kelola yang masih terfragmentasi (Marcucci et al., 2023). Meskipun demikian, sebagian besar studi masih berfokus pada aspek normatif tanpa menguji secara mendalam efektivitas penerapan norma dalam menghadapi ancaman siber aktual yang terus berkembang. Keterbatasan ini menunjukkan belum adanya integrasi analitis yang kuat antara perspektif hukum internasional dan dinamika keamanan siber global.

Berdasarkan kondisi tersebut, penelitian ini diarahkan untuk menganalisis secara kritis norma internasional dalam perlindungan data lintas negara dengan menempatkan ancaman siber global sebagai variabel utama dalam evaluasi efektivitasnya. Pendekatan ini diharapkan mampu menghasilkan kerangka analisis yang lebih terfokus dalam mengidentifikasi kelemahan struktural, khususnya pada aspek implementasi, koordinasi lintas yurisdiksi, dan mekanisme kepatuhan. Kebaruan penelitian ini terletak pada integrasi sistematis antara perspektif hukum internasional dan keamanan siber dalam satu kerangka analitis yang komprehensif tanpa memisahkan keduanya secara parsial. Dengan demikian, penelitian ini memberikan kontribusi teoritis dalam pengembangan kajian hukum internasional sekaligus menawarkan dasar praktis bagi perumusan kebijakan yang lebih adaptif, responsif, dan kontekstual terhadap tantangan perlindungan data global.

Berbeda dengan penelitian terdahulu yang umumnya hanya menelaah instrumen perlindungan data atau ancaman siber secara terpisah, penelitian ini menawarkan model evaluasi normatif berbasis empat dimensi analisis, yaitu prinsip perlindungan data, mekanisme transfer lintas negara, sistem kepatuhan, dan kapasitas penegakan hukum internasional. Melalui pendekatan tersebut, penelitian mampu mengidentifikasi kesenjangan antara perkembangan ancaman siber global dan kemampuan norma internasional dalam memberikan perlindungan yang efektif.

II. METODE PENELITIAN

A. Pendekatan Yuridis Normatif Dan Kerangka Analisis

Penelitian ini disusun dengan menggunakan pendekatan kualitatif berbasis hukum normatif yang menempatkan norma internasional sebagai objek utama kajian. Pendekatan ini dipilih karena penelitian berfokus pada analisis struktur, prinsip, dan daya ikat aturan hukum internasional yang tidak memerlukan pengujian empiris, melainkan penafsiran sistematis terhadap norma yang berlaku. Fokus analisis diarahkan pada bagaimana aturan-aturan global mengenai perlindungan data lintas negara dirumuskan, diinterpretasikan, dan diterapkan dalam menghadapi ancaman siber yang terus berkembang. Untuk memperdalam pembahasan, digunakan pendekatan konseptual guna menelaah prinsip-prinsip dasar yang melandasi regulasi tersebut, pendekatan perundang-undangan (*statute approach*) untuk mengkaji instrumen hukum yang berlaku, serta pendekatan perbandingan untuk

melihat perbedaan pengaturan antarrezim hukum. Melalui kerangka ini, penelitian tidak hanya memetakan norma yang ada, tetapi juga menilai relevansinya terhadap praktik aktual dalam tata kelola data global.

B. Klasifikasi Sumber Hukum Dan Strategi Pemilihan Data

Data penelitian terdiri atas 32 instrumen hukum internasional yang dipilih secara *purposive* berdasarkan relevansi terhadap perlindungan data lintas negara. Instrumen tersebut meliputi *Convention 108* dan *Convention 108+*, *OECD Privacy Guidelines 1980* dan revisinya tahun 2013, *APEC Privacy Framework*, *ASEAN Framework on Digital Data Governance*, *United Nations Guidelines for the Regulation of Computerized Personal Data Files*, *General Data Protection Regulation* (GDPR) sebagai rujukan global, *African Union Convention on Cyber Security* and *Personal Data Protection* (*Malabo Convention*), serta berbagai deklarasi, rekomendasi, dan pedoman internasional yang mengatur transfer data lintas batas, keamanan informasi, dan perlindungan privasi digital. Seluruh instrumen kemudian dibandingkan berdasarkan empat dimensi utama, yaitu prinsip perlindungan data, mekanisme transfer data lintas negara, sistem kepatuhan dan penegakan hukum, serta pengaturan kerja sama internasional dalam penanganan insiden siber (Tajik et al., 2024).

C. Proses Sistematis Pengumpulan Data Kepustakaan

Pengumpulan data dilakukan melalui penelusuran literatur secara terstruktur dengan memanfaatkan berbagai basis data ilmiah seperti *Scopus*, *Web of Science*, dan *HeinOnline*. Tahap awal dimulai dengan penentuan kata kunci yang relevan, kemudian dilanjutkan dengan proses penyaringan berdasarkan kualitas, reputasi jurnal, dan keterkaitan isi dengan fokus penelitian. Dokumen yang terpilih selanjutnya dikaji secara mendalam untuk mengidentifikasi informasi yang sesuai dengan kebutuhan analisis. Selain itu, data pendukung berupa laporan ancaman siber juga dikumpulkan untuk memberikan gambaran kontekstual terhadap penerapan norma hukum. Teknik ini mencerminkan metode studi kepustakaan yang sistematis dan dapat direplikasi dalam penelitian hukum (Pichlak et al., 2025).

D. Instrumen Penelitian Dan Dukungan Perangkat Analisis

Dalam penelitian ini, peneliti berperan sebagai instrumen utama yang menentukan arah dan kedalaman analisis. Untuk membantu proses pengolahan data, digunakan alat bantu berupa lembar kategorisasi yang memudahkan pengelompokan informasi berdasarkan tema tertentu. Selain itu, perangkat lunak seperti *Mendeley* atau *Zotero* dimanfaatkan dalam pengelolaan referensi agar lebih sistematis. Proses analisis data kualitatif juga didukung oleh aplikasi seperti *NVivo* atau *ATLAS.ti* untuk membantu pengkodean dan identifikasi pola tematik. Penggunaan perangkat tersebut mendukung konsistensi analisis dan meminimalkan bias dalam pengolahan data kualitatif (Dalkin et al., 2021).

E. Teknik Analisis Normatif Dan Komparatif

Analisis data dilakukan melalui beberapa tahapan yang saling berkaitan, dimulai dari penyaringan data hingga interpretasi hasil. Data yang telah terkumpul terlebih dahulu dipilih berdasarkan relevansi,

kemudian dikelompokkan ke dalam tema-tema utama yang mencerminkan fokus penelitian. Selanjutnya, dilakukan penafsiran terhadap hubungan antara norma hukum internasional dan dinamika ancaman siber global. Pendekatan perbandingan digunakan untuk melihat perbedaan pengaturan antarinstrumen hukum serta menilai efektivitasnya dalam konteks lintas negara. Teknik ini memungkinkan peneliti menghasilkan analisis yang tidak hanya bersifat deskriptif, tetapi juga kritis dan argumentatif (Polat, 2025).

F. Tahapan Pelaksanaan Penelitian Secara Sistematis

Pelaksanaan penelitian dilakukan secara bertahap agar alur kerja tetap terstruktur dan mudah ditelusuri. Tahap awal mencakup identifikasi masalah dan penentuan fokus kajian berdasarkan literatur awal yang relevan. Selanjutnya dilakukan pengumpulan dan seleksi data untuk memastikan hanya sumber yang sesuai yang dianalisis. Data yang telah dipilih kemudian diklasifikasikan dan dianalisis menggunakan pendekatan normatif dan komparatif sesuai dengan kerangka yang telah ditetapkan. Tahap akhir berupa penyusunan kesimpulan dan rekomendasi yang didasarkan pada hasil analisis secara menyeluruh, sehingga menghasilkan temuan yang dapat dipertanggungjawabkan secara akademik.

G. Prinsip Etika dalam Penggunaan Data Penelitian

Penelitian ini tetap memperhatikan aspek etika meskipun tidak melibatkan subjek manusia secara langsung. Seluruh sumber yang digunakan dipastikan berasal dari referensi yang kredibel dan dapat dipertanggungjawabkan secara akademik. Setiap kutipan dicantumkan secara tepat untuk menghindari pelanggaran integritas ilmiah. Selain itu, penggunaan data terkait ancaman siber dilakukan secara proporsional agar tidak menimbulkan kesalahan interpretasi atau bias terhadap pihak tertentu. Dengan menjaga prinsip objektivitas dan transparansi, hasil penelitian diharapkan memiliki tingkat kepercayaan yang tinggi.

III. HASIL DAN DISKUSI

Hasil

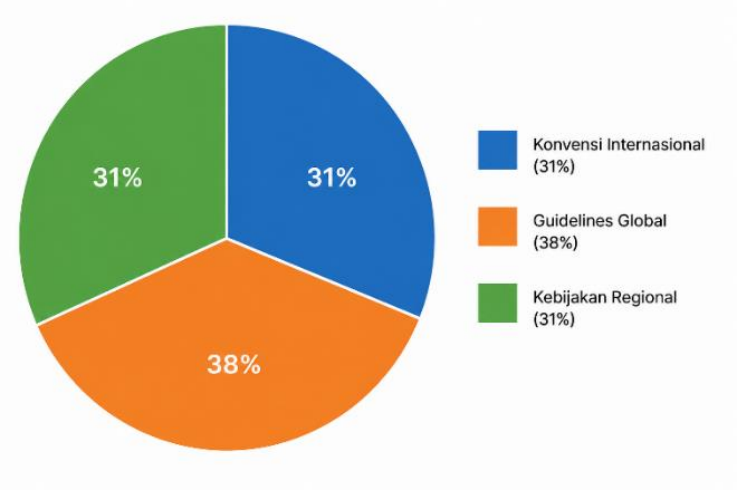
A. Distribusi dan Karakteristik Norma Internasional Perlindungan Data

Hasil pengolahan terhadap 32 dokumen hukum internasional dan 45 artikel ilmiah menunjukkan bahwa pengaturan perlindungan data lintas negara tersebar dalam berbagai instrumen dengan karakteristik yang berbeda. Norma yang tersedia umumnya berorientasi pada prinsip dasar tanpa disertai mekanisme implementasi yang seragam, sehingga belum membentuk sistem global yang terkoordinasi. Kondisi ini berdampak pada variasi penerapan di berbagai yurisdiksi, khususnya dalam merespons perkembangan ancaman siber yang semakin kompleks (Khan et al., 2024). Selain itu, literatur yang dianalisis memperlihatkan bahwa perkembangan ancaman digital berlangsung lebih cepat dibandingkan pembaruan norma yang ada (Radanliev, 2024). Sebagaimana ditunjukkan pada Tabel 1, distribusi instrumen hukum memperlihatkan dominasi pedoman global yang bersifat tidak mengikat, diikuti oleh konvensi internasional dan kebijakan regional dengan proporsi yang relatif seimbang.

Tabel 1. Klasifikasi Instrumen Hukum Perlindungan Data Internasional

No	Jenis Instrumen	Jumlah Dokumen	Karakteristik Utama
1	Konvensi Internasional	10	Mengikat secara hukum, cakupan terbatas
2	Pedoman/Guidelines Global	12	Tidak mengikat, bersifat rekomendatif
3	Kebijakan Regional	10	Variatif, tergantung sistem hukum regional
	Total	**32**	

Tabel menunjukkan bahwa sebagian besar norma berada pada kategori yang tidak mengikat, sehingga penerapannya sangat bergantung pada kebijakan nasional masing-masing negara. Kondisi ini mencerminkan belum adanya standar global yang seragam dalam perlindungan data lintas negara. Distribusi tersebut juga divisualisasikan dalam Gambar 1, yang memperlihatkan perbandingan proporsi antarjenis instrumen hukum.



Gambar 1. Distribusi Instrumen Hukum Internasional

Gambar menegaskan bahwa pedoman global memiliki proporsi terbesar dibandingkan dengan instrumen lainnya, sehingga pendekatan non-binding masih menjadi pola dominan dalam pengaturan internasional. Lebih lanjut, perkembangan ancaman siber lintas negara dapat diamati melalui tren yang dirangkum dalam Tabel 2.

Tabel 2. Tren Ancaman Siber Global (Berdasarkan Literatur 2018–2025)

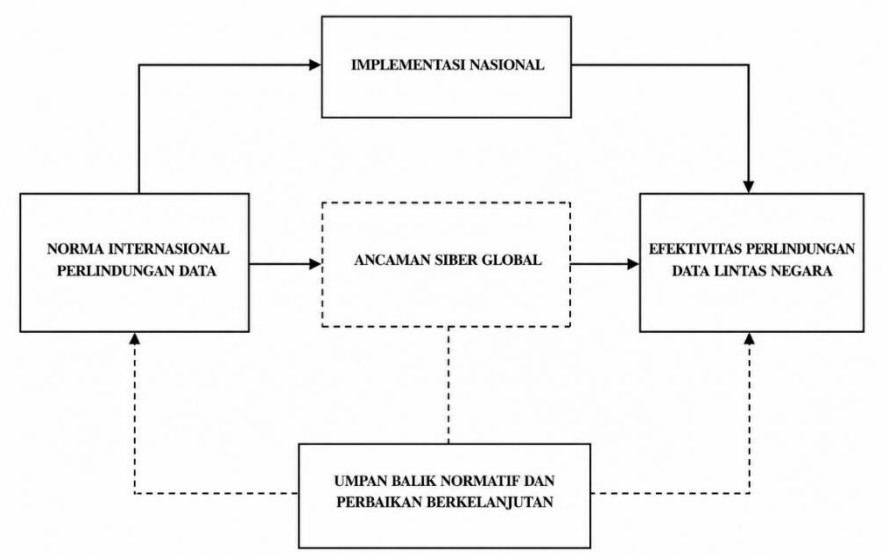
Tahun	Jumlah Pelanggaran Data Global (Juta Rekaman)	Sumber
2018	4.5 miliar	*IBM Security Report*
2020	37 miliar	*Risk Based Security*
2022	22 miliar	*Surfshark Data Breach Statistics*
2024	>35 miliar	*Verizon DBIR & IBM Report*

Data pada Tabel 2 tidak menunjukkan tingkat ancaman berdasarkan penilaian subjektif penulis, melainkan disusun berdasarkan laporan keamanan siber internasional yang mendokumentasikan jumlah pelanggaran data (*data breaches*) dan insiden keamanan informasi secara global. Penggunaan indikator jumlah pelanggaran data dipilih karena merupakan ukuran yang paling sering digunakan dalam literatur keamanan siber untuk menggambarkan peningkatan risiko terhadap perlindungan data lintas negara.

B. Temuan Berdasarkan Tujuan Penelitian

Hasil analisis menunjukkan bahwa struktur norma internasional perlindungan data didominasi oleh prinsip umum seperti perlindungan privasi, keamanan informasi, dan pengaturan transfer data lintas

batas. Prinsip-prinsip tersebut telah diadopsi secara luas, namun tidak seluruh instrumen menyediakan ketentuan operasional yang rinci, sehingga membuka ruang perbedaan interpretasi dalam penerapannya (Ribalta et al., 2024). Dalam aspek implementasi, ditemukan variasi antarnegara yang dipengaruhi oleh perbedaan sistem hukum, kesiapan teknologi, dan kapasitas kelembagaan (Judijanto, 2025). Variasi ini berdampak pada perbedaan tingkat penerapan norma dalam praktik. Sementara itu, koordinasi lintas yurisdiksi dalam penanganan pelanggaran data masih terbatas pada kerja sama regional dan bilateral, sehingga belum membentuk mekanisme global yang terpadu. Hubungan antarvariabel dalam penelitian ini divisualisasikan dalam Gambar 2.



Gambar 2. Kerangka Analisis Normatif Penelitian

Gambar 2 menunjukkan kerangka analisis normatif yang menggambarkan keterkaitan antara norma internasional, implementasi nasional, ancaman siber global, dan efektivitas perlindungan data. Kerangka ini dibangun berdasarkan kajian literatur hukum internasional, perlindungan data, dan tata kelola keamanan siber sebagai dasar dalam menganalisis efektivitas norma internasional terhadap perlindungan data lintas negara di tengah perkembangan ancaman siber global.

C. Pola Tematik Dalam Analisis Data

Hasil kategorisasi tematik terhadap seluruh sumber menunjukkan adanya pola isu yang muncul secara konsisten. Sebagaimana disajikan dalam Tabel 3, fragmentasi regulasi dan keterbatasan penegakan merupakan tema yang paling dominan.

Tabel 3. Hasil Kategorisasi Analisis Tematik

Tema Utama	Frekuensi Kemunculan	Keterangan
Fragmentasi Regulasi	Tinggi	Ditemukan di sebagian besar studi
Keterbatasan Penegakan	Tinggi	Tidak ada mekanisme global kuat
Ketimpangan Kapasitas	Sedang	Negara berkembang lebih rentan
Ancaman Siber Terorganisir	Tinggi	Tren dominan terbaru

Tabel 3 disusun berdasarkan analisis tematik terhadap 32 instrumen hukum internasional dan 45 artikel ilmiah. Analisis dilakukan melalui tiga tahap, yaitu *open coding* untuk mengidentifikasi isu utama terkait perlindungan data lintas negara, ancaman siber, kepatuhan hukum, dan kerja sama internasional; *axial*

coding untuk mengelompokkan isu yang memiliki kesamaan substansi; serta *selective coding* untuk menentukan tema yang paling dominan dan relevan dengan tujuan penelitian. Hasil analisis menghasilkan empat tema utama, yaitu fragmentasi regulasi, keterbatasan penegakan hukum, ketimpangan kapasitas nasional, dan meningkatnya ancaman siber terorganisir. Oleh karena itu, kategorisasi dalam tabel merupakan hasil sintesis sistematis dari seluruh sumber yang dianalisis, bukan semata-mata interpretasi subjektif penulis (Luo, 2022).

D. Ringkasan Temuan Utama Penelitian

Temuan utama penelitian ini menunjukkan bahwa norma internasional perlindungan data lintas negara masih tersebar dalam berbagai instrumen dengan tingkat kekuatan hukum yang berbeda (Jiang, 2025). Selain itu, efektivitas perlindungan sangat dipengaruhi oleh variasi implementasi di tingkat nasional (Buckley et al., 2024). Penelitian ini juga menemukan adanya perbedaan kapasitas antarnegara yang berdampak pada tingkat perlindungan data (Fitriani, 2024). Di sisi lain, perkembangan ancaman siber menunjukkan peningkatan kompleksitas yang signifikan. Kondisi tersebut berlangsung bersamaan dengan terbatasnya mekanisme koordinasi lintas negara dalam menangani pelanggaran data.

Diskusi

Hasil penelitian menunjukkan bahwa norma internasional dalam perlindungan data lintas negara belum membentuk sistem yang terintegrasi secara global karena masih didominasi oleh instrumen yang bersifat *non-binding*, sehingga tingkat kepatuhan negara lebih bergantung pada komitmen sukarela dibanding kewajiban hukum yang mengikat (Atanda-lawal & Onuchukwu, 2025). Kondisi ini menjelaskan adanya variasi implementasi di tingkat nasional, terutama dalam merespons ancaman siber yang berkembang cepat dan semakin kompleks (Rahimi et al., 2025). Selain itu, keterkaitan antara norma internasional, implementasi domestik, dan dinamika ancaman siber menunjukkan adanya kesenjangan antara perkembangan teknologi digital dengan adaptasi regulasi yang tersedia (Kour et al., 2024). Dengan demikian, efektivitas perlindungan data tidak hanya ditentukan oleh keberadaan prinsip hukum, tetapi juga oleh kapasitas implementasi dan koordinasi lintas yurisdiksi yang masih terbatas.

Analisis terhadap instrumen hukum internasional menunjukkan bahwa sebagian besar norma perlindungan data lintas negara dibangun berdasarkan prinsip-prinsip universal yang mencakup *lawfulness*, *fairness*, *transparency*, *purpose limitation*, data *minimization*, *accountability*, dan *security safeguards*. Prinsip-prinsip tersebut ditemukan secara konsisten dalam *Convention 108+*, *OECD Privacy Guidelines*, *GDPR*, maupun *APEC Privacy Framework*. Meskipun memiliki tujuan yang sama, instrumen-instrumen tersebut menunjukkan perbedaan dalam tingkat daya ikat hukum, mekanisme pengawasan, dan prosedur penegakan kepatuhan. *Convention 108+* dan *GDPR* memiliki mekanisme kepatuhan yang relatif lebih kuat dibandingkan instrumen berbasis *soft law* seperti *OECD Privacy Guidelines* dan *APEC Privacy Framework* yang bergantung pada komitmen sukarela negara peserta.

Selain perbedaan daya ikat hukum, penelitian juga menemukan bahwa persoalan yurisdiksi lintas negara masih menjadi hambatan utama dalam penegakan perlindungan data internasional. Pelanggaran data sering kali melibatkan pelaku, korban, penyedia layanan digital, dan lokasi penyimpanan data yang berada pada negara yang berbeda. Kondisi tersebut menyebabkan munculnya konflik yurisdiksi dan perbedaan standar perlindungan hukum yang mempersulit proses investigasi maupun penegakan hukum. Akibatnya, efektivitas norma internasional sangat dipengaruhi oleh kemampuan negara untuk membangun kerja sama lintas yurisdiksi yang efektif melalui mekanisme pertukaran informasi, bantuan hukum timbal balik, dan koordinasi antarotoritas perlindungan data. Temuan ini memperlihatkan bahwa tantangan utama perlindungan data global tidak hanya terletak pada keberadaan norma hukum, tetapi juga pada kesenjangan antara norma, kapasitas implementasi, dan mekanisme penegakan hukum internasional. Oleh karena itu, efektivitas perlindungan data lintas negara memerlukan kombinasi antara harmonisasi regulasi, peningkatan kapasitas kelembagaan nasional, dan penguatan mekanisme kepatuhan internasional yang mampu menjawab karakter ancaman siber yang semakin kompleks.

Temuan ini sejalan dengan penelitian sebelumnya yang menekankan adanya fragmentasi regulasi global sebagai hambatan utama dalam perlindungan data lintas negara, namun penelitian ini memperluas analisis dengan menempatkan ancaman siber sebagai variabel yang secara langsung memengaruhi efektivitas norma (Kuzio et al., 2022). Berbeda dengan studi terdahulu yang cenderung memisahkan aspek hukum dan keamanan siber, penelitian ini menunjukkan bahwa keduanya memiliki hubungan yang saling bergantung dan tidak dapat dianalisis secara terpisah (Kianpour, 2024). Selain itu, penelitian ini menegaskan bahwa ketimpangan kapasitas antarnegara bukan sekadar faktor pendukung, melainkan elemen utama yang menentukan tingkat keberhasilan penerapan norma internasional dalam praktik (Ko et al., 2024). Berbeda dengan penelitian sebelumnya yang umumnya hanya berfokus pada harmonisasi regulasi perlindungan data atau perkembangan ancaman siber secara terpisah, penelitian ini mengembangkan kerangka evaluasi normatif yang menghubungkan empat dimensi utama, yaitu norma internasional, implementasi nasional, ancaman siber global, dan efektivitas perlindungan data. Pendekatan tersebut memungkinkan identifikasi yang lebih komprehensif terhadap faktor-faktor yang menyebabkan kesenjangan antara perkembangan ancaman digital dan kemampuan instrumen hukum internasional dalam memberikan perlindungan yang efektif. Dengan demikian, kontribusi penelitian ini tidak hanya terletak pada integrasi dua bidang kajian, tetapi juga pada penyusunan kerangka analisis yang dapat digunakan untuk mengevaluasi efektivitas tata kelola perlindungan data lintas negara secara lebih sistematis (Leventopoulos et al., 2024).

Di sisi lain, temuan yang menunjukkan dominasi instrumen *non-binding* dalam konteks meningkatnya ancaman siber yang terorganisir menjadi indikasi adanya ketidaksesuaian antara kebutuhan global dan respons regulasi yang tersedia. Secara rasional, peningkatan risiko lintas negara seharusnya diikuti dengan penguatan norma yang mengikat, namun realitas menunjukkan bahwa negara tetap mempertahankan fleksibilitas regulasi demi menjaga kedaulatan dan kepentingan nasional. Kondisi ini

dapat dijelaskan oleh perbedaan sistem hukum, kepentingan ekonomi digital, serta sensitivitas data sebagai aset strategis yang memengaruhi posisi negara dalam negosiasi internasional. Oleh karena itu, dinamika politik global menjadi faktor penting yang membentuk arah perkembangan norma internasional, sehingga harmonisasi regulasi sulit dicapai secara menyeluruh.

Penelitian ini memberikan implikasi penting dalam pengembangan kajian hukum internasional, khususnya dengan menekankan bahwa efektivitas norma tidak dapat dilepaskan dari konteks teknologi dan kapasitas negara. Pendekatan yang mengintegrasikan aspek hukum dan keamanan siber menunjukkan bahwa kerangka normatif perlu bersifat adaptif terhadap perubahan ancaman digital yang cepat. Dalam praktiknya, hasil ini mengindikasikan perlunya penguatan kerja sama internasional yang lebih operasional serta peningkatan kapasitas teknis dan kelembagaan di tingkat nasional. Selain itu, perumusan kebijakan perlindungan data perlu mempertimbangkan keseimbangan antara fleksibilitas regulasi dan kepastian hukum agar dapat diterapkan secara efektif dalam konteks global yang dinamis.

Penelitian ini memiliki keterbatasan yang perlu diperhatikan, terutama karena menggunakan pendekatan normatif yang tidak melibatkan pengujian empiris secara langsung sehingga belum mampu mengukur efektivitas implementasi secara kuantitatif. Ketergantungan pada data sekunder juga berpotensi memengaruhi subjektivitas dalam interpretasi hasil, meskipun telah dilakukan seleksi sumber secara ketat. Selain itu, ruang lingkup analisis yang berfokus pada level internasional menyebabkan kurangnya pembahasan mendalam terkait praktik implementasi di tingkat negara tertentu. Faktor eksternal seperti dinamika politik dan ekonomi global juga belum dianalisis secara spesifik, padahal memiliki pengaruh terhadap pembentukan dan penerapan norma internasional.

Berdasarkan temuan yang diperoleh, penelitian selanjutnya disarankan untuk mengembangkan pendekatan empiris guna menguji efektivitas implementasi norma internasional dalam konteks yang lebih spesifik. Studi komparatif antarnegara dapat dilakukan untuk mengidentifikasi praktik terbaik dalam perlindungan data lintas negara. Selain itu, integrasi pendekatan interdisipliner yang melibatkan aspek teknologi, hukum, dan kebijakan publik perlu diperkuat agar menghasilkan analisis yang lebih komprehensif. Penelitian lanjutan juga dapat mengeksplorasi peran aktor non-negara dalam tata kelola data global sehingga mampu memberikan kontribusi yang lebih luas terhadap pengembangan norma internasional yang adaptif dan berkelanjutan.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa norma internasional perlindungan data lintas negara masih belum terintegrasi secara global dan belum efektif menghadapi ancaman siber yang terus berkembang. Hal ini disebabkan oleh dominasi instrumen non-binding, lemahnya mekanisme penegakan, serta terbatasnya koordinasi antarnegara. Perbedaan kapasitas dan implementasi di tingkat nasional juga memperbesar ketidakkonsistenan perlindungan data dalam praktik. Temuan ini menegaskan bahwa keberhasilan norma internasional tidak cukup bergantung pada prinsip hukum, tetapi sangat ditentukan oleh efektivitas implementasi, koordinasi lintas yurisdiksi, dan kesiapan infrastruktur keamanan digital.

Dengan menggabungkan perspektif hukum internasional dan keamanan siber, penelitian ini menawarkan kerangka analisis yang lebih utuh dalam melihat kelemahan tata kelola data global.

Sebagai rekomendasi kebijakan, penelitian ini mengusulkan pengembangan mekanisme *Mutual Legal Assistance for Data Protection* (MLADP) sebagai instrumen kerja sama lintas negara dalam investigasi dan penegakan hukum terhadap pelanggaran data pribadi. Selain itu, diperlukan peningkatan interoperabilitas antara berbagai rezim perlindungan data internasional seperti *GDPR*, *Convention 108+*, dan *APEC Privacy Framework* untuk mengurangi fragmentasi regulasi global. Pada tingkat kelembagaan, pembentukan forum koordinasi internasional yang secara khusus berfokus pada perlindungan data lintas negara dapat menjadi langkah strategis untuk memperkuat mekanisme kepatuhan, pertukaran informasi, dan penyelesaian sengketa antarnegara. Secara praktis, hasil penelitian ini menekankan perlunya harmonisasi regulasi, penguatan mekanisme kepatuhan, dan peningkatan kerja sama internasional yang lebih responsif. Dengan demikian, penelitian ini berkontribusi dalam pengembangan kajian hukum internasional sekaligus menjadi dasar bagi perumusan kebijakan perlindungan data yang lebih adaptif.

REFERENCES

Atanda-lawal & Onuchukwu. (2025). The Global Governance of AI : Between Soft Law and Binding Obligations in International Law, *13*(11), 159–184.

Buckley et al. (2024). GDPR and the Indefinable Effectiveness of Privacy Regulators : Can Performance Assessment be Improved ? *Journal of Cybersecurity*, *10*. https://doi.org/10.1093/cybsec/tyae017

Coche et al. (2024). Unravelling Cross-Country Regulatory Intricacies of Data Governance: The Relevance of Legal Insights for Digitalization and International Business. *Journal of International Business Policy*, *7*(1), 112–127. https://doi.org/10.1057/s42214-023-00172-1

Dalkin et al. (2021). Using Computer Assisted Qualitative Data Analysis Software (CAQDAS ; NVivo) to Assist in the Complex Process of Realist Theory Generation , Refinement and Testing Generation , Refinement and Testing. *International Journal of Social Research Methodology*, *24*(1), 123–134. https://doi.org/10.1080/13645579.2020.1803528

Fitriani, L. (2024). Cybersecurity and Digital Sovereignty : An Analysis of National Data Governance Capacity in the Global Platform Era : A Literature Review, *1*(2), 65–77.

Jampani, S. K. (2025). Cross-Border Cybersecurity Collaboration-Building a Global Framework for Threat, *14*(December 2024), 1–10.

Jiang, S. (2025). Fragmented Rules , Global Flows : How Legal Differences Shape the Cross-Border Data Landscape - Evidence from the, *0*, 47–57. https://doi.org/10.54254/2753-7048/96/2025.BO23772

Judijanto, L. (2025). Juridical Analysis of Personal Data Protection in the Digital Era : A Case Study of PDP Law Implementation, (April), 140–153.

Khan et al. (2024). Cross-Jurisdictional Cybersecurity Resilience and the Governance of Digital Infrastructure Risks Date : December 16 , 2024.

Khan, M. N. I. (2025). Cross-Border Data Privacy and Legal Support: a Systematic Review of International Compliance Standards and Cyber Law Practices. *American Journal of Scholarly Research and Innovation*, *04*(01), 138–174. https://doi.org/10.63125/a4gbeb22

Kianpour, M. (2024). More than Malware : Unmasking the Hidden Risk Of Cybersecurity Regulations, 169–212. https://doi.org/10.1365/s43439-024-00111-7

Ko et al. (2024). Research in Globalization Reinforcing Inequalities : A Critical Examination of International Sanctions and Bureaucratic Decline in the Global South. *Research in Globalization*, *9*(October), 100258. https://doi.org/10.1016/j.resglo.2024.100258

Kour et al. (2024). Cybersecurity for Industry 5 . 0 : Trends and Gaps, (July). https://doi.org/10.3389/fcomp.2024.1434436

Kuzio et al. (2022). Building Better Global Data Governance, 1–17. https://doi.org/10.1017/dap.2022.17

Laksito, J., Idris, M. F., Waryanto, A., Studi, P., Hukum, I., Studi, P., … Komunikasi, D. (2024). Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif, *2*(4), 774–790. https://doi.org/10.51903/hakim.v2i04.2154

Leventopoulos et al. (2024). Retaliating Against Cyber-Attacks : A Decision-Taking Framework for Policy-Makers and Enforcers of International and Cybersecurity Law, 237–262. https://doi.org/10.1365/s43439-024-00113-5

Luo, Q. (2022). Organisational Structure of Chinese Cybercrime. *Humanities and Social Sciences Communications*, (2024), 1–12. https://doi.org/10.1057/s41599-024-04042-w

Marcucci et al. (2023). Informing the Global Data Future : Benchmarking Data Governance Frameworks. https://doi.org/10.1017/dap.2023.24

Pichlak et al. (2025). Systematic Literature Review Method in Legal Research, 1–23. https://doi.org/10.5553/REM/.000085

Polat. (2025). Thematic Analysis in Qualitative Research : Common Pitfalls and Practical Insights for Academic Writing, *24*, 1–10. https://doi.org/10.1177/16094069251372835

Putra, R. K., Agustin, Y., Ihsan, L. N., & Dafiqi, Z. A. (2025). Institutional Dysfunction in Personal Data Protection: A Legal-Political Analysis Based on New Institutional Theory. Perkara : Jurnal Ilmu Hukum Dan Politik, 3(2), 938–949. https://doi.org/10.51903/BKKTEY52

Radanliev, P. (2024). *Digital security by design*. *Security Journal* (Vol. 37). Palgrave Macmillan UK. https://doi.org/10.1057/s41284-024-00435-3

Rahimi et al. (2025). Evolving Cybersecurity Policy : Addressing Modern Threats and Enhancing Resilience in a Digital Age, *16*(2), 330–340. https://doi.org/10.4236/jis.2025.162017

Ribalta et al. (2024). Understanding the GDPR from a Requirements Engineering Perspective — A Systematic Mapping Study on Regulatory Data Protection Requirements. *Requirements Engineering*, *29*(4), 523–549. https://doi.org/10.1007/s00766-024-00423-4

Tajik et al. (2024). Purposive Sampling, *2*(November), 1–9.

Xia et al. (2024). Paradigm Transformation of Global Health Data Regulation : Challenges in

Governance and Human Rights Protection of Cross-Border Data Flows Paradigm Transformation of Global Health Data Regulation : Challenges in Governance and Human Rights Protection of C, *1594*. https://doi.org/10.2147/RMHP.S450082