

KEDAULATAN DATA DI ERA *CLOUD COMPUTING*: ANALISIS YURIDIS PENEMPATAN PUSAT DATA DAN YURISDIKSI EKSTRATERITORIAL DALAM HUKUM INDONESIA

*Data Sovereignty In The Cloud Computing Era: A Juridical Analysis Of Data Center Placement And
Extraterritorial Jurisdiction In Indonesian Law*

Hendra Simak

Badan Pembinaan Hukum Nasional
Jl. Mayjen Sutoyo No.10 4, RT.4/RW.14, Cililitan,
Kec. Kramat Jati, Kota Jakarta Timur, DKI Jakarta
e-mail: hendrasimak@bphn.go.id

Abstrak

Kedaulatan data telah menjadi isu krusial di tengah dominasi penyedia layanan cloud global yang mendisrupsi batas-batas teritorial hukum konvensional. Penelitian ini menganalisis pertentangan paradigmatik antara kebijakan lokalisasi data yang diamanatkan dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dengan kompleksitas penyidikan tindak pidana siber yang secara inheren bersifat lintas batas. Dengan menggunakan metode yuridis normatif melalui pendekatan perundang-undangan dan pendekatan konseptual kedaulatan digital, tulisan ini membedah problematika yurisdiksi di ruang maya. Hasil pembahasan mengungkap bahwa meskipun rezim hukum nasional telah mengadopsi asas ekstrateritorialitas dan mengakomodasi konsep *quasi jurisdiction*, implementasinya kerap mengalami kebuntuan akibat benturan kedaulatan dan birokrasi *Mutual Legal Assistance* (MLA) yang tidak selaras dengan volatilitas bukti elektronik. Temuan utama menegaskan perlunya rekonseptualisasi MLA menjadi mekanisme kerja sama antar-agensi yang lebih responsif. Secara praktis dan kebijakan, penelitian ini merekomendasikan penguatan peran strategis institusi penegak hukum seperti Badan Siber dan Sandi Negara dan Polri dalam arsitektur koordinasi formal global, serta urgensi ratifikasi instrumen internasional, guna memastikan penegakan hukum berjalan efektif tanpa mereduksi esensi kedaulatan digital nasional.

Kata kunci: kedaulatan data, lokalisasi data, yurisdiksi ekstrateritorial, tindak pidana siber, mutual legal assistance.

Abstract

Data sovereignty has become a crucial issue amid the dominance of global cloud service providers that disrupt the boundaries of conventional legal territories. This research analyzes the paradigmatic conflict between the data localization policy mandated in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and the complexity of cybercrime investigations, which are inherently cross-border. Using the normative juridical method thru a legislative approach and the conceptual approach of digital sovereignty, this paper dissects the jurisdictional problems in cyberspace. The discussion reveals that although the national legal regime has adopted the principle of extraterritoriality and accommodated the concept of quasi-jurisdiction, its implementation often encounters deadlocks due to sovereignty clashes and Mutual Legal Assistance (MLA) bureaucracy that are not aligned with the volatility of electronic evidence. The main findings emphasize the need to reconceptualize MLA into a more responsive inter-agency cooperation mechanism. Practically and policy-wise, this research recommends strengthening the strategic role of law enforcement institutions such as the National Cyber and Crypto Agency and the National Police in the global formal coordination architecture, as well as the urgency of ratifying international instruments, to ensure effective law enforcement without reducing the essence of national digital sovereignty.

Keywords: data sovereignty, data localization, extraterritorial jurisdiction, cybercrime, mutual legal assistance.

A. PENDAHULUAN

Saat ini, kita sedang mengalami arus globalisasi digital yang sangat cepat. Ini disebabkan oleh perkembangan teknologi komputasi awan yang sangat pesat. Akibatnya, kita harus memikirkan kembali tentang konsep kedaulatan negara dan batasan wilayah. Selama berabad-abad, kita telah menggunakan konsep ini untuk mengatur hubungan antar negara. Namun, sekarang semuanya berubah. Dalam dunia ekonomi dan politik modern, data telah menjadi sangat penting. Data ini bukan hanya sekedar informasi, tapi telah menjadi komoditas yang sangat berharga. Bahkan, nilai data ini dapat melebihi nilai komoditas fisik lainnya. Ketika data pribadi dan informasi strategis disimpan, diproses, dan ditransmisikan melalui *server* yang ada di seluruh dunia, negara harus berhadapan dengan tantangan baru. Tantangan ini bukan lagi tentang pergerakan barang, tapi tentang aliran data yang tidak terlihat. Situasi ini memunculkan pertanyaan tentang kedaulatan digital. Kedaulatan digital adalah kemampuan negara untuk mengontrol dan mengatur data warga negaranya, tanpa memandang di mana data tersebut disimpan. Ini adalah tantangan besar bagi negara, karena mereka harus menemukan cara untuk mempertahankan kendali atas data warga negaranya di era digital ini.

Dalam konteks nasional, peralihan besar-besaran ke ruang digital membawa tantangan yang kompleks bagi Indonesia. Di satu sisi, pertumbuhan ekonomi digital yang cepat dan jumlah pengguna internet di Indonesia hanya 72,7 juta orang pada tahun 2015. Dalam

kurun waktu enam tahun jumlah pengguna internet bertambah menjadi 202,6 juta orang atau 178,68%, kondisi ini tentu saja membuka peluang besar bagi bisnis, inovasi teknologi, dan pelayanan publik.¹ Namun, sistem digital yang terbuka membuat Indonesia lebih rentan terhadap ancaman kejahatan siber yang bersifat internasional. Jumlah kasus kejahatan siber meningkat signifikan, mulai dari peretasan infrastruktur penting, penipuan online terorganisir seperti *romance scam* dan *phishing*, hingga kebocoran data pribadi jutaan orang yang memicu ketidakstabilan dan krisis kepercayaan publik.²

Dampak dari perkembangan penggunaan internet yang semakin bertambah, mengakibatkan kejahatan siber semakin bertambah dan kejahatan modern ini memiliki skema yang rumit, pelaku intelektual bisa berada di satu benua, infrastruktur komputasi awan yang digunakan untuk melakukan kejahatan berada di benua lain, sementara korban dan dampak kerugian finansial maupun non finansial berada di dalam wilayah hukum Indonesia. kondisi ini menunjukkan kelemahan sistem perlindungan hukum di Indonesia, terutama ketika penegakan hukum masih bergantung pada metode konvensional yang berfokus pada lokasi fisik terjadinya kejahatan.

Untuk mengantisipasi hal tersebut, Pemerintah telah mengambil langkah-langkah untuk melindungi yurisdiksi hukum negara dari ancaman yang mungkin mengikisnya. Salah satu cara yang dilakukan adalah dengan menerapkan kebijakan lokalisasi data. Kebijakan ini diatur dalam Peraturan Pemerintah Nomor

¹ Astuti, A.W., Sayudin, S. and Muharam, A; Perkembangan Bisnis Di Era Digital. "Jurnal Multidisiplin Indonesia", Volume 2, Nomor 9 (2023), hlm 2788. <https://doi.org/10.58344/jmi.v2i9.554>, (Diakses 16 Mei 2026)

² Agus Wibowo dan Sri Yulianingsih, Hukum Teknologi Informasi (Semarang:Yayasan Prima Agus Teknis, 2023), hlm 70.

71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019). Pada prinsipnya Peraturan ini meminta penyelenggara sistem elektronik lingkup publik untuk melakukan pengelolaan, pemrosesan dan/atau penyimpanan sistem elektronik dan data elektronik di dalam Indonesia.³ Sementara itu, untuk penyelenggara sistem elektronik lingkup privat, peraturan ini memperbolehkan penempatan data di luar negeri asalkan memenuhi syarat aksesibilitas data untuk kepentingan pengawasan dan penegakan hukum di Indonesia dalam hal ini teknologi penyimpanan tidak tersedia di dalam negeri.⁴

Kebijakan lokalisasi data ini memiliki alasan yang kuat untuk melindungi kedaulatan data. Namun, dalam prakteknya, kebijakan ini seringkali bertentangan dengan model bisnis *cloud computing global* yang mengandalkan distribusi data lintas negara untuk efisiensi operasional. Hal ini juga berpotensi menimbulkan friksi geopolitik dengan negara asal perusahaan teknologi global, seperti Amerika Serikat. Amerika Serikat memiliki regulasi yang memungkinkan otoritas asing mengakses data secara sepihak, yang berimplikasi pada tantangan terhadap kedaulatan hukum Indonesia.⁵

Dalam penegakan hukum pidana, Indonesia telah berupaya merespons fenomena nirbatas ini melalui pembaruan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik. Regulasi ini secara progresif mengadopsi asas ekstrateritorialitas, yang memberikan mandat kepada aparat penegak hukum untuk menjangkau tindak pidana yang terjadi di luar yurisdiksi nasional. Namun, efektivitas rumusan normatif ini sering kali menemui jalan buntu dalam realitas investigasi. Ketiadaan yurisdiksi teritorial terhadap *server* yang berlokasi di luar negeri memaksa penyidik untuk membentur batasan kedaulatan negara lain. Hal ini secara sistematis berpotensi memicu konflik yurisdiksi serta penolakan kooperasi investigasi atas dasar asas kriminalitas ganda, di mana perbuatan yang dikategorikan sebagai tindak pidana di Indonesia belum tentu diklasifikasikan serupa di negara tempat data tersebut tersimpan

Untuk mengatasi masalah yurisdiksi tersebut, hukum internasional memiliki cara yang disebut *Mutual Legal Assistance*. Cara ini membantu negara-negara untuk bekerja sama dan berbagi informasi tentang bukti elektronik yang ada di luar batas wilayah mereka. Namun, cara ini seringkali tidak cukup cepat dan efektif dalam memberikan solusi yang dibutuhkan. Sistem *Mutual Legal Assistance* yang ada sekarang dirancang beberapa dekade yang lalu untuk menangani kejahatan yang terjadi di dalam wilayah tertentu. Sistem ini membutuhkan proses birokratis yang panjang dan memakan waktu. Seringkali, dibutuhkan waktu berbulan-bulan atau bahkan bertahun-

³ Pasal 20 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, "Penyelenggara Sistem Elektronik Lingkup Publik wajib melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia".

⁴ Pasal 20 ayat (3) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, "Penyelenggara Sistem Elektronik Lingkup Publik dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di luar wilayah Indonesia dalam hal teknologi penyimpanan tidak tersedia di dalam negeri".

⁵ Rahayudin, R., Naseer, M., Agustina, N., & Guterres, A. *Digital Sovereignty and The Right To Data: A Comparative Study Between Indonesia, The European Union, and The United States*. Journal of Law and Social Politics, Volume 3 Nomor 2, (2025), hlm 89-90. <https://doi.org/10.59261/jlsp.v3i2.71>. (Diakses 16 Mei 2026)

tahun untuk mendapatkan izin dari otoritas yang terkait. Di era digital sekarang, bukti elektronik dapat berubah atau hilang dengan sangat cepat. Karena itu, sistem yang ada sekarang tidak cukup cepat untuk menangani kejahatan yang terjadi di dunia maya.⁶ Oleh karena hal tersebut terdapat perbedaan antara keinginan untuk melindungi data nasional dan kebutuhan untuk bekerja sama dengan negara lain secara internasional telah menciptakan celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan.

Penelitian ini bertujuan untuk meninjau kembali bagaimana Indonesia menangani masalah yurisdiksi di luar wilayahnya dan bagaimana cara menyelaraskan kebijakan lokalisasi data dengan kebutuhan untuk bekerja sama dengan negara lain. Penelitian ini akan memfokuskan pada bagaimana peraturan yang ada sekarang dapat diperbarui untuk menangani kejahatan di dunia maya. Secara teoretis, penelitian ini akan membantu memperkaya diskusi tentang bagaimana yurisdiksi di dunia maya dapat diperbarui. Secara praktis, hasil penelitian ini diharapkan dapat membantu pembuat kebijakan dalam merekonstruksi model kerja sama internasional. Penelitian ini akan berfokus pada dua masalah utama yaitu pertama, bagaimana efektifitas penerapan asas ekstrateritorialitas dalam menangani kejahatan siber yang melintasi batas negara dan kedua, bagaimana cara menyelaraskan kebijakan lokalisasi data dengan kebutuhan untuk bekerja

sama dengan negara lain melalui *Mutual Legal Assistance* di tengah kecepatan perubahan bukti elektronik.

B. METODE

Penelitian ini menggunakan jenis penelitian hukum yuridis normatif. Artinya, hukum dilihat sebagai sebuah sistem norma yang utuh. Pendekatan yang digunakan adalah mempelajari perundang-undangan yang ada, terutama Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 11 Tahun 2008), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU 27 Tahun 2022), dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71 Tahun 2019). Penelitian ini juga mengurai beberapa konsep-konsep hukum internasional yang terkait dengan ruang siber. Beberapa teori tersebut ialah teori kedaulatan digital, penegakan asas yurisdiksi ekstrateritorial, penerapan *konsep quasi jurisdiction*, dan prosedural *Mutual Legal Assistance* dalam investigasi kriminal lintas negara.⁷ Analisis dilakukan dengan cara mempelajari bahan hukum primer dan literatur sekunder dari artikel akademik. Analisis ini dilakukan secara deskriptif kualitatif, yang berarti penelitian ini berupaya mengurai makna, mengidentifikasi potensi inkonsistensi antar regulasi, serta memetakan pola implementasi hukum yang relevan dalam prakteknya.⁸

⁶ Sari, Ratih Mega Puspa. "Analysis of the Implementation of the Criminal Procedure Code in Handling Cyber Crimes: Between Effectiveness and Justice." *Jurnal Hukum Dan Keadilan*, Volume 2, Nomor 6, (2025). <https://doi.org/10.61942/jhk.v2i6.454>. (Diakses 16 Mei 2026)

⁷ Abdelkarim, Ya. A. "UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age." *Journal of Digital Technologies and Law*, Volume 3, Nomor 4, (2025), <https://doi.org/10.21202/jdtl.2025.22>. (Diakses 16 Mei 2026).

⁸ Rasji, Antonio Bravo, Baharuddin Jusuf Habibie Hasta, Matthew Alexander Nainggolan. "Tantangan Demokrasi sebagai Suatu Sistem yang Dinamis di Era Digital: Analisis Pengaruh Media Sosial terhadap Proses Politik Nasional" *Jurnal Ilmu Multidisiplin*, Volume 4, Nomor. 1, (2025), hlm 68. <https://doi.org/10.38035/jim.v4i1>. (Diakses 16 Mei 2026)

C. PEMBAHASAN

Untuk menjawab masalah pertama tentang bagaimana efektifnya penerapan asas ekstrateritorialitas dalam menangani tindak pidana siber yang melintasi batas negara, kita perlu memahami bagaimana paradigma yurisdiksi dalam hukum internasional berubah seiring waktu. Secara historis, hukum pidana internasional didasarkan pada doktrin kedaulatan Westphalia, yang menegaskan bahwa setiap negara memiliki otoritas eksklusif untuk menerapkan hukum dan mengadili tindak pidana berdasarkan lokasi fisik kejadian tersebut. Namun, dengan munculnya teknologi *cloud computing* (komputasi awan), konsep ini telah berubah secara drastis.⁹ Ruang siber yang tidak terikat oleh batas geografis memungkinkan tindak pidana dilakukan dari mana saja dan kapan saja. Sebagai contoh, seorang peretas di Eropa Timur bisa membuat algoritma untuk menyerang sistem perbankan di Jakarta melalui server di Amerika Utara. Dalam situasi seperti ini, mengandalkan yurisdiksi teritorial fisik saja tidak cukup untuk menangani tindak pidana siber yang kompleks.¹⁰

Oleh karena itu, perlu dilakukan perubahan dengan menerapkan asas ekstrateritorialitas untuk mengatasi kendala institusional atau prosedural dalam penegakan hukum di ranah siber. Pendekatan ini memfokuskan pada keterkaitan substantif antara aktivitas siber dan dampaknya terhadap kedaulatan digital dan kepentingan nasional, bukan hanya pada lokasi fisik kejadian. Dengan memperkuat basis hukum ekstrateritorial, otoritas penegak hukum dapat menindak entitas asing yang melanggar hukum

nasional, bahkan jika server atau infrastruktur mereka berada di luar wilayah negara. Ini memungkinkan negara untuk melindungi kepentingan nasional tanpa terhambat oleh batasan geografis.

Namun, hal ini juga memerlukan sinkronisasi dengan konvensi internasional, seperti Konvensi Budapest tentang *Cybercrime*,¹¹ untuk memastikan bahwa penerapan asas ekstrateritorialitas memiliki landasan yang kuat dan diakui secara global. Koordinasi antarnegara yang efektif sangat penting untuk mengatasi tantangan penegakan hukum di era digital. Diperlukan integrasi prinsip-prinsip yang jelas terkait kewenangan investigatif lintas negara dan penentuan lokasi tindak pidana untuk mengisi ruang vakum hukum yang sering dimanfaatkan oleh aktor transnasional.

Saat ini kemajuan pesat dalam teknologi komputasi awan telah mengubah batas-batas wilayah tradisional, sehingga memerlukan pemikiran ulang mengenai konsep kedaulatan negara. Dalam konteks digital kontemporer, data tidak lagi hanya dianggap sebagai informasi, melainkan telah menjadi aset strategis yang pergerakannya sering kali tidak terlihat dan melintasi berbagai wilayah geografis di seluruh dunia. Akibatnya, kedaulatan digital Indonesia tidak akan cukup jika hanya mengacu pada doktrin Westphalia yang berfokus pada lokasi fisik infrastruktur. Sebaliknya, kedaulatan ini harus berevolusi untuk mencakup penguasaan akses dan kendali atas data warga negara, terlepas dari di mana data tersebut disimpan.

Perubahan paradigma ini terwujud dalam konsep *quasi jurisdiction*, yang secara analogis menerapkan prinsip hukum antariksa untuk

⁹ Christian Fuchs. "Digital Democracy and the Digital Public Sphere". Media Communication and Society Volume 6. (2022), hlm 164 <https://doi.org/10.4324/9781003331087>.

¹⁰ *Ibid*, hlm 34.

¹¹ *Ibid*, hlm 164.

mengatur entitas yang beroperasi di luar batas fisik negara. Dalam konteks ini, kedaulatan tidak lagi bergantung pada lokasi fisik pusat data, melainkan pada kemampuan negara untuk menerapkan kendali yang efektif dan kewajiban peraturan terhadap aliran data elektronik. Konsep inilah yang menjadi dasar dari apa yang dikenal sebagai kedaulatan fungsional, di mana perdebatan mengenai kedaulatan beralih ke arah kemampuan relasional negara dalam menerapkan kendali operasional, akses, dan perlindungan data secara fungsional melintasi berbagai yurisdiksi.

Secara teknis, penerapan kedaulatan fungsional dalam regulasi di Indonesia terlihat pada pergeseran strategi dari PP Nomor 82 Tahun 2012 yang mewajibkan penempatan fisik data, menjadi PP Nomor 71 Tahun 2019 yang lebih mengandalkan mekanisme audit berbasis kepatuhan. Melalui regulasi ini, pemerintah memberikan fleksibilitas bagi penyelenggara sistem elektronik (PSE) lingkup privat untuk menggunakan infrastruktur luar negeri, namun tetap menetapkan syarat ketat berupa transparansi dan aksesibilitas data bagi kepentingan penegakan hukum. Dengan demikian, negara tetap memegang kontrol operasional atas data warga negaranya meskipun secara fisik data tersebut berada di luar wilayah teritorial nasional.

Untuk memastikan bahwa implementasi kontrol operasional ini sesuai dengan prinsip hukum internasional, Indonesia berpegang teguh pada prinsip ekstrateritorialitas. Prinsip ini memberikan kewenangan yurisdiksi terhadap tindakan hukum yang memiliki dampak di wilayah Indonesia atau merugikan kepentingan nasional. Konsep ini sejalan dengan evolusi

hukum internasional yang mengakui hak negara untuk melindungi kepentingan vitalnya melalui yurisdiksi personal dan prinsip perlindungan. Melalui Pasal 2 Undang-Undang tentang Informasi dan Transaksi Elektronik (ITE) beserta pembaruannya dalam UU Nomor 1 Tahun 2024, Indonesia menegaskan kewenangannya untuk mengambil tindakan terhadap entitas asing yang menargetkan pasar domestik, mengingat aktivitas tersebut menciptakan hubungan hukum yang tunduk pada peraturan nasional.

Namun, keberhasilan kedaulatan fungsional tersebut bergantung pada adanya sistem kerja sama internasional yang praktis guna mengatasi penundaan dan ketidaksesuaian birokrasi *Mutual Legal Assistance* (MLA). Pendekatan operasional yang dianjurkan adalah memaksimalkan peran jaringan NCB Interpol untuk memperlancar pertukaran informasi intelijen dan memungkinkan "pembekuan segera" terhadap bukti elektronik secara langsung. Upaya ini, bersamaan dengan pentingnya pengesahan Konvensi Budapest, akan menyelaraskan standar teknis dan penamaan kejahatan siber Indonesia dengan praktik internasional. Hal ini akan mengurangi tantangan terkait *dual criminality* tanpa mengkompromikan prinsip kedaulatan digital nasional.

Lebih lanjut Hukum internasional telah mengalami perkembangan dalam menghadapi keterbatasan doktrin teritorial. Perluasan kewenangan ini terjadi melalui asas ekstrateritorialitas, yang memungkinkan negara melindungi kepentingan vitalnya meskipun perbuatan terjadi di luar teritorial fisik. Asas ini termanifestasi dalam yurisdiksi personal dan asas perlindungan yang melegitimasi negara untuk melindungi kepentingan vitalnya.¹²

¹² David Leslie. "Don't 'Research Fast and Break Things': On the Ethics of Computational Social Science." Cornell University, (2022), hlm 20. <https://doi.org/10.48550/arxiv.2206.06370>. (Diakses 20 Mei 2026)

Perkembangan ini juga memicu diskursus tentang teori *quasi jurisdiction*. Konsep ini secara analogis mengadopsi prinsip dalam hukum keantariksaan terkait pengaturan yurisdiksi atas entitas yang beroperasi di luar jangkauan fisik negara. Dalam paradigma *quasi jurisdiction*, kedaulatan tidak lagi berpijak pada lokalisasi fisik infrastruktur, melainkan pada kemampuan negara untuk melaksanakan kontrol efektif, akses otoritatif, serta kewajiban regulatif terhadap arus data elektronik.

Penerapan *quasi jurisdiction* menjadi instrumen esensial bagi negara untuk menegaskan kendali yurisdiksional atas aktivitas digital warganya yang tersimpan di infrastruktur penyedia layanan lintas batas.¹³ Ketika sebuah entitas asing beroperasi dan menysar pasar Indonesia, entitas tersebut telah membentuk pertalian hukum yang menundukkannya pada regulasi domestik. Hal ini memungkinkan aparat penegak hukum melakukan intervensi perlindungan hak tanpa terhambat oleh batasan fisik wilayah.

Transformasi yurisdiksi ini menandai pergeseran dari kriteria teritorial yang kaku menuju model yang lebih fleksibel. Model ini tidak menegasikan paradigma wilayah,

melainkan mengadaptasi kedaulatan negara ke dalam realitas siber yang nirbatas. Integrasi kategori penilaian fleksibel ini memungkinkan hukum untuk menjembatani kesenjangan antara tuntutan kedaulatan digital dengan realitas teknis infrastruktur yang tersebar di lintas yurisdiksi.¹⁴ Dalam konteks hukum Indonesia, ekstrateritorialitas telah diakomodasi sejak UU 11 Tahun 2008. Norma tersebut dituangkan dalam Pasal 2, yang menetapkan keberlakuan yurisdiksi atas perbuatan di luar wilayah Indonesia yang memiliki akibat hukum di wilayah Indonesia atau merugikan kepentingan nasional. Namun, frasa “merugikan kepentingan Indonesia” sempat memicu tantangan interpretasi dalam praktik penyidikan.¹⁵

Kehadiran Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU 11 Tahun 2008 (UU 1 Tahun 2004) kemudian hadir memberikan kepastian hukum yang lebih rigid. Secara umum perubahan ini memperluas cakupan pemidanaan termasuk pengaturan lebih detail mengenai informasi bohong, persekusi siber, serta perlindungan keamanan data sekaligus mempertegas otoritas negara dalam penegakan hukum siber.¹⁶ Konsekuensi logis dari pemberlakuan UU 1 Tahun 2004 ini

¹³ Onyema Onyeani. “*The Need To Apply Full Protection And Security (Fps) Standard To Cyber Security: Digital Assets*.” Istanbul University, (2023), hlm 20. <https://dergipark.org.tr/tr/pub/blr/issue/80477/1303597>. (Diakses 20 Mei 2026).

¹⁴ Cedric Ryngaert. “*Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*” German Law Journal, Volume 24, Nomor 3, (2023), hlm 549. <https://doi.org/10.1017/glj.2023.24>. (Diakses 20 Mei 2026).

¹⁵ Walaupun secara substansi UU 11 Tahun 2008 telah dicabut, namun penerapan norma merugikan kepentingan Indonesia juga diperkuat dengan Asas Wilayah/Teritorial dan Asas Universal yang ada dalam Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Substansi Pasal 2 UU 11 Tahun 2008 sendiri menyebutkan “*Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia*”. Hal ini sejalan dengan Pasal 4 dan Pasal 5 Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

¹⁶ Pemberitahuan/Informasi Bohong/ Diatur secara spesifik pada Pasal 28 ayat (3) yang melarang penyebaran pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat, dengan sanksi pidana pada Pasal 45A ayat (3). Persekusi Siber dan Penghinaan/Pencemaran Nama Baik. Ditambahkan dan dipertegas melalui Pasal 27A yang melarang penyerangan kehormatan atau nama baik orang lain, serta Pasal 27B mengenai ancaman

adalah penguatan basis hukum bagi aparat dalam melakukan tindakan penegakan hukum terhadap entitas asing yang tidak mematuhi regulasi perlindungan data di Indonesia. Walaupun landasan normatif telah diperkuat melalui revisi legislasi, efektivitas penegakan hukum siber tetap dihadapkan pada tantangan operasional yang nyata, terutama karena instrumen hukum sering kali tertinggal dalam memitigasi kompleksitas ancaman siber lintas negara yang kian canggih.¹⁷

Sekalipun Indonesia telah memiliki beberapa regulasi yang mengatur norma mengenai ekstrateritorial, namun penerapannya sering menghadapi ujian. Ujian sesungguhnya muncul saat norma tersebut dihadapkan pada realitas hukum internasional. Kendala utama terkait efektivitas asas ekstrateritorialitas adalah fenomena benturan yurisdiksi. Situasi ini merepresentasikan konflik kedaulatan, di mana beberapa negara yang berdaulat merasa memiliki kewenangan hukum setara untuk memeriksa, mengadili, dan menghukum tindak pidana yang sama. Dalam konteks komputasi awan, data tidak lagi tersimpan secara utuh dalam satu storage fisik.¹⁸ Data tersebut dipecah dan direplikasi melintasi berbagai zona ketersediaan lintas benua demi menjamin cadangan/*backup* data serta keandalan layanan. Sebagai contoh, ketika aparat penegak hukum di Indonesia berupaya mengungkap

distribusi konten manipulatif atau penipuan investasi sindikat internasional, mereka kerap menghadapi stagnasi birokrasi,¹⁹ yaitu *traffic* komunikasi mungkin melalui jaringan perantara di Eropa, sementara basis data finansial tersimpan di pusat data penyedia layanan yang berpusat di Amerika Serikat.

Dalam skenario ini, negara tempat infrastruktur *server* berada memiliki hak kedaulatan teritorial yang diakui hukum internasional untuk secara sepihak menolak permohonan akses data oleh aparat penegak hukum di Indonesia. Dalih yang sering digunakan mencakup perlindungan nilai investasi infrastruktur hingga kewajiban negara untuk menjaga privasi data warga dan pelanggan dari intervensi pemerintah asing. Ketidadaan kerangka bantuan hukum timbal balik yang komprehensif serta adaptif terhadap karakteristik data terfragmentasi semakin memperburuk hambatan prosedural ini. Proses formal untuk mengakses bukti elektronik lintas negara sering kali tersandera oleh birokrasi yurisdiksi yang berlarut-larut. Kendala ini diperparah dengan absennya *mutual legal assistance treaties* yang memadai, sehingga prosedur diplomatik yang berlarut larut kerap kali tidak mampu mengimbangi volatilitas bukti elektronik, yang berisiko menyebabkan hilangnya bukti krusial sebelum otorisasi resmi diperoleh. Akibatnya, sering kali mengakibatkan

pencemaran/pemerasan. Keamanan Data Pribadi dan Otoritas Negara. Pengamanan data elektronik diatur dalam perubahan ketentuan Pasal 26 mengenai data pribadi, sementara perluasan kewenangan negara dalam pemblokiran dan penegakan hukum siber tertuang pada perubahan Pasal 40.

¹⁷ Olukunle Oladipupo Amoo, et al. "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System". World Journal of Advanced Research and Reviews, Volume 21, Nomor 2, (2024), hlm 214 <https://doi.org/10.30574/wjarr.2024.21.2.0438>. (Diakses 20 Mei 2026)

¹⁸ Primavera de Filippi, Smari Mccarthy. "Cloud Computing : Centralization and Data Sovereignty" HAL (Le Centre Pour La Communication Scientifique Directe), Centre National de la Recherche Scientifique, (2012), hlm 14 <https://hal.science/hal-00746065>. (Diakses 20 Mei 2026)

¹⁹ Idham Qrida Nusa, et al. "Law Enforcement of Cybercrime: Tracking Digital Footprints of Cross-Border Hackers" International Journal of Islamic Education Research and Multiculturalism (IJIEMR), Volume 7, Nomor 2, (2025), hlm 785-786. <https://doi.org/10.47006/ijierm.v7i2.475>. (Diakses 20 Mei 2026).

hilangnya barang bukti sebelum persetujuan resmi diperoleh.²⁰

Permasalahan kedaulatan yang menghambat penegakan hukum ini diperumit oleh prinsip kriminalitas ganda, sebuah doktrin yang masih menjadi rujukan utama dalam kerja sama hukum pidana internasional. Prinsip ini mensyaratkan bahwa pengajuan bantuan hukum timbal balik, ekstradisi, maupun permohonan akses data hanya dapat diproses apabila perbuatan yang didakwakan juga diklasifikasikan sebagai tindak pidana di negara tempat bukti atau tersangka berada.²¹ Disparitas antar rezim hukum siber global ini memicu terbentuknya *cyber safe havens*, yakni wilayah vakum hukum yang kerap dimanfaatkan oleh pelaku kejahatan.²²

Sebagai contoh empiris, kompleksitas penanganan kasus ujaran kebencian atau penistaan agama yang diunggah dari Amerika Serikat, seperti pada kasus Abraham Ben Moses, menunjukkan tantangan nyata dalam penegakan hukum lintas negara. Walaupun Indonesia memiliki dasar yurisdiksi ekstrateritorial melalui asas nasionalitas aktif, upaya penindakan sering kali terbentur pada perbedaan filosofi hukum. Dalam skenario ini, prinsip kriminalitas ganda (*dual criminality*) menjadi hambatan struktural utama, yang mensyaratkan bahwa perbuatan yang didakwakan harus diklasifikasikan sebagai tindak pidana di kedua yurisdiksi agar bantuan hukum dapat diproses.²³

Berdasarkan *First Amendment*, Amerika Serikat menjamin kebebasan berekspresi secara luas,²⁴ sehingga tindakan yang disangkakan di Indonesia tidak dianggap sebagai tindak pidana di yurisdiksi tersebut. Kesenjangan rezim hukum ini menciptakan ruang yang membatasi efektivitas yurisdiksi ekstrateritorial Indonesia, membuktikan bahwa perbedaan dalam perlindungan hak konstitusional sering kali menjadi penghalang lebih besar daripada sekadar kendala teknis administratif.

Beralih pada **permasalahan kedua**, yaitu bagaimana menyatukan antara kebijakan lokalisasi data nasional dengan kebutuhan kerja sama internasional. Pada bagian ini kita perlu memahami postur pertahanan siber yang sedang dibangun oleh pemerintah. Saat ini Indonesia secara tegas memperkuat fondasi kedaulatan digitalnya melalui kebijakan lokalisasi data yang strategis, sebagaimana diamanatkan dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP Nomor 71 Tahun 2019). Regulasi ini berpijak pada prinsip fundamental bahwa kedaulatan atas entitas data mustahil diwujudkan tanpa kendali penuh terhadap keberadaan fisik data tersebut di dalam yurisdiksi nasional. Menegaskan urgensi tersebut PP Nomor 71 Tahun 2019 menetapkan distingsi kewajiban yang ketat bagi Penyelenggara Sistem Elektronik Lingkup

²⁰ Els De Busser. "EU-US Digital Data Exchange to Combat Financial Crime: Fast Is the New Slow" *German Law Journal*, Volume 19, Nomor 5, (2018), hlm 1258. <https://doi.org/10.1017/s2071832200023026>. (Diakses 202 Mei 2026).

²¹ Bambang Hartono, Recca Ayu Hapsari. "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi Di Indonesia" *SASI*, volume 25, Nomor 1, (2019), hlm 65, <https://doi.org/10.47268/sasi.v25i1.136>. (Diakses 202 Mei 2026)

²² Vijaykumar Shrikrushna Cho, Suryakant S. Bhosale. "Beyond Borders: Addressing the Legal Quagmire of Jurisdiction in Cyberspace." *International Journal For Multidisciplinary Research*, Volume 6, Nomor 6, (2024), hlm 12. <https://doi.org/10.36948/ijfmr.2024.v06i06.30051>. (Diakses 202 Mei 2026)

²³ Bambang Hartono, Recca Ayu Hapsari, *Op.Cit.*

²⁴ Vijaykumar Shrikrushna Cho, Suryakant S. Bhosale. *Op.Cit.*

Publik. Kewajiban mutlak ini menuntut agar pengelolaan data strategis kenegaraan serta informasi vital yang berdampak pada hajat hidup orang banyak wajib diproses, disimpan, dan dikelola secara mandiri di dalam negeri.²⁵

Namun disisi lain, untuk Penyelenggara Sistem Elektronik Lingkup Privat yang berorientasi komersial, pemerintah memberikan fleksibilitas dalam penggunaan infrastruktur komputasi awan yang berlokasi di luar negeri.²⁶ Kelonggaran ini tetap disertai dengan kewajiban audit yang ketat serta tuntutan untuk menjamin transparansi dan aksesibilitas data bagi kepentingan penegakan hukum. Pemisahan entitas dalam regulasi ini mencerminkan upaya kompromistis pemerintah dalam menyeimbangkan antara pilar pertumbuhan ekonomi digital dan pilar ketahanan nasional. Bagi platform digital swasta asing, kepatuhan terhadap proses registrasi dan audit merupakan prasyarat kedaulatan. Ketidakpatuhan terhadap ketentuan ini akan berimplikasi pada sanksi administratif, mulai dari pemutusan akses hingga pemblokiran layanan di pasar digital Indonesia. Meski demikian, efektivitas instrumen lokalisasi ini masih menghadapi tantangan nyata akibat adanya disparitas kapasitas teknis.²⁷

Disparitas perlakuan tersebut mempertegas bahwa kompleksitas algoritma serta infrastruktur raksasa digital global sering kali

melampaui kapabilitas pengawasan otoritas dalam negeri. Kesenjangan sumber daya ini semakin memperlebar celah kerentanan, terutama pasca peralihan regulasi dari Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik yang mewajibkan penempatan fisik data²⁸ menjadi PP Nomor 71 Tahun 2019 yang mengandalkan mekanisme audit berbasis kepatuhan. Pergeseran ini menuntut standar pengawasan yang jauh lebih mutakhir. Akibatnya, timbul ketimpangan antara fleksibilitas operasional yang diberikan kepada penyelenggara sistem elektronik privat dengan tuntutan akses data untuk kepentingan penegakan hukum, yang hingga kini masih terhambat oleh keterbatasan infrastruktur pemantauan secara *real time*.

Kondisi ini secara nyata melemahkan posisi tawar negara dalam menjaga privasi data warga dari intervensi eksternal sekaligus menggerus integritas mekanisme kerja sama internasional. Situasi mendesak ini menuntut reorientasi strategi pengawasan siber nasional yang jauh lebih pragmatis, dengan memprioritaskan penguatan kapabilitas forensik digital yang terintegrasi. Optimalisasi regulasi, terutama melalui implementasi tegas Undang-Undang Perlindungan Data Pribadi, menjadi keharusan mutlak untuk memastikan data warga negara

²⁵ Muhammad Prakoso Aji, Putrawan Yuliandri. "Analysis of the Government's Political Will to Achieve Data Sovereignty Through National Data Center Development Policies." *Society*, Volume 13, Nomor 3, Dec. (2025), hlm 1197, <https://doi.org/10.33019/society.v13i3.932>. (Diakses 20 Mei 2026).

²⁶ Pasal 20 ayat (3) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, "Penyelenggara Sistem Elektronik Lingkup Publik dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di luar wilayah Indonesia dalam hal teknologi penyimpanan tidak tersedia di dalam negeri".

²⁷ Sanghyun Han. "Data and Statecraft: Why and How States Localize Data." *Business and Politics*, Volume 26, Nomor 2, (2024), hlm 276. <https://doi.org/10.1017/bap.2023.41>. (Diakses 20 Mei 2026).

²⁸ Pasal 17 ayat (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik menyebutkan bahwa "Penyelenggara Sistem Elektronik untuk pelayanan publik wajib menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia untuk kepentingan penegakan hukum, perlindungan, dan penegakan kedaulatan negara terhadap data warga negaranya"

tidak sekadar terlokalisasi secara domestik, melainkan benar-benar terlindungi dari eksploitasi sistemik platform digital global. Lebih jauh, negara harus mempertegas kerangka kerja sama lintas batas guna memitigasi risiko hilangnya kendali otoritas domestik atas data warga akibat dominasi platform asing. Langkah strategis ini menuntut sinergi transformatif antara pemerintah dan sektor swasta yang melampaui sekadar kepatuhan administratif menuju kesiapan infrastruktur komprehensif demi menjamin kedaulatan data yang substantif dan berkelanjutan.

Mengapa kondisi diatas perlu menjadi perhatian, dikarenakan sebagai negara adidaya penguasa teknologi, Amerika Serikat memegang kendali atas mayoritas korporasi infrastruktur *cloud*. Melalui *Clarifying Lawful Overseas Use of Data Act* tahun 2018, otoritas penegak hukum Amerika Serikat berwenang menuntut kepatuhan korporasi terhadap akses data pengguna, tanpa memandang lokasi fisik pusat data baik di Eropa, Asia, maupun Indonesia.²⁹ Praktik ekstrateritorial ini memicu konflik hukum yang mendasar karena data, yang secara teknis tidak memiliki kebangsaan, kini dipaksa tunduk pada yurisdiksi negara asal penyedia layanan, alih-alih mengikuti hukum teritorial tempat data tersebut berada.³⁰ Kebijakan ini secara nyata meruntuhkan argumen bahwa kedaulatan data Indonesia dengan menempatkan platform digital global dalam dilema kepatuhan antara regulasi domestik dan hukum asing, yang pada gilirannya membatasi efektivitas yurisdiksi domestik atas data warga negara.

Kesenjangan hukum ini menciptakan zona abu-abu di mana entitas asing dapat mengekstraksi data secara masif tanpa memedulikan batasan kedaulatan digital nasional, sehingga menuntut adanya mekanisme kerja sama internasional yang lebih komprehensif untuk mengatasi tumpang tindih yurisdiksi. Absennya konvensi internasional yang mengikat mengenai kepemilikan data digital saat ini memang memperparah fragmentasi yurisdiksi, di mana sengketa kepemilikan sering kali tidak terselesaikan akibat ketidakselarasan antara regulasi kedaulatan data nasional dan praktik operasional korporasi multinasional.

Dalam konteks ini, Indonesia perlu mempertimbangkan strategi non blok digital yang menekankan kemandirian teknologi serta diplomasi siber multilateral untuk memitigasi ketergantungan pada ekosistem platform asing. Strategi ini memerlukan pergeseran dari pendekatan defensif semata menuju penguatan kedaulatan informasional melalui pengembangan infrastruktur komputasi domestik yang mandiri. Pengembangan infrastruktur ini mencakup pembangunan pusat data nasional yang tangguh serta proyek-proyek strategis seperti satelit SATRIA-1 guna mengurangi ketergantungan pada penyedia layanan luar negeri.³¹ Langkah ini sejalan dengan upaya pemerintah dalam memperkuat ekosistem digital nasional melalui pembangunan infrastruktur krusial, yang menjadi fondasi utama dalam mengelola data secara mandiri tanpa intervensi asing.

²⁹ Sergi Vazquez Maymir. "Anchoring the Need to Revise Cross-Border Access to e-Evidence." Internet Policy Review, (2020), hlm 5. <https://doi.org/10.14763/2020.3.1495>. (Diakses 20 Juni 2026)

³⁰ Filippi, Primavera De, and Smari McCarthy. *Op.Cit.* hlm 14.

³¹ M. H Syafi'i, et al. "Kajian Ilmu Pertahanan Dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital Di Indonesia." Journal on Education, Volume 5, Nomor 2, (2023), hlm 4071. <https://doi.org/10.31004/joe.v5i2.1100>. (Diakses 20 Mei 2026).

Lebih jauh lagi, urgensi lokalisasi data tidak hanya berfokus pada kemandirian fisik, tetapi juga sebagai strategi mitigasi terhadap risiko yurisdiksi ekstrateritorial yang menyulitkan penegak hukum dalam mengakses bukti elektronik saat data tersimpan di luar negeri. Namun, efektivitas strategi ini sangat bergantung pada kemampuan negara dalam mengintegrasikan standar teknis dan hukum yang harmonis, mengingat fragmentasi global yang ada saat ini sering kali menempatkan negara berkembang dalam posisi rentan. Oleh karena itu, diperlukan perumusan kerangka kerja kebijakan yang tidak hanya menitikberatkan pada regulasi administratif, tetapi juga mengedepankan penguatan kapabilitas teknis dan literasi digital penegak hukum untuk memitigasi kompleksitas ancaman siber yang semakin canggih. Mengingat tantangan tersebut, pembentukan lembaga khusus seperti Komisi Digital Nasional menjadi langkah mendesak untuk mengoordinasikan kebijakan lintas sektor guna mengatasi tumpang tindih otoritas serta fragmentasi standar keamanan siber.

Lembaga ini nantinya harus memprioritaskan pembangunan infrastruktur jaringan dan pusat data yang dikelola secara mandiri oleh anak bangsa, guna memastikan jalur transmisi data nasional tetap berada di bawah kendali penuh otoritas domestik. Selain itu, integrasi model pertahanan siber yang menyinergikan kapasitas enkripsi, kecerdasan sinyal, dan keamanan siber secara holistik sangat penting untuk memperkuat resiliensi nasional terhadap infiltrasi pihak asing.

Langkah pencegahan ini seyogianya didukung oleh modernisasi infrastruktur digital yang lebih canggih, termasuk peningkatan kemampuan deteksi dini dan respons cepat terhadap ancaman siber yang semakin kompleks. Dalam upaya mewujudkan ketahanan tersebut, pembentukan tim tanggap insiden yang siaga dan memiliki kewenangan penuh untuk melakukan investigasi forensik menjadi prasyarat mutlak bagi tata kelola digital yang profesional. Namun, tantangan yang dihadapi tidak hanya bersifat internal tapi juga datang dari perluasan wewenang yang agresif oleh pihak asing turut menciptakan ketimpangan kedaulatan. Ironinya, ketika penyidik Indonesia harus menempuh proses diplomasi yang panjang untuk mengakses data yang tersimpan di server luar negeri, mekanisme kontrol seperti *Clarifying Lawful Overseas Use of Data Act*³² mampu menembus batas teritorial tanpa mengindahkan kedaulatan yang diproteksi oleh PP Nomor 71 Tahun 2019.

Fakta ini menegaskan bahwa lokalisasi data menghadapi tantangan dalam mencapai kedaulatan selama fondasi infrastruktur komputasi masih bergantung pada teknologi dan lisensi pihak asing. Akibatnya, tata kelola aliran data lintas batas akan senantiasa menjadi arena pertarungan yang tidak seimbang bagi negara berkembang. Oleh karena itu, diperlukan peninjauan kembali terhadap kebijakan yang tidak hanya bertumpu pada aspek legalitas, tetapi juga memprioritaskan kemandirian ekosistem digital guna memperkecil celah eksploitasi oleh aktor global. Pada akhirnya, upaya penguatan ketahanan siber nasional

³² *Clarifying Lawful Overseas Use of Data (CLOUD) Act* adalah undang-undang federal Amerika Serikat yang disahkan pada Maret 2018. Aturan ini memungkinkan penegak hukum AS untuk memaksa perusahaan teknologi AS menyerahkan data digital pengguna baik yang disimpan di server dalam maupun luar negeri guna menyelidiki kasus kejahatan serius. <https://www.justice.gov/criminal/cloud-act-resources>. (Diakses 20 Mei 2026)

memerlukan pendekatan komprehensif yang mengintegrasikan aspek hukum, teknologi, serta tata kelola organisasi yang konsisten dan efektif.

Harmonisasi kebijakan ini harus didukung oleh penguatan standar teknis, seperti penerapan strategi cadangan data yang tersinkronisasi dengan kerangka perlindungan data pribadi untuk menjamin kesiapan operasional dalam menghadapi insiden siber. Sejalan dengan hal tersebut, reformasi kelembagaan intelijen melalui restrukturisasi organisasi yang adaptif sangat krusial untuk memastikan respons cepat terhadap ancaman siber yang kian kompleks. Transformasi ini perlu diperkuat dengan mandat konstitusional yang secara eksplisit mengakui ruang siber sebagai wilayah kedaulatan negara guna menutup celah kekosongan hukum yang selama ini melemahkan posisi tawar Indonesia di tingkat global. Pengakuan konstitusional ini berfungsi sebagai landasan yuridis bagi negara untuk menyatukan wewenang atas domain digital, sekaligus menegaskan bahwa kedaulatan siber bukan sekadar opsi kebijakan, melainkan perintah untuk menjaga legitimasi negara di era transformasi digital.³³

Terkait dengan urusan diplomasi, hukum internasional menyediakan kanal Mutual Legal Assistance atau Bantuan Hukum Timbal Balik, yang di Indonesia diatur melalui Undang-Undang Nomor 1 Tahun 2006. Namun, birokrasi MLA melibatkan estafet lintas sektoral yang kompleks mulai dari penyidik, Kementerian Hukum selaku *Central Authority*, hingga

verifikasi Kementerian Luar Negeri yang kurang adaptif bagi ekosistem siber. Rantai birokrasi yang dirancang untuk kejahatan fisik ini menjadi kontraproduktif, mengingat bukti elektronik bersifat volatil dan memiliki masa hidup singkat. Keterlambatan proses MLA akibat hambatan administratif serta kompleksitas penyelarasan sistem hukum memberikan keleluasaan bagi sindikat kejahatan siber untuk menghapus jejak atau memutasikan aset digital.³⁴

Ketergantungan pada skema MLA tradisional secara signifikan membatasi kemampuan negara dalam memberikan rasa keadilan bagi korban kejahatan siber transnasional. Oleh karena itu, diperlukan rekonseptualisasi mekanisme kerja sama internasional yang lebih adaptif melalui pembaruan legislasi serta penguatan kapasitas teknis aparat penegak hukum agar mampu merespons bukti elektronik yang bersifat sementara dan kompleksitas operasional sindikat kejahatan siber. Mengingat adanya ketidaksesuaian antara lambatnya birokrasi dalam skema MLA dan peningkatan drastis kejahatan siber, harmonisasi kebijakan lokalisasi data nasional perlu disertai dengan reformulasi signifikan terhadap protokol diplomasi penegakan hukum. Pergeseran paradigma krusial diperlukan, yakni dari ketergantungan pada skema diplomasi formal yang kaku menuju kolaborasi taktis antar instansi yang bersifat *real time* dan pragmatis.³⁵

Fenomena komputasi awan yang mereplikasi data di berbagai zona ketersediaan lintas benua telah melahirkan tantangan yuridis

³³ Syaiful Anwar, Johan Edi Nepri. "Harmonisasi Hukum Digital: Tantangan Global Dan Strategi Adaptif Indonesia Dalam Era Kedaulatan Siber." *Hutanasyah Jurnal Hukum Tata Negara*, Volume 4, Nomor 1, (2025), hlm 70. <https://doi.org/10.37092/hutanasyah.v4i1.1297>. (Diakses 20 Mei 2026)

³⁴ Jean Baptiste Maillart. "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime." *ERA Forum*, Volume 19, Nomor 3, (2018), hlm 384. <https://doi.org/10.1007/s12027-018-0527-2>. (Diakses 20 Mei 2026)

³⁵ Annisa Erikha, Ade Saptomo. "Dilemma of Legal Policy to Address Cybercrime in the Digital Era." *Asian Journal of Social and Humanities*, Volume 3, Nomor 3, (2024), hlm 500 <https://doi.org/10.59888/ajosh.v3i3.452>. (Diakses 20 Mei 2026).

baru yang dikenal sebagai "dilema kepatuhan" bagi penyedia layanan *cloud* global. Dilema ini muncul ketika perusahaan teknologi yang berbasis di Amerika Serikat namun beroperasi di Indonesia, terjebak di antara dua rezim hukum yang saling bertentangan secara ekstrateritorial. Di satu sisi, PP Nomor 71 Tahun 2019 mewajibkan setiap penyelenggara sistem elektronik untuk menjamin transparansi dan aksesibilitas data bagi kepentingan penegakan hukum domestik Indonesia. Di sisi lain, otoritas Amerika Serikat melalui US cloud Act Tahun 2018 memiliki wewenang untuk menuntut akses data pengguna dari korporasi mereka tanpa memedulikan lokasi fisik pusat data tersebut, baik itu di Indonesia maupun wilayah lainnya.

Konflik ini menghasilkan situasi di mana peraturan dari kedua negara saling menghambat, yang mengakibatkan penurunan efektivitas kewenangan hukum domestik terhadap data penduduk. Sebagai ilustrasi, saat petugas penegak hukum Indonesia mengajukan permintaan akses data untuk investigasi kasus penipuan atau penyebaran kebencian, penyedia layanan *cloud internasional* kerap menghadapi hambatan karena perlu menyelaraskan permintaan tersebut dengan kewajiban hukum mereka di negara asal. Ketidakselarasan ini semakin memburuk akibat tidak adanya perjanjian internasional yang mewajibkan mengenai kepemilikan data, yang menyebabkan sengketa kewenangan yurisdiksi sering kali berujung pada kegagalan otoritas Indonesia dalam memperoleh akses data.

Kondisi tersebut diatas, semakin diperumit oleh mekanisme Mutual Legal Assistance (MLA) yang saat ini dirancang dengan birokrasi yang sangat lambat dan kurang adaptif terhadap ekosistem siber. Rantai birokrasi MLA tradisional yang melibatkan estafet lintas sektoral sering

kali memakan waktu berbulan-bulan hingga bertahun-tahun, yang berakibat pada hilangnya bukti elektronik yang bersifat volatil dan fana. Ketidaksesuaian antara lambatnya prosedur formal dengan kecepatan perubahan data di ruang maya menciptakan celah hukum yang dapat dimanfaatkan oleh sindikat kejahatan untuk menghapus jejak digital mereka sebelum izin resmi diperoleh.

Sebagai solusi teknis sementara untuk mengatasi kebuntuan hukum tersebut, Indonesia perlu mengoptimalkan jalur kolaborasi taktis melalui jejaring National Central Bureau (NCB) Interpol. Melalui kanal ini, aparat dapat melakukan pertukaran data intelijen pra-penyidikan dan mengajukan mekanisme "pembekuan darurat" terhadap data atau aliran aset digital target dalam hitungan jam tanpa harus menunggu dokumen formal MLA yang berlarut-larut. Strategi ini sangat krusial untuk mengamankan bukti elektronik agar tidak dimutasikan atau dihapus, sembari menunggu penyelesaian prosedur hukum formal antar-negara.

Langkah taktis ini pada akhirnya harus didukung dengan penguatan posisi tawar Indonesia melalui arsitektur diplomasi siber yang lebih modern, termasuk ratifikasi Konvensi Budapest. Dengan mengintegrasikan standar teknis dan nomenklatur tindak pidana global, hambatan *dual criminality* yang sering menghambat akses data lintas batas dapat direduksi secara signifikan. Sinergi antara tindakan operasional *real-time* melalui NCB Interpol dengan reformasi legislasi internasional akan memastikan kedaulatan digital Indonesia tetap substantif di tengah agresivitas perluasan wewenang yurisdiksi asing.

Selanjutnya langkah strategis lain yang dapat dilakukan untuk mengatasi rumitnya

diplomasi tersebut adalah mengoptimalkan jejaring komunikasi intelijen kepolisian global melalui National Central Bureau Interpol (NCB).³⁷ Daripada menunggu surat resmi yang memakan waktu berbulan-bulan, NCB mampu memfasilitasi pertukaran data intelijen pra penyidikan dalam hitungan jam. Informasi non formal namun berharga dapat dipertukarkan melalui jalur aman Interpol seperti dalam kasus pembongkaran sindikat penipuan lintas benua guna memberikan dasar bagi aparat di negara lain untuk segera mengambil tindakan pembekuan sementara terhadap aliran data target. Strategi pembekuan darurat ini sangat krusial guna memastikan bukti elektronik tidak hilang atau terhapus sembari menunggu penyelesaian dokumen formal mekanisme bantuan hukum timbal balik.³⁸

Selain itu, urgensi transformasi peran Badan Siber dan Sandi Negara (BSSN) menjadi agenda yang penting. BSSN tidak lagi memadai jika hanya diposisikan sebagai entitas pertahanan jaringan domestik sebaliknya, institusi ini harus memproyeksikan perannya sebagai garda terdepan dalam diplomasi siber internasional. Kolaborasi strategis dengan otoritas keamanan *cloud global* menjadi sangat penting, mengingat kapasitas mitigasi terhadap lebih dari 361

juta anomali trafik siber di Indonesia.³⁹ Guna merespons tantangan hambatan yurisdiksi dan asas *double criminality*, Indonesia perlu mengintegrasikan diri ke dalam kerangka konvensi internasional yang memiliki daya ikat universal. Dalam konteks ini, penting bagi Indonesia meratifikasi Konvensi Dewan Eropa mengenai Kejahatan Siber tahun 2001 (Budapest Convention).⁴⁰ Walaupun nilai-nilai fundamental konvensi tersebut telah diadopsi ke dalam revisi UU ITE dan KUHP, ketiadaan status Indonesia sebagai negara pihak secara substantif membatasi akses otoritas penegak hukum terhadap kanal kolaborasi *real time* yang eksklusif bagi negara anggota.

Dengan meratifikasi konvensi ini, akan memperkuat dasar hukum Indonesia dalam mengajukan ekstradisi dan *transfer of proceedings*, sehingga hambatan yuridis yang membatasi kolaborasi lintas negara dapat segera dimitigasi. Adopsi konvensi ini juga akan memfasilitasi integrasi sistem hukum nasional dengan standar global, sekaligus menyediakan kerangka kerja untuk menutup celah regulasi dalam penindakan kejahatan siber lintas batas. Partisipasi dalam konvensi ini memungkinkan Indonesia memodernisasi *prosedur transfer of proceedings* serta mengadopsi standarisasi

³⁷ National Central Bureau (NCB) Interpol adalah pusat koordinasi penegakan hukum di setiap negara anggota untuk bekerja sama dengan Interpol. NCB berfungsi sebagai penghubung utama antara kepolisian nasional dan jaringan global dalam memberantas kejahatan transnasional, seperti *cybercrime* dan buronan lintas negara. <https://www.neliti.com/publications/19137/peran-national-central-bureau-ncb-interpol-indonesia-dalam-pemberantasan-tindak>. (Diakses 20 Mei 2026)

³⁸ Midian Hosiholan Rumahorbo, Risa Mahdewi, Desia Rakhma Banjarani. "The Role of Prosecutors in The Effort For Assets Recovery From Corruption Crimes." *Ius Poenale*, Volume 3, Nomor 2, (2022), hlm 87. <https://doi.org/10.25041/ip.v3i2.2752>. (Diakses 20 Mei 2026)..

³⁹ Agung Tri Wicaksono, Ikhsan Fatah Yasin. "Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection." *Al-Jinayah Jurnal Hukum Pidana Islam*, Volume 10, Nomor 2, (2024), hlm 237. <https://doi.org/10.15642/aj.2024.10.2.237-261>. (Diakses 20 Mei 2026).

⁴⁰ Konvensi Dewan Eropa mengenai Kejahatan Siber atau dikenal luas sebagai Konvensi Budapest adalah perjanjian internasional pertama yang mengikat secara hukum untuk mengatasi kejahatan internet dan komputer. Dirancang pada 2001, konvensi ini bertujuan menyelaraskan undang-undang nasional, meningkatkan teknik investigasi, dan memperkuat kerja sama lintas negara. <https://www-crossborderdataforum-org.translate.goog/budapest-convention-what-is-it-and-how-is-it-being-updated/>, (Diakses 20 Mei 2026).

nomenklatur tindak pidana siber yang diakui secara internasional. Dampaknya, penolakan permohonan akses data yang kerap berlandung di balik dalih *double criminality* dapat direduksi secara signifikan.⁴¹

D. PENUTUP

Tarik ulur mengenai supremasi hukum dalam kompleksitas komputasi awan pada akhirnya mengantarkan kita pada kesimpulan mengenai arah kebijakan kedaulatan data nasional. Meninjau rumusan masalah pertama, penegasan asas ekstrateritorialitas melalui pembaruan Undang-Undang Nomor 1 Tahun 2024 serta pengakuan doktrinal terhadap *quasi jurisdiction* telah memberikan legitimasi yang penting bagi aparat penegak hukum Indonesia. Meski tampak kuat secara normatif, efektivitas operasional instrumen ini di lapangan cenderung lemah akibat terbentur tembok kedaulatan asing yang memicu *concurrent jurisdiction* dan polemik *double criminality*.

Beralih pada permasalahan kedua, harmonisasi antara kebijakan lokalisasi data dalam PP Nomor 71 Tahun 2019 dengan instrumen penegakan hukum global belum terwujud optimal. Mekanisme *Mutual Legal Assistance* konvensional yang diharapkan menjadi tulang punggung diplomasi bukti elektronik masih terbebani birokrasi peradilan yang lamban, sehingga tidak koheren dengan karakteristik bukti elektronik pada komputasi awan yang bersifat fana. Temuan ini berimplikasi mendasar bahwa diskursus kedaulatan digital saat ini tidak relevan jika sekadar diukur melalui kemampuan negara dalam memaksakan kendali fisik atas infrastruktur teritorial. Konsep

kedaulatan perlu bergeser menjadi kapabilitas relasional negara untuk memaksakan kontrol operasional, akses, serta perlindungan data secara fungsional lintas yurisdiksi.

Dalam perspektif kebijakan praktis, penelitian ini mensyaratkan transformasi kelembagaan yang komprehensif. Sebagai rekomendasi, pemerintah didorong untuk segera meratifikasi penuh *Budapest Convention* guna mengeliminasi hambatan prosedural *double criminality* serta memastikan akses data lintas batas yang ekspedien. Selain itu, diperlukan investasi strategis untuk memperkuat protokol koordinasi antar agensi yang mengintegrasikan intelijen antara NCB Interpol, BSSN, dan otoritas keamanan siber global.

Sinergi antara kebijakan lokalisasi data nasional yang protektif dengan kemudahan akses bantuan internasional melalui konvensi inklusif merupakan prasyarat mutlak bagi Indonesia untuk membangun ekosistem peradilan siber yang modern, adil, dan berdaulat di era tanpa batas. Transformasi kelembagaan harus mencakup peningkatan kompetensi teknis sumber daya manusia, mengingat disparitas keahlian digital aparat penegak hukum masih menjadi kendala signifikan dalam eksekusi mekanisme forensik siber yang kompleks. Investasi pada pelatihan berkelanjutan dan penguasaan perangkat forensik mutakhir tidak hanya akan mengatasi defisit keahlian teknis yang menghambat investigasi lintas yurisdiksi, tetapi juga krusial bagi aparat dalam mengoptimalkan skema kerja sama internasional untuk penelusuran bukti elektronik secara real-time.

⁴¹ Badan Pembinaan Hukum Nasional, "*Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi*", (2009). https://bphn.go.id/data/documents/kajian_eu_convention_on_cybercrime.pdf, hlm 6-7. (Diakses 20 Mei 2026).

DAFTAR PUSTAKA

Buku

Agus Wibowo and Sri Yulianingsih, *Hukum Teknologi Informasi* (Semarang:Yayasan Prima Agus Teknis, 2023).

Makalah/Artikel/Prosiding/Hasil Penelitian

Abdelkarim, Ya. A. "UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age." *Journal of Digital Technologies and Law*, Volume 3, Nomor 4, (2025), <https://doi.org/10.21202/jdtl.2025.22>.

Agung Tri Wicaksono, Ikhsan Fatah Yasin. "Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection." *Al-Jinayah Jurnal Hukum Pidana Islam*, Volume 10, Nomor 2, (2024). <https://doi.org/10.15642/aj.2024.10.2.237-261>.

Annisa Erikha, Ade Saptomo. "Dilemma of Legal Policy to Address Cybercrime in the Digital Era." *Asian Journal of Social and Humanities*, Volume 3, Nomor 3, (2024). <https://doi.org/10.59888/ajosh.v3i3.452>.

Astuti, A. W., Sayudin, S., & Muharam, A, "Perkembangan Bisnis Di Era Digital," *Jurnal Multidisiplin Indonesia*, Volume 2, Nomor 9, (2023), <https://doi.org/10.58344/jmi.v2i9.554>.

Badan Pembinaan Hukum Nasional, "Kajian EU Convention On Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi", (2009). https://bphn.go.id/data/documents/kajian_eu_convention_on_cybercrime.

Bambang Hartono, Recca Ayu Hapsari. "Mutual Legal Assistance Pada Pemberantasan Cyber Crime Lintas Yurisdiksi Di Indonesia" *SASI*, volume 25, Nomor 1, (2019). <https://doi.org/10.47268/sasi.v25i1.136>.

Cedric Ryngaert. "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts" *German Law Journal*, Volume 24, Nomor 3, (2023). <https://doi.org/10.1017/glj.2023.24>.

Christian Fuchs. "Digital Democracy and the Digital Public Sphere". *Media Communication and Society* Volume 6. (2022). <https://doi.org/10.4324/9781003331087>.

David Leslie. "Don't 'Research Fast and Break Things': On the Ethics of Computational Social

Science." Cornell University, (2022). <https://doi.org/10.48550/arxiv.2206.06370>.

Els De Busser. "EU-US Digital Data Exchange to Combat Financial Crime: Fast Is the New Slow" *German Law Journal*, Volume 19, Nomor 5, (2018), hlm 1258. <https://doi.org/10.1017/s2071832200023026>.

Idham Qrida Nusa, et al. "Law Enforcement of Cybercrime: Tracking Digital Footprints of Cross-Border Hackers" *International Journal of Islamic Education Research and Multiculturalism (IJIERM)*, Volume 7, Nomor 2, (2025), <https://doi.org/10.47006/ijierm.v7i2.475>.

Jean Baptiste Maillart. "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime." *ERA Forum*, Volume 19, Nomor 3, (2018). <https://doi.org/10.1007/s12027-018-0527-2>.

Midian Hosiholan Rumahorbo, Risa Mahdewi, Desia Rakhma Banjarani. "The Role of Prosecutors in The Effort For Assets Recovery From Corruption Crimes." *Ius Poenale*, Volume 3, Nomor 2, (2022). <https://doi.org/10.25041/ip.v3i2.2752>.

Muhammad Prakoso Aji, Putrawan Yuliandri. "Analysis of the Government's Political Will to Achieve Data Sovereignty Through National Data Center Development Policies." *Society*, Volume 13, Nomor 3, Dec. (2025), <https://doi.org/10.33019/society.v13i3.932>.

M. H Syafi'i, et al. "Kajian Ilmu Pertahanan Dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital Di Indonesia." *Journal on Education*, Volume 5, Nomor 2, (2023). <https://doi.org/10.31004/joe.v5i2.1100>.

Olukunle Oladipupo Amoo, et al. "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System". *World Journal of Advanced Research and Reviews*, Volume 21, Nomor 2, (2024), <https://doi.org/10.30574/wjarr.2024.21.2.0438>.

Onyema Onyeani. "The Need To Apply Full Protection And Security (Fps) Standard To Cyber Security: Digital Assets." *Istanbul University*, (2023). <https://dergipark.org.tr/tr/pub/blr/issue/80477/1303597>.

Primavera de Filippi, Smari Mccarthy. "Cloud Computing : Centralization and Data Sovereignty" *HAL (Le Centre Pour La*

- Communication Scientifique Directe), Centre National de la Recherche Scientifique, (2012), <https://hal.science/hal-00746065>.
- Rahayudin, R., Naseer, M., Agustina, N., & Guterres, A. "Digital Sovereignty and The Right To Data: A Comparative Study Between Indonesia, The European Union, and The United States" *Journal of Law and Social Politics*, Volume 3, Nomor 2, (2025). <https://doi.org/10.46799/jlsp.v3i2.71>
- Rasji, Antonio Bravo, Baharuddin Jusuf Habibie Hasta, Matthew Alexander Nainggolan. "Tantangan Demokrasi sebagai Suatu Sistem yang Dinamis di Era Digital: Analisis Pengaruh Media Sosial terhadap Proses Politik Nasional" *Jurnal Ilmu Multidisplin*, Volume 4, Nomor. 1, (2025). <https://doi.org/10.38035/jim.v4i1>.
- Sari, Ratih Mega Puspa. "Analysis of the Implementation of the Criminal Procedure Code in Handling Cyber Crimes: Between Effectiveness and Justice." *Jurnal Hukum Dan Keadilan*, Volume 2, Nomor 6, (2025). <https://doi.org/10.61942/jhk.v2i6.454>.
- Sanghyun Han. "Data and Statecraft: Why and How States Localize Data." *Business and Politics*, Volume 26, Nomor 2, (2024). <https://doi.org/10.1017/bap.2023.41>.
- Sergi Vazquez Maymir. "Anchoring the Need to Revise Cross-Border Access to e-Evidence." *Internet Policy Review*, (2020). <https://doi.org/10.14763/2020.3.1495>.
- Syaiful Anwar, Johan Edi Nepri. "Harmonisasi Hukum Digital: Tantangan Global Dan Strategi Adaptif Indonesia Dalam Era Kedaulatan Siber." *Hutanasyah Jurnal Hukum Tata Negara*, Volume 4, Nomor 1, (2025). <https://doi.org/10.37092/hutanasyah.v4i1.1297>.
- Vijaykumar Shrikrushna Cho, Suryakant S. Bhosale. "Beyond Borders : Addressing the Legal Quagmire of Jurisdiction in Cyberspace." *International Journal For Multidisciplinary Research*, Volume 6, Nomor 6, (2024). <https://doi.org/10.36948/ijfmr.2024.v06i06.30051>.

Website

- Clarifying Lawful Overseas Use of Data (CLOUD) Act. <https://www.justice.gov/criminal/cloud-act-resources>.
- Konvensi Budapest. <https://www-crossborderdataforum-org.translate.google/budapest-convention-what-is-it-and-how-is-it-being-updated/>
- National Central Bureau (NCB) Interpol. <https://www.neliti.com/publications/19137/peran-national-central-bureau-ncb-interpol-indonesia-dalam-pemberantasan-tindak>.

Peraturan Perundang-Undangan

- Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana
- Undang-undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.