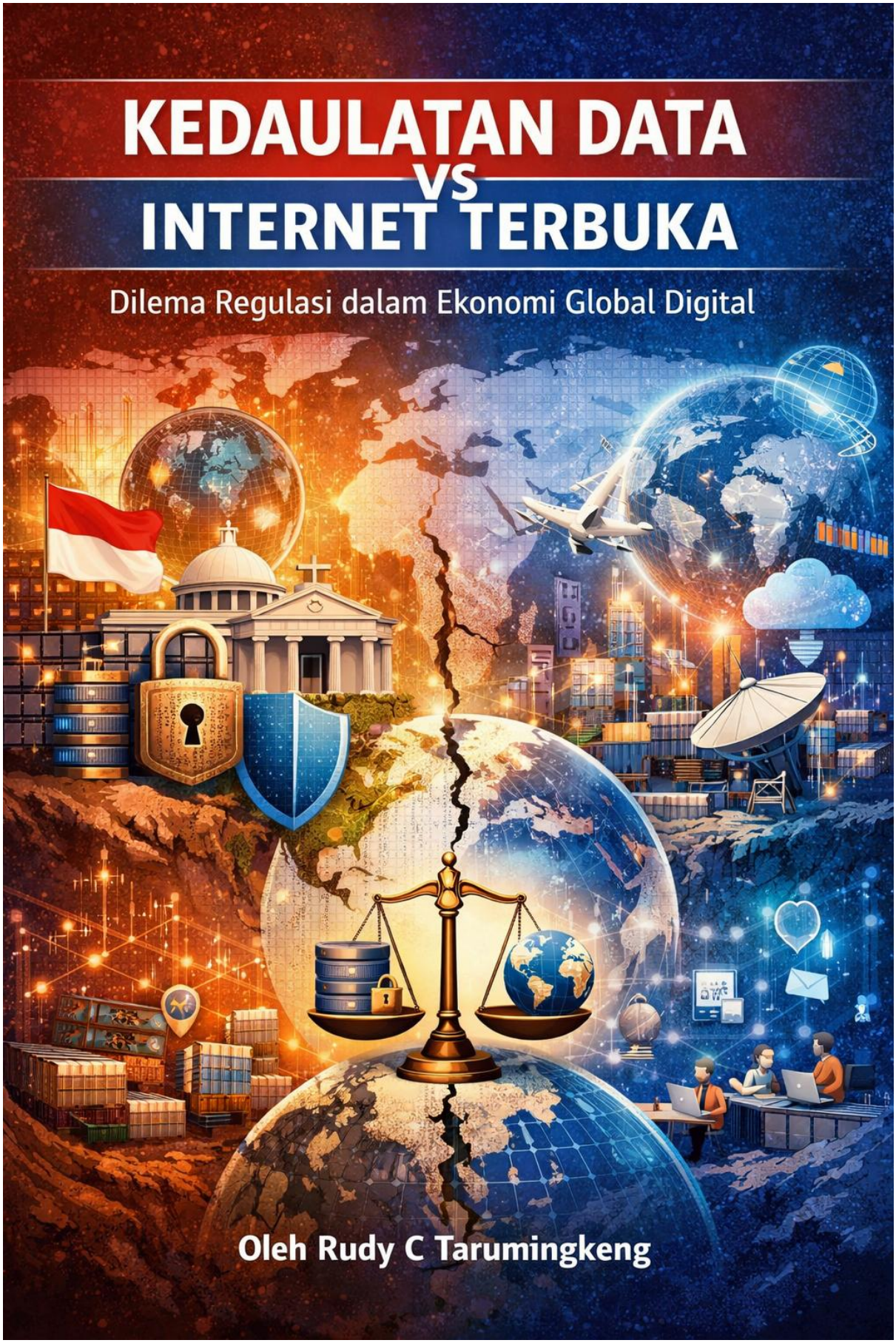
KEDAULATAN DATA
VS
INTERNET TERBUKA
Dilema Regulasi dalam Ekonomi Global Digital
Oleh Rudy C Tarumingkeng

Oleh:
Prof Ir Rudy C Tarumingkeng, PhD
Professor of Management NUP: 9903252922
Rektor, Universitas Cenderawasih, Papua (1978-1988, dan
Rektor, Kampus AGRO Manokwari sekarang Universitas Papua Manokwari)
Coordinator, CIDA/DIKTI SFU Burnaby BC Canada 1988-1991
Rektor, Universitas Kristen Krida Wacana, Jakarta (1991-2000)
Ketua Dewan Guru Besar, IPB-University, Bogor (2005-2006)
AI - Data Analyst, dan Ketua Senat Akademik, IBM-ASMI, Jakarta 2024-

---

rudyct75@gmail.com
1 Maret 2026

KEDAULATAN DATA VS. INTERNET TERBUKA: DILEMA REGULASI DALAM EKONOMI GLOBAL DIGITAL

1. Pendahuluan

Perdebatan mengenai **kedaulatan data** dan **internet terbuka** telah menjadi salah satu isu sentral dalam ekonomi global digital. Pada masa awal internet komersial, banyak kalangan membayangkan ruang digital sebagai wilayah yang relatif tanpa batas: informasi bergerak lintas negara, perusahaan dapat melayani pasar global dari satu pusat komputasi, dan inovasi lahir dari keterhubungan yang luas. Namun, seiring pertumbuhan ekonomi digital, negara-negara menyadari bahwa data bukan sekadar "jejak" aktivitas daring, melainkan sumber daya strategis yang menentukan daya saing industri, keamanan nasional, perlindungan warga, kapasitas fiskal, bahkan kedaulatan politik. OECD menekankan bahwa di jantung perdagangan digital terdapat arus data lintas batas; data bukan hanya sarana produksi dan distribusi, tetapi juga aset yang diperdagangkan dan medium yang mengorganisasi rantai nilai global. Pada saat yang sama, OECD juga menegaskan bahwa arus data lintas batas perlu dipadukan dengan kepercayaan—*data free flow with trust*—karena isu privasi, keamanan, dan kekayaan intelektual tidak dapat diabaikan. (OECD)

Ketegangan itu makin nyata ketika nilai perdagangan digital meningkat cepat. WTO melaporkan bahwa ekspor jasa yang dikirim secara digital mencapai **US$ 4,25 triliun pada 2023**, naik 9 persen dari tahun

sebelumnya dan menyumbang **13,8 persen** dari ekspor barang dan jasa dunia. Sebelumnya, jasa yang dikirim secara digital telah mencapai **US$ 3,82 triliun pada 2022**, atau sekitar **54 persen** dari total ekspor jasa global. Angka-angka ini menunjukkan bahwa ekonomi digital bukan lagi lapisan tambahan di atas ekonomi "riil", melainkan bagian struktural dari perdagangan internasional kontemporer. Dengan demikian, pertanyaan regulasinya bukan lagi apakah data perlu diatur, melainkan **bagaimana** mengatur data tanpa mematikan inovasi, perdagangan, dan keterhubungan. (World Trade Organization)

Di sinilah dilema muncul. Di satu sisi, negara memerlukan instrumen untuk memastikan bahwa data warganya tidak diproses secara sewenang-wenang, bahwa data strategis nasional tidak bocor ke yurisdiksi yang lemah perlindungannya, dan bahwa perusahaan digital global tidak mengekstraksi nilai ekonomi tanpa akuntabilitas. Di sisi lain, apabila regulasi terlalu proteksionis—misalnya melalui lokalisasi data yang luas, larangan transfer lintas batas, atau rezim perizinan yang berat—maka biaya ekonomi meningkat, inovasi berbasis komputasi awan melambat, UMKM digital kehilangan akses ke pasar global, dan internet mulai terfragmentasi menjadi sekumpulan "intranet nasional". OECD bahkan menyatakan bahwa tidak adanya regulasi sama sekali bukan solusi optimal, tetapi pembatasan menyeluruh terhadap arus data juga dapat menekan pertumbuhan; rezim yang menggabungkan arus data dengan kepercayaan justru menghasilkan luaran ekonomi yang lebih baik. (OECD)

Perserikatan Bangsa-Bangsa melalui **Global Digital Compact** juga menangkap ketegangan ini. Dokumen tersebut merumuskan visi tentang masa depan digital yang **inklusif, terbuka, berkelanjutan, adil, aman, dan terlindungi**, sekaligus mengakui bahwa arus data lintas batas merupakan penggerak kritis ekonomi digital dan perlu dikelola secara aman, terjamin, dan tepercaya. Dengan kata lain, komunitas internasional mulai bergerak dari dua ekstrem—*laissez-faire digital* versus

proteksionisme data—menuju upaya mencari tata kelola yang lebih bertanggung jawab, interoperabel, dan berpihak pada pembangunan. (United Nations)

Tulisan ini berargumentasi bahwa dilema "kedaulatan data versus internet terbuka" sesungguhnya bukan pilihan biner. Masalah utamanya terletak pada pencarian desain regulasi yang mampu menyeimbangkan **empat kepentingan besar** sekaligus: efisiensi ekonomi, perlindungan hak, keamanan strategis, dan distribusi nilai pembangunan. Untuk itu, pembahasan akan bergerak dari definisi konseptual, akar konflik regulasi, model-model global yang sedang berkembang, hingga implikasinya bagi Indonesia.

2. Memahami Dua Kutub: Kedaulatan Data dan Internet Terbuka

Secara konseptual, **kedaulatan data** dapat dipahami sebagai klaim bahwa negara, masyarakat, atau subjek hukum tertentu memiliki hak untuk menentukan bagaimana data tentang warganya, institusinya, dan aktivitas ekonomi di dalam yurisdiksinya dikumpulkan, diproses, disimpan, dipindahkan, dan dimanfaatkan. Dalam versi yang sempit, kedaulatan data sering diterjemahkan menjadi **lokalisasi data**: kewajiban agar data disimpan atau diproses di dalam negeri. Dalam versi yang lebih luas, kedaulatan data juga mencakup hak menentukan standar perlindungan, kewajiban transfer, syarat persetujuan, audit, akses aparat, serta tata kelola nilai ekonomi yang dihasilkan dari data. UNCTAD mencatat bahwa terdapat alasan kebijakan publik yang sah bagi negara untuk mengatur arus data lintas batas, termasuk perlindungan privasi dan hak asasi lain, keamanan nasional, serta tujuan pembangunan ekonomi. (UN Trade and Development (UNCTAD))

Sementara itu, **internet terbuka** bukan berarti internet tanpa hukum. Internet terbuka merujuk pada ekosistem digital yang relatif interoperabel, berbasis standar bersama, memungkinkan pertukaran informasi lintas batas, tidak terfragmentasi secara berlebihan, dan

memberi ruang bagi inovasi, kompetisi, dan partisipasi lintas negara. Dalam kerangka ekonomi, internet terbuka memungkinkan perusahaan menggunakan infrastruktur komputasi awan global, mengintegrasikan rantai pasok digital, melakukan pembayaran elektronik lintas yurisdiksi, serta menjual jasa yang dikirim secara digital ke pasar internasional. OECD menegaskan bahwa transformasi digital telah menurunkan biaya partisipasi dalam perdagangan internasional, mengubah apa yang diperdagangkan, bagaimana diperdagangkan, dan siapa yang dapat ikut serta. Namun, digitalisasi itu juga melahirkan tantangan regulasi baru yang mempersulit upaya pemerintah untuk merealisasikan potensi perdagangan digital secara inklusif. (OECD)

Dengan demikian, kedua konsep itu tidak sepenuhnya bertolak belakang. Kedaulatan data lahir dari kebutuhan akan **otoritas**, sedangkan internet terbuka lahir dari kebutuhan akan **interoperabilitas**. Ketika suatu negara memperketat kontrol demi melindungi hak atau keamanan, ia berpotensi mengurangi interoperabilitas. Sebaliknya, ketika suatu rezim terlalu mendorong keterbukaan arus data, ia berpotensi mengurangi kontrol domestik atas privasi, penegakan hukum, dan distribusi manfaat ekonomi. Dilema regulasi muncul justru karena kedua kebutuhan itu sama-sama sah.

3. Mengapa Konflik Ini Menguat?

Ada beberapa alasan mengapa perdebatan ini semakin tajam.

Pertama, **data telah menjadi faktor produksi**. Dalam ekonomi industri klasik, negara memperebutkan bahan baku, tenaga kerja, dan modal. Dalam ekonomi digital, data ikut menjadi sumber daya kunci untuk melatih model AI, mengoptimalkan logistik, mempersonalisasi pemasaran, menilai risiko kredit, dan mengembangkan produk berbasis platform. OECD menyebut bahwa data berada di pusat teknologi yang berkembang pesat seperti AI, komputasi awan, Internet of Things, dan

manufaktur aditif. Karena itu, kontrol atas data makin diasosiasikan dengan kontrol atas inovasi dan daya saing. (OECD)

Kedua, **konsentrasi kekuatan digital** memicu kekhawatiran negara berkembang. UNCTAD berulang kali menekankan bahwa ekonomi digital global sangat terkonsentrasi pada sejumlah kecil ekonomi dan perusahaan besar, sehingga pertanyaan "untuk siapa data mengalir?" menjadi relevan. Jika data mentah mengalir keluar sementara nilai tambah analitik, kecerdasan buatan, dan monetisasi terkonsentrasi di pusat-pusat teknologi global, maka negara berkembang berisiko hanya menjadi penyedia data tanpa memperoleh bagian proporsional dari nilai ekonomi yang tercipta. (UN Trade and Development (UNCTAD))

Ketiga, **privasi dan hak warga** menjadi isu politik dan hukum utama. Gelombang kebocoran data, profilisasi, iklan perilaku, serta pengambilan keputusan otomatis telah mengubah privasi dari isu teknis menjadi isu konstitusional. Laporan kedua Komisi Eropa tentang penerapan GDPR menegaskan bahwa GDPR merupakan salah satu landasan pendekatan Uni Eropa terhadap transformasi digital, dengan prinsip dasar pemrosesan data yang adil, aman, dan transparan sehingga individu tetap memegang kendali atas data pribadinya. Ini menunjukkan bahwa bagi banyak yurisdiksi, regulasi data kini diperlakukan sebagai bagian dari rezim hak dasar, bukan sekadar kebijakan perdagangan. (EUR-Lex)

Keempat, **keamanan nasional** dan **geopolitik** masuk ke ruang data. Negara tidak lagi melihat data hanya sebagai komoditas ekonomi, tetapi juga sebagai unsur keamanan. Artikel kebijakan resmi pemerintah Tiongkok, misalnya, menekankan perlunya memastikan arus data lintas batas yang aman dan sah, disertai peninjauan keamanan nasional atas aktivitas seperti pemrosesan data dan arus data lintas batas. Dengan demikian, data memasuki ranah yang sebelumnya didominasi oleh isu pertahanan, intelijen, dan kedaulatan teritorial. (State Council of China)

Kelima, **ketidaksinkronan rezim hukum antarnegara** menambah beban pelaku usaha. OECD mencatat bahwa ketidakpastian rezim privasi dan ketidakcocokan rezim hukum merupakan hambatan utama bagi arus data lintas batas. Perusahaan global harus mengelola perbedaan definisi data pribadi, syarat persetujuan, kewajiban audit, hak subjek data, dan syarat transfer antarrezim. Akibatnya, masalahnya bukan hanya "boleh atau tidak boleh" data mengalir, tetapi juga "dengan syarat hukum yang mana". (OECD)

4. Mengapa Negara Menuntut Kedaulatan Data?

Argumen untuk kedaulatan data biasanya berangkat dari empat dimensi.

Dimensi pertama adalah **perlindungan warga**. Negara memiliki kewajiban untuk memastikan bahwa data pribadi tidak ditransfer ke yurisdiksi yang perlindungannya lebih lemah. Di Indonesia, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, dan pelindungannya sebagai upaya menjamin hak konstitusional subjek data. Undang-undang ini mewajibkan pengendali data melindungi keamanan data, mencegah akses tidak sah, dan untuk pemrosesan berisiko tinggi melakukan penilaian dampak pelindungan data pribadi. Ini menunjukkan bahwa regulasi data ditempatkan dalam kerangka perlindungan hak, bukan semata administrasi teknologi. (JDIH Kemkomdigi)

Dimensi kedua adalah **penegakan hukum dan akuntabilitas yurisdiksional**. Tanpa kontrol tertentu, data warga negara dapat berada di server atau pengendali yang sulit dijangkau aparat penegak hukum domestik. Dalam logika negara, hal ini menyulitkan investigasi kebocoran, penipuan, pencurian identitas, atau pelanggaran konsumen. Karena itu, banyak negara tidak selalu melarang transfer data, tetapi menuntut adanya dasar hukum yang membuat pelaku di luar negeri tetap akuntabel.

Dimensi ketiga adalah **keamanan strategis**. Negara dapat memandang jenis data tertentu—misalnya data pertahanan, infrastruktur kritis, kesehatan populasi, atau mobilitas warga—sebagai aset strategis. Dalam konteks ini, tuntutan kedaulatan data mirip dengan tuntutan kedaulatan energi atau pangan: negara tidak mau bergantung sepenuhnya pada sistem luar yang tidak dikendalikan sendiri. Hal ini makin kuat di tengah rivalitas geopolitik, sanksi ekonomi, dan kekhawatiran mengenai akses pemerintah asing terhadap data yang disimpan di luar negeri. (UN Trade and Development (UNCTAD))

Dimensi keempat adalah **nilai tambah pembangunan**. Negara berkembang khawatir bahwa arus data yang sepenuhnya terbuka justru mempercepat ekstraksi nilai oleh perusahaan platform global. Jika data konsumen, pola mobilitas, preferensi pasar, dan perilaku transaksi terus mengalir ke luar negeri lalu diproses menjadi kecerdasan bisnis, model AI, dan keuntungan iklan oleh entitas asing, maka keuntungan terbesar dari ekonomi data tidak tinggal di dalam negeri. Dalam perspektif ini, kedaulatan data dipahami bukan hanya sebagai pembatasan, tetapi sebagai strategi pembangunan industri digital domestik.

Narasi ini tampak meyakinkan, dan dalam banyak hal memang sah. Namun, masalahnya muncul ketika konsep kedaulatan data direduksi menjadi kebijakan tunggal berupa **lokalisasi menyeluruh**. Di sinilah argumen tandingan dari kubu internet terbuka menjadi penting.

5. Mengapa Internet Terbuka Tetap Diperlukan?

Argumen untuk internet terbuka tidak semata datang dari perusahaan teknologi besar. Ia juga berhubungan dengan fungsi ekonomi digital modern secara umum.

Pertama, **perdagangan digital dan jasa lintas batas sangat bergantung pada arus data**. Jasa konsultasi, pendidikan daring, telehealth, perangkat lunak berbasis langganan, desain, riset, pemasaran

digital, sistem pembayaran, hingga logistik modern berjalan di atas pertukaran data yang relatif lancar. OECD secara eksplisit menyatakan bahwa pada jantung perdagangan digital terdapat arus data, sementara WTO dan Bank Dunia menunjukkan besarnya nilai ekspor jasa yang dikirim secara digital. Artinya, membatasi arus data secara berlebihan sama dengan membatasi salah satu mesin pertumbuhan utama abad ke-21. (OECD)

Kedua, **UMKM dan negara berkembang juga diuntungkan oleh keterbukaan tertentu**. Dalam banyak kasus, perusahaan kecil tidak mampu membangun pusat data sendiri, mengelola redundansi server, atau memenuhi semua kebutuhan komputasi secara lokal. Mereka bergantung pada layanan awan global yang efisien dan skalabel. Internet terbuka menurunkan biaya masuk ke pasar, memungkinkan usaha kecil menjual lintas negara, dan memberi akses pada alat digital yang sebelumnya hanya dinikmati perusahaan besar. Itulah sebabnya WTO dan Bank Dunia sering menekankan bahwa perdagangan digital membuka jalur baru bagi perusahaan kecil dan menengah untuk memasuki pasar global. (World Bank Blogs)

Ketiga, **inovasi AI modern memerlukan ekosistem data dan komputasi yang terhubung**. Model AI, keamanan siber, analitik penipuan, maupun layanan platform global bergantung pada integrasi data dari banyak lokasi. Karena itu, regulasi yang terlalu teritorial dapat mengurangi kualitas layanan, memperlambat eksperimen, dan menghambat pembelajaran mesin yang memerlukan skala. APEC bahkan mencatat pentingnya lingkungan kebijakan yang mendukung adopsi AI, termasuk keterbukaan perbatasan untuk jasa digital, regulasi penggunaan data yang jelas, akuntabilitas, dan kepastian hukum yang lebih baik. (APEC)

Keempat, **fragmentasi internet menimbulkan biaya nyata**. OECD menunjukkan bahwa langkah-langkah lokalisasi data dapat menaikkan

biaya pengelolaan data sebesar **15–55 persen**. OECD juga mencatat bahwa jika semua negara membatasi arus data, PDB global dapat turun **5 persen**. Sebaliknya, jika negara mengadopsi rezim yang menggabungkan arus data dengan kepercayaan, PDB global dapat naik **1,77 persen** dan ekspor **3,6 persen**. Bahkan untuk lokalisasi data, OECD/WTO memperkirakan bahwa penghapusan langkah-langkah lokalisasi yang ada akan mendorong ekspor naik **0,26 persen** dan PDB naik **0,18 persen**, dengan keuntungan yang berpotensi lebih besar bagi ekonomi berpendapatan rendah. (OECD)

Di titik ini terlihat bahwa internet terbuka bukan proyek ideologis belaka. Ia merupakan kondisi operasional bagi ekonomi digital global. Karena itu, kebijakan yang baik bukanlah menolak keterbukaan, melainkan **mendisiplinkan keterbukaan**.

6. Dari Keterbukaan Tanpa Aturan ke Keterbukaan Bersyarat

Salah satu kesalahan terbesar dalam debat publik adalah menganggap bahwa pilihan regulasi hanya ada dua: membiarkan data mengalir bebas atau menahannya di dalam negeri. Padahal, praktik global menunjukkan adanya spektrum model antara kedua kutub itu.

OECD memakai istilah **Data Free Flow with Trust (DFFT)** untuk merumuskan gagasan bahwa arus data memang harus difasilitasi, tetapi tidak dengan mengorbankan kepercayaan. Dalam pendekatan ini, fokus regulasi bergeser dari "apakah data boleh keluar?" menjadi "dalam kondisi apa data boleh keluar, kepada siapa, untuk tujuan apa, dengan jaminan apa, dan dengan mekanisme penegakan apa?" OECD juga menyimpulkan bahwa rezim tanpa regulasi sama sekali bukanlah pilihan optimal; hasil ekonomi terbaik justru lahir dari kombinasi keterbukaan dan tata kelola yang kredibel. (OECD)

UN Global Digital Compact bergerak ke arah yang sama. Dokumen ini tidak mendorong proteksionisme data, tetapi juga tidak mengidealkan

kebebasan total. Ia menekankan tata kelola data yang bertanggung jawab, adil, dan interoperabel, serta pembentukan dialog multistakeholder tentang tata kelola data di semua level. Jadi, arah global yang mulai terbaca adalah **keterbukaan bersyarat**, bukan keterbukaan absolut. (United Nations)

7. Pelajaran dari Uni Eropa: Arus Data Ya, Tetapi dengan Adequacy dan Hak Dasar

Uni Eropa merupakan contoh penting bagaimana suatu kawasan berusaha mempertahankan keterbukaan ekonomi digital tanpa melepaskan perlindungan hak. Dalam laporan kedua penerapan GDPR, Komisi Eropa menegaskan bahwa GDPR adalah salah satu pilar pendekatan UE terhadap transformasi digital, dengan prinsip pemrosesan yang adil, aman, dan transparan, serta orientasi bahwa individu tetap memegang kendali atas data. Laporan itu juga menekankan bahwa salah satu fokus utama evaluasi GDPR adalah **fungsi transfer internasional data pribadi ke negara ketiga** di bawah Bab V GDPR. (EUR-Lex)

Keunikan model Eropa adalah bahwa ia **tidak menutup arus data**, melainkan mensyaratkannya. Dalam keputusan kecukupan (*adequacy decision*) 2025, Komisi Eropa kembali menyatakan bahwa arus data personal ke luar Uni Eropa penting bagi perluasan perdagangan lintas batas dan kerja sama internasional, tetapi tingkat perlindungan data warga Uni tidak boleh dirusak oleh transfer tersebut. Standar yang dipakai bukanlah peniruan sempurna hukum UE, melainkan perlindungan yang "secara esensial ekuivalen". Ini adalah contoh bahwa kedaulatan data dapat diterjemahkan ke dalam mekanisme **kecukupan, kesetaraan perlindungan, supervisi, dan penegakan**, bukan semata lokalisasi fisik. (EUR-Lex)

Hubungan UE–AS juga menunjukkan logika interoperabilitas itu. Situs resmi **Data Privacy Framework** menyatakan bahwa kerangka tersebut

menyediakan mekanisme yang andal bagi organisasi AS untuk menerima transfer data pribadi dari Uni Eropa, Inggris, dan Swiss. Di pihak AS, Departemen Kehakiman melalui Executive Order 14086 membentuk **Data Protection Review Court (DPRC)** sebagai tingkat kedua dari mekanisme redres yang mengikat. Dari sini terlihat bahwa solusi politik-hukum yang dicari bukanlah pemutusan arus data transatlantik, melainkan penciptaan **jembatan kepercayaan institusional**. (dataprivacyframework.gov)

Pelajaran akademiknya jelas: rezim yang matang berusaha memindahkan perdebatan dari pertanyaan geografis—"server di mana?"—menuju pertanyaan normatif dan institusional—"apakah ada perlindungan setara, pengawasan independen, dan jalur pemulihan hak?" Itu merupakan bentuk kedaulatan yang lebih canggih.

8. Pelajaran dari Asia-Pasifik: Interoperabilitas Praktis melalui APEC CBPR

Kawasan Asia-Pasifik menawarkan pendekatan yang cenderung lebih pragmatis. APEC mengembangkan **Cross-Border Privacy Rules (CBPR) system** sebagai mekanisme yang menyeimbangkan arus informasi lintas batas dengan perlindungan efektif atas data pribadi, yang penting bagi kepercayaan pasar daring. APEC menegaskan bahwa CBPR membangun seperangkat aturan dasar yang disepakati bersama, sehingga dapat menjembatani perbedaan pendekatan privasi domestik antar-ekonomi. Pada 2025, APEC melaporkan bahwa **sembilan ekonomi** dan **82 perusahaan terdaftar** telah berpartisipasi dalam sistem CBPR. Di samping itu, APEC juga memiliki **Cross-border Privacy Enforcement Arrangement (CPEA)** sebagai kerangka kerja sama regional bagi otoritas penegak hukum privasi. (APEC)

Nilai model APEC bukan pada kekuatan hak dasar setingkat GDPR, melainkan pada upaya menciptakan **mekanisme interoperabilitas yang operasional**. Bagi banyak ekonomi Asia-Pasifik yang sistem hukumnya

beragam, pendekatan seperti ini penting karena dapat mengurangi biaya koordinasi, meningkatkan kepercayaan bisnis, dan menyediakan jalur kerja sama penegakan tanpa memaksakan harmonisasi total. Dalam bahasa yang lebih sederhana, APEC mencoba menjawab pertanyaan: apabila dunia tidak mungkin memiliki satu hukum privasi global, dapatkah kita setidaknya memiliki **mekanisme saling percaya yang dapat dipakai bersama?**

9. China dan India: Dua Variasi Kedaulatan Data yang Sedang Berkembang

Tiongkok sering dibaca sebagai contoh kuat dari pendekatan kedaulatan data yang lebih berorientasi negara. Sumber resmi pemerintahnya menekankan perlindungan informasi pribadi, tata kelola data publik, personal, dan korporasi, serta perlunya memastikan arus data lintas batas yang aman dan sah. Kebijakan tersebut juga mengaitkan arus data lintas batas dengan infrastruktur perdagangan digital, partisipasi dalam pembentukan standar internasional, dan peninjauan keamanan nasional. Dalam logika ini, data dipandang sekaligus sebagai sumber daya ekonomi, objek regulasi keamanan, dan instrumen tata kelola negara. (State Council of China)

India memberi contoh yang berbeda: bukan menutup diri sepenuhnya, melainkan membangun rezim nasional yang kuat sambil tetap mengakui kebutuhan pemrosesan data untuk tujuan yang sah. **Digital Personal Data Protection Act, 2023** menyatakan secara eksplisit bahwa hukum itu dibuat untuk mengakui hak individu melindungi data personalnya sekaligus kebutuhan memproses data tersebut untuk tujuan yang sah. Regulasi lanjutannya, **Digital Personal Data Protection Rules, 2025**, dipublikasikan pada November 2025 dengan pemberlakuan bertahap. Ini menunjukkan bahwa negara besar seperti India juga bergerak ke arah tata kelola data yang lebih berdaulat, tetapi tidak identik dengan pelarangan total arus data. (MeitY)

Dari dua contoh ini, tampak bahwa "kedaulatan data" sendiri bukan konsep tunggal. Ada versi yang sangat berorientasi keamanan-negara, ada pula versi yang lebih menekankan perlindungan hak dan kapasitas institusional domestik. Perbedaan ini penting karena sering kali debat publik memperlakukan semua regulasi data ketat sebagai satu kategori yang sama, padahal motif, instrumen, dan dampaknya bisa berbeda jauh.

10. WTO, ASEAN, dan Tata Kelola Regional: Antara Fragmentasi dan Konvergensi

Di tingkat perdagangan multilateral, WTO belum menjadi arena penyelesaian final, tetapi tetap penting. Pada 2024, perundingan *Joint Initiative on E-commerce* mencapai tahap draf yang distabilkan dan memasuki fase finalisasi politik. Pada Desember 2024, anggota yang berpartisipasi mengajukan komunikasi ke General Council untuk memasukkan *Agreement on E-commerce* ke dalam kerangka WTO, sambil tetap membuka negosiasi isu yang belum selesai. Fakta bahwa pembahasan masih berlangsung menunjukkan bahwa dunia belum mencapai konsensus penuh, tetapi juga memperlihatkan adanya dorongan kuat untuk mencegah fragmentasi regulasi digital yang terlalu jauh. (World Trade Organization)

ASEAN bergerak dengan cara yang lebih regional dan mungkin lebih relevan bagi Indonesia. Ringkasan studi resmi **ASEAN Digital Economy Framework Agreement (DEFA)** menyatakan bahwa negosiasi formal antarnegara anggota dimulai pada Desember 2023 dengan target penyelesaian pada akhir 2025. Pada Oktober 2025, Dewan Masyarakat Ekonomi ASEAN menyatakan **substantial conclusion** atas negosiasi DEFA dan menekankan visi ekonomi digital ASEAN yang ditopang oleh aturan yang memungkinkan arus barang, jasa, dan data yang **lancar dan aman**. Studi ASEAN sebelumnya bahkan memperkirakan bahwa DEFA yang ambisius dapat membantu mendorong ekonomi digital ASEAN mendekati **US$ 2 triliun pada 2030**. (ASEAN Main Portal)

Bagi kawasan seperti ASEAN, dilema regulasi tidak dapat diselesaikan dengan meniru sepenuhnya Eropa, Amerika, atau Tiongkok. Negara-negara ASEAN memiliki tingkat kesiapan hukum, kapasitas institusional, dan struktur ekonomi digital yang berbeda. Karena itu, DEFA menarik justru karena mencoba merancang **keterbukaan regional yang aman**, bukan keterbukaan liar. Ini sangat sesuai bagi negara berkembang yang membutuhkan pasar digital regional, tetapi tidak ingin melepaskan perlindungan dan kebijakan pembangunan.

11. Risiko Jika Kedaulatan Data Diterjemahkan secara Berlebihan

Meskipun kedaulatan data memiliki dasar normatif yang kuat, penerjemahan yang terlalu ekstrem dapat menimbulkan beberapa masalah.

Pertama, ia dapat berubah menjadi **proteksionisme digital terselubung**. Ketika kewajiban lokalisasi diterapkan terlalu luas, pelaku asing dan domestik menghadapi kenaikan biaya infrastruktur, duplikasi penyimpanan, kebutuhan kepatuhan lintas sistem, serta keterbatasan skalabilitas. OECD mencatat bahwa hampir **100 langkah lokalisasi data** telah berlaku di sekitar **40 negara** pada awal 2023, dan lebih dari dua pertiganya menggabungkan kewajiban penyimpanan dengan larangan aliran data. Ini berarti tren menuju restriksi memang nyata dan semakin ketat. (OECD)

Kedua, kebijakan yang terlalu keras dapat merugikan **negara berkembang sendiri**. OECD/WTO menemukan bahwa penghapusan langkah lokalisasi yang ada justru berpotensi memberi kenaikan PDB yang lebih besar bagi ekonomi berpendapatan rendah. Artinya, negara yang paling berharap memperoleh manfaat dari proteksi belum tentu menjadi pihak yang paling diuntungkan olehnya. Dalam banyak kasus, ekonomi kecil justru lebih bergantung pada integrasi digital untuk mengakses pasar, teknologi, dan layanan global. (OECD)

Ketiga, lokalisasi yang luas tidak otomatis menghasilkan **kedaulatan teknologi**. Menyimpan data di dalam negeri tidak serta-merta berarti pusat analitik, algoritme, chip, layanan awan, dan platform strategis juga dimiliki domestik. Negara bisa saja memiliki "data lokal", tetapi tetap bergantung pada perangkat lunak, perangkat keras, dan penyedia layanan asing. Jika demikian, lokalisasi hanyalah kedaulatan administratif, bukan kedaulatan teknologi substantif.

Keempat, pembatasan yang terlalu besar bisa melahirkan **internet yang terpecah**. Risiko ini bukan sekadar teknis, tetapi juga ekonomi dan sosial. Fragmentasi berarti meningkatnya biaya kepatuhan, menurunnya interoperabilitas sistem, sulitnya kolaborasi riset, turunnya efisiensi lintas batas, dan menyempitnya ruang inovasi. Karena itu, pertanyaan kebijakan yang baik bukan apakah suatu negara berhak mengatur data—jelas berhak—melainkan **sejauh mana** pengaturan itu diperlukan, **di sektor apa**, dan **dengan dasar risiko apa**.

12. Risiko Jika Internet Terbuka Diterjemahkan secara Naif

Sebaliknya, kubu internet terbuka juga dapat jatuh pada penyederhanaan yang berbahaya bila menganggap semua pembatasan sebagai hambatan perdagangan.

Pertama, keterbukaan tanpa tata kelola membuka ruang bagi **regulatory arbitrage**. Perusahaan dapat memindahkan data ke yurisdiksi dengan aturan lebih longgar, memanfaatkan perbedaan rezim, dan menghindari akuntabilitas yang diharapkan warga negara asal data. Di sini, "kebebasan arus data" dapat berubah menjadi "kebebasan memilih hukum yang paling lemah".

Kedua, internet terbuka tanpa perlindungan memadai memperbesar risiko **surveillance capitalism**. Data perilaku warga dikumpulkan, digabungkan, diprofilkan, dan dimonetisasi dalam skala besar, sering kali tanpa pemahaman penuh dari subjek data. Komisi Eropa secara

konsisten menempatkan kendali individu atas data sebagai pilar transformasi digital. Jika kendali itu hilang, maka keterbukaan ekonomi digital dibayar dengan pelemahan otonomi warga. (EUR-Lex)

Ketiga, keterbukaan penuh dapat memperdalam **ketimpangan nilai tambah**. UNCTAD menyoroti pertanyaan tentang bagaimana manfaat data dibagi secara adil dan bagaimana pendekatan tata kelola data perlu relevan bagi pembangunan. Tanpa mekanisme pembagian manfaat, ekonomi data global cenderung memperkuat konsentrasi pada sedikit negara dan perusahaan besar. (Sustainable Development Goals)

Keempat, pendekatan yang semata-mata menekankan efisiensi ekonomi sering meremehkan kenyataan bahwa **negara tetap aktor sentral** dalam perlindungan hak, keamanan, dan ketertiban digital. Dalam ekonomi digital, internet terbuka tidak mungkin bertahan lama tanpa legitimasi politik. Dan legitimasi politik menuntut adanya perlindungan yang dapat dirasakan publik.

13. Posisi Indonesia: Menarik Antara Perlindungan, Keterbukaan, dan Diplomasi Regional

Indonesia berada pada posisi yang sangat menarik. Sebagai ekonomi digital besar di Asia Tenggara, Indonesia membutuhkan internet yang relatif terbuka untuk e-commerce, fintech, logistik digital, AI, pendidikan daring, layanan profesional, dan integrasi UMKM ke pasar regional. Namun, sebagai negara berpenduduk besar dengan sensitivitas tinggi terhadap kebocoran data, Indonesia juga memerlukan regulasi yang kuat.

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi tonggak penting. Komdigi menegaskan bahwa UU PDP resmi berlaku mulai **17 Oktober 2024**. Undang-undang ini tidak menganut pendekatan penutupan total. Pasal 56 menyatakan bahwa pengendali data dapat melakukan transfer data pribadi ke luar wilayah hukum

Indonesia. Namun, transfer itu harus memenuhi syarat: negara penerima harus memiliki tingkat pelindungan yang **setara atau lebih tinggi**; jika itu tidak terpenuhi, pengendali harus memastikan adanya perlindungan yang **memadai dan mengikat**; dan jika kedua syarat tersebut tidak terpenuhi, diperlukan **persetujuan subjek data**. Di sisi lain, untuk pemrosesan berisiko tinggi, pengendali wajib melakukan **penilaian dampak pelindungan data pribadi**. (djkpm.komdigi.go.id)

Arsitektur ini penting karena menunjukkan bahwa Indonesia, setidaknya pada tingkat undang-undang, sedang memilih **jalan tengah**. Indonesia tidak menutup pintu arus data lintas batas, tetapi menuntut dasar perlindungan. Secara normatif, ini lebih dekat ke model **keterbukaan bersyarat** daripada model lokalisasi menyeluruh. Bagi ekonomi digital Indonesia, pendekatan ini rasional: terlalu tertutup akan menghambat integrasi regional dan global, terlalu terbuka akan menggerus kepercayaan publik dan membuat negara lemah di hadapan platform besar.

Akan tetapi, tantangan Indonesia justru ada pada **implementasi**. Hukum yang baik belum tentu efektif bila tidak didukung kapasitas pengawasan, pedoman transfer yang jelas, mekanisme audit, standar kontraktual, kompetensi forensik, dan kerja sama lintas negara. Dalam konteks inilah perkembangan ASEAN DEFA menjadi sangat penting bagi Indonesia. Jika ASEAN berhasil membangun kerangka saling percaya regional untuk arus data yang aman, maka Indonesia dapat menikmati pasar digital kawasan yang lebih besar tanpa harus memilih antara keterbukaan dan perlindungan secara ekstrem. (ASEAN Main Portal)

14. Dunia Nyata: Regulasi Data Bukan Isu Teknologi Saja, Melainkan Isu Politik Ekonomi

Untuk memahami dilema ini secara lebih mendalam, kita perlu melihat bahwa regulasi data sesungguhnya adalah soal **politik ekonomi internasional**.

Ketika Uni Eropa memperketat perlindungan data, ia tidak hanya sedang membela hak warga; ia juga sedang memproyeksikan kekuatan normatif global. Ketika Amerika Serikat mendukung mekanisme interoperabilitas, ia tidak hanya sedang memfasilitasi bisnis; ia juga sedang mempertahankan arsitektur ekonomi digital yang kompatibel dengan perusahaan-perusahaannya. Ketika Tiongkok menegaskan keamanan dan tata kelola nasional atas data, ia tidak hanya sedang melindungi warga; ia juga sedang membangun model kedaulatan digital yang selaras dengan strategi negara. Ketika negara berkembang menuntut nilai tambah data bagi pembangunan, mereka bukan sekadar menolak globalisasi, tetapi sedang mempertanyakan distribusi manfaat dalam kapitalisme platform.

Karena itu, dilema "kedaulatan data versus internet terbuka" tidak boleh dibaca secara teknokratis semata. Di belakangnya terdapat pertanyaan yang lebih besar: **siapa yang mengendalikan infrastruktur digital? siapa yang menetapkan standar? siapa yang menanggung risiko? dan siapa yang menikmati surplus ekonomi dari data?** Selama jawaban atas pertanyaan-pertanyaan itu masih sangat timpang, tuntutan kedaulatan data akan terus menguat.

15. Menuju Kerangka Jalan Tengah: Open by Default, Trusted by Law, Strategic by Exception

Berdasarkan pengalaman global, jalan paling masuk akal bukanlah internet tanpa batas dan bukan pula benteng digital nasional. Yang lebih realistis adalah kerangka yang dapat dirumuskan sebagai: **terbuka secara default, tepercaya secara hukum, dan strategis melalui pengecualian yang sempit**.

Pertama, negara perlu membedakan **jenis data**. Tidak semua data memerlukan perlakuan yang sama. Data pribadi sensitif, data kesehatan, data infrastruktur kritis, data keamanan nasional, dan data statistik publik

tidak bisa diatur dengan satu pendekatan. Semakin tinggi risikonya, semakin kuat justifikasi pembatasan atau persyaratan transfernya.

Kedua, transfer lintas batas sebaiknya diizinkan **sebagai prinsip umum**, tetapi dengan mekanisme yang jelas: *adequacy*, klausul kontraktual, sertifikasi, standar keamanan, audit, dan redres. Pendekatan Indonesia dalam Pasal 56 UU PDP serta pendekatan Uni Eropa dalam Bab V GDPR menunjukkan arah ini. (JDIH Kemkomdigi)

Ketiga, **lokalisasi data** sebaiknya digunakan sebagai instrumen yang benar-benar berbasis risiko, bukan sebagai refleks kebijakan umum. OECD menunjukkan bahwa dampak ekonomi lokalisasi sangat tergantung pada bentuk kebijakan yang dipilih; sebab itu, syarat penyimpanan lokal hanya layak untuk sektor yang secara nyata kritis, bukan untuk seluruh ekonomi digital. (OECD)

Keempat, negara perlu membangun **interoperabilitas regulasi**, baik bilateral, regional, maupun multilateral. APEC CBPR, adekuasi UE, dan DEFA ASEAN memperlihatkan bahwa interoperabilitas lebih produktif daripada pengisolasian. Negara tidak harus menyerahkan kedaulatan untuk bekerja sama; yang diperlukan adalah mekanisme saling percaya yang dapat diverifikasi. (APEC)

Kelima, tata kelola data harus mencakup **persaingan usaha dan distribusi manfaat**. Tanpa kebijakan persaingan, akses data, interoperabilitas platform, dan pengembangan kapasitas domestik, keterbukaan arus data mudah berubah menjadi dominasi platform besar. Dengan kata lain, kedaulatan data tidak hanya soal server dan hukum privasi, tetapi juga soal struktur pasar.

Keenam, negara berkembang perlu memperlakukan data sebagai bagian dari **strategi pembangunan digital nasional**. Itu berarti investasi pada pusat komputasi, talenta AI, lembaga pengawas, identitas digital, keamanan siber, dan kemampuan negosiasi internasional. Tanpa

kapasitas seperti ini, negara hanya akan menjadi "pengatur di atas kertas" tanpa daya tawar nyata.

16. Refleksi Akademik: Dari "Batas" ke "Tata Kelola"

Secara teoretis, perdebatan ini menandai pergeseran besar dalam pemikiran regulasi global. Pada fase awal globalisasi digital, perhatian utama tertuju pada **penghapusan batas**. Kini, perhatian beralih pada **pengelolaan batas**. Batas tidak lagi dipahami hanya sebagai garis teritorial yang menghalangi arus, tetapi sebagai instrumen yang menentukan syarat keterhubungan. Negara tidak hilang di era digital; negara justru kembali dengan fungsi baru sebagai arsitek tata kelola data.

Namun, negara juga tidak dapat bertindak seolah-olah ekonomi digital bisa ditutup seperti ekonomi analog. Data, layanan awan, AI, pembayaran digital, dan platform lintas batas bekerja dalam arsitektur yang secara inheren saling terhubung. Itulah sebabnya tata kelola data abad ke-21 memerlukan seni menyeimbangkan **teritorialitas hukum** dengan **non-teritorialitas jaringan**. Regulasi yang terlalu kaku akan kalah oleh realitas teknologi; regulasi yang terlalu longgar akan kalah oleh tuntutan legitimasi politik dan perlindungan warga.

Dalam perspektif ini, dilema kedaulatan data versus internet terbuka sesungguhnya merupakan dilema klasik ilmu manajemen dan kebijakan publik: **bagaimana menciptakan kontrol tanpa mematikan adaptabilitas**. Organisasi yang terlalu longgar kehilangan arah; organisasi yang terlalu kaku kehilangan inovasi. Demikian pula tata kelola digital global.

17. Penutup

Pada akhirnya, "kedaulatan data" dan "internet terbuka" tidak seharusnya diposisikan sebagai musuh konseptual. Kedaulatan data adalah tuntutan akan hak, keamanan, dan kapasitas negara dalam menghadapi ekonomi

digital yang sangat asimetris. Internet terbuka adalah syarat bagi inovasi, perdagangan, efisiensi, dan partisipasi yang luas dalam ekonomi global digital. Keduanya lahir dari kebutuhan yang sah.

Masalah muncul ketika salah satu dikukuhkan sebagai dogma tunggal. **Kedaulatan tanpa interoperabilitas** berisiko melahirkan proteksionisme digital, inefisiensi, dan fragmentasi. **Keterbukaan tanpa tata kelola** berisiko menghasilkan ekstraksi data, pelemahan hak, dan ketimpangan nilai tambah. Karena itu, dilema regulasi yang sesungguhnya bukan memilih salah satu, melainkan merancang institusi yang mampu menggabungkan keduanya secara proporsional.

Arah global terkini memberi petunjuk yang cukup jelas. OECD mendorong *data free flow with trust*; Uni Eropa mempertahankan transfer data melalui mekanisme kecukupan dan perlindungan setara; APEC mengembangkan interoperabilitas praktis; WTO berupaya menghindari fragmentasi; PBB melalui Global Digital Compact menekankan tata kelola data yang bertanggung jawab dan interoperabel; ASEAN melalui DEFA mengarah pada arus data yang aman dan lancar di kawasan; dan Indonesia sendiri, melalui UU PDP, tampak bergerak ke jalur keterbukaan bersyarat. (OECD)

Bagi Indonesia dan negara berkembang lainnya, tantangannya bukan sekadar mengikuti model negara maju, melainkan membangun **arsitektur kebijakan data yang sesuai dengan kepentingan pembangunan**. Arsitektur itu harus cukup terbuka untuk mendorong inovasi dan perdagangan, cukup kuat untuk melindungi warga dan menjaga keamanan strategis, dan cukup cerdas untuk memastikan bahwa nilai ekonomi dari data tidak sepenuhnya mengalir keluar. Dengan demikian, masa depan regulasi digital tidak terletak pada slogan "semua data harus tinggal di dalam negeri" atau "semua data harus bebas mengalir", melainkan pada kemampuan negara membangun

kepercayaan, interoperabilitas, dan keadilan nilai dalam ekonomi global digital.

Berikut **glosarium** dan **referensi** untuk tema *"Kedaulatan Data vs Internet Terbuka: Dilema Regulasi dalam Ekonomi Global Digital."* Saya susun dalam gaya akademik ringkas agar langsung dapat dipakai dalam makalah.

Glosarium

Kedaulatan data (data sovereignty)
Gagasan bahwa negara atau yurisdiksi memiliki otoritas untuk menentukan bagaimana data yang berkaitan dengan warga, organisasi, atau aktivitas di wilayahnya dikumpulkan, diproses, disimpan, dipindahkan, dan dimanfaatkan. Dalam praktik, konsep ini sering terkait dengan privasi, keamanan nasional, dan tujuan pembangunan ekonomi. (UN Trade and Development (UNCTAD))

Internet terbuka (open internet)
Ekosistem internet yang interoperabel, lintas batas, dan tidak terfragmentasi secara berlebihan, sehingga memungkinkan pertukaran informasi, layanan digital, inovasi, dan perdagangan lintas negara berlangsung lebih efisien. Gagasan ini tidak berarti tanpa aturan, melainkan keterbukaan yang tetap tunduk pada tata kelola. (OECD)

Arus data lintas batas (cross-border data flows)
Perpindahan data dari satu negara ke negara lain melalui jaringan digital. OECD dan PBB menempatkan arus data lintas batas sebagai unsur kunci

ekonomi digital modern, tetapi menegaskan bahwa arus tersebut perlu dikelola secara aman dan tepercaya. (OECD)

Data Free Flow with Trust (DFFT)
Konsep kebijakan yang dipopulerkan OECD dan G7 untuk mendorong arus data lintas batas sambil menjaga kepercayaan melalui perlindungan privasi, keamanan, serta hak kekayaan intelektual. Intinya, data perlu dapat mengalir, tetapi tidak tanpa pagar hukum. (OECD)

Lokalisasi data (data localisation)
Kebijakan yang mewajibkan data tertentu disimpan, diproses, atau disalin di dalam wilayah suatu negara. OECD mencatat bahwa kebijakan semacam ini dapat meningkatkan biaya dan, bila diterapkan terlalu luas, berisiko memicu fragmentasi ekonomi digital. (OECD)

Fragmentasi digital
Kondisi ketika internet global pecah menjadi ruang-ruang digital yang makin tertutup karena aturan nasional yang berbeda-beda, terutama terkait transfer data, platform, keamanan siber, dan konten. OECD memperingatkan bahwa "data autarky" atau pembatasan total arus data dapat menurunkan PDB global dan ekspor dunia. (OECD)

Data pribadi (personal data)
Dalam UU No. 27 Tahun 2022, data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun nonelektronik. Definisi ini menjadi dasar semua kewajiban pelindungan data di Indonesia. (JDIH Kemkomdigi)

Pelindungan data pribadi
Menurut UU PDP Indonesia, pelindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data demi menjamin hak konstitusional subjek data.

Dengan demikian, isu data di Indonesia diposisikan sebagai isu hak, bukan sekadar isu teknis. (JDIH Kemkomdigi)

Subjek data pribadi (data subject)
Individu yang data pribadinya diproses dan yang memiliki hak hukum atas data tersebut, seperti hak untuk mengetahui, memperbaiki, menarik persetujuan, atau menuntut ganti rugi bila terjadi pelanggaran. Dalam kerangka GDPR maupun UU PDP, subjek data adalah pusat perlindungan hukum. (JDIH Kemkomdigi)

Pengendali data pribadi (data controller)
Pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan data pribadi. Dalam praktik regulasi, pengendali memikul tanggung jawab utama untuk memastikan kepatuhan, keamanan, dan dasar hukum pemrosesan data. (JDIH Kemkomdigi)

Prosesor data pribadi (data processor)
Pihak yang memproses data pribadi atas nama pengendali data. Kedudukannya berbeda dari pengendali karena prosesornya menjalankan pemrosesan sesuai instruksi dan kerangka yang ditetapkan pengendali. (JDIH Kemkomdigi)

Transfer data ke luar negeri
Dalam UU PDP Indonesia, transfer data pribadi ke luar wilayah hukum Indonesia diperbolehkan, tetapi pengendali wajib memastikan negara penerima memiliki tingkat pelindungan yang setara atau lebih tinggi; bila tidak, harus ada pelindungan yang memadai dan mengikat; bila itu pun tidak ada, diperlukan persetujuan subjek data. Ini menunjukkan bahwa Indonesia memilih model keterbukaan bersyarat, bukan penutupan total. (JDIH Kemkomdigi)

Adequacy / tingkat perlindungan yang setara
Prinsip yang menilai apakah suatu negara tujuan transfer memiliki tingkat perlindungan data yang “secara esensial ekuivalen” dengan

yurisdiksi asal. Uni Eropa memakai pendekatan ini dalam transfer data ke negara ketiga, sehingga arus data tetap dimungkinkan tanpa mengorbankan standar perlindungan. (EUR-Lex)

GDPR (General Data Protection Regulation)
Regulasi pelindungan data Uni Eropa yang menjadi salah satu standar global paling berpengaruh. Laporan Komisi Eropa 2024 menegaskan bahwa GDPR bukan hanya instrumen privasi, tetapi juga pilar pendekatan Eropa terhadap transformasi digital dan transfer internasional data. (EUR-Lex)

Data Privacy Framework (DPF)
Mekanisme resmi untuk memungkinkan transfer data pribadi dari Uni Eropa, Inggris, dan Swiss ke organisasi di Amerika Serikat yang berpartisipasi, dengan dasar perlindungan tertentu. DPF merupakan contoh *interoperability bridge* antara dua rezim hukum berbeda. (dataprivacyframework.gov)

CBPR (Cross-Border Privacy Rules)
Sistem APEC yang dirancang untuk membantu arus data lintas batas sambil menjamin perlindungan privasi. Per Februari 2025, APEC melaporkan ada sembilan ekonomi dan 82 perusahaan terdaftar dalam sistem ini. (APEC)

Interoperabilitas regulasi
Kemampuan rezim hukum yang berbeda untuk tetap saling berhubungan dan memungkinkan transfer data yang sah tanpa harus memiliki undang-undang yang identik. Konsep ini sangat penting karena dunia tidak memiliki satu hukum privasi global yang seragam. (OECD)

Digital trust / kepercayaan digital
Keadaan ketika individu, pelaku usaha, dan pemerintah merasa bahwa pemrosesan serta pertukaran data berlangsung dengan aman, transparan, dan akuntabel. OECD dan PBB menempatkan kepercayaan

sebagai syarat utama agar arus data lintas batas dapat diterima secara politik dan ekonomi. (OECD)

Jasa yang dikirim secara digital (digitally delivered services)
Jasa yang diperdagangkan melintasi perbatasan melalui jaringan komputer, termasuk layanan profesional, pendidikan daring, streaming, game daring, dan banyak layanan bisnis digital. WTO melaporkan ekspor global jasa jenis ini mencapai US$ 4,25 triliun pada 2023. (World Trade Organization)

Ekonomi digital
Ruang kegiatan ekonomi yang bergantung pada data, jaringan, platform, perangkat lunak, komputasi awan, AI, dan transaksi elektronik. PBB, WTO, OECD, dan UNCTAD sama-sama menempatkannya sebagai arena strategis pertumbuhan global sekaligus sumber ketimpangan baru. (United Nations)

Global Digital Compact
Dokumen PBB yang menyerukan masa depan digital yang inklusif, terbuka, aman, dan terlindungi, serta mengakui pentingnya arus data lintas batas yang aman dan tepercaya bagi pembangunan. Dokumen ini penting karena menunjukkan arah normatif global menuju tata kelola data yang lebih seimbang. (United Nations)

ASEAN DEFA (Digital Economy Framework Agreement)
Kerangka perjanjian ekonomi digital ASEAN yang pada 24 Oktober 2025 mencapai *substantial conclusion* dalam negosiasinya. Salah satu elemen pentingnya mencakup arus data, pembayaran elektronik, dan pelindungan data pribadi di tingkat kawasan. (ASEAN Main Portal)

Penilaian dampak pelindungan data (data protection impact assessment / DPIA)
Penilaian risiko yang wajib dilakukan ketika pemrosesan data memiliki potensi risiko tinggi terhadap subjek data. Dalam UU PDP Indonesia, hal

ini mencakup misalnya keputusan otomatis, pemrosesan data sensitif, pemrosesan skala besar, dan penggunaan teknologi baru. (JDIH Kemkomdigi)

Akuntabilitas pengendali data
Prinsip bahwa pengendali data tidak cukup hanya "mengaku patuh", tetapi harus dapat menunjukkan pertanggungjawaban atas pemrosesan data dan pemenuhan prinsip pelindungan data. Prinsip ini tercermin jelas dalam UU PDP Indonesia dan praktik GDPR. (JDIH Kemkomdigi)

Data autarky
Istilah OECD untuk menggambarkan situasi "fragmentasi penuh" ketika semua negara membatasi arus data secara menyeluruh. Simulasi OECD menunjukkan bahwa skenario ini dapat menurunkan PDB global 4,5 persen dan ekspor 8,5 persen. (OECD)

Referensi

Di bawah ini adalah **daftar referensi pilihan** yang relevan untuk makalah tersebut. Saya tulis dalam bentuk ringkas akademik.

ASEAN. (2025). *ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations* (24 October 2025, Kuala Lumpur). (ASEAN Main Portal)

APEC. (2025). *2025 Update to Evaluating Progress on the Aotearoa Plan of Action*. Bagian yang memuat perkembangan **APEC CBPR**, termasuk partisipasi sembilan ekonomi dan 82 perusahaan. (APEC)

European Commission. (2024). *Second Report on the Application of the General Data Protection Regulation (GDPR)*, COM(2024) 357 final. (EUR-Lex)

European Union. (2025). *Commission Implementing Decision* terkait *adequacy* dan prinsip perlindungan yang "essentially equivalent" untuk transfer data ke negara ketiga. (EUR-Lex)

Government of India, Ministry of Electronics and Information Technology. (2023). *The Digital Personal Data Protection Act, 2023*. (MeitY)

Government of India, Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025* dan dokumen konsultasi publik terkait. (MeitY)

Kementerian Komunikasi dan Digital Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. JDIH Komdigi. (JDIH Kemkomdigi)

Kementerian Komunikasi dan Digital Republik Indonesia. (2024). *Era Baru Perlindungan Data Pribadi*. Direktorat Jenderal Pengawasan Ruang Digital / Komdigi. (DJKPM)

OECD. (2024). *Economic Implications of Data Regulation*. OECD Publishing. (OECD)

OECD. (2024–2025). *Cross-border Data Flows*; *Data Free Flow with Trust*; dan *Fostering Cross-border Data Flows with Trust*. Seri kebijakan OECD tentang arus data, interoperabilitas, dan lokalisasi data. (OECD)

United Nations. (2024). *Global Digital Compact* (Annex I to the Pact for the Future). (United Nations)

UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development — For Whom the Data Flow*. Geneva: United Nations Conference on Trade and Development. (UN Trade and Development (UNCTAD))

U.S. Department of Commerce. (2025). *Data Privacy Framework* dan *Program Overview*. Kerangka resmi transfer data pribadi dari

UE/Inggris/Swiss ke organisasi AS yang berpartisipasi. (dataprivacyframework.gov)

World Trade Organization. (2024). *Global Trade Outlook and Statistics 2024*; serta rilis terkait pertumbuhan jasa yang dikirim secara digital. (World Trade Organization)

World Trade Organization. (2024). *Joint Initiative on E-commerce* — perkembangan negosiasi dan tahap finalisasi politik. (ASEAN Main Portal)

Copilot for this article - Chatgpt 5.2 Thinking. Access date: 1 Maret 2026
Prompting on Writer's account (Rudy C Tarumingkeng)

https://chatgpt.com/c/69a41951-b56c-8399-85e8-6a8fac9ff87c