JUDICATUM:
Jurnal Dimensi Catra Hukum
https://doi.org/10.35326/judicatum.v3i1.7734
Vol. 3 No.1, Juni 2025

DILEMA YURIDIKSI DI RUANG SIBER: TANTANGAN DAN STRATEGI PENEGAKAN KEAMANAN LINTAS NEGARA

Andi Cakra Cindrapole[1*], Arianty Anggraeny Mangarengi[2]

[1,2] Fakultas Hukum, Universitas Muslim Indonesia, Makassar

*Correspondence: andicakra.cindrapole@umi.ac.id

ARTICLE HISTORY

Terkirim: 07.05.2025
Diterima: 05.06.2025
Publikasi: 29.06.2025

ABSTRAK

Penegakan hukum terhadap kejahatan siber lintas negara menghadapi berbagai tantangan kompleks. Hal ini disebabkan oleh karakteristik kejahatan siber yang tidak terikat wilayah geografis, perkembangan teknologi informasi yang sangat cepat, serta keterlibatan banyak negara dalam berbagai tahap tindak pidana tersebut. Tulisan ini bertujuan untuk mengkaji hambatan-hambatan yuridis dalam upaya menjaga keamanan siber global, sekaligus menilai respons normatif dari sistem hukum nasional di sejumlah negara. Melalui pendekatan yuridis normatif dan metode studi perbandingan, penelitian ini menganalisis kebijakan dan regulasi siber di Amerika Serikat, Jerman (mewakili sistem hukum Uni Eropa), dan Tiongkok, serta menelusuri posisi hukum Indonesia dalam konteks hukum siber internasional. Temuan penelitian menunjukkan bahwa perbedaan sistem hukum dan ideologi politik mulai dari pendekatan liberal hingga sistem sentralistik yang otoriter menjadi penghambat utama dalam pembentukan tata kelola hukum siber global yang terpadu. Sementara itu, Indonesia menghadapi sejumlah tantangan di tingkat domestik, seperti ketidaksesuaian regulasi nasional dengan standar global, rendahnya partisipasi dalam kerja sama internasional, serta keterbatasan kapasitas kelembagaan dalam menegakkan hukum di ranah digital. Penelitian ini merekomendasikan pentingnya upaya harmonisasi hukum siber secara global, antara lain dengan meratifikasi instrumen hukum internasional seperti Konvensi Budapest, memperkuat kolaborasi teknis dan pertukaran intelijen antarnegara, serta membentuk forum multilateral yang inklusif dan adaptif. Langkah-langkah ini dianggap krusial untuk menciptakan sistem hukum siber yang adil, efektif, serta sejalan dengan prinsip kedaulatan digital dan perlindungan hak asasi manusia.

Kata Kunci : Kejahatan Siber, Yurisdiksi, Harmonisasi Hukum, Regulasi Global.

ABSTRACT

Law enforcement against transnational cybercrime faces various complex challenges. This is due to the geographically unbound nature of cybercrime, the rapid development of information technology, and the involvement of many countries in various stages of the crime. This paper aims to examine the legal obstacles to maintaining global cybersecurity, while also assessing the normative responses of national legal systems in several countries. Using a normative legal approach and comparative study methods, this research analyzes cyber policies and regulations in the United States, Germany (representing the European Union legal system), and China, and explores Indonesia's legal position within the context of international cyber law. Research findings indicate that differences in legal systems and political ideologies, ranging from liberal approaches to authoritarian, centralized systems, are major obstacles to the establishment of integrated global cyber law governance. Meanwhile, Indonesia faces a number of domestic challenges, such as the inconsistency of national regulations with global standards, low participation in international cooperation, and limited

institutional capacity to enforce laws in the digital realm. This study recommends the importance of global cyber law harmonization efforts, including ratifying international legal instruments such as the Budapest Convention, strengthening technical collaboration and intelligence exchange between countries, and establishing inclusive and adaptive multilateral forums. These steps are considered crucial to creating a fair and effective cyber legal system that aligns with the principles of digital sovereignty and human rights protection.

***Keywords**: Cyber Crime, Jurisdiction, Law Harmonization, Global Regulation*

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan terhadap struktur sosial, ekonomi, politik, dan hukum, baik dalam lingkup nasional maupun internasional](Ariyaningsih et al., 2023) Era digital menciptakan suatu realitas baru yang ditandai oleh keterhubungan tak terbatas, di mana berbagai sektor kehidupan — mulai dari ekonomi, hubungan sosial, hingga pelayanan publik — kini sangat terintegrasi dan bergantung pada infrastruktur siber.(Goni et al., 2022) Dalam konteks tersebut, keamanan siber (*cybersecurity*) memegang peranan krusial, tidak hanya dalam menjaga data dan sistem informasi, tetapi juga berkaitan erat dengan kedaulatan negara, stabilitas nasional, dan kepastian hukum. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi digital, potensi risiko dan ancaman siber turut melonjak secara signifikan, terutama dalam bentuk serangan yang melintasi batas-batas yurisdiksi.(Lola Sariani, 2024)

Serangan siber lintas negara (*cross-border cyber attacks*) telah berkembang menjadi permasalahan global yang sangat rumit. Serangan semacam ini memungkinkan pelaku di satu negara untuk menargetkan sistem di negara lain tanpa perlu hadir secara fisik di lokasi sasaran. Aksi tersebut dapat berupa pencurian data antarnegara, peretasan sistem keuangan global, penyebaran malware secara masif, hingga sabotase terhadap infrastruktur penting seperti jaringan listrik, sistem telekomunikasi, dan layanan pemerintahan digital.(Phillips et al., 2022) Karakter lintas batas yang dimiliki kejahatan siber membuatnya berbeda secara fundamental dari tindak pidana konvensional yang selama ini diatur dalam kerangka hukum pidana nasional.

Dalam bidang hukum, kejahatan siber yang melintasi yurisdiksi menimbulkan tantangan serius bagi aparat penegak hukum. Hal ini disebabkan oleh sistem hukum nasional yang umumnya bertumpu pada prinsip teritorialitas, di mana kewenangan hukum suatu negara hanya berlaku dalam batas geografisnya. Sementara itu, kejahatan siber dapat berlangsung secara lintas negara dalam waktu singkat, melibatkan pelaku, korban, serta infrastruktur digital yang tersebar di berbagai sistem hukum. Situasi ini memunculkan persoalan krusial mengenai efektivitas penegakan hukum terhadap kejahatan yang melampaui batas-batas negara.

Salah satu hambatan utama adalah adanya ketimpangan regulasi antarnegara dalam merespons tindak pidana siber. Tiap negara menerapkan pendekatan hukum yang berbeda, baik dari segi definisi kejahatan, prosedur penyidikan dan penuntutan, hingga standar perlindungan hak asasi manusia. Beberapa negara memiliki perangkat hukum yang ketat dan komprehensif, sementara yang lain masih belum membentuk kerangka hukum yang memadai. Ketidakharmonisan ini menyulitkan terwujudnya kerja sama internasional dalam memberantas pelaku kejahatan siber yang beroperasi secara lintas batas.

Selain itu, pelaksanaan proses hukum terhadap pelaku kejahatan siber antarnegara sering terkendala oleh lemahnya koordinasi dan kerja sama yuridis antarnegara. Mekanisme bantuan hukum timbal balik (*mutual legal assistance*/MLA) maupun ekstradisi kerap

memerlukan waktu lama dan terhambat oleh kendala birokrasi maupun pertimbangan politik. Dalam sejumlah kasus, negara tempat pelaku berada tidak memiliki perjanjian ekstradisi dengan negara korban, atau menolak memberikan kerja sama karena alasan strategis atau geopolitik. Akibatnya, banyak pelaku memanfaatkan celah yurisdiksi untuk menghindari proses hukum.

Perbedaan prinsip dan standar hukum internasional juga menjadi faktor penghambat yang signifikan. Sebagai ilustrasi, dalam hal perlindungan data pribadi, negara-negara di Eropa menerapkan standar yang tinggi melalui *General Data Protection Regulation (*GDPR), sedangkan negara lain mungkin memiliki aturan yang lebih longgar atau belum berkembang secara optimal.(Saputra et al., 2024) Dalam praktik penegakan hukum, kebutuhan untuk mengakses data yang berada di yurisdiksi negara lain sering kali memunculkan konflik antara kepentingan investigatif dan perlindungan data pribadi. Selain itu, perbedaan perspektif antarnegara terkait isu kebebasan berekspresi, penyensoran konten digital, serta perlindungan terhadap pelapor pelanggaran (*whistleblower*), turut menjadi sumber ketegangan dalam menjalin kerja sama hukum internasional.

Sebagai tanggapan atas tantangan tersebut, berbagai inisiatif global telah diluncurkan guna membentuk kerangka hukum siber yang lebih terintegrasi. Salah satu instrumen internasional yang paling signifikan adalah Konvensi Budapest mengenai Kejahatan Siber, yang diadopsi oleh Dewan Eropa pada tahun 2001. Konvensi ini menjadi langkah awal dalam membangun sistem hukum internasional yang bertujuan untuk menanggulangi kejahatan siber serta memperkuat koordinasi antarnegara dalam penegakan hukum di ruang digital.(Sviatun et al., 2021) Konvensi tersebut mencakup pengaturan mengenai aspek kriminalisasi, prosedur penegakan hukum, serta mekanisme kerja sama internasional dalam proses investigasi. Namun demikian, efektivitas implementasinya masih menghadapi keterbatasan, mengingat beberapa negara besar seperti Rusia, Tiongkok, dan sejumlah negara berkembang termasuk Indonesia belum meratifikasi instrumen ini, umumnya karena perbedaan prinsip hukum dan kekhawatiran terkait isu kedaulatan nasional.(Tamhidah, 2023) Kondisi ini menunjukkan adanya ketimpangan signifikan antara kebutuhan mendesak akan keamanan siber di tingkat global dan kesiapan sistem hukum internasional dalam meresponsnya. Oleh karena itu, diperlukan analisis komparatif terhadap regulasi dan kebijakan siber di berbagai negara untuk menilai sejauh mana efektivitas sistem hukum nasional masing-masing dalam menghadapi tantangan global tersebut. Kajian semacam ini juga berguna untuk mengidentifikasi praktik-praktik terbaik, hambatan dalam pelaksanaan kebijakan, serta peluang penguatan kerja sama hukum baik secara bilateral maupun multilateral.

Di Indonesia sendiri, urgensi isu keamanan siber semakin meningkat. Berbagai insiden telah terjadi, mulai dari peretasan terhadap lembaga pemerintahan, kebocoran data pribadi, hingga gangguan pada sistem keuangan nasional.(Aji, 2023) Walaupun Indonesia telah mengadopsi perangkat hukum seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) serta membentuk Badan Siber dan Sandi Negara (BSSN), upaya penegakan hukum di bidang siber masih menghadapi tantangan serius, khususnya dalam menangani pelaku yang beroperasi lintas negara.(Aji, 2023)

Kerangka hukum nasional saat ini dianggap belum sepenuhnya mampu merespons dinamika kejahatan siber di tingkat global. Selain permasalahan terkait substansi regulasi, tantangan juga muncul dalam hal ketersediaan sumber daya manusia yang kompeten, kemampuan teknologi forensik digital, serta efektivitas koordinasi antar lembaga terkait.(Tobing et al., 2024) Ketidakterlibatan Indonesia dalam Konvensi Budapest turut melemahkan posisinya dalam menjalin kerja sama internasional di bidang keamanan siber.

Oleh karena itu, penyesuaian hukum nasional dengan standar internasional menjadi kebutuhan mendesak.

Berangkat dari latar belakang tersebut, penelitian ini bertujuan untuk mengkaji lebih dalam persoalan yuridis dalam penegakan keamanan siber yang melintasi yurisdiksi negara. Fokus utama diarahkan pada analisis komparatif terhadap sistem hukum siber di beberapa negara, seperti Amerika Serikat, Jerman, Tiongkok, dan Indonesia, untuk mengidentifikasi kekuatan, kelemahan, serta potensi integrasi hukum antarnegara. Hasil kajian ini diharapkan dapat memberikan kontribusi dalam merumuskan kebijakan hukum yang adaptif terhadap tantangan global, sekaligus mendorong terbentuknya rezim hukum internasional yang lebih adil, efektif, dan terkoordinasi dalam menanggulangi kejahatan siber lintas batas. Dengan demikian, penelitian ini diharapkan tidak hanya memperkaya khazanah keilmuan dalam bidang hukum internasional dan hukum pidana modern, tetapi juga memberikan manfaat praktis dalam pengembangan kebijakan keamanan siber nasional yang lebih responsif dan bersifat kolaboratif di tataran global.

B. Metode Penelitian

Dalam penlitian jurnal ini menggunakan penelitian normatif, yaitu penelitian dengan melakukan studi kepustakaan (*library*) yakni mengkaji buku-buku yang relevan dengan penelitian ini. Penelitian jurnal ini menggunakan pendekatan undang-undang dan pendekatan konseptual. Sumber data yang digunakan dalam penelitian ini adalah sumber data sekunder, dengan cara mengkaji berbagai literature yakni jurnal, artikel, buku, dan internet yang relevan dengan penelitian ini.

C. Pembahasan

1. Karakteristik Kejahatan Siber Lintas Yurisdiksi

Karakteristik Kejahatan Siber Lintas Yurisdiksi Kejahatan siber lintas yurisdiksi merepresentasikan bentuk kejahatan modern yang berakar pada pemanfaatan kemajuan teknologi informasi dan komunikasi (TIK), dengan dampak yang menjangkau melampaui batas yurisdiksi negara-negara berdaulat.[11] Salah satu karakteristik utama dari kejahatan siber adalah ketidakterikatannya pada batas-batas geografis, baik dalam konteks pelaku, sarana yang digunakan, maupun korban yang terdampak. Berbeda dengan kejahatan konvensional yang biasanya bersifat lokal dan terbatas pada ruang fisik tertentu, kejahatan siber dapat dilakukan oleh individu atau kelompok dari satu negara, dengan memanfaatkan infrastruktur digital di negara lain, untuk menyerang sasaran di yurisdiksi berbeda. Tingkat kompleksitas ini menimbulkan tantangan besar bagi sistem hukum pidana nasional, yang secara konseptual dibangun di atas asas kedaulatan dan prinsip teritorial.

Secara teoretis, asas teritorial menegaskan bahwa yurisdiksi pidana suatu negara hanya berlaku dalam batas-batas wilayah kekuasaannya, dan hanya mencakup tindak pidana yang terjadi di dalam wilayah tersebut.[12] Namun, karakter global dari dunia maya yang mengaburkan batas-batas fisik menjadikan prinsip teritorialitas semakin kurang relevan. Dalam ranah siber, penentuan lokasi terjadinya kejahatan menjadi kabur, karena satu tindakan kriminal dapat melibatkan banyak wilayah geografis secara bersamaan. Misalnya,

seorang pelaku dapat berada di Ukraina, menggunakan server yang berlokasi di Belanda, dan mencuri data milik warga negara Indonesia dari sistem yang dihosting di Amerika Serikat. Situasi seperti ini menimbulkan persoalan serius terkait yurisdiksi hukum: negara mana yang berwenang mengadili pelaku? Bagaimana aparat penegak hukum dapat melanjutkan proses penyidikan jika bukti digital tersebar di berbagai negara?

Sifat lintas negara dari kejahatan ini mengakibatkan munculnya konflik yurisdiksi antara negara-negara yang terlibat, baik dalam hal pelaksanaan penegakan hukum maupun dalam proses permintaan bantuan hukum dan pengumpulan alat bukti.[13] Perbedaan dalam sistem hukum, mekanisme penyidikan, dan standar pembuktian antarnegara kerap menjadi hambatan signifikan, terutama ketika tidak tersedia perjanjian bantuan hukum timbal balik (mutual legal assistance treaty/MLAT). Dalam banyak kasus, proses investigasi terhenti sebelum mencapai hasil akibat kendala administratif, ketidaksesuaian kebijakan, atau bahkan konflik kepentingan politik antarnegara.

Contoh konkret adalah kasus Yahoo Data Breach (2013–2014) yang melibatkan peretasan terhadap lebih dari 500 juta akun pengguna. Pelaku diduga berbasis di Rusia, sedangkan korban tersebar di Amerika Serikat dan Eropa. Proses investigasi mengalami kebuntuan karena Rusia menolak mengekstradisi warganya meskipun FBI telah mengeluarkan dakwaan resmi. Kasus ini menggambarkan keterbatasan MLAT dan lemahnya efektivitas kerja sama internasional ketika berbenturan dengan kepentingan politik dan prinsip kedaulatan negara.

Selain isu yurisdiksi, kejahatan siber juga memiliki karakteristik lain berupa tingkat anonimitas pelaku yang sangat tinggi. Dengan memanfaatkan teknologi seperti Virtual Private Network (VPN), proxy server, teknik penyamaran alamat IP, serta akses ke jaringan gelap (dark web), para pelaku dapat menyembunyikan identitas asli mereka dan menghindari deteksi oleh aparat penegak hukum.[14] Banyak kasus kejahatan siber berakhir tanpa kepastian mengenai identitas pelakunya. Kalaupun identitas berhasil diungkap, sering kali negara tempat pelaku berada tidak memiliki perjanjian ekstradisi dengan negara korban. Kondisi ini melahirkan konsep yang dikenal sebagai *safe haven jurisdictions*, yaitu wilayah-wilayah hukum yang menjadi tempat perlindungan bagi pelaku kejahatan siber akibat lemahnya regulasi atau absennya kerja sama internasional yang efektif.

Skala dan dampak serangan siber saat ini tidak hanya menargetkan individu, tetapi juga dapat mengganggu infrastruktur vital suatu negaraseperti jaringan listrik, sistem transportasi, layanan air bersih, sistem keuangan, hingga pemerintahan digital. Serangan ransomware WannaCry pada tahun 2017 merupakan contoh nyata, di mana dalam waktu kurang dari 24 jam, serangan tersebut menyebar ke lebih dari 150 negara dan menginfeksi ratusan ribu perangkat komputer di seluruh dunia.[15] Kecepatan serta daya destruktif dari serangan siber menjadikan pendekatan hukum tradisional kurang memadai dalam menghadapi ancaman yang berlangsung secara simultan dan real-time. Selain itu, perbedaan norma serta standar hukum antarnegara semakin mempersulit upaya kolaborasi internasional dalam memberantas kejahatan siber. Suatu tindakan yang dikategorikan sebagai tindak pidana di satu negara belum tentu diperlakukan serupa di negara lain. Misalnya, ujaran kebencian dapat dijerat hukum di berbagai negara Eropa, namun di Amerika Serikat, ekspresi serupa bisa dilindungi oleh Amandemen Pertama sebagai bentuk kebebasan berpendapat.

Hal yang sama juga berlaku terhadap tindakan peretasan atau akses ilegal, yang belum tentu memiliki pijakan hukum yang jelas di sejumlah negara. Perbedaan fundamental ini menjadi hambatan besar dalam perumusan kerangka hukum global yang bersifat menyeluruh dan berlaku lintas yurisdiksi.

Di Indonesia, isu kejahatan siber semakin menonjol seiring dengan meningkatnya penetrasi internet yang tidak sepenuhnya diimbangi dengan kesiapan sistem hukum siber yang memadai. Meskipun regulasi telah tersedia, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) serta keberadaan Badan Siber dan Sandi Negara (BSSN), pendekatan hukum nasional masih bersifat domestik. Tidak adanya keterlibatan Indonesia dalam instrumen hukum internasional, misalnya Konvensi Budapest tentang Kejahatan Siber, turut menjadi kendala signifikan dalam memperkuat efektivitas kerja sama global. Akibatnya, kapasitas negara untuk membangun kolaborasi lintas batas dalam penanggulangan kejahatan siber menjadi terbatas.

Fenomena peretasan oleh Bjorka pada tahun 2022 memperlihatkan kelemahan tersebut secara konkret. Kebocoran data publik yang menimbulkan kegaduhan nasional hanya dapat ditangani dengan instrumen hukum dalam negeri. Namun, ketika pelaku diduga beroperasi dari luar negeri, Indonesia mengalami kesulitan serius karena tidak memiliki perangkat hukum transnasional yang efektif untuk melakukan penindakan.

Sebagai upaya menjawab keterbatasan itu, Perserikatan Bangsa-Bangsa pada tahun 2019 membentuk *Ad Hoc Committee on Cybercrime* yang diberi mandat menyusun suatu konvensi global mengenai kejahatan siber. Hingga tahun 2025, proses perundingan masih berlangsung dengan tujuan melahirkan kerangka hukum internasional yang mampu mengatasi persoalan yurisdiksi, harmonisasi tindak pidana, dan mekanisme kerja sama penegakan hukum antarnegara. Meski demikian, perdebatan terkait isu kedaulatan digital, akses terhadap data lintas batas, serta perlindungan hak asasi manusia menjadikan proses perumusan konvensi tersebut berjalan lambat dan menghadapi berbagai hambatan.

2. Tantangan Hukum dalam Penegakan Keamanan Siber

Di era digital yang kian terhubung, ancaman terhadap keamanan siber tidak hanya meningkat secara kuantitatif, melainkan juga semakin kompleks secara kualitatif. Kejahatan siber (*cybercrime*) telah menjadi fenomena global yang tidak mengenal batas negara, karena pelaku dapat beroperasi secara anonim dan lintas yurisdiksi, menggunakan teknologi yang melampaui kemampuan pengawasan negara secara konvensional.(Phillips et al., 2022) Dalam konteks tersebut, upaya penegakan hukum atas kejahatan siber menghadapi sejumlah tantangan mendasar, baik dari sisi struktur hukum nasional maupun dari dimensi hukum internasional. Tantangan ini mencakup perbedaan definisi dan klasifikasi hukum, belum adanya instrumen hukum universal yang mengikat, konflik yurisdiksi antarnegara, keterbatasan mekanisme kerja sama internasional, hingga lemahnya kapasitas penegakan hukum di negara berkembang.

Para penyerang siber juga telah berhasil memanfaatkan lanskap layanan kesehatan yang berubah dengan cepat sejak awal pandemic COVID-19. Kerja jarak jauh, perawatan virtual, dan konsultasi elektronik telah menciptakan target baru bagi para pelaku kejahatan siber. Dokter sebagian besar merupakan kontraktor independen, yang memiliki hak istimewa

untuk bekerja di lingkungan layanan kesehatan mereka masing-masing. Mereka umumnya menggunakan perangkat mereka sendiri yang meningkatkan kompleksitas dalam pengelolaan perangkat titik akhir, yang merupakan faktor yang paling berkontribusi terhadap keamanan siber organisasi secara keseluruhan.(Clarke & Martin, 2024)

2.1. Perbedaan Definisi dan Klasifikasi Kejahatan Siber antar Negara

Tantangan pertama dan paling mendasar adalah belum adanya konsensus global mengenai definisi dan klasifikasi kejahatan siber. Setiap negara merumuskan sendiri apa yang dianggap sebagai tindak pidana siber sesuai dengan karakteristik sistem hukum dan nilai-nilai sosial budayanya masing masing. Misalnya, tindakan seperti *hacking, phishing*, atau penyebaran *malware* dikriminalisasi secara eksplisit di banyak negara Barat, tetapi di sejumlah negara berkembang, pengaturan terhadap perbuatan-perbuatan tersebut masih bersifat umum dan tidak terperinci. Bahkan dalam beberapa yurisdiksi, tindakan tersebut belum tentu dianggap sebagai tindak pidana karena belum adanya peraturan perundang-undangan yang spesifik.

Perbedaan ini bukan hanya bersifat substantif, tetapi juga berdampak pada mekanisme pembuktian dan proses peradilan. Suatu tindakan yang merupakan delik di satu negara belum tentu dapat diproses hukum di negara lain, karena tidak memenuhi asas double criminality yang mensyaratkan bahwa suatu perbuatan harus dianggap sebagai kejahatan di kedua yurisdiksi untuk dapat dilakukan ekstradisi atau kerja sama hukum lainnya. Akibatnya, pelaku kejahatan siber dapat mengeksploitasi disparitas hukum ini dengan mengoperasikan kejahatannya dari negara-negara yang memiliki regulasi longgar atau belum mengkriminalisasi tindakan tersebut secara khusus.

2.2. Ketiadaan Instrumen Hukum Universal yang Mengikat Seluruh Negara

Tantangan berikutnya adalah belum adanya instrumen hukum internasional yang bersifat mengikat secara universal dalam hal penanganan kejahatan siber. Satu-satunya kerangka kerja internasional yang paling dikenal dalam bidang ini adalah Budapest *Convention on Cybercrime* (2001), yang diprakarsai oleh Dewan Eropa dan didukung oleh negara-negara seperti Amerika Serikat, Jepang, dan beberapa negara Asia lainnya. Konvensi ini memberikan landasan hukum bagi kriminalisasi kejahatan siber, mekanisme kerja sama lintas negara, dan pengumpulan bukti elektronik. Namun, konvensi ini belum mencakup banyak negara penting seperti Tiongkok, Rusia, dan India yang justru menjadi pusat aktivitas siber global, baik yang bersifat sah maupun ilegal.

Beberapa negara menolak bergabung dengan konvensi tersebut karena menganggapnya bias terhadap kepentingan hukum negara-negara Barat, dan karena substansinya dinilai tidak sepenuhnya menghormati prinsip kedaulatan digital. Indonesia sendiri hingga saat ini belum meratifikasi Konvensi Budapest, meskipun telah menunjukkan minat dalam mengikuti perkembangan hukum siber global. Akibatnya, Indonesia menghadapi keterbatasan dalam menjalin kerja sama formal dengan negara-negara pihak Konvensi dalam rangka investigasi dan penuntutan tindak pidana siber lintas negara.

2.3. Konflik Kepentingan antar Negara dalam Hal Data, Kedaulatan Digital, dan Hak Asasi Manusia

Dalam upaya penegakan hukum terhadap kejahatan siber, seringkali terjadi benturan kepentingan antarnegara yang melibatkan isu-isu fundamental seperti perlindungan data pribadi, hak atas privasi, kebebasan berekspresi, serta pengawasan negara atas ruang digital. Di satu sisi, negara memiliki kewajiban untuk melindungi warganya dari serangan siber dan tindak pidana digital lainnya. Namun di sisi lain, upaya penegakan hukum seringkali memerlukan akses terhadap data pribadi atau komunikasi elektronik yang berada di bawah perlindungan hukum negara lain.

Sebagai contoh, permintaan akses data dari server yang berlokasi di negara lain sering kali ditolak dengan alasan pelanggaran terhadap undang-undang perlindungan data lokal seperti *General Data Protection Regulation* (GDPR) di Uni Eropa. Selain itu, perbedaan persepsi terhadap hak digital juga menimbulkan persoalan. Di Amerika Serikat, prinsip kebebasan berekspresi dijadikan dasar untuk membatasi regulasi terhadap konten daring, sementara di negara lain seperti Jerman atau Tiongkok, pengawasan terhadap konten sangat ketat karena dianggap bagian dari perlindungan keamanan nasional atau ketertiban publik.

Perbedaan prinsip ini menciptakan ketidak harmonisan dalam penegakan hukum lintas batas, dan dalam beberapa kasus menyebabkan negara saling menuduh melakukan pelanggaran hukum internasional. Hal ini dapat dilihat dalam berbagai insiden diplomatik terkait tuduhan spionase siber antarnegara, seperti yang terjadi antara Amerika Serikat dan Tiongkok dalam kasus peretasan data pemerintah AS tahun 2015.

2.4. Keterbatasan Mekanisme Kerja Sama Internasional

Mekanisme kerja sama internasional dalam penanganan kejahatan siber pada umumnya masih menggunakan instrumen tradisional seperti *Mutual Legal Assistance Treaty* (MLAT) dan perjanjian ekstradisi. Mekanisme ini dirancang untuk tindak pidana konvensional, dan kurang responsif terhadap sifat kejahatan siber yang menuntut kecepatan, fleksibilitas, dan koordinasi waktu nyata (*real-time cooperation*). Dalam banyak kasus, proses MLA dapat memakan waktu berbulan-bulan hingga bertahun-tahun karena harus melalui saluran diplomatik dan prosedur formal yang rumit. Padahal, bukti digital memiliki karakteristik yang mudah berubah dan dapat hilang dalam hitungan jam, jika tidak segera diamankan.

Selain itu, banyak negara yang belum memiliki perjanjian MLA atau ekstradisi dengan negara lain, sehingga proses kerja sama hukum menjadi semakin sulit. Dalam kasus tertentu, negara bahkan enggan bekerja sama karena pelaku berada dalam wilayah kekuasaannya dan dianggap sebagai aset strategis atau bagian dari operasi intelijen. Hal ini memunculkan tantangan serius terhadap asas akuntabilitas dan supremasi hukum, karena pelaku dapat berlindung di negara yang tidak kooperatif dan lolos dari jerat hukum.

2.5. Keterbatasan Kapasitas Penegakan Hukum Siber di Negara Berkembang

Tantangan kelima adalah keterbatasan kapasitas institusional negara berkembang dalam menghadapi kejahatan siber, baik dari segi regulasi, sumber daya manusia, maupun infrastruktur teknologi. Negara-negara berkembang pada umumnya belum memiliki undang-undang yang komprehensif tentang keamanan siber, dan apabila ada pun implementasinya sering kali terbentur oleh minimnya anggaran, keterbatasan teknologi forensik digital, dan kurangnya tenaga ahli di bidang tersebut.

Sebagai contoh, Indonesia telah memiliki beberapa peraturan seperti Undang-Undang ITE dan pembentukan Badan Siber dan Sandi Negara (BSSN), namun masih menghadapi kesenjangan signifikan dalam kapasitas penanganan insiden siber, sistem pelaporan insiden, serta mekanisme respons cepat terhadap serangan. Di tingkat aparat penegak hukum, pemahaman terhadap proses investigasi digital dan pengumpulan alat bukti elektronik masih sangat terbatas. Kesenjangan ini menjadikan negara berkembang lebih rentan terhadap serangan siber dari aktor transnasional, sekaligus kesulitan untuk menjalin kerja sama setara dalam forum internasional.

Kelima tantangan yang telah diuraikan mencerminkan bahwa penegakan hukum terhadap kejahatan siber lintas yurisdiksi tidak dapat diselesaikan secara unilateral oleh satu negara, melainkan memerlukan pendekatan kolaboratif, lintas sektoral, dan multilateral. Harmonisasi definisi hukum, penyusunan konvensi internasional yang inklusif, peningkatan kapasitas penegakan hukum digital, serta penguatan kerja sama antarnegara menjadi agenda mendesak untuk mewujudkan sistem keamanan siber global yang adil, efektif, dan responsif terhadap perkembangan zaman. Tanpa langkah-langkah struktural ini, kejahatan siber akan terus menjadi ancaman laten bagi keamanan nasional, supremasi hukum, dan kepercayaan publik terhadap institusi negara.

3. Studi Komparatif Regulasi Siber Global

Negara	Instrumen Hukum Utama	Karakteristik
Amerika Serikat	*Computer Fraud and Abuse Act (CFAA)*, CLOUD Act	Fokus pada perlindungan infrastruktur kritis dan perluasan yurisdiksi ekstra-teritorial
Jerman (Uni Eropa)	GDPR, NetzDG, NIS Directive	Menekankan perlindungan data pribadi dan kewajiban pelaporan insiden keamanan
Tiongkok	*Cybersecurity Law 2017*, Data Security Law	Fokus pada kedaulatan data dan kontrol negara terhadap sistem digital domestik

Dalam rangka memahami kompleksitas penegakan hukum keamanan siber lintas yurisdiksi, pendekatan komparatif terhadap regulasi di beberapa negara utama menjadi penting. Setiap negara memiliki kerangka hukum siber yang mencerminkan prioritas kebijakan, sistem hukum, dan nilai-nilai politiknya masing-masing. Studi komparatif ini mengkaji tiga yurisdiksi kunci, yaitu Amerika Serikat, Jerman (mewakili Uni Eropa), dan Tiongkok. Ketiga negara ini dipilih karena masing-masing mewakili pendekatan hukum yang berbeda: model liberal berbasis pasar (AS), model protektif berbasis hak asasi (UE), dan model sentralistik-otoriter (Tiongkok). Perbandingan ini menunjukkan bagaimana perbedaan ideologis dan institusional turut memengaruhi efektivitas serta arah kerja sama global dalam penanggulangan kejahatan siber.

Amerika Serikat

Amerika Serikat merupakan pelopor dalam pengembangan regulasi kejahatan siber melalui berbagai legislasi, dengan *Computer Fraud and Abuse Act* (CFAA) tahun 1986 sebagai dasar hukum utama. CFAA mengkriminalisasi akses tidak sah terhadap sistem komputer,

serta memberikan kewenangan luas bagi lembaga federal seperti FBI untuk menangani kasus kejahatan siber, termasuk yang bersifat lintas negara. CFAA sering dikritik karena definisinya yang luas dan potensi penyalahgunaan terhadap pelaku pelanggaran kecil, tetapi di sisi lain memberikan kerangka yang fleksibel bagi penegakan hukum di lingkungan digital.

Selain CFAA, Amerika Serikat mengesahkan *Clarifying Lawful Overseas Use Of Data Act* (CLOUD Act) pada 2018. Undang-undang ini secara eksplisit memperluas yurisdiksi hukum pidana AS atas data digital yang disimpan oleh perusahaan teknologi AS di luar negeri. CLOUD Act juga memungkinkan perjanjian bilateral dengan negara lain untuk pertukaran data secara langsung antara otoritas penegak hukum dan penyedia layanan digital, tanpa perlu melalui proses *mutual legal assistance treaty* (MLAT) tradisional yang lambat.

Pendekatan Amerika Serikat menekankan perlindungan terhadap infrastruktur kritis nasional, pencegahan terhadap serangan dari aktor negara asing, dan kebebasan perusahaan teknologi dalam mengatur data pengguna, selama tidak melanggar hukum federal. Namun, pendekatan ini menimbulkan dilema internasional: di satu sisi mempermudah akses otoritas AS terhadap data di luar negeri, tetapi di sisi lain berpotensi berbenturan dengan hukum data protection negara lain, seperti GDPR di Uni Eropa, yang justru melarang transfer data tanpa mekanisme hukum tertentu.

Uni Eropa (Jerman sebagai Representasi)

Negara-negara Uni Eropa, dengan Jerman sebagai salah satu pelopornya, menerapkan pendekatan yang menekankan perlindungan data pribadi sebagai hak asasi manusia. Regulasi utama dalam hal ini adalah *General Data Protection Regulation* (GDPR) yang berlaku sejak 2018. GDPR memberikan standar tinggi bagi pengelolaan data pribadi oleh organisasi publik maupun swasta, termasuk hak-hak pengguna seperti hak untuk dihapus, hak atas akses data, dan hak atas portabilitas data. Pelanggaran terhadap ketentuan GDPR dapat dikenai sanksi administratif yang berat, hingga 4% dari total pendapatan tahunan global perusahaan.

Dalam konteks keamanan siber, Uni Eropa juga memiliki *Network and Information Security Directive* (NIS Directive) yang mengatur kewajiban pelaporan insiden keamanan bagi penyedia layanan penting. Negara anggota diwajibkan memiliki *Computer Security Incident Response Teams* (CSIRTs) nasional yang dikoordinasikan melalui badan seperti ENISA. Selain itu, *Netzwerkdurchsetzungsgesetz* (NetzDG) di Jerman mengatur kewajiban platform media sosial untuk menindaklanjuti konten ilegal, sebagai bentuk komitmen melawan ujaran kebencian dan radikalisme digital.

Namun, standar tinggi yang diusung GDPR menimbulkan problem koordinasi internasional. Contoh nyata adalah konflik yurisdiksi dengan CLOUD Act. Ketika perusahaan teknologi AS yang menyimpan data pengguna Eropa diperintahkan oleh otoritas AS untuk menyerahkan data (berdasarkan CLOUD Act), perusahaan tersebut berpotensi melanggar GDPR jika menyerahkan data tanpa dasar hukum yang sah. Situasi ini menciptakan ketegangan hukum yang rumit, di mana perusahaan global terjebak antara dua kewajiban hukum yang saling bertentangan. Hal ini menunjukkan bahwa tanpa harmonisasi atau perjanjian internasional yang lebih kuat, kerja sama dalam penegakan hukum siber akan terus menghadapi hambatan.

Tiongkok

Tiongkok mengambil pendekatan berbeda yang menekankan prinsip *cyber sovereignty* atau kedaulatan digital. Hal ini tertuang dalam *Cybersecurity Law* (2017), *Data Security Law* (2021), dan *Personal Information Protection Law* (PIPL). Regulasi tersebut mewajibkan data penting yang dikumpulkan di Tiongkok untuk disimpan secara lokal (*data localization*), dan hanya dapat ditransfer ke luar negeri setelah melalui audit keamanan. Pemerintah memiliki wewenang penuh mengakses data perusahaan domestik maupun asing dengan alasan keamanan nasional.

Pendekatan ini sering dikritik karena membatasi kebebasan berekspresi dan transparansi. Namun, bagi Tiongkok, regulasi tersebut merupakan instrumen strategis untuk menjaga kedaulatan digital dan memperkuat posisi geopolitik melawan dominasi perusahaan teknologi Barat. Instrumen seperti *Great Firewall* memperlihatkan bagaimana penyaringan konten berbasis ideologi-politik dijadikan instrumen kontrol domestik sekaligus kebijakan keamanan nasional.

Dari perspektif kerja sama internasional, pendekatan Tiongkok menimbulkan hambatan serius. Standar proteksi data yang berbasis keamanan nasional dan kontrol negara seringkali bertentangan dengan standar perlindungan data berbasis hak asasi manusia ala Uni Eropa. Misalnya, perusahaan Eropa yang beroperasi di Tiongkok diwajibkan menyimpan data secara lokal dan membuka akses kepada pemerintah, padahal kewajiban ini dapat dianggap melanggar GDPR. Dengan demikian, perbedaan pendekatan ini tidak hanya bersifat normatif, tetapi juga memiliki implikasi praktis terhadap arsitektur global tata kelola siber.

Implikasi Perbedaan Regulasi dalam Praktik Internasional

Analisis perbandingan ini memperlihatkan bahwa keberagaman pendekatan hukum siber memunculkan implikasi serius dalam praktik internasional. Setidaknya terdapat dua titik ketegangan utama:

1. **Konflik Yurisdiksi (CLOUD Act vs GDPR):**

   CLOUD Act memungkinkan otoritas AS untuk meminta data dari perusahaan teknologi meskipun data tersebut berada di wilayah Uni Eropa. Namun, GDPR secara ketat membatasi transfer data lintas batas tanpa perlindungan yang memadai. Situasi ini membuat perusahaan multinasional berada dalam dilema hukum yang sulit dihindari.

2. **Ketegangan Ideologis (UE vs Tiongkok):**

   Standar perlindungan data Uni Eropa yang berbasis pada hak fundamental individu sering berbenturan dengan regulasi Tiongkok yang berorientasi pada kedaulatan negara. Akibatnya, kerja sama hukum, ekstradisi digital, maupun investigasi siber menjadi terbatas karena perbedaan prinsip dasar mengenai siapa yang seharusnya memiliki kendali atas data—individu atau negara.

Kedua ketegangan tersebut menunjukkan bahwa upaya membangun rezim global keamanan siber tidak hanya bersifat teknis, tetapi juga politis dan ideologis. Tanpa adanya mekanisme harmonisasi hukum yang lebih inklusif, konflik yurisdiksi dan perbedaan nilai ini

akan terus menjadi hambatan utama dalam efektivitas penegakan hukum siber lintas batas negara.

4. Perbedaan Ideologis terhadap Kolaborasi Global

Studi komparatif terhadap ketiga yurisdiksi tersebut menunjukkan bahwa perbedaan ideologis dan prinsip hukum mendasar turut memengaruhi kesulitan dalam membangun tata kelola hukum siber global. Amerika Serikat dan Uni Eropa mewakili model liberal demokratis yang menekankan transparansi, perlindungan data, dan kerja sama lintas sektor, meskipun dengan pendekatan yang berbeda. Di sisi lain, Tiongkok menerapkan model otoriter sentralistik yang menempatkan kontrol negara sebagai prioritas utama, dan menolak dominasi nilai-nilai hukum Barat.

Menurut De Nardis (2014), ketidaksamaan paradigma ini memperumit upaya kolaborasi global dalam penanggulangan kejahatan siber.(Fatmala Putri & Ratna Sari, 2023) Tanpa adanya konsensus mengenai prinsip-prinsip dasar seperti yurisdiksi, kedaulatan digital, dan hak digital warga negara, pembentukan konvensi global yang mengikat seluruh negara menjadi sangat sulit.

Lebih lanjut, perbedaan model regulasi ini juga menciptakan risiko *"fragmentasi internet global" (internet Balkanization*), di mana ruang siber tidak lagi bersifat terbuka dan universal, melainkan terpecah menjadi sistem-sistem tertutup yang dikontrol negara secara ketat. Hal ini tidak hanya berdampak pada efektivitas penegakan hukum terhadap kejahatan siber, tetapi juga pada arus perdagangan digital, pertukaran informasi ilmiah, dan kebebasan sipil global.

5. Posisi dan Tantangan Regulasi Siber di Indonesia

Sebagai negara dengan populasi pengguna internet terbesar keempat di dunia, Indonesia menghadapi tantangan serius dalam mewujudkan sistem keamanan siber yang tangguh, inklusif, dan responsif terhadap ancaman kejahatan digital yang terus berkembang. Dalam beberapa tahun terakhir, Indonesia telah mengadopsi sejumlah regulasi serta membentuk lembaga negara khusus yang bertugas menangani aspek keamanan siber. Namun, meskipun langkah-langkah ini menunjukkan komitmen pemerintah dalam merespons risiko digital, masih terdapat sejumlah kelemahan struktural dan normatif yang menghambat efektivitas penegakan hukum siber, khususnya dalam konteks lintas yurisdiksi.

6. Upaya Harmonisasi Hukum Siber Internasional

Di tengah meningkatnya eskalasi kejahatan siber yang bersifat lintas yurisdiksi dan melampaui otoritas hukum nasional, kebutuhan akan sistem hukum siber internasional yang terkoordinasi dan harmonis menjadi semakin mendesak. Saat ini, belum terdapat satu kerangka hukum global yang secara universal mengatur dan mengikat negara-negara dalam penanganan kejahatan siber. Fragmentasi regulasi, perbedaan ideologi politik, serta disparitas kapasitas teknis telah menyebabkan kesenjangan signifikan dalam respons hukum terhadap ancaman siber global. Oleh karena itu, harmonisasi hukum siber internasional menjadi tujuan strategis yang tidak hanya bertujuan menyatukan norma hukum antarnegara, tetapi juga untuk menciptakan sistem keamanan digital global yang adil, kolaboratif, dan inklusif. Upaya

menuju harmonisasi hukum siber internasional setidaknya harus mencakup empat strategi utama, yaitu ratifikasi instrumen hukum internasional, penguatan kerja sama teknis dan intelijen lintas negara, pembangunan kapasitas hukum nasional, serta pembentukan forum multilateral yang berorientasi pada penyusunan norma global. Keempat pendekatan ini saling melengkapi dan memerlukan komitmen politik jangka panjang dari negara-negara di seluruh dunia.

D. Penutup

Penegakan hukum terhadap kejahatan siber lintas yurisdiksi merupakan salah satu tantangan paling signifikan dalam tatanan hukum global era digital. Kompleksitas tersebut muncul dari sifat kejahatan siber yang tidak terikat pada batas wilayah, cepat beradaptasi, memanfaatkan infrastruktur digital yang tersebar di berbagai negara, serta melibatkan pelaku dan korban dari yurisdiksi yang berbeda. Dalam konteks ini, sistem hukum nasional yang masih berlandaskan prinsip kedaulatan teritorial sering kali tidak mampu menjangkau pelaku maupun membuktikan unsur pidana secara efektif.

Melalui studi perbandingan terhadap kebijakan hukum siber di Amerika Serikat, Uni Eropa (dengan representasi Jerman), dan Tiongkok, ditemukan perbedaan pendekatan yang mendasar: Amerika Serikat menitikberatkan pada perlindungan infrastruktur kritis dan penerapan yurisdiksi ekstra-teritorial; Uni Eropa fokus pada perlindungan data pribadi dan hak-hak digital warga negara; sementara Tiongkok menempatkan kedaulatan data dan kontrol negara sebagai prioritas utama. Perbedaan ideologi dan paradigma ini menjadi penghalang besar bagi upaya pembentukan kerja sama internasional yang terkoordinasi dan menyeluruh dalam menghadapi kejahatan siber.

Di sisi lain, Indonesia telah menunjukkan kemajuan dalam aspek normatif melalui kehadiran instrumen hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), pembentukan Badan Siber dan Sandi Negara (BSSN), serta pengesahan Undang-Undang Perlindungan Data Pribadi. Meski demikian, kelemahan struktural masih terlihat, antara lain belum diratifikasinya instrumen internasional seperti Konvensi Budapest, lemahnya keterlibatan dalam kerja sama global, dan keterbatasan kapasitas aparat penegak hukum dalam menangani kejahatan digital secara efektif.

Dengan demikian, upaya harmonisasi hukum siber internasional menjadi sangat mendesak dan memerlukan komitmen kolektif dari negara-negara di dunia. Langkah langkah strategis yang dapat dilakukan antara lain meliputi ratifikasi instrumen hukum global, penguatan kerja sama teknis dan pertukaran intelijen, peningkatan kapasitas penegakan hukum nasional—khususnya di negara-negara berkembang—serta pembentukan forum multilateral yang inklusif untuk menyusun norma global yang menjunjung prinsip keadilan, keterbukaan, dan non-diskriminasi.

Tanpa langkah konkret dan sinergis menuju tata kelola hukum siber yang terintegrasi secara global, ruang digital akan tetap menjadi wilayah yang rawan dieksploitasi oleh pelaku kejahatan lintas batas, yang pada akhirnya dapat meruntuhkan kepercayaan masyarakat terhadap sistem hukum, baik di tingkat nasional maupun internasional.

DAFTAR PUSTAKA

A. F. Yamin, A. Rachmawati, R. A. Pratama, and J. K. Wijaya, "Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi," Meraja J., vol. 5, no. 3, pp. 115 137, 2022.

A. H. Abdurrohman, C. N. Uzmawi, R. Khoiruddin, and A. M. Mustain, "Cybersecurity dan Pancasila : Harmonisasi Regulasi Hukum Internasional dengan Kepentingan Nasional," vol. 1, no. March, pp. 23–29, 2025.

A. L. S. Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia," AL-DALIL J. Ilmu Sos. Polit. dan Huk., vol. 2, no. 2, pp. 69–77, 2024, doi: 10.58707/aldalil.v2i2.777.

Achmad, Naswar, M. Assidiq, Hasbi, A. Safira, and S. N. Lubis, Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional. 2020.

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). https://doi.org/10.56457/jjih.v1i1.38

C. I. Tobing et al., "Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas," J. Huk. Sasana, vol. 10, no. 2, pp. 105 123, 2024, doi: 10.31599/sasana.v10i2.3170.

Clarke M, Martin K, "Managing cybersecurity risk in healthcare settings", Healthcare Management Forum (2024) 37(1) 17-20

D. Fatmala Putri and W. Ratna Sari, "Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking," J. Ilm. Ekon. dan Manaj., vol. 1, 4, pp. 173–181, https://doi.org/10.61722/jiem.v1i4.331 2023, [Online]. Available:

Goni, O., Md. Haidar Ali, Showrov, Md. Mahbub Alam, & Md. Abu Shameem. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2). https://doi.org/10.56556/jtie.v1i2.113

J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int., vol. 13, no. 2, pp. 222–238, 2023, doi: 10.22212/jp.v13i2.3299.

L. Judijanto and B. Nugroho, "Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia," Sanskara Huk. dan HAM, vol. 3, no. 03, pp. 118 124, 2025, doi: 10.58812/shh.v3i03.544.

Lola Sariani, A. (2024). *Al-Dalil Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia*. *2*(2). https://ejournal.indrainstitute.id/index.php/al-dalil/index

M. fadel Roihan, "penerapan Prinsip Yuridisdiksi Ekstrateritorial Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Yang Dilakukan Secara Lintas Batas Negara," no. 8.5.2017, pp. 2003–2005, 2022.

M. P. Aji, "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],"

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. In *Forensic Sciences* (Vol. 2, Issue 2). https://doi.org/10.3390/forensicsci2020028

R. B. Mochammad, R. F. F. Mahlafi, A. T. Ridho, K. A. Wianto, and Nurhidayat, "Intervensi Negara Dalam Yurisdiksi Teritorial," J. Media Akad., vol. 1, no. 1, p. 34, 2023.

Saputra, A., Kristiawanto, K., & Ismed, M. (2024). Rekonstruksi Penegakan Hukum Tindak Pidana Siber di Indonesia. *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum*, *3*(1). https://doi.org/10.55681/seikat.v3i1.1186

Sviatun, O. v., Goncharuk, O. v., Chernysh, R., Kuzmenko, O., & Kozych, I. v. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*. https://doi.org/10.37394/23207.2021.18.72\

T. Cahyono, S. T., Erni, W., & Hidayat, "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," DJH Dame J. Huk., vol. 1, no. 1, pp. 1–23, 2025. [15] R.

Tamhidah, M. A. R. (2023). Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu Dan Kejahatan Siber. *Innovative: Journal Of Social Science Research*, *3*(6)