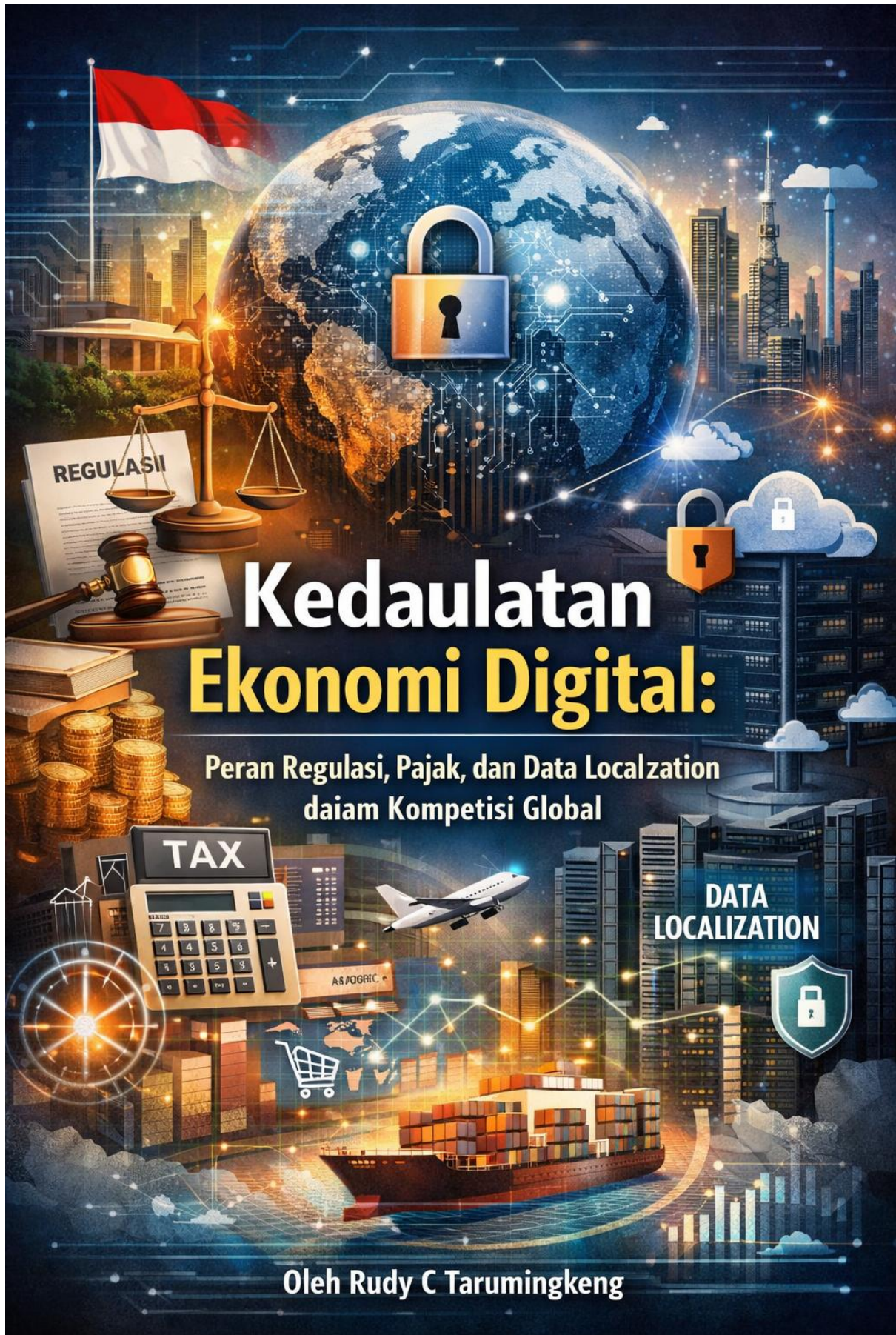




*Rudy C Tarumingkeng*: Kedaulatan Ekonomi Digital: Peran Regulasi,  
Pajak, dan Data Localization dalam Kompetisi Global

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-

---

© RudyCT Academic Series

[rudyc75@gmail.com](mailto:rudyc75@gmail.com)

15 Februari 2026

Bogor, Indonesia

## **KEDAULATAN EKONOMI DIGITAL: PERAN REGULASI, PAJAK, DAN DATA LOCALIZATION DALAM KOMPETISI GLOBAL**

Makalah ini menjelaskan “kedaulatan ekonomi digital” sebagai *kemampuan negara menguasai aturan main, menangkap nilai ekonomi, dan melindungi warga*—dengan fokus pada tiga tuas kebijakan: regulasi, pajak, dan *data localization*, serta implikasinya bagi kompetisi global.

---

### **Abstrak**

Kedaulatan ekonomi digital bukan semata slogan proteksionisme, melainkan strategi negara untuk memastikan bahwa transformasi digital menghasilkan *nilai tambah nasional* (national value capture), memperkuat *kepercayaan publik* (trust), dan menjaga *keamanan nasional* di tengah kompetisi geopolitik data. Dalam praktiknya, kedaulatan ini dijalankan melalui tiga instrumen besar: **(1) regulasi digital** (tata kelola platform, perlindungan konsumen, keamanan siber, privasi, interoperabilitas, persaingan usaha), **(2) pajak ekonomi digital** (VAT/PPN layanan digital, pajak penghasilan atas aktivitas lintas batas, koordinasi pajak global), dan **(3) data localization** (kewajiban penempatan/penyimpanan/pemrosesan data di wilayah negara, serta

syarat transfer lintas batas). Ketiga instrumen tersebut saling menguatkan—tetapi juga memunculkan *trade-off* terhadap inovasi, biaya kepatuhan, investasi, serta arsitektur komputasi awan dan rantai pasok digital global.

Esai ini mengembangkan kerangka konseptual kedaulatan ekonomi digital, membahas evolusi kebijakan dan praktik di Indonesia serta membandingkannya dengan rezim global (misalnya European Union, China, India, United States). Pada akhirnya, esai menawarkan desain kebijakan “berdaulat namun terkoneksi”: pendekatan berbasis risiko (risk-based), klasifikasi data, penguatan otoritas perlindungan data, *sovereign cloud/hybrid*, serta diplomasi data dan pajak agar negara tidak terjebak dalam fragmentasi internet (*splinternet*) tetapi tetap mampu mengamankan kepentingan nasional.

---

## 1. Pendahuluan: Mengapa “Kedaulatan Ekonomi Digital” Menjadi Agenda Strategis?

Ekonomi digital mengubah cara nilai diciptakan dan diperebutkan. Jika pada ekonomi industri abad ke-20 nilai bertumpu pada pabrik, mesin, dan logistik fisik, maka pada ekonomi digital nilai bertumpu pada **data, jaringan (network effects), algoritma, dan kendali atas infrastruktur komputasi**. Di sinilah kedaulatan menjadi isu sentral: siapa menentukan aturan main, siapa menguasai aliran data, siapa menikmati pajak dan laba, dan siapa menanggung risiko (kebocoran data, penipuan digital, monopoli platform, ketimpangan akses).

Kedaulatan ekonomi digital pada dasarnya menjawab tiga pertanyaan besar:

**Jurisdiksi (rule-making power):** Apakah negara mampu menegakkan aturan pada aktor digital lintas batas—platform global, penyedia cloud, marketplace, aplikasi keuangan, *ad-tech*, sampai AI?

**Value capture (pembagian nilai):** Apakah negara mampu memastikan nilai ekonomi (pajak, lapangan kerja, industri pusat data, inovasi lokal) tidak “bocor” keluar melalui struktur bisnis digital global?

**Trust & security (kepercayaan dan keamanan):** Apakah warga dan organisasi terlindungi dari penyalahgunaan data, manipulasi algoritma, dan akses lintas yurisdiksi yang tidak transparan?

Tiga instrumen kebijakan—regulasi, pajak, dan data localization—adalah “tuas” utama untuk menjawab pertanyaan itu. Namun, setiap tuas membawa konsekuensi. Regulasi yang ketat dapat memperkuat perlindungan publik, tetapi berpotensi memperlambat inovasi. Pajak digital dapat memperkuat penerimaan negara, tetapi memicu sengketa pajak internasional atau *double taxation*. Data localization dapat memperkuat kontrol dan mendorong industri pusat data domestik, tetapi menambah biaya, menurunkan efisiensi cloud global, bahkan memicu retaliasi perdagangan.

---

## 2. Kerangka Konseptual: Dari “Digital Sovereignty” ke “Economic Digital Sovereignty”

Istilah “kedaulatan digital” sering dipakai luas, tetapi untuk kepentingan analisis ekonomi, kita perlu membedakan:

**Kedaulatan digital:** fokus pada kontrol negara atas infrastruktur digital, standar, keamanan siber, dan kebijakan data.

**Kedaulatan ekonomi digital:** fokus pada *nilai ekonomi dan distribusinya*—pajak, investasi, industri domestik, inovasi, *local champions*, dan daya saing nasional.

Dengan kata lain, kedaulatan ekonomi digital adalah *kedaulatan digital yang dioperasionalkan untuk tujuan ekonomi*: pertumbuhan, produktivitas, dan pemerataan—tanpa mengorbankan keamanan dan hak warga.

Secara operasional, ada tiga lapisan kebijakan:

**Lapisan Regulasi (governance layer)**

Menetapkan “aturan main”: siapa boleh beroperasi, standar keamanan, perlindungan konsumen, kewajiban transparansi, tata kelola konten, hingga persaingan usaha.

**Lapisan Fiskal (taxation layer)**

Menetapkan “pembagian manfaat”: bagaimana aktivitas digital menghasilkan penerimaan negara secara adil, termasuk transaksi lintas batas dan model bisnis berbasis data.

**Lapisan Data (data localization & transfer layer)**

Menetapkan “kendali atas aset strategis”: di mana data disimpan, bagaimana data lintas batas ditransfer, siapa berhak mengakses dalam rangka penegakan hukum.

Ketiganya saling terkait. Misalnya, pajak digital efektif bila regulator mampu mewajibkan pendaftaran/registrasi platform dan menegakkan pelaporan transaksi. Atau, perlindungan data pribadi sulit ditegakkan bila data bebas bergerak tanpa mekanisme transfer yang dapat diaudit.

---

### **3. Regulasi sebagai Instrumen Kedaulatan: Menata Pasar, Risiko, dan Kekuasaan Platform**

#### **3.1. Regulasi bukan sekadar “membatasi”, tetapi “mendesain pasar”**

Dalam ekonomi digital, pasar cenderung terkonsentrasi karena *network effects* dan ekonomi skala data. Regulasi modern tidak hanya mencegah kerugian konsumen, tetapi juga mencegah dominasi platform yang menutup akses bagi inovator baru.

Di tingkat global, European Commission melalui rezim *platform regulation* seperti Digital Markets Act (DMA) mencoba mengendalikan “gatekeeper” (platform besar yang menjadi pintu gerbang pasar digital) dengan kewajiban dan larangan tertentu. DMA secara eksplisit

mendefinisikan gatekeeper dan mewajibkan kepatuhan pada daftar *do's and don'ts*. ([Digital Markets Act \(DMA\)](#)) Di sini regulasi bukan hanya hukum konsumen; ia menjadi *industrial policy* untuk memastikan kompetisi tetap terbuka.

**Pelajaran penting:** kedaulatan ekonomi digital membutuhkan regulator yang mampu membaca struktur pasar digital, bukan sekadar merespons kasus per kasus.

### **3.2. Regulasi penyelenggara sistem elektronik: registrasi dan akuntabilitas**

Salah satu fondasi kedaulatan adalah memastikan negara mengetahui “siapa pemainnya” (visibility) dan dapat menuntut pertanggungjawaban (accountability). Untuk konteks Indonesia, regulasi terkait penyelenggara sistem elektronik (PSE) menjadi contoh upaya membangun visibility dan accountability, termasuk registrasi PSE privat. Pedoman registrasi PSE privat merujuk pada kerangka regulasi yang ditetapkan pemerintah. ([komdigi.go.id](http://komdigi.go.id))

Di sini logika kedaulatan muncul: platform asing bisa beroperasi lintas batas, namun negara menuntut “kehadiran regulatif” melalui pendaftaran, kepatuhan, dan kemungkinan penegakan sanksi.

### **3.3. Regulasi privasi sebagai fondasi trust**

Privasi bukan isu “mewah”. Di ekonomi digital, trust adalah modal: tanpa trust, transaksi digital macet. Kerangka UU Pelindungan Data Pribadi (UU PDP) menjadi pilar untuk memastikan pemrosesan data pribadi berjalan sah, aman, dan bertanggung jawab. ([BPK Regulations](#))

Namun, privasi juga bersifat lintas batas. Karena itu, desain regulasi harus menjawab: kapan data boleh ditransfer keluar negeri, syarat apa yang harus dipenuhi, dan bagaimana audit kepatuhan dilakukan. Pada titik ini, privasi bertemu dengan data localization dan geopolitik data (dibahas di bagian berikut).

## **4. Pajak Ekonomi Digital: Menangkap Nilai di Era Transaksi Lintas Batas**

### **4.1. Mengapa pajak digital rumit?**

Model bisnis digital sering memisahkan lokasi pengguna, lokasi server, lokasi perusahaan, dan lokasi keuntungan. Platform bisa memperoleh pendapatan besar dari pasar suatu negara tanpa kantor fisik yang signifikan. Inilah akar masalah pajak digital: sistem pajak klasik bertumpu pada *permanent establishment* (kehadiran fisik), sementara ekonomi digital bertumpu pada *user base* dan *data-driven value*.

Pajak digital biasanya bergerak melalui dua kanal besar:

**Pajak konsumsi (VAT/PPN) atas layanan digital**

**Pajak penghasilan (income tax) atas laba platform/penyedia layanan digital**

### **4.2. VAT/PPN atas layanan digital: instrumen “paling cepat” dan relatif efektif**

Untuk banyak negara, memajaki konsumsi layanan digital (PPN atas barang/jasa digital) adalah langkah paling cepat karena lebih mudah diadministrasikan dibanding menilai laba perusahaan global.

Pemerintah Indonesia mengumumkan pemungutan PPN atas produk/jasa digital melalui PMSE mulai 1 Juli 2020, berlaku pada pelaku usaha yang memenuhi kriteria tertentu. ([Sekretariat Kabinet Republik Indonesia](#)) Kebijakan ini memotong satu jalur “kebocoran nilai”: konsumsi domestik yang sebelumnya sulit dikenai pajak ketika penyedia layanan berada di luar negeri.

Menariknya, informasi resmi otoritas pajak Indonesia juga menunjukkan skema tarif PPN PMSE dengan rate yang berlaku (ditampilkan sebagai 12% pada laman otoritas pajak). ([Directorate General of Taxes](#)) Ini

menggambarkan bahwa pajak konsumsi digital adalah instrumen yang terus disesuaikan seiring dinamika kebijakan PPN nasional.

**Implikasi kedaulatan ekonomi:** VAT/PPN digital bukan hanya penerimaan. Ia mengirim sinyal bahwa pasar domestik adalah yurisdiksi fiskal yang tidak “gratis” bagi platform global.

#### **4.3. Pajak penghasilan: dari “kehadiran fisik” ke “kehadiran ekonomi”**

Bagian yang lebih kompleks adalah pajak penghasilan. Banyak yurisdiksi mengeksplorasi konsep *significant economic presence* atau pemajakan berbasis kehadiran ekonomi, terutama untuk perusahaan digital besar. Diskursus Indonesia tentang pemajakan layanan digital juga menyinggung pendekatan ini. ([ASEAN Briefing](#))

Namun, pajak penghasilan digital cepat masuk ke ranah sengketa internasional: negara asal perusahaan (home country) dan negara pasar (market country) sama-sama mengklaim hak pemajakan. Karena itu lahir upaya koordinasi global.

#### **4.4. Koordinasi pajak global: OECD Pillar One dan Pillar Two**

Upaya paling menonjol adalah paket reformasi pajak global yang dibahas dalam kerangka OECD/G20. Pilar yang relevan:

**Pillar One (Amount A):** realokasi sebagian hak pemajakan laba perusahaan multinasional terbesar dan paling menguntungkan ke yurisdiksi pasar; dioperasikan melalui sebuah *Multilateral Convention (MLC)*. ([OECD](#))

**Pillar Two:** pajak minimum global untuk mengurangi praktik pengalihan laba ke yurisdiksi pajak rendah.

Pada 5 Januari 2026, OECD merilis pernyataan tentang kesepakatan “way forward” terkait paket pajak minimum global, menekankan stabilitas dan kepastian sistem pajak internasional serta kemampuan yurisdiksi—

termasuk negara berkembang—mempertahankan hak pemajakan atas pendapatan yang dihasilkan di wilayahnya. ([OECD](#))

**Interpretasi kebijakan:** bagi negara berkembang, koordinasi global penting untuk mencegah “race to the bottom” pajak dan mengurangi penghindaran pajak oleh perusahaan raksasa. Namun, koordinasi global juga bisa membatasi ruang kebijakan domestik (misalnya penerapan DST sepihak).

---

## **5. Data Localization: Antara Kontrol, Keamanan, dan Biaya Ekonomi**

### **5.1. Mengapa negara mendorong data localization?**

Data localization biasanya didorong oleh empat motif:

**Keamanan nasional & penegakan hukum:** akses cepat untuk investigasi, forensik digital, dan mitigasi insiden.

**Perlindungan warga & privasi:** mencegah penyalahgunaan lintas yurisdiksi.

**Kedaulatan ekonomi:** mendorong investasi pusat data, pekerjaan digital, dan industri cloud domestik.

**Kontrol geopolitik:** mengurangi ketergantungan pada infrastruktur asing dan risiko ekstrateritorial.

Namun, data localization juga membawa biaya: investasi infrastruktur lokal, latensi, kompleksitas arsitektur, dan potensi retaliasi perdagangan.

### **5.2. Kerangka Indonesia: PP 71/2019 dan pembedaan public vs private scope**

Dalam kerangka Indonesia, PP 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menjadi rujukan penting. ([BPK Regulations](#))

Salah satu poin yang sering dibahas adalah pembedaan penyelenggara sistem elektronik lingkup publik dan privat: lingkup publik memiliki

tuntutan lebih kuat untuk penempatan sistem elektronik di Indonesia, sementara lingkup privat lebih fleksibel dengan syarat pengawasan efektif. ([dentons.hprplawyers.com](https://www.dentons.hprplawyers.com))

Dari sudut kedaulatan ekonomi, perbedaan ini mencerminkan kompromi: data dan sistem yang terkait layanan publik dianggap lebih sensitif bagi kedaulatan, sementara sektor privat diberi ruang efisiensi melalui cloud global.

### **5.3. UU PDP dan transfer lintas batas: “localization yang cerdas”**

UU PDP tidak identik dengan data localization total. Ia lebih menekankan syarat **transfer lintas batas** yang menjaga tingkat perlindungan. Salah satu penjelasan praktis yang banyak dikutip: pengirim harus memastikan negara penerima memiliki tingkat perlindungan setara/lebih tinggi, atau menyediakan perlindungan yang memadai dan mengikat bila tidak setara. ([makarim.com](https://www.makarim.com))

Dengan demikian, *kedaulatan* dapat diwujudkan bukan hanya dengan “menahan data di dalam negeri”, tetapi juga dengan “membawa standar perlindungan melekat pada data” melalui mekanisme legal dan kontraktual.

### **5.4. Perbandingan global: EU, China, India, dan dinamika model**

#### **(a) Model European Union: adequacy dan safeguards**

EU menegaskan bahwa perlindungan GDPR “ikut bepergian bersama data” dan transfer ke negara ketiga memerlukan mekanisme seperti *adequacy decision* atau safeguards lain. ([European Commission](https://europeancommission.eu)) Ini bukan localization murni, tetapi model “ekspor standar” (standard export).

#### **(b) Model China: localization kuat untuk sektor strategis**

Dalam konteks China, data localization kuat terutama untuk operator *critical information infrastructure (CII)*. Salah satu rujukan menyebut bahwa hukum keamanan siber China mensyaratkan data tertentu yang

dihasilkan dalam operasi CII disimpan di dalam China. ([California Lawyers Association](#)) Model ini dekat dengan logika keamanan nasional dan kontrol negara atas data strategis.

### **(c) Model India: kecenderungan “blacklist/whitelist” transfer lintas batas**

Kerangka DPDP Act India membuka transfer lintas batas secara prinsip, tetapi memungkinkan pemerintah membatasi transfer ke negara yang dinotifikasi (pendekatan “blacklist”). ([DLA Piper Data Protection](#)) Ini menandai model yang lebih fleksibel daripada localization total, namun tetap memberi alat politik-regulatif pada negara.

**Kesimpulan komparatif:** Data localization tidak satu bentuk. Ada spektrum dari *full localization* sampai *conditional transfer*. Pilihan spektrum sangat dipengaruhi oleh kapasitas infrastruktur domestik, tujuan industri, dan sensitivitas keamanan nasional.

---

## **6. Geopolitik Data dan Ekstrateritorialitas: Mengapa Server “di luar negeri” bukan sekadar isu teknis**

### **6.1. Masalah “akses lintas yurisdiksi” dan United States CLOUD Act**

Perdebatan besar di era cloud adalah: jika data warga negara disimpan pada penyedia layanan asing atau perusahaan berbasis di negara tertentu, apakah negara asal penyedia dapat meminta data itu—meskipun servernya berada di negara lain?

Laporan CRS (Congressional Research Service) tentang CLOUD Act menjelaskan bahwa perubahan hukum tersebut mewajibkan perusahaan teknologi memenuhi warrant atas data dalam *possession, custody, or control*, terlepas dari lokasi fisik data. ([Congress](#))

Bagi banyak negara, ini menciptakan dorongan data localization: bukan karena anti-perdagangan, tetapi karena ingin mengurangi risiko akses ekstrateritorial dan konflik hukum lintas yurisdiksi.

## **6.2. Narasi kasus (ilustratif): “SakuPay” dan dilema cloud lintas batas**

Bayangkan sebuah fintech Indonesia bernama **SakuPay**. Dalam fase awal, SakuPay memilih cloud regional di luar negeri karena biaya lebih murah dan layanan AI fraud detection lebih matang. Dalam 18 bulan, SakuPay tumbuh pesat: jutaan pengguna, data transaksi harian besar, dan mulai melayani merchant UMKM.

Masalah muncul saat:

Regulator menuntut audit keamanan dan kepatuhan privasi yang lebih ketat.

Terjadi insiden kebocoran data pihak ketiga.

Ada permintaan penegakan hukum yang membutuhkan akses cepat ke log transaksi.

Di titik ini, penyimpanan data di luar negeri bukan lagi sekadar keputusan IT. Ia menjadi **isu kedaulatan ekonomi**: siapa berdaulat atas jejak transaksi warga? Berapa biaya sosial jika akses insiden lambat? Bagaimana memastikan transfer lintas batas sesuai UU PDP? Apakah SakuPay perlu *hybrid cloud*—data sensitif di pusat data Indonesia, analitik tertentu di luar dengan mekanisme perlindungan?

Kisah semacam ini menjelaskan mengapa kedaulatan digital selalu “menempel” pada desain arsitektur teknologi.

---

## **7. Trade-off Ekonomi: Ketika Regulasi dan Localization Menghasilkan Manfaat, tetapi Juga Biaya**

### **7.1. Manfaat ekonomi yang sering diharapkan**

**Mendorong investasi pusat data domestik:** localization dapat menciptakan permintaan (demand pull) bagi industri pusat data, *managed services*, dan SDM keamanan siber.

**Meningkatkan kepatuhan dan penegakan hukum:** data yang dapat diaudit dan diakses sesuai prosedur mempercepat investigasi.

**Memperkuat trust:** rezim perlindungan data dan kewajiban keamanan memperkuat kepercayaan publik, yang pada gilirannya meningkatkan transaksi digital.

## 7.2. Biaya ekonomi yang sering terjadi

**Biaya kepatuhan & investasi:** membangun *redundant infrastructure* (lokal + global) meningkatkan biaya.

**Penurunan efisiensi cloud:** kehilangan manfaat *scale* global, layanan AI tertentu, atau latensi yang optimal.

**Risiko fragmentasi:** jika setiap negara menerapkan aturan inkompatibel, perusahaan menghadapi “puzzle compliance” yang mahal.

Di sinilah peran desain kebijakan: tujuan kedaulatan harus dicapai *tanpa* menciptakan beban yang tidak proporsional.

---

## 8. Desain Kebijakan “Berdaulat namun Terkoneksi”: Rekomendasi Strategis

### 8.1. Prinsip 1 — Regulasi berbasis risiko, bukan “satu aturan untuk semua”

Alih-alih mewajibkan localization total, negara dapat menerapkan **klasifikasi data:**

**Data strategis/layanan publik:** penempatan lokal kuat, audit intensif.

**Data pribadi sensitif:** kontrol ketat, enkripsi, syarat transfer ketat.

**Data non-sensitif/anonim:** lebih fleksibel untuk inovasi dan efisiensi.

Kerangka PP 71/2019 yang membedakan lingkup publik dan privat dapat dibaca sebagai embrio pendekatan berbasis risiko. ([BPK Regulations](#))

## **8.2. Prinsip 2 — Bangun “sovereign cloud” secara bertahap: hybrid, bukan isolasi**

Kedaulatan tidak harus berarti memutus koneksi global. Strategi yang realistis adalah:

**Hybrid cloud:** data inti dan sensitif di domestik; komputasi elastis/analitik tertentu di luar dengan mekanisme legal yang kuat.

**Sovereign controls:** enkripsi, manajemen kunci (key management) di yurisdiksi domestik, logging dan audit.

## **8.3. Prinsip 3 — Otoritas perlindungan data yang kuat dan operasional**

UU PDP memberi dasar, tetapi kedaulatan membutuhkan *institusi* yang menjalankan: standar, audit, penegakan sanksi, serta panduan transfer lintas batas. Tanpa institusi yang kuat, UU berisiko menjadi “dokumen normatif” tanpa daya eksekusi.

## **8.4. Prinsip 4 — Pajak digital yang adil: kombinasi VAT yang kuat + partisipasi aktif pada solusi global**

**VAT/PPN digital** adalah instrumen yang paling cepat mengamankan penerimaan dan menegaskan yurisdiksi pasar. ([Sekretariat Kabinet Republik Indonesia](#))

Untuk pajak penghasilan, partisipasi pada kerangka global (Pillar One/Two) membantu mengurangi konflik dan meningkatkan kepastian. ([OECD](#))

## **8.5. Prinsip 5 — Diplomasi data: gunakan standar interoperabilitas lintas kawasan**

Sebagai alternatif terhadap fragmentasi, negara dapat memanfaatkan kerangka kerja lintas batas yang memperkuat kerja sama penegakan privasi. Misalnya, APEC membangun kerangka kerja kerja sama penegakan privasi lintas batas (CPEA) dan menjelaskan sistem CBPR

sebagai mekanisme sertifikasi kebijakan dan praktik privasi perusahaan di kawasan. ([APEC](#))

Di tingkat global, forum Global CBPR juga mengembangkan pengaturan kerja sama penegakan privasi lintas negara. ([Global CBPR Forum](#))

---

## 9. Penutup: Kedaulatan Ekonomi Digital sebagai “Kemampuan Negara Menata Nilai”

Jika kedaulatan ekonomi digital diringkas dalam satu kalimat, ia adalah **kemampuan negara menata nilai**: menata aturan main pasar digital, memastikan pembagian manfaat yang adil melalui pajak, serta menjaga kendali atas data sebagai aset strategis—tanpa menutup diri dari arus inovasi global.

Bagi Indonesia, tantangannya bukan memilih antara “lokal vs global”, melainkan merancang *arsitektur kebijakan* yang:

**melindungi warga dan memperkuat trust** (UU PDP dan tata kelola keamanan),

**menangkap nilai ekonomi secara wajar** (PPN digital yang efektif dan reformasi pajak lintas batas),

**mendorong industri domestik** (pusat data, cloud, keamanan siber, talenta),

**tetap kompatibel dengan ekosistem global** (mekanisme transfer data dan kerja sama internasional).

Ke depan, kompetisi global bukan sekadar siapa punya aplikasi terbaik, melainkan siapa memiliki kombinasi paling matang antara **regulasi yang cerdas, pajak yang adil, dan tata kelola data yang berdaulat namun lincah**.

---

Berikut **Refleksi & Diskusi** yang bisa dipakai sebagai penutup esai sekaligus bahan kelas (Magister/eksekutif). Saya susun dalam gaya reflektif–analitis, lalu diakhiri paket pertanyaan diskusi dan latihan kelas berbasis kasus.

---

### **Refleksi Akademik: Kedaulatan Digital Itu “Kedaulatan atas Nilai”**

Di era ekonomi digital, kedaulatan tidak lagi identik dengan batas geografis semata, melainkan **batas yurisdiksi atas nilai**: siapa menentukan aturan, siapa memungut pajak, siapa mengendalikan data, dan siapa menanggung risiko. Tiga instrumen—regulasi, pajak, dan data localization—adalah “alat negara” untuk memastikan transformasi digital tidak hanya mempercepat konsumsi teknologi, tetapi juga **memperkuat kapasitas ekonomi nasional**, meningkatkan keadilan, serta menjaga keamanan dan martabat warga.

Namun, refleksi pentingnya: **kedaulatan bukanlah tujuan akhir**, melainkan *cara* untuk mencapai tujuan publik (kesejahteraan, keamanan, keadilan, dan daya saing). Karena itu, kedaulatan ekonomi digital selalu mengandung dilema: bila terlalu longgar, negara kehilangan nilai (pajak, industri domestik, kontrol risiko); bila terlalu ketat, negara kehilangan inovasi (investasi, efisiensi cloud, pertumbuhan startup) dan bisa terseret ke fragmentasi internet (*splinternet*).

Di sinilah kualitas desain kebijakan diuji: bukan pada “ketegasan slogan”, tetapi pada **ketelitian arsitektur tata kelola**—risk-based, proporsional, dapat diaudit, serta kompatibel dengan ekosistem global.

---

### **Refleksi 1 — Regulasi: Melindungi Publik atau Mengatur Kompetisi?**

Regulasi digital sering dipahami sebagai “rem” agar platform tidak liar. Tetapi dalam ekonomi platform, regulasi juga adalah **mesin desain pasar**: siapa boleh menjadi gatekeeper, bagaimana interkoneksi dan interoperabilitas bekerja, bagaimana transparansi algoritma ditegakkan, bagaimana konsumen terlindungi, dan bagaimana pelaku kecil tidak tersisih.

Refleksi kritisnya:

Apakah regulasi kita lebih banyak menjadi *compliance theatre* (dokumen dan pelaporan) atau benar-benar mengubah perilaku pasar?

Apakah negara memiliki kapasitas teknis—auditor, forensik, *policy lab*, dan mekanisme sanksi—untuk menegakkan aturan terhadap perusahaan lintas batas?

Di titik ini, kedaulatan tidak cukup hanya “menetapkan aturan”; ia harus sanggup **menegakkan** (enforce) dan **mengukur dampak** (evaluate). Negara yang lemah dalam eksekusi berpotensi menghasilkan regulasi yang berat bagi pemain kecil, tetapi tetap “ringan” bagi pemain besar karena asimetri sumber daya.

---

### **Refleksi 2 — Pajak: Adil bagi Negara Pasar, Realistis bagi Dunia Bisnis**

Pajak digital adalah arena “perebutan hak pemajakan” antara negara pasar dan negara asal perusahaan. Secara etis, masuk akal bahwa pasar yang menyediakan pengguna, data, dan pendapatan iklan juga berhak

atas bagian penerimaan. Namun secara praktis, pajak digital menghadapi:

struktur bisnis global yang memecah rantai nilai (marketing di satu negara, IP di negara lain, server di tempat lain),

potensi *double taxation*,

ketegangan antara kebijakan domestik dan koordinasi internasional.

Refleksi kuncinya: *keadilan pajak* harus berjalan bersama *kepastian pajak*. Tanpa kepastian, investasi bisa menurun; tanpa keadilan, legitimasi negara turun. Dalam kompetisi global, negara yang mampu merancang pajak digital yang sederhana, dapat diaudit, dan konsisten akan lebih menarik bagi investasi jangka panjang daripada negara yang sering berubah-ubah dan penuh ketidakpastian.

(Sebagai konteks global, pendekatan koordinasi seperti yang didorong OECD mencoba meredam konflik antarnegara—walau implementasinya penuh negosiasi.)

---

### **Refleksi 3 — Data Localization: Antara “Keamanan” dan “Biaya Ekonomi”**

Data localization sering dijual sebagai “jalan cepat” menuju kedaulatan: data disimpan di dalam negeri, maka negara aman. Tetapi realitasnya lebih kompleks:

keamanan tidak otomatis lahir dari lokasi server; keamanan lahir dari tata kelola (enkripsi, manajemen kunci, kontrol akses, logging, incident response),

data lokal tanpa standar keamanan justru bisa menjadi “kolam risiko”, kewajiban lokal bisa mendorong investasi pusat data, tetapi juga bisa meningkatkan biaya kepatuhan dan menurunkan efisiensi komputasi awan.

Refleksi penting: pilihan terbaik sering bukan “lokalisasi total”, melainkan **lokalisasi selektif + transfer lintas batas yang diawasi**. Model ini menuntut kapasitas klasifikasi data, standar audit, dan perangkat kontraktual/teknis yang matang (misalnya hybrid cloud dan manajemen kunci di yurisdiksi domestik).

---

#### **Refleksi 4 — Kompetisi Global: Kedaulatan vs Interdependensi**

Ekonomi digital adalah sistem yang saling bergantung. Tidak ada negara yang sepenuhnya “mandiri” dalam rantai pasok chip, cloud, *open-source*, standar keamanan, hingga model AI. Karena itu, kedaulatan yang efektif bukan isolasi, melainkan **kekuatan bernegosiasi**: negara mampu menentukan syarat operasi bagi pemain global, tetapi tetap menjaga konektivitas untuk inovasi dan perdagangan.

Maka pertanyaannya bergeser:

Kedaulatan seperti apa yang meningkatkan posisi tawar Indonesia dalam ekonomi digital global?

Kapan proteksi menjadi strategi industrial yang sehat, dan kapan ia menjadi beban biaya yang menurunkan daya saing?

---

#### **Diskusi Kelas: Pertanyaan Kritis (Bertingkat)**

##### **A. Pertanyaan Konseptual (pemahaman & framing)**

Apa bedanya “kedaulatan digital”, “kedaulatan data”, dan “kedaulatan ekonomi digital”? Berikan contoh kebijakan yang masuk ke masing-masing kategori.

Jika data adalah “aset strategis”, siapa pemilik nilai data: individu, platform, atau negara? Argumenkan dari perspektif ekonomi dan etika.

Dalam ekonomi platform, mengapa pasar cenderung terkonsentrasi? Apa risiko bagi inovasi lokal dan UMKM digital?

### **B. Pertanyaan Analitis (trade-off & desain kebijakan)**

Regulasi ketat biasanya meningkatkan trust, tetapi juga menambah biaya kepatuhan. Kapan biaya itu “layak” dan kapan menjadi penghambat inovasi?

Bandingkan dua pendekatan: (a) data localization ketat, (b) transfer lintas batas bersyarat (adequacy/safeguards). Mana yang lebih tepat untuk sektor kesehatan? Pendidikan? Perbankan?

Bagaimana mengukur keberhasilan kedaulatan ekonomi digital? Usulkan 6 indikator (pajak, investasi data center, insiden keamanan, inovasi, persaingan usaha, dll.).

Apakah kebijakan pajak digital lebih efektif melalui PPN (konsumsi) atau pajak penghasilan (laba)? Jelaskan dari sisi administrasi dan keadilan.

Bagaimana mencegah regulasi menjadi “beban UMKM digital” sementara pemain global tetap dominan?

### **C. Pertanyaan Normatif (keadilan, hak warga, legitimasi)**

Apakah data localization dapat dibenarkan sebagai kebijakan keadilan sosial (melindungi warga) atau ia lebih dekat pada proteksionisme ekonomi?

Dalam kondisi kebocoran data, siapa yang paling bertanggung jawab: perusahaan, regulator, atau pengguna? Apa batas tanggung jawab pengguna?

Apakah negara berhak mengakses data warga untuk keamanan nasional? Apa batas yang harus dijaga agar tidak melanggar privasi?

### **D. Pertanyaan Strategis (kompetisi global & negosiasi)**

Apakah kedaulatan ekonomi digital harus didorong lewat “local champions” (platform nasional) atau lewat “aturan main yang adil” bagi semua? Pilih satu, pertahankan argumen Anda.

Risiko *splinternet*: apakah fragmentasi internet tak terhindarkan? Jika ya, apa strategi adaptasi bagi bisnis dan pemerintah?

Bagaimana desain kebijakan yang tetap menarik investasi cloud global tetapi memastikan kontrol data sensitif di domestik?

---

### **Mini-Case untuk Diskusi (narasi singkat)**

#### **Kasus 1 — Fintech “SakuPay”: Hybrid Cloud dan Audit Kepatuhan**

SakuPay tumbuh cepat dan memakai cloud regional di luar negeri untuk efisiensi dan fitur anti-fraud. Ketika terjadi insiden kebocoran data pada vendor analitik, regulator meminta audit menyeluruh dan menuntut perbaikan tata kelola data. SakuPay dihadapkan pada pilihan: migrasi penuh ke pusat data domestik (mahal, lambat), atau membangun hybrid cloud (data sensitif lokal, analitik tertentu lintas batas dengan safeguards).

#### **Pertanyaan diskusi:**

Data apa yang wajib dilokalkan? Apa kriteria “sensitif” yang Anda gunakan?

Bagaimana desain kontrak, enkripsi, dan audit untuk transfer lintas batas?

Bagaimana menghitung biaya kepatuhan vs risiko reputasi dan risiko sanksi?

#### **Kasus 2 — E-Commerce “PasarKita”: Pajak Digital dan Level Playing Field**

PasarKita (lokal) bersaing dengan marketplace global. PasarKita mengeluh biaya kepatuhan lebih besar, sementara pemain global memonetisasi iklan dan layanan digital lintas batas. Pemerintah ingin menciptakan level playing field melalui pajak digital dan kewajiban registrasi PSE.

**Pertanyaan diskusi:**

Kebijakan apa yang paling tepat: pajak, persaingan usaha, atau kewajiban transparansi algoritma?

Bagaimana mencegah kebijakan “terasa adil” tapi justru menaikkan harga bagi konsumen?

Metrik apa yang Anda gunakan untuk menguji apakah persaingan makin sehat?

**Kasus 3 — “GovCloud”: Layanan Publik dan Data Warga**

Pemerintah ingin mempercepat digitalisasi layanan publik (kesehatan, bantuan sosial, pendidikan). Ada dorongan kuat agar data warga dan sistem inti ditempatkan di domestik. Namun, beberapa layanan AI dan keamanan terbaik tersedia dari penyedia global.

**Pertanyaan diskusi:**

Apakah “lokalisasi total” perlu untuk layanan publik, atau cukup untuk data dan sistem inti?

Bagaimana mengelola vendor global agar tetap patuh pada standar domestik (audit, logging, key management)?

Apa desain tata kelola yang mencegah penyalahgunaan akses data warga?

---

**Latihan Kelas: Debat dan Policy Memo (praktis)**

**Latihan 1 — Debat Terstruktur (2 tim)**

**Mosi:** "Data localization ketat adalah prasyarat kedaulatan ekonomi digital."

Tim A (pro): tekankan keamanan nasional, investasi data center, kontrol akses data.

Tim B (kontra): tekankan biaya ekonomi, efisiensi cloud, inovasi, risiko splinternet.

**Output:** masing-masing tim menutup dengan 3 rekomendasi kebijakan yang *operasional* (bukan slogan).

## **Latihan 2 — Policy Memo 2 Halaman (individu/kelompok kecil)**

Tulis memo untuk menteri/regulator berisi:

- tujuan kebijakan (maks 3),
- instrumen (regulasi–pajak–data),
- desain berbasis risiko (klasifikasi data),
- dampak ekonomi (biaya & manfaat),
- rencana implementasi 12 bulan (quick wins + fondasi institusi).

---

## **Penutup Reflektif**

Kedaulatan ekonomi digital pada akhirnya adalah **permainan kapasitas**: kapasitas regulasi (rule-making dan enforcement), kapasitas fiskal (menangkap nilai tanpa menghambat investasi), dan kapasitas tata kelola data (menjaga hak warga sekaligus menjamin keamanan nasional).

Negara yang berhasil bukan yang paling keras melokalisasi, melainkan yang paling **cermat menimbang risiko**, paling **konsisten menegakkan aturan**, dan paling **pandai menjaga konektivitas global** sambil memperkuat industri domestik.

Berikut **Glosarium** (istilah kunci) dan **Referensi** (sumber rujukan utama) untuk topik "*Kedaulatan Ekonomi Digital: Regulasi, Pajak, dan Data Localization dalam Kompetisi Global.*"

---

## **Glosarium**

### **Adequacy Decision (Keputusan Kecukupan)**

Keputusan otoritas (mis. Komisi Eropa) yang menyatakan suatu negara/rezim di luar wilayahnya memiliki tingkat perlindungan data yang "memadai", sehingga transfer data dapat dilakukan tanpa safeguards tambahan. Ini adalah mekanisme *trusted transfer* yang mengurangi friksi bisnis sambil menjaga standar perlindungan. ([European Commission](#))

### **Ad-Tech (Advertising Technology)**

Ekosistem teknologi iklan digital (lelang iklan, pelacakan perilaku, pengukuran konversi) yang bergantung pada data pengguna. Di sinilah banyak nilai ekonomi digital "dipanen" melalui profiling dan segmentasi, sehingga isu privasi, persetujuan, dan transparansi menjadi sangat krusial.

### **Algorithmic Accountability (Akuntabilitas Algoritma)**

Kewajiban organisasi untuk menjelaskan, menguji, dan bertanggung jawab atas dampak keputusan algoritmik (mis. penentuan harga, moderasi konten, credit scoring). Ini menuntut audit, dokumentasi, dan mitigasi bias.

### **Anti-Competitive Self-Preferencing**

Praktik platform yang memprioritaskan layanan/produk miliknya sendiri dibanding pihak ketiga (mis. di marketplace atau app store). Regulasi kompetisi digital banyak menargetkan pola ini karena dapat menutup kesempatan inovator kecil.

### **Auditability (Keter-auditan)**

Kemampuan sistem untuk menyediakan jejak bukti (logs, akses,

perubahan, transfer data) sehingga kepatuhan regulasi dan investigasi insiden dapat dilakukan secara kredibel.

### **Cloud / Cloud Computing**

Model komputasi berbasis layanan (IaaS/PaaS/SaaS) yang menyediakan elastisitas, skala, dan layanan keamanan/AI. Dalam debat kedaulatan, cloud adalah “infrastruktur strategis” karena menyangkut lokasi data, akses, dan kontrol.

### **Compliance Burden (Beban Kepatuhan)**

Biaya dan kompleksitas yang timbul karena kewajiban regulasi (pelaporan, audit, sertifikasi, registrasi). Jika tidak proporsional, beban ini cenderung lebih berat bagi UMKM dan startup dibanding pemain besar.

### **Cross-Border Data Transfer (Transfer Data Lintas Batas)**

Pemindahan data pribadi ke yurisdiksi lain. Umumnya mensyaratkan dasar hukum, safeguards (mis. klausul kontrak standar), dan/atau keputusan kecukupan. ([European Commission](#))

### **CPEA (Cross-border Privacy Enforcement Arrangement)**

Kerangka kerja sama penegakan hukum privasi lintas ekonomi APEC—memungkinkan otoritas privasi berkoordinasi atas pelanggaran yang berdimensi lintas negara. ([APEC](#))

### **Critical Information Infrastructure (CII) / Infrastruktur Informasi Kritis**

Sistem yang jika terganggu berdampak besar pada layanan publik/keamanan (energi, telekomunikasi, keuangan, kesehatan). Banyak rezim data localization lebih ketat untuk CII.

### **Cybersecurity / Keamanan Siber**

Upaya perlindungan sistem dan data dari serangan, gangguan, atau akses tidak sah. Dalam kedaulatan ekonomi digital, keamanan siber adalah prasyarat trust dan stabilitas transaksi.

### **Data Controller / Data Processor (Pengendali/Pemroses Data)**

Peran organisasi dalam menentukan tujuan/alat pemrosesan data (controller) atau memproses atas nama controller (processor).

Pembagian peran ini menentukan tanggung jawab hukum, audit vendor, dan desain kontrak.

### **Data Classification (Klasifikasi Data)**

Pengelompokan data (publik, internal, rahasia, sensitif) untuk menentukan kontrol keamanan, lokasi penyimpanan, serta syarat transfer lintas batas—ini inti pendekatan *risk-based*.

### **Data Governance (Tata Kelola Data)**

Kebijakan, struktur, peran, standar kualitas, serta mekanisme kontrol atas siklus hidup data. Tata kelola data yang matang menurunkan risiko kebocoran dan memperbaiki kepatuhan UU privasi.

### **Data Localization (Lokalisasi Data)**

Kebijakan yang mewajibkan data disimpan/diolah di dalam wilayah negara. Tujuannya bisa keamanan nasional, penegakan hukum, perlindungan warga, dan/atau strategi industri pusat data—namun berpotensi menambah biaya dan menurunkan efisiensi cloud.

### **Data Residency (Domisili Data)**

Persyaratan tempat data “berdiam” (disimpan). Berbeda dari localization penuh, residency kadang hanya mensyaratkan lokasi penyimpanan, bukan seluruh pemrosesan.

### **Data Sovereignty (Kedaulatan Data)**

Prinsip bahwa data tunduk pada hukum yurisdiksi tempat data berada atau tempat subjek data berada. Dalam praktik, konsep ini beririsan dengan ekstrateritorialitas dan konflik yurisdiksi.

### **Digital Markets / Gatekeeper**

Kondisi pasar digital yang didominasi platform besar (gatekeeper) yang mengontrol akses pelaku lain ke pengguna. Banyak rezim regulasi modern menargetkan gatekeeper dengan kewajiban perilaku. ([OECD](#))

### **Digital Services Tax (DST)**

Pajak yang dikenakan pada pendapatan jasa digital tertentu (mis. iklan digital) di yurisdiksi pasar. DST sering memicu negosiasi internasional karena berpotensi memunculkan konflik pemajakan.

### **Economic Presence (Kehadiran Ekonomi Signifikan)**

Konsep pemajakan lintas batas yang tidak lagi menuntut kehadiran fisik, tetapi mengakui aktivitas ekonomi signifikan melalui pengguna, transaksi, dan monetisasi data.

### **Enforcement Capacity (Kapasitas Penegakan)**

Kemampuan negara menegakkan aturan (inspektur, auditor, forensik, sanksi, kerja sama lintas batas). Tanpa kapasitas ini, regulasi cenderung hanya menjadi dokumen normatif.

### **Encryption (Enkripsi)**

Teknik kriptografi untuk melindungi data saat disimpan atau ditransmisikan. Dalam desain kedaulatan, isu kunci adalah *key management*: siapa memegang kunci, di yurisdiksi mana.

### **Fragmentation / Splinternet**

Fragmentasi internet menjadi blok-blok regulasi dan standar yang berbeda, meningkatkan biaya kepatuhan lintas negara dan menurunkan interoperabilitas.

### **Hybrid Cloud**

Arsitektur yang menggabungkan pusat data lokal/private cloud dan public cloud global. Dipakai untuk kompromi: data sensitif tetap lokal, komputasi elastis memanfaatkan layanan global.

### **Jurisdiction (Yurisdiksi)**

Wewenang hukum suatu negara/otoritas atas orang, perusahaan, aktivitas, atau data. Dalam ekonomi digital, yurisdiksi sering beririsan dan menimbulkan konflik lintas batas.

### **Key Management (Manajemen Kunci Kriptografi)**

Pengelolaan siklus hidup kunci (pembuatan, penyimpanan, rotasi, pencabutan). Banyak model “sovereign cloud” menekankan kunci dikelola di yurisdiksi domestik.

### **Market Jurisdiction (Yurisdiksi Pasar)**

Negara tempat pengguna/konsumen berada. Perdebatan pajak digital modern menuntut agar yurisdiksi pasar memperoleh bagian hak pemajakan yang lebih adil.

### **Network Effects (Efek Jaringan)**

Nilai layanan meningkat saat jumlah pengguna bertambah. Efek ini mendorong konsentrasi pasar dan membuat kompetisi “winner-takes-most”.

### **PDP Law (UU Pelindungan Data Pribadi)**

Kerangka hukum yang mengatur hak subjek data, dasar pemrosesan, kewajiban pengendali/pemroses, serta sanksi. Ini fondasi trust ekonomi digital. ([BPK Regulations](#))

### **PSE (Penyelenggara Sistem Elektronik)**

Entitas yang menyelenggarakan sistem elektronik. Pengaturan PSE umumnya mencakup kewajiban registrasi, keamanan, dan akuntabilitas operasional.

### **PMSE (Perdagangan Melalui Sistem Elektronik)**

Konteks transaksi digital (termasuk lintas batas) yang menjadi basis kebijakan PPN atas produk/jasa digital tertentu. ([Directorate General of Taxes](#))

### **Privacy by Design**

Prinsip memasukkan perlindungan privasi sejak tahap desain sistem, bukan “tambalan” setelah insiden terjadi.

### **Regulatory Sandbox**

Ruang uji coba terbatas untuk inovasi (fintech/AI) dengan pengawasan

regulator. Sandbox membantu menyeimbangkan inovasi dan mitigasi risiko.

### **Risk-Based Regulation (Regulasi Berbasis Risiko)**

Pendekatan yang membedakan kewajiban menurut tingkat risiko (mis. data sensitif, layanan publik, CII), sehingga kebijakan lebih proporsional dan tidak membunuh inovasi.

### **Safeguards (Pengaman Transfer Data)**

Mekanisme hukum/teknis untuk menjaga perlindungan data saat ditransfer lintas batas (klausul kontrak, audit, enkripsi, standar keamanan). ([European Commission](#))

### **Significant Digital Presence**

Variasi konsep kehadiran ekonomi, menekankan keberadaan digital yang nyata (basis pengguna, interaksi, monetisasi) sebagai dasar pemajakan dan pengaturan.

### **Tax Base Erosion (Erosi Basis Pajak)**

Hilangnya potensi pajak akibat pengalihan laba, struktur IP, atau model bisnis lintas batas yang tidak tertangkap aturan domestik.

### **Two-Pillar Solution (OECD/G20)**

Kerangka reformasi pajak global: realokasi sebagian hak pemajakan ke yurisdiksi pasar (Pilar 1/Amount A) dan pajak minimum global (Pilar 2). ([OECD](#))

### **VAT on Digital Services (PPN Digital)**

Pajak konsumsi atas pemanfaatan barang/jasa digital lintas batas. Di Indonesia, PPN PMSE mulai diberlakukan 1 Juli 2020. ([Directorate General of Taxes](#))

### **Value Capture (Penangkapan Nilai)**

Kemampuan negara/ekosistem domestik mengambil bagian nilai ekonomi (pajak, pekerjaan, industri data center, inovasi) dari aktivitas digital yang berlangsung di pasar domestik.

### **Vendor Risk Management**

Pengelolaan risiko pihak ketiga (cloud, analytics, payment gateway) melalui due diligence, SLA, audit, dan rencana respons insiden.

### **Warrant Extraterritoriality (Ekstrateritorialitas Permintaan Data)**

Situasi ketika hukum suatu negara mewajibkan perusahaan menyerahkan data meskipun data disimpan di luar wilayahnya. Dalam konteks AS, CLOUD Act menegaskan kewajiban atas data dalam “possession, custody, or control” terlepas dari lokasi data. ([Congress](#))

---

### **Referensi**

**Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.** (2022). ([BPK Regulations](#))

**Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.** (2019). ([BPK Regulations](#))

**Peraturan Menteri Keuangan Republik Indonesia Nomor 48/PMK.03/2020** tentang tata cara penunjukan pemungut, pemungutan, penyetoran, dan pelaporan PPN atas pemanfaatan BKP tidak berwujud/JKP dari luar daerah pabean melalui PMSE. (2020). ([Kementerian Keuangan Republik Indonesia](#))

Direktorat Jenderal Pajak. (n.d.). *PPN atas Produk dan Jasa Digital melalui Transaksi Elektronik (PMSE)*. ([Directorate General of Taxes](#))

Sekretariat Kabinet Republik Indonesia. (2020, 28 May). *Gov't to Charge VAT on e-Commerce Purchases Starting 1 July 2020*. ([Sekretariat Kabinet Republik Indonesia](#))

OECD. (2023, 11 October). *Multilateral Convention to Implement Amount A of Pillar One*. ([OECD](#))

OECD. (2023, October). *The Multilateral Convention to Implement Amount A of Pillar One—Overview*. ([OECD](#))

OECD. (2026, 5 January). *International community agrees way forward on global minimum tax package* (Press release). ([OECD](#))

OECD. (n.d.). *Global Minimum Tax* (overview page; Side-by-Side package context). ([OECD](#))

European Commission. (n.d.). *What rules apply if my organisation transfers data outside the EU?* ([European Commission](#))

European Commission. (n.d.). *Rules on international data transfers*. ([European Commission](#))

APEC. (n.d.). *APEC Cross-border Privacy Enforcement Arrangement (CPEA)*. ([APEC](#))

APEC. (2009). *Cooperation Arrangement for Cross-Border Privacy Enforcement* (CBPR/CPEA background). ([APEC](#))

Congressional Research Service. (2018). *Cross-Border Data Sharing Under the CLOUD Act (R45173)*. ([Congress](#))

Schwartz, P. M. (2018). *Legal Access to the Global Cloud*. *Columbia Law Review*. ([Columbia Law Review](#))

Galbraith, E. J. (2018). *Congress Enacts the CLOUD Act, Reshaping U.S. Law Governing Cross-Border Access to Data*. *American Journal of International Law* (Cambridge Core page). ([Cambridge University Press & Assessment](#))

Reuters. (2026, 5 January). *More than 145 countries agree update to global minimum tax deal, addressing US concerns*. ([Reuters](#))

Bruegel. (2026, 14 January). *How the global minimum tax amendments could reshape Europe's tax incentives*. ([Bruegel](#))

*Rudy C Tarumingkeng*: Kedaulatan Ekonomi Digital: Peran Regulasi,  
Pajak, dan Data Localization dalam Kompetisi Global

Copilot for this article - Chatgpt 5.2 Thinking. Access date: 15 Februari  
2026. Prompting on Writer's account ([Rudy C Tarumingkeng](#))  
<https://chatgpt.com/c/69918d59-34b8-83a0-a733-769ed8ddab71>