

KOLONIALISME DATA DI ERA DIGITAL: ANCAMAN HARMONISASI GLOBAL TERHADAP KEDAULATAN SIBER INDONESIA

Panggalih Husodo¹, Nurul Amin², Andri Rifandi³, Fernandes Situngkir⁴

Universitas Muhammadiyah Kalimantan Timur

Email: ¹2511102437034@umkt.ac.id, ²2511102437038@umkt.ac.id,

³2511102437041@umkt.ac.id, ⁴2511102437045@umkt.ac.id

Abstract: *Global digital transformation has created a new form of colonialism oriented toward the control of data, algorithms, and digital infrastructure through the domination of transnational technology corporations. The phenomenon of data colonialism develops when public data is extracted, monetized, and controlled by global digital platforms without proportional distribution of benefits to developing countries. This study aims to analyze the development of data colonialism through the harmonization of global digital regulations and its implications for Indonesia's cyber sovereignty, while also formulating an ideal legal policy framework to strengthen national data sovereignty. This research employs a doctrinal (normative juridical) legal research method using statutory, conceptual, and philosophical approaches through the analysis of national regulations and the theories of data colonialism, cyber sovereignty, digital dependency, rule of law, and rule of code. The findings reveal that the harmonization of global digital regulations tends to represent the interests of developed countries and global technology corporations through the liberalization of cross-border data flows, which potentially weakens state control over strategic national data. The dominance of foreign digital platforms has caused Indonesia to experience structural dependency on foreign technology and digital infrastructure. The paradigm shift from rule of law to rule of code also demonstrates how algorithms and global platform systems are gradually taking over the state's regulatory functions within digital spaces. Therefore, strengthening Indonesia's cyber sovereignty requires a reformulation of digital legal policies through stronger data localization measures, the development of national data centers, the advancement of domestic technology, the reinforcement of cybersecurity systems, and the establishment of data governance oriented toward national interests and the protection of citizens' digital rights.*

Keywords: *Data Colonialism, Global Harmonization, Cyber Sovereignty, Data Protection.*

Abstrak: Transformasi digital global telah menciptakan bentuk kolonialisme baru yang berorientasi pada penguasaan data, algoritma, dan infrastruktur digital melalui dominasi korporasi teknologi transnasional. Fenomena *data colonialism* berkembang, ketika data masyarakat diekstraksi, dimonetisasi, dan dikendalikan oleh *platform* digital global tanpa distribusi manfaat yang proporsional bagi negara berkembang. Penelitian ini bertujuan untuk menganalisis perkembangan kolonialisme data melalui harmonisasi regulasi digital global serta implikasinya terhadap kedaulatan siber Indonesia, sekaligus merumuskan formulasi kebijakan hukum yang ideal dalam memperkuat kedaulatan data nasional. Penelitian ini menggunakan metode penelitian doktrinal (yuridis normative) dengan pendekatan peraturan perundang-undangan, konseptual, dan filosofis melalui analisis terhadap regulasi nasional, teori *data colonialism*, *cyber sovereignty*, *digital dependency*, *rule of law* dan *rule of code*. Hasil penelitian menunjukkan bahwa harmonisasi regulasi digital global cenderung merepresentasikan kepentingan negara maju dan korporasi teknologi global melalui liberalisasi arus data lintas negara yang berpotensi memperlemah kontrol negara terhadap data strategis nasional. Dominasi platform asing menyebabkan Indonesia mengalami ketergantungan struktural terhadap teknologi dan

infrastruktur digital asing. Pergeseran paradigma dari *rule of law* menuju *rule of code* juga memperlihatkan posisi algoritma dan sistem *platform* global secara bertahap mengambil alih fungsi pengaturan negara dalam ruang digital. Oleh karena itu, penguatan kedaulatan siber Indonesia memerlukan reformulasi kebijakan hukum digital melalui penguatan *data localization*, pembangunan pusat data nasional, pengembangan teknologi domestik, penguatan keamanan siber, dan pembentukan tata kelola data yang berorientasi pada kepentingan nasional serta perlindungan hak digital masyarakat.

Kata kunci: Kolonialisme Data, Harmonisasi Global, Kedaulatan Siber, Perlindungan Data.

PENDAHULUAN

Transformasi digital global telah menggeser data dari komoditas informasi menjadi instrumen kekuasaan ekonomi, politik, bahkan geopolitik (Ambardi et al., 2025). Dalam konfigurasi kapitalisme digital modern, data diproduksi, dikumpulkan, dianalisis, dan diperdagangkan secara masif oleh korporasi teknologi transnasional melalui ekosistem *platform* digital yang terintegrasi lintas negara (Sadowski, 2019). Fenomena ini menciptakan konsep *data colonialism* atau kolonialisme data sebagaimana dikemukakan oleh Nick Couldry dan Ulises A. Mejias yang memandang bahwa praktek ekstraksi data masyarakat sebagai bentuk kolonialisme baru di era digital (Couldry & Mejias, 2023). Jika, kolonialisme klasik berorientasi pada eksploitasi sumber daya alam dan tenaga kerja, maka kolonialisme digital beroperasi melalui penguasaan data, algoritma, infrastruktur komputasi awan (*cloud computing*), dan sistem kecerdasan buatan yang memungkinkan dominasi ekonomi dan pengawasan sosial secara transnasional. Dalam konteks tersebut, individu sebagai subyek hukum tidak hanya menjadi pengguna teknologi, melainkan menjadi obyek eksploitasi digital melalui pengumpulan data masif yang berlangsung secara sistematis, permanen, dan seringkali tanpa distribusi manfaat yang adil.

Perkembangan digitalisasi memperlihatkan adanya pergeseran paradigma dari *rule of law* menuju *rule of code*. Pada sistem *rule of law*, negara

menjadi aktor utama yang mengendalikan tata kelola melalui norma hukum, konstitusi, dan mekanisme regulasi formal (Syafitri & Santos, 2025). Namun, dalam ekosistem digital kontemporer, kekuasaan secara perlahan bergeser ke arah *rule of code*, yaitu situasi ketika algoritma, sistem platform, dan arsitektur teknologi lebih menentukan perilaku sosial dibandingkan hukum negara (Puluhulawa et al., 2026). Lawrence Lessig melalui adagium “*code is law*” menjelaskan bahwa kode digital dan desain teknologi mampu berfungsi layaknya hukum, karena mengatur akses, perilaku, preferensi, hingga kontrol terhadap pengguna secara otomatis tanpa mekanisme demokratis (Hicks, 2023). Akibatnya, otoritas negara mengalami reduksi, karena regulasi nasional seringkali berlaku surut dalam dinamika perkembangan teknologi global yang dikendalikan korporasi digital transnasional. Dalam konteks kolonialisme data, *rule of code* menciptakan bentuk dominasi baru, ketika penguasaan algoritma dan infrastruktur digital memungkinkan korporasi asing menentukan arus informasi, pola konsumsi, perilaku masyarakat, bahkan arah ekonomi digital suatu negara tanpa keterlibatan penuh otoritas nasional.

Indonesia sebagai salah satu pasar digital terbesar di kawasan *Association of Southeast Asian Nations* menghadapi ancaman serius terhadap kedaulatan siber akibat dominasi perusahaan teknologi global, seperti *Google*, *Meta Platforms*, *TikTok*, dan *Amazon* yang menguasai

infrastruktur digital, layanan komputasi awan, distribusi informasi, hingga lalu lintas data nasional (Salistia et al., 2022). Dominasi tersebut, menimbulkan ketergantungan structural, karena sebagian besar data masyarakat Indonesia tersimpan dan diproses melalui sistem digital asing yang berada diluar yurisdiksi penuh negara. Kondisi ini menimbulkan kompleksitas yang serius yang disebabkan oleh lemahnya kapasitas pusat data nasional, rendahnya kemandirian teknologi strategis, terbatasnya penguasaan kecerdasan buatan domestik, dan tingginya indikasi kebocoran data publik serta privat yang menunjukkan disentrigrasi sistem perlindungan data nasional. Dalam perspektif teori dependensi digital (*digital dependency theory*), negara berkembang cenderung berada dalam posisi subordinat karena hanya menjadi pasar pengguna sekaligus sumber data bagi negara dan korporasi maju yang menguasai teknologi inti (Fatmawati et al., 2025).

Urgensi harmonisasi regulasi digital global melalui peraturan perdagangan internasional dan ekonomi digital mendorong liberalisasi arus data lintas negara (*cross border data flow*) dengan dalih efisiensi ekonomi dan integrasi global (Fahriawan et al., 2025). Akan tetapi, harmonisasi tersebut berpotensi menciptakan asimetri kekuasaan digital dalam ruang lingkup negara berkembang, karena dipaksa menyesuaikan regulasi nasional dengan standar global yang didominasi kepentingan negara maju dan korporasi teknologi transnasional. Dalam perspektif teori *cyber sovereignty*, negara seharusnya memiliki otoritas penuh untuk mengatur, melindungi, dan mengendalikan data strategis nasional sebagai bagian dari kedaulatan modern (Kristalia & Wibisono, 2024). Namun, realisasi dari harmonisasi global justru dapat membatasi ruang regulasi nasional, melemahkan kebijakan *data localization*, dan mempersempit kemampuan negara dalam membangun kemandirian infrastruktur digital. Akibatnya, Indonesia beresiko mengalami subordinasi digital,

yakni kondisi ketika negara secara formal tetap berdaulat, tetapi secara substantif kehilangan kontrol atas data, sistem digital, dan arsitektur sibernya sendiri (Syaiful Anwar & Johan Edi Nepri, 2025).

Berdasarkan uraian tersebut, perkembangan kolonialisme data menunjukkan bahwa harmonisasi regulasi digital global dan dominasi korporasi teknologi transnasional telah menciptakan relasi kekuasaan baru yang berpotensi melemahkan kedaulatan siber Indonesia. Pergeseran paradigma dari *rule of law* menuju *rule of code* memperkuat dominasi algoritma dan *platform* digital dalam mengendalikan arus informasi, perilaku pengguna, serta tata kelola data yang sebelumnya berada dalam otoritas negara. Kondisi ini menjadi kompleks, ketika realita menyatakan tingginya ketergantungan Indonesia terhadap infrastruktur digital asing, meningkatnya resiko kebocoran data, dan menguatnya liberalisasi arus data lintas negara yang berpotensi mereduksi kontrol negara atas data strategis nasional. Novelty penelitian ini terlihat pada analisis keterkaitan antara kolonialisme data, harmonisasi digital global, dan pergeseran *rule of law* menuju *rule of code* sebagai faktor yang mempercepat subordinasi digital negara berkembang. Berbeda dengan penelitian lainnya yang hanya berfokus pada perlindungan data atau keamanan siber secara parsial, penelitian ini menawarkan formulasi penguatan kedaulatan siber melalui pendekatan *data localization*, penguatan infrastruktur digital nasional, dan kedaulatan data sebagai instrumen strategis dalam menghadapi dominasi ekosistem digital global. Oleh karena itu, diperlukan reformulasi kebijakan hukum yang mampu menjamin tata kelola digital yang berdaulat, adaptif, dan berorientasi pada kepentingan nasional.

METODE

Penelitian ini menggunakan metode penelitian doktrinal dengan pendekatan

yuridis normatif (Yulia Audina Sukmawan, 2025), berfokus pada analisis terhadap norma hukum, prinsip kedaulatan siber, regulasi perlindungan data, dan kebijakan tata kelola ruang digital nasional maupun internasional. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan komparatif (*comparative approach*). Bahan hukum primer terdiri atas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta instrumen regulasi internasional terkait tata kelola data digital. Bahan hukum sekunder diperoleh dari jurnal ilmiah, teori kolonialisme data, teori kedaulatan siber, literatur keamanan siber, dan kebijakan digital global. Analisis dilakukan secara preskriptif analitis untuk menemukan formulasi hukum yang mampu memperkuat kedaulatan data Indonesia di era harmonisasi digital global.

HASIL DAN PEMBAHASAN

Kolonialisme Data sebagai Bentuk Dominasi Baru di Era Digital

Perkembangan transformasi digital global dalam teori *data colonialism* oleh Nick Couldry dan Ulises A. Mejias menjelaskan bahwa data diposisikan sebagai sumber daya ekonomi baru (*new raw material*) yang diekstraksi secara sistematis melalui aktivitas digital masyarakat (Couldry & Mejias, 2019). Praktek tersebut, dilakukan melalui media sosial, mesin pencarian (internet), layanan *cloud computing*, *e-commerce*, hingga aplikasi berbasis kecerdasan buatan yang secara terus-menerus mengumpulkan perilaku, preferensi, lokasi, komunikasi, dan identitas pengguna (user). Dalam konteks ini, kolonialisme digital bekerja melalui mekanisme pengawasan (*surveillance*), ekstraksi data, dan monetisasi informasi tanpa melibatkan

penguasaan teritorial secara langsung (Riski M Baskoro, 2025).

Secara faktual, Indonesia menjadi salah satu target utama ekonomi data global karena memiliki jumlah pengguna internet dan media sosial yang sangat besar. Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna Internet di Indonesia akan mencapai 221.563.479 jiwa pada tahun 2024, dari jumlah penduduk Indonesia sebesar 278.696.200 jiwa pada tahun 2023. Berdasarkan hasil Survei Penetrasi Internet Indonesia 2024 yang dipublikasikan oleh APJII, tingkat penetrasi internet Indonesia meningkat sebesar 79,5% (Prasetyo et al., 2024). Besarnya aktivitas digital tersebut, menjadikan Indonesia sebagai pasar strategis bagi korporasi teknologi global yang menguasai infrastruktur *cloud*, sistem algoritma, dan distribusi lalu lintas data nasional. Akan tetapi, dominasi tersebut menimbulkan ketimpangan struktural, karena Indonesia lebih banyak berperan sebagai penyedia data mentah, sedangkan penguasaan nilai ekonomi digital, teknologi inti, dan kontrol informasi tetap terpusat pada negara maju serta korporasi transnasional. Dalam perspektif teori *digital dependency*, kondisi ini menciptakan ketergantungan struktural negara berkembang terhadap teknologi asing, karena kemampuan penguasaan infrastruktur digital nasional masih sangat terbatas (Islam & Jerin, 2025).

Dominasi korporasi teknologi global juga memperlihatkan adanya pergeseran paradigma, Lawrence Lessig melalui konsep *code is law* menegaskan bahwa kode digital mampu berfungsi layaknya hukum karena dapat mengatur akses, preferensi, perilaku, dan kontrol pengguna secara otomatis melalui sistem teknologi. Akibatnya, korporasi digital global memperoleh kekuatan *quasi sovereign* yang memungkinkan mereka menentukan pola komunikasi, distribusi informasi, hingga perilaku ekonomi masyarakat lintas negara tanpa pengawasan penuh negara (Indarta, 2025).

Dalam konteks Indonesia, kondisi ini menyebabkan lemahnya kontrol terhadap lalu lintas data nasional, ketergantungan terhadap sistem *cloud* asing, dan minimnya kedaulatan negara atas algoritma digital strategis.

Secara sosiologis, masyarakat Indonesia telah mengalami transformasi digital yang mengakibatkan menjadi obyek eksploitasi ekonomi berbasis data tanpa kesadaran penuh mengenai nilai strategis data pribadi. Mayoritas pengguna *platform* digital secara *indirectly* menyerahkan data melalui mekanisme *consent* formalistik tanpa memahami data tersebut diproses, dianalisis, dan dimonetisasi oleh korporasi digital (Bagenda et al., 2025). Kondisi tersebut, dalam teori *surveillance capitalism* Shoshana Zuboff yang menjelaskan bahwa perilaku manusia telah dikomodifikasi menjadi bahan baku utama ekonomi digital (Zuboff, 2022). Masyarakat tidak hanya berperan sebagai konsumen teknologi, tetapi juga menjadi sumber produksi data yang terus dieksploitasi untuk kepentingan iklan digital, prediksi perilaku, hingga pengembangan kecerdasan buatan. Ketimpangan relasi kuasa ini memperlihatkan bahwa pengguna tidak memiliki posisi tawar yang setara terhadap korporasi digital global dalam pengelolaan data pribadinya.

Secara filosofis, kolonialisme data bertentangan dengan prinsip keadilan digital dan kedaulatan negara modern. Dalam teori keadilan distributif, manfaat ekonomi digital seharusnya didistribusikan secara proporsional kepada masyarakat dan negara yang menghasilkan data (Hidayanto, 2026). Namun, realitas ekonomi digital menunjukkan bahwa keuntungan terbesar justru terpusat pada korporasi teknologi global yang menguasai infrastruktur, algoritma, dan sistem pemrosesan data. Negara berkembang seperti Indonesia hanya menjadi pasar pengguna sekaligus objek ekstraksi data tanpa memperoleh kemandirian teknologi yang memadai. Situasi tersebut, menciptakan

ketimpangan digital (*digital inequality*) yang memperkuat subordinasi ekonomi dan teknologi terhadap negara maju. Oleh karena itu, data tidak lagi dapat dipandang sekadar komoditas ekonomi, melainkan bagian dari aset strategis negara yang berkaitan langsung dengan keamanan nasional, hak privasi, dan kedaulatan siber.

Secara yuridis, Indonesia telah memiliki dasar hukum perlindungan data melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur hak subyek data, kewajiban pengendali data, transfer data lintas negara, hingga sanksi administratif dan pidana. Pasal 56, UU PDP mengatur bahwa transfer data pribadi ke luar wilayah Indonesia hanya dapat dilakukan apabila negara penerima memiliki tingkat perlindungan data yang setara atau lebih tinggi, terdapat perlindungan hukum yang mengikat, atau memperoleh persetujuan subjek data pribadi. Namun secara substantif, UU PDP belum secara tegas mengatur kewajiban *data localization* strategis nasional, sehingga sebagian besar data masyarakat Indonesia tetap tersimpan pada sistem dan pusat data asing. Kondisi tersebut, menunjukkan bahwa regulasi nasional masih cenderung kompromistis terhadap liberalisasi arus data lintas negara yang didorong oleh harmonisasi ekonomi digital global.

Selain itu, lemahnya kapasitas infrastruktur digital nasional semakin memperkuat posisi subordinatif Indonesia dalam tata kelola ruang siber global. Insiden kebocoran data nasional pada tahun 2024 menunjukkan bahwa sistem data strategis nasional masih menghadapi persoalan serius terkait keamanan siber, integrasi sistem, dan ketahanan infrastruktur digital (Imanuel Toding Bua & Nur Isdah Idris, 2025). Faktor lainnya menunjukkan bahwa belum optimalnya pembentukan lembaga pengawas perlindungan data pribadi dan lambatnya penyusunan regulasi turunan UU PDP menyebabkan penegakan hukum perlindungan data di Indonesia masih

berada dalam *grey area* kepastian hukum. Negara Indonesia belum memiliki kapasitas regulatif dan teknologis yang cukup kuat untuk mengimbangi dominasi korporasi digital global.

Maka, kolonialisme data tidak hanya menjadi persoalan ekonomi digital, melainkan telah berkembang menjadi ancaman terhadap kedaulatan siber Indonesia. Penguasaan data, algoritma, dan infrastruktur digital oleh korporasi asing berpotensi melemahkan otoritas negara dalam mengendalikan ruang siber nasional, menentukan arah kebijakan digital, dan melindungi kepentingan strategis masyarakat. Oleh karena itu, penguatan regulasi nasional, pembangunan pusat data domestik, pengembangan teknologi nasional, serta penerapan kebijakan kedaulatan data (*data sovereignty*) menjadi langkah strategis untuk mencegah terjadinya subordinasi digital Indonesia terhadap kepentingan global.

Harmonisasi Global dan Ancaman terhadap Kedaulatan Siber Indonesia

Harmonisasi regulasi digital global pada dasarnya bertujuan menciptakan interoperabilitas sistem ekonomi digital internasional melalui standarisasi tata kelola data, perdagangan elektronik, kecerdasan buatan, dan arus data lintas negara (Utomo et al., 2025). Dalam kerangka ekonomi digital global, harmonisasi memiliki peranan penting untuk mempercepat integrasi pasar, efisiensi layanan digital, dan memperluas investasi teknologi transnasional. Namun realitanya, harmonisasi regulasi digital seringkali bertendensi pada kompleksitas dalam menjaga netralitas, karena lebih merepresentasikan kepentingan negara maju dan korporasi teknologi global yang memiliki dominasi terhadap infrastruktur digital, algoritma, dan sistem *cloud computing*. Harmonisasi global berpotensi menjadi instrumen baru dalam mempertahankan hegemoni digital negara maju terhadap negara berkembang melalui liberalisasi arus data global.

Konsep *free flow of data* yang menjadi agenda utama ekonomi digital internasional pada prinsipnya mendorong kebebasan transfer data lintas negara tanpa hambatan regulatif yang ketat, dalam gagasan tersebut banyak didorong dalam forum internasional, seperti *World Trade Organization*, *Group of Twenty*, dan kerja sama ekonomi digital regional (Chin, 2022). Akan tetapi, liberalisasi data tersebut menimbulkan persoalan serius bagi negara berkembang, karena mempersempit ruang negara dalam mengendalikan data strategis nasional. Dalam perspektif teori *cyber sovereignty*, negara memiliki hak eksklusif untuk mengatur, mengontrol, dan melindungi ruang digital domestik sebagai bagian dari kedaulatan modern (Indra Duari, Muhammad Saiful, 2025). Konsep ini berkembang kuat di negara, seperti Cina dan Rusia yang menerapkan kontrol ketat terhadap data domestik dan infrastruktur digital nasional. Namun, tekanan global terhadap liberalisasi data justru menciptakan dilema bagi negara berkembang, seperti Indonesia antara kebutuhan integrasi ekonomi digital global dan kepentingan perlindungan keamanan nasional.

Secara faktual, Indonesia menghadapi ketergantungan yang tinggi terhadap infrastruktur digital asing dan sebagian besar layanan digital nasional bergantung pada sistem *cloud computing* global yang dikuasai oleh *Amazon Web Services*, *Google Cloud*, dan *Microsoft* (Rahardian, 2025). Kondisi tersebut, menyebabkan lalu lintas dan penyimpanan data nasional berada dalam ekosistem teknologi asing yang tidak sepenuhnya berada di bawah yurisdiksi Indonesia. Padahal data strategis nasional, khususnya yang berkaitan dengan sektor pemerintahan, keuangan, kesehatan, pertahanan, dan pelayanan publik, memiliki keterkaitan langsung dengan keamanan nasional. Dalam konteks geopolitik digital, penguasaan infrastruktur data tidak hanya menghasilkan keuntungan ekonomi, tetapi juga menciptakan kekuatan strategis

dalam pengawasan, kontrol informasi, dan dominasi teknologi global (Chhaty et al., 2025).

Kerentanan tersebut, menjadi problematika kontinu yang dibuktikan melalui tingginya kasus kebocoran data di Indonesia. Kebocoran data yang melibatkan institusi publik maupun sektor privat menunjukkan lemahnya sistem keamanan siber nasional serta rendahnya kesiapan infrastruktur digital domestik. Pada tahun 2021, data pengguna BPJS Kesehatan dilaporkan bocor hingga mencapai sekitar 279 juta data penduduk Indonesia yang diperjualbelikan di forum *daring* (Komdigi.com, 2021). Selain itu, Kebocoran data juga terjadi pada Komisi Pemilihan Umum, sektor perbankan, hingga berbagai *platform* digital nasional yang melibatkan data pribadi masyarakat. Pada tahun 2023, dugaan kebocoran data pemilih tetap milik KPU dilaporkan mencapai sekitar 204 juta data warga negara yang diperjualbelikan di forum *daring*, termasuk data Nomor Induk Kependudukan, kartu keluarga, dan informasi identitas lainnya (Wibowo, 2024). Sedangkan, sektor perbankan dan layanan finansial digital menghadapi ancaman serangan siber berupa *phishing*, pencurian identitas, hingga akses ilegal terhadap data nasabah yang menunjukkan tingginya kerentanan sistem keamanan digital nasional (Ilman Maulana Kholis, 2025). Dalam perspektif teori *risk society*, Ulrich Beck menjelaskan bahwa perkembangan teknologi modern menciptakan bentuk resiko baru yang bersifat global, tidak terprediksi, dan sulit dikendalikan oleh negara (Kusvianti et al., 2023). Resiko tersebut, dalam konteks digital muncul melalui kebocoran data, pengawasan siber, manipulasi algoritma, dan dominasi infrastruktur teknologi asing.

Secara yuridis, Indonesia telah memiliki beberapa instrumen hukum terkait keamanan siber dan perlindungan data, antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi

dan Transaksi Elektronik (UU ITE) sebagaimana diubah terakhir melalui Undang-Undang Nomor 1 Tahun 2024, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Akan tetapi, pengaturan tersebut masih menghadapi berbagai kelemahan substantif dan implementatif. PP 71 Tahun 2019 misalnya membuka peluang penyelenggara sistem elektronik lingkup privat untuk melakukan pengelolaan data di luar wilayah Indonesia sepanjang memenuhi syarat efektivitas pengawasan. Kebijakan tersebut menunjukkan adanya kecenderungan kompromi terhadap liberalisasi arus data lintas negara dibanding penguatan kebijakan lokalisasi data nasional. Hal ini menyebabkan negara Indonesia belum optimal melaksanakan kontrol penuh terhadap penyimpanan dan pengelolaan data strategis domestik.

Harmonisasi global juga berpotensi memengaruhi independensi kebijakan nasional dalam tata kelola data digital. Dalam perjanjian ekonomi digital internasional, negara berkembang seringkali berada dalam posisi tawar yang lemah, karena ketergantungan terhadap investasi dan teknologi asing. Kondisi tersebut, menciptakan asimetri kekuasaan digital (*digital power asymmetry*) antara negara maju dan negara berkembang. Harmonisasi regulasi digital global juga memiliki tendensi mempersempit ruang negara dalam menerapkan kebijakan proteksi data nasional, pengembangan industri digital domestik, dan penguatan keamanan siber nasional. Secara sosiologis, ketergantungan terhadap platform dan infrastruktur digital asing juga menciptakan kerentanan pengawasan digital (*digital surveillance*). Korporasi teknologi global memiliki kemampuan untuk mengumpulkan, memetakan, dan menganalisis perilaku masyarakat secara masif melalui algoritma dan kecerdasan buatan. Dalam konteks tertentu, penguasaan data tersebut dapat digunakan untuk kepentingan ekonomi, politik, bahkan geopolitik. Realita yang terjadi,

seperti skandal *Cambridge Analytica* menunjukkan posisi data pengguna media sosial dapat dimanfaatkan untuk memengaruhi preferensi politik dan perilaku pemilih dalam proses demokrasi (Rahmatullah, 2021). Hal ini memperlihatkan bahwa data tidak hanya menjadi aset ekonomi, tetapi merupakan instrumen kekuasaan strategis yang mampu memengaruhi stabilitas sosial dan politik suatu negara.

Dalam perspektif geopolitik digital, negara yang menguasai data, algoritma, dan kecerdasan buatan akan memiliki superioritas ekonomi serta kontrol strategis terhadap masyarakat global. Data menjadi fondasi utama untuk pengembangan kecerdasan buatan (*Artificial Intelligence*), ekonomi digital, teknologi pertahanan, dan sistem pengawasan modern. Oleh karena itu, perebutan dominasi data global pada hakikatnya merupakan bentuk kontestasi kekuasaan baru antarnegara di era digital. Dalam konteks tersebut, negara Indonesia tidak hanya berperan sebagai pasar digital dan penyedia data mentah, tetapi harus memperkuat kedaulatan siber nasional melalui pembangunan pusat data domestik, penguatan keamanan siber, pengembangan teknologi nasional, serta penerapan regulasi perlindungan data yang lebih progresif dan berorientasi pada kepentingan nasional.

Reformulasi Kebijakan Kedaulatan Data Nasional sebagai Strategi Perlindungan Siber Indonesia

Penguatan kedaulatan siber Indonesia memerlukan reformulasi kebijakan hukum digital yang tidak hanya berorientasi pada pertumbuhan ekonomi digital, tetapi juga perlindungan data strategis nasional, keamanan siber, dan kemandirian teknologi domestik. Dalam konteks geopolitik digital modern, data telah berkembang menjadi aset strategis negara yang memiliki keterkaitan langsung dengan keamanan nasional, stabilitas ekonomi, pertahanan, hingga pengambilan kebijakan publik. Oleh karena itu, tata kelola data tidak dapat

diserahkan pada mekanisme pasar digital global, melainkan harus ditempatkan dalam kerangka kedaulatan negara (*state sovereignty*) dan *cyber sovereignty*. Dalam hal ini, negara memiliki hak eksklusif untuk mengatur, mengontrol, dan melindungi ruang digital domestik sebagai bagian dari integritas nasional di era teknologi informasi.

Pertama, negara perlu memperkuat kebijakan *data localization* terhadap data strategis nasional guna memastikan kontrol yurisdiksi tetap berada dibawah otoritas Indonesia. Kebijakan lokalisasi data menjadi penting karena sebagian besar data masyarakat Indonesia saat ini masih tersimpan pada infrastruktur *cloud computing* asing yang berada diluar kendali penuh negara. Padahal data pemerintahan, kesehatan, keuangan, pertahanan, dan pelayanan publik merupakan bagian dari aset strategis nasional yang berpotensi memengaruhi keamanan negara apabila dikelola pihak asing. Secara yuridis, pengaturan mengenai lokalisasi data dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mewajibkan Penyelenggara Sistem Elektronik publik menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia, namun ketentuan tersebut belum sepenuhnya mencakup sektor strategis privat yang mengelola data masyarakat dalam skala besar. Dominasi layanan *cloud* asing seperti *Amazon Web Services*, *Google Cloud*, dan *Microsoft Azure* tetap menciptakan ketergantungan struktural terhadap teknologi luar negeri.

Kedua, diperlukan penguatan regulasi transfer data lintas negara (*cross border data flow*) melalui mekanisme pengawasan ketat terhadap korporasi digital global yang beroperasi di Indonesia. Liberalisasi arus data global dalam rezim ekonomi digital internasional berpotensi memperlemah kontrol negara terhadap data strategis nasional. Dalam prakteknya, korporasi teknologi transnasional memiliki kemampuan untuk memindahkan, memproses, dan

memonetisasi data masyarakat lintas yurisdiksi tanpa pengawasan optimal negara berkembang. Oleh karena itu, implementasi UU PDP harus diperkuat melalui pengawasan independen, audit keamanan data, dan mekanisme sanksi yang efektif terhadap pelanggaran transfer data internasional. Dalam implementasi norma tersebut, masih menghadapi persoalan lemahnya pengawasan teknis dan belum optimalnya kelembagaan pengawas perlindungan data pribadi nasional. Kondisi ini menunjukkan bahwa regulasi perlindungan data belum sepenuhnya mampu mengimbangi kecepatan perkembangan teknologi digital global.

Ketiga, pembangunan pusat data nasional, penguatan teknologi domestik, dan pengembangan ekosistem kecerdasan buatan nasional menjadi langkah strategis untuk mengurangi ketergantungan terhadap teknologi asing. Secara faktual, Indonesia masih menghadapi persoalan rendahnya kapasitas infrastruktur digital nasional dan tingginya ketergantungan terhadap teknologi impor. Gangguan Pusat Data Nasional menunjukkan bahwa sistem data strategis nasional masih rentan terhadap serangan siber dan lemahnya integrasi infrastruktur digital. Selain itu, dominasi *platform* asing menyebabkan sebagian besar nilai ekonomi digital nasional mengalir keluar negeri melalui monetisasi data dan layanan teknologi. Oleh karena itu, negara perlu mendorong investasi strategis pada pusat data nasional, industri semikonduktor, pengembangan kecerdasan buatan domestik, serta riset keamanan siber untuk memperkuat kemandirian teknologi nasional.

Secara yuridis, implementasi kebijakan perlindungan data harus diintegrasikan dengan kebijakan keamanan siber nasional dan tata kelola ekonomi digital. Regulasi perlindungan data tidak dapat berdiri sendiri, karena ancaman kolonialisme digital berkaitan langsung dengan keamanan nasional, pertahanan siber, dan stabilitas ekonomi negara. Oleh sebab itu, diperlukan

harmonisasi antara UU PDP dan UU ITE, serta kebijakan keamanan siber nasional dalam satu kerangka regulasi yang terpadu. Selain itu, pembentukan otoritas perlindungan data independen menjadi penting untuk memastikan pengawasan terhadap korporasi digital berjalan efektif dan tidak terfragmentasi secara kelembagaan. Dalam perspektif *rule of law*, negara harus tetap menjadi aktor utama dalam mengendalikan tata kelola ruang digital, agar fungsi regulasi tidak sepenuhnya diambil alih oleh mekanisme algoritma dan korporasi global sebagaimana terjadi dalam fenomena *rule of code*.

Secara filosofis, kedaulatan data merupakan bagian dari hak negara untuk melindungi kepentingan publik dan martabat digital masyarakat. Data pribadi tidak hanya dipandang sebagai komoditas ekonomi, melainkan bagian dari hak asasi manusia (HAM) yang berkaitan dengan privasi, kebebasan, dan kontrol individu terhadap identitas digitalnya. Dalam prinsip keadilan digital, distribusi manfaat ekonomi digital seharusnya berlangsung secara proporsional dan tidak hanya terpusat pada korporasi teknologi global. Maka, negara memiliki legitimasi moral dan konstitusional untuk melakukan intervensi regulatif guna melindungi masyarakat dari eksploitasi data yang bersifat monopolistik dan eksploitatif.

Sedangkan, secara sosiologis peningkatan literasi digital dan kesadaran masyarakat mengenai perlindungan data pribadi menjadi faktor penting dalam menghadapi kolonialisme data global. Rendahnya kesadaran masyarakat terhadap keamanan digital menyebabkan pengguna seringkali menyerahkan data pribadi tanpa memahami resiko penyalahgunaan data, pengawasan digital, maupun manipulasi algoritma. Kondisi tersebut, memperkuat praktek *surveillance capitalism*, karena masyarakat secara tidak sadar menjadi objek produksi data ekonomi digital. Maka, negara harus memperkuat pendidikan literasi digital, keamanan siber, dan etika penggunaan teknologi

melalui kebijakan pendidikan nasional, serta kampanye publik yang berkelanjutan. Dengan demikian, masyarakat tidak hanya menjadi pengguna teknologi, tetapi juga memiliki kesadaran kritis terhadap hak digitalnya.

SIMPULAN

Kolonialisme data merupakan bentuk dominasi baru di era digital yang beroperasi melalui penguasaan data, algoritma, dan infrastruktur teknologi oleh korporasi digital transnasional. Praktek tersebut, menunjukkan bahwa relasi kekuasaan global tidak hanya berorientasi pada penguasaan wilayah fisik, melainkan pada kontrol terhadap data sebagai aset strategis ekonomi, politik, dan geopolitik modern. Harmonisasi regulasi digital global yang mendorong liberalisasi arus data lintas negara (*cross border data flow*) pada realitanya cenderung merepresentasikan kepentingan negara maju dan korporasi teknologi global, sehingga memperkuat asimetri kekuasaan digital antara negara maju dan negara berkembang. Dalam konteks negara Indonesia, dominasi *platform* asing telah menciptakan ketergantungan struktural terhadap teknologi dan infrastruktur digital luar negeri yang berdampak pada lemahnya kontrol negara terhadap data strategis nasional. Pergeseran paradigma dari *rule of law* menuju *rule of code* memperlihatkan bahwa algoritma, sistem *platform*, dan arsitektur teknologi digital secara bertahap mengambil alih fungsi pengaturan negara dalam ruang siber yang menyebabkan negara Indonesia menghadapi keterbatasan dalam mengendalikan lalu lintas data, mengawasi aktivitas korporasi digital global, dan melindungi keamanan siber nasional.

Oleh karena itu, penguatan kedaulatan siber Indonesia memerlukan reformulasi kebijakan hukum digital yang berorientasi pada perlindungan data strategis nasional, penguatan keamanan

siber, dan kemandirian teknologi domestik. Negara harus memperkuat kebijakan *data localization*, memperkuat pengawasan transfer data lintas negara, membangun pusat data nasional, dan mengembangkan ekosistem teknologi dan kecerdasan buatan nasional guna mengurangi ketergantungan terhadap teknologi asing. Selain itu, integrasi antara kebijakan perlindungan data pribadi, keamanan siber, dan tata kelola ekonomi digital menjadi langkah strategis, agar posisi negara tetap memiliki otoritas utama dalam mengendalikan ruang siber nasional. Dengan demikian, negara Indonesia tidak hanya menjadi pasar digital dan objek eksploitasi data global, tetapi mampu menjadi negara berdaulat yang memiliki kontrol penuh terhadap tata kelola data dan masa depan digital nasional

DAFTAR PUSTAKA

- Ambardi, K., Widhyharto, D. S., Madya, S. H., & Wibawanto, G. R. (2025). *Masyarakat digital: Teknologi kekuasaan dan kekuasaan teknologi*. UGM Press.
- Bagenda, C., Harimurti, D. A., Maria, A., Djou, G., & Bosco, Y. D. (2025). Legalitas Monetisasi Data Pengguna Oleh Perusahaan Perlindungan Konsumen Dan Hukum Perekonomian Nasional Teknologi. *Jurnal Kolaboratif Sains*, 8(12), 8708–8716. <https://doi.org/10.56338/jks.v8i12.7939>
- Chhaty, H., Almubaroq, H. Z., & Risdhianto, A. (2025). Geoekonomi Digital Dan Dampaknya Terhadap Perekonomian Nasional Indonesia. *Jurnal Economica*, 13(2), 332–344. <https://doi.org/10.46750/economica.v13i2.415>
- Chin, Y. C. (2022). Governing Cross-Border Data Flows: International trade agreements and their limits. *MDPI Laws*, 11(4), 1–29.

- <https://doi.org/10.13140/RG.2.2.24810.39360>
- Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television and New Media*, 20(4), 336–349. <https://doi.org/10.1177/1527476418796632>
- Couldry, N., & Mejias, U. A. (2023). The decolonial turn in data and technology research: what is at stake and where is it heading? *Information Communication and Society*, 26(4), 786–802. <https://doi.org/10.1080/1369118X.2021.1986102>
- Fahriawan, H., Hasibuan, I. H., & Rahmawati, A. (2025). Global Digital Trade Regulation : An International Law Perspective on Cross-Border Data Flows and Privacy Standards. *Jurnal Ilmu Hukum Dan Sosial (HAKIM)*, 3(3), 1291–1304. <https://doi.org/10.51903/qgrchv12>
- Fatmawati, F., Alisyahbana, A. N. Q. A., & Nurbayani, S. U. (2025). *Digital Monopoly: Unveiling The Dynamics Of Market Power And The New Era Of Economic Regulation*. Penerbit Tahta Media.
- Hicks, A. (2023). Transparency, Compliance, And Contestability When Code Is(n't) Law. In *ACM International Conference Proceeding Series* (Vol. 1, Issue 1). Association for Computing Machinery. <https://doi.org/10.1145/3584318.3584854>
- Hidayanto, S. (2026). Mewujudkan Keadilan Digital : Analisis Kesenjangan Akses Informasi. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, 4(1), 5456–5472. <https://doi.org/10.61104/alz.v4i1.4058>
- Ilman Maulana Kholis. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, 4(2), 275–299. <https://doi.org/10.14421/t5sfe747>
- Immanuel Toding Bua, & Nur Isdah Idris. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, 2(2), 100–114. <https://doi.org/10.62383/desentralisasi.v2i2.653>
- Indarta, Y. (2025). *Cyber Law: Dimensi Hukum dalam Era Digital*. Pustaka Galeri Mandiri.
- Indra Duari, Muhammad Saiful, H. P. (2025). Kedaulatan Siber Tantangan dan Implikasi terhadap Hukum Internasional Modern. *Legal Note*, 1(2), 31–36. <https://doi.org/10.1039/AN9396400737>
- Islam, R., & Jerin, A. J. (2025). Digital Dependency and Political Economy in Developing Countries : A Theoretical and Empirical Analysis. *Interdisiplin: Journal of Qualitative and Quantitative Research*, 2(5), 357–368. <https://doi.org/10.61166/interdisiplin.v2i5.127>
- Komdigi.com. (2021). *Gerak Cepat Kominfo Melindungi Data Pribadi*. <https://www.komdigi.go.id/berita/artikel/detail/gerak-cepat-kominfo-melindungi-data-pribadi>
- Kristalia, B. Y. Y., & Wibisono, I. W. (2024). Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari. *JUKIM: Jurnal Ilmiah Multidisiplin*, 3(2), 83–93. <https://doi.org/10.56127/jukim.v3i02.1584>
- Kusvianti, P., Ashari, A. P. R., & Izzah, A. N. (2023). Pandangan Ulrich Beck Tentang Risiko dan Ketidakpastian yang Dialami Oleh Masyarakat Modern. *Jurnal Ilmiah Ecosystem*, 23(1), 149–163. <https://doi.org/10.35965/eco.v23i1.2495>

- Prasetyo, S. M., Gustiawan, R., Albani, F. R., Komputer, I., Informatika, T., Pamulang, U., & Selatan, T. (2024). Pertumbuhan Tingkat Penetrasi Indonesia. *BIIKMA : Buletin Ilmiah Ilmu Komputer Dan Multimedia*, 2(1), 65–71.
- Puluhulawa, F. Y., Kurniasih, S., Utami, A. D., & Widowati, I. G. A. R. (2026). *Media, Budaya, Dan Komunikasi*. CV. Hei Publishing Indonesia.
- Rahardian, R. L. (2025). Analisa Perbandingan Cloud Management Pada Google Cloud Platform dan Amazon Web Services. *Digital Transformation Technology*, 5(1), 97–106.
<https://doi.org/10.47709/digitech.v5i1.5862>
- Rahmatullah, T. (2021). Teknologi Persuasif: Aktor Penting Media Sosial Dalam Mengubah Sikap Dan Perilaku Pengguna. *Jurnal Soshum Insentif*, 4(1), 60–78.
<https://doi.org/10.36787/jsi.v4i1.509>
- Riski M Baskoro, U. R. (2025). Melampaui Batas-Batas Vincent Mosco: Memperluas Ranah Ekonomi Politik Media Ke Ruang Digital. *Jurnal Netnografi Komunikasi (JNK)*, 4(1), 99–115.
<https://doi.org/10.59408/jnk.v4i1.96>
- Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data and Society*, 6(1), 1–12.
<https://doi.org/10.1177/2053951718820549>
- Salistia, F., Junaedi, D., & Amalia, R. S. (2022). Ekosistem SDM dan Inovasi Ekonomi Digital di Indonesia. *Sci-Tech Journal*, 2(1), 11–31.
<https://doi.org/10.56709/stj.v2i1.60>
- Syafitri, M., & Santos, A. J. (2025). Tantangan dan Solusi Penerapan Prinsip Rule of Law dalam Sistem Hukum Indonesia. *Karimah Tauhid*, 4(4), 2248–2257.
<https://doi.org/10.30997/karimahtauhid.v4i4.18674>
- Syaiful Anwar, & Johan Edi Nepri. (2025). Harmonisasi Hukum Digital: Tantangan Global dan Strategi Adaptif Indonesia dalam Era Kedaulatan Siber. *Hutanasyah: Jurnal Hukum Tata Negara*, 4(1), 69–88.
<https://doi.org/10.37092/hutanasyah.v4i1.1297>
- Utomo, A. P., Ibrohim, N. M., Ramadhani, N., Muhammad, N., & Wahyuaristy, D. S. (2025). Konsep Ideal Regulasi Identitas Digital Tunggal dalam Konvergensi Teknologi sebagai Instrumen Penguatan Perdagangan Digital Berbasis Ekonomi Virtual The Ideal Concept of Single Digital Identity Regulation in Technological Convergence as an Instrument to S. *Forschungsforum Law Journal*, 2(2), 119–141.
<https://doi.org/10.35586/flj.v2i02.11161>
- Wibowo, M. K. T. (2024). Tanggung Jawab Komisi Pemilihan Umum Atas Kegagalan Pelindungan Data Pribadi Dalam Pemilihan Umum Tahun 2024. *Media Hukum Indonesia (MHI)*, 2(4), 88–95.
<https://doi.org/10.5281/zenodo.14008008>
- Yulia Audina Sukmawan, D. D. (2025). Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum. *Notary Law Journal*, 4(1), 114–128.
<https://doi.org/10.32801/nolaj.v4i3.116>
- Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. In *Organization Theory* (Vol. 3).
<https://doi.org/10.1177/26317877221129290>