


6 ADALAH

Buletin Hukum & Keadilan

Digitalisasi dan Tantangan Kedaulatan Hukum Nasional: Studi tentang Pergeseran Otoritas dari Negara ke Entitas Digital Global

Gilang Rizki Aji Putra

Universitas Islam Negeri Syarif Hidayatullah Jakarta

 [10.15408/adalah.v4i6.51074](https://doi.org/10.15408/adalah.v4i6.51074)

Abstract:

Digitalization has blurred the geographical boundaries underpinning state legal sovereignty. This article analyzes how digitalization erodes national legal sovereignty through three mechanisms: extraterritorial foreign regulation, dominance of digital platforms as quasi-sovereign actors, and reliance on global technical standards. Using normative legal research with conceptual and statutory approaches, the study finds that Indonesia's legal sovereignty is continuously negotiated with market forces and transnational regulatory regimes. The Brussels Effect and corporate-controlled code architectures limit national legislation. Maintaining sovereignty requires shifting toward functional sovereignty focused on controlling critical infrastructure and data.

Keywords: Legal Sovereignty, Digitalization, Extraterritoriality, Digital Platforms, Data Sovereignty

A. PENDAHULUAN

Kedaulatan hukum merupakan salah satu mahkota utama negara modern. Dalam pengertian klasiknya, kedaulatan mengandung supremasi untuk membuat dan menegakkan norma di dalam suatu teritori yang eksklusif tanpa campur tangan kekuatan eksternal. Konsep ini, yang dimatangkan sejak Perjanjian Westphalia, berasumsi bahwa dunia terbagi dalam unit-unit politik yang jelas batas-batasnya secara geografis (Besson, 2011). Namun, digitalisasi telah menciptakan sebuah ruang interaksi baru yang tidak mengenal demarkasi teritorial. Lalu lintas data, transaksi, dan komunikasi digital berlangsung dalam hitungan milidetik melintasi yurisdiksi tanpa pemeriksaan perbatasan tradisional. Realitas ini menantang fondasi kedaulatan hukum nasional secara fundamental: mampukah negara tetap berdaulat ketika warganya hidup dalam ekosistem digital yang infrastrukturnya dimiliki, dibangun, dan diatur oleh entitas asing?

Fenomena platform global seperti Google, Meta, dan X (sebelumnya Twitter) menunjukkan bahwa korporasi teknologi kini menjalankan fungsi-fungsi yang dulunya menjadi monopoli negara, seperti pengelolaan ruang publik, pembuatan aturan konten, hingga resolusi sengketa melalui mekanisme terms of service (Klonick, 2018). Keadaan ini memunculkan apa yang disebut sebagai networked sovereignty atau kedaulatan yang

terdistribusi, di mana otoritas tidak lagi terpusat pada pemerintah nasional, melainkan tersebar di antara aktor-aktor privat transnasional (Mueller, 2020). Indonesia, sebagai negara dengan lebih dari 200 juta pengguna internet, berada di persimpangan antara keinginan untuk menegaskan yurisdiksi digitalnya dan kenyataan ketergantungan yang mendalam terhadap teknologi asing. Artikel ini merumuskan dua permasalahan pokok: Pertama, bagaimanakah digitalisasi menggerus dimensi-dimensi kedaulatan hukum nasional? Kedua, langkah-langkah strategis apakah yang dapat ditempuh oleh Indonesia untuk merespons tantangan tersebut tanpa mengisolasi diri dari ekosistem global? Tujuannya adalah untuk mengeksplorasi titik-titik rentan kedaulatan hukum di era digital serta menawarkan kerangka respons yang realistis dan adaptif.

B. KEDAULATAN HUKUM DALAM TEGANGAN ANTARA KODE DAN REGULASI

Untuk memahami tantangan digitalisasi terhadap kedaulatan hukum, diperlukan tinjauan teoretis tentang konsep kedaulatan itu sendiri dan pergeserannya di ruang digital. Secara klasik, Jean Bodin memaknai kedaulatan sebagai kekuasaan tertinggi untuk membuat hukum yang tidak dapat dibatasi oleh kekuasaan lain. Dalam evolusinya, kedaulatan eksternal berarti kemerdekaan dari intervensi asing, sementara kedaulatan internal berarti supremasi atas semua entitas

di dalam teritori negara. Kedua dimensi ini mengalami guncangan hebat ketika arus data melintasi perbatasan tanpa dapat diintersep secara efektif.

Lawrence Lessig (2006) dalam karya monumentalnya *Code and Other Laws of Cyberspace* memperkenalkan tesis yang provokatif: "Kode adalah hukum" (*Code is Law*). Lessig menjelaskan bahwa regulasi di ruang siber tidak hanya ditentukan oleh norma hukum yang dibuat parlemen, tetapi juga dan bahkan terutama oleh arsitektur teknis atau kode pemrograman yang membentuk platform digital. Ketika sebuah platform media sosial mendesain algoritmanya untuk memoderasi konten tertentu, ia sedang menjalankan fungsi yudisial dan legislatif privat yang memiliki dampak global. Arsitektur ini tidak tunduk pada prosedur demokratis yang dikenal dalam negara hukum nasional, melainkan pada keputusan bisnis korporasi yang berkantor pusat di negara lain. Dengan demikian, kedaulatan hukum tergerus karena warga negara lebih banyak berinteraksi dengan "hukum kode" yang dibuat di Silicon Valley daripada dengan hukum nasional yang dibentuk di Senayan (DeNardis, 2020).

Di sisi lain, Anu Bradford (2020) mengajukan konsep *Brussels Effect* yang menjelaskan bagaimana Uni Eropa secara efektif mengeksport standar regulasinya ke seluruh dunia. Melalui instrumen seperti *General Data Protection Regulation* (GDPR), Uni Eropa memaksa

perusahaan-perusahaan global untuk mematuhi standar Eropa jika mereka ingin mengakses pasar Eropa. Efek domino dari kebijakan ini adalah banyak negara, termasuk Indonesia, yang secara tidak langsung menyesuaikan hukum nasionalnya agar tidak tertinggal atau justru mengadopsi standar serupa. *Brussels Effect* adalah bentuk ekstrateritorialitas halus yang mendesak kedaulatan legislatif negara lain, karena pilihan untuk membuat aturan yang berbeda menjadi sangat mahal secara ekonomi. Dalam kerangka ini, kedaulatan hukum nasional tidak hilang, tetapi ruang diskresinya menyempit secara signifikan karena dipaksa berkiblat pada standar global yang didikte oleh sedikit kekuatan ekonomi digital.

C. TIGA LOCUS TANTANGAN TERHADAP KEDAULATAN HUKUM NASIONAL

1. Ekstrateritorialitas Penegakan Hukum dan Konflik Yurisdiksi

Tantangan pertama terletak pada kesulitan negara untuk menegakkan hukum pada entitas yang tidak memiliki kehadiran fisik di wilayahnya. Prinsip yurisdiksi tradisional didasarkan pada teritorialitas, tetapi digitalisasi membuat korporasi global dapat beroperasi penuh di suatu negara tanpa memiliki kantor pusat, aset, atau bahkan server di negara tersebut. Ketika terjadi pelanggaran, misalnya penyebaran konten ilegal,

penipuan daring, atau pelanggaran data—negara harus berhadapan dengan persoalan: dapatkah mereka memaksa platform asing untuk mematuhi putusan pengadilan nasional?

Indonesia pernah mengalami situasi ini secara akut. Dalam berbagai kasus ujaran kebencian dan disinformasi yang viral, pemerintah kesulitan meminta data pengguna atau meminta penghapusan konten secara langsung kepada perusahaan yang servernya berada di luar negeri. Upaya melalui mekanisme *Mutual Legal Assistance* (MLA) seringkali lamban dan birokratis, sementara konten yang merusak sudah menyebar luas dalam hitungan jam. Ketidakmampuan untuk menegakkan perintah secara cepat dan efektif ini merupakan pukulan langsung terhadap klaim kedaulatan hukum, karena negara tampak tidak berdaya melindungi ketertiban di wilayahnya sendiri (Kusumawardhani, 2023).

2. Dominasi Platform Digital sebagai *Quasi-Sovereign*

Platform digital raksasa telah menjelma menjadi semacam *quasi-sovereign* yang memiliki kewenangan untuk menetapkan aturan main di ruang publik digital. Melalui *community guidelines* dan *terms of service*, mereka menentukan ekspresi apa yang diizinkan, data apa yang dikumpulkan, dan bagaimana sengketa diselesaikan. Mekanisme ini bersifat privat dan

seringkali tidak transparan. Ketika Facebook *Oversight Board* memutuskan apakah seorang mantan presiden boleh kembali ke platform, ia sedang menjalankan fungsi quasi-konstitusional yang mempengaruhi hak politik jutaan orang, tanpa mandat demokratis sama sekali (Douek, 2022).

Bagi Indonesia, situasi ini menciptakan paradoks kedaulatan. Di satu sisi, negara memiliki kewajiban konstitusional untuk melindungi kebebasan berpendapat dan hak privasi warga negaranya. Di sisi lain, ketika platform melakukan deplatforming atau shadow banning terhadap akun warga Indonesia, negara hampir tidak memiliki mekanisme hukum untuk menuntut akuntabilitas dari platform tersebut. UU ITE dan UU PDP memberikan kerangka normatif untuk memproses data, tetapi tidak menyentuh kebijakan moderasi konten yang dibuat oleh perusahaan asing. Ruang publik yang seharusnya diatur oleh hukum nasional secara diam-diam telah diserahkan kepada kebijakan privat yang berada di luar jangkauan pengadilan Indonesia (Safitri, 2023). Ini adalah erosi kedaulatan yang berlangsung secara halus namun masif.

3. Ketergantungan pada Infrastruktur dan Standar Teknis Global

Kedaulatan hukum juga terancam oleh ketergantungan pada infrastruktur digital global.

Mayoritas layanan komputasi awan yang digunakan oleh pemerintah dan sektor swasta di Indonesia dikelola oleh perusahaan asing seperti *Amazon Web Services*, *Google Cloud*, atau *Microsoft Azure*. Data-data strategis, termasuk data pemerintahan, rentan terhadap yurisdiksi asing melalui *Cloud Act* Amerika Serikat, yang memungkinkan penegak hukum AS untuk mengakses data yang disimpan oleh perusahaan AS di mana pun data itu berada secara global. Kondisi ini menempatkan Indonesia dalam posisi tawar yang rendah dan membahayakan kedaulatan data (*data sovereignty*) sebagai dimensi baru kedaulatan negara (Pratiwi & Nugroho, 2023).

Lebih dari sekadar persoalan yurisdiksi dan kedaulatan teritorial yang telah dibahas sebelumnya, realitas yang lebih mendasar dan sering luput dari perhatian adalah bahwa standar teknis yang menjadi fondasi operasional dunia digital seperti protokol enkripsi, arsitektur protokol internet (TCP/IP), sistem pembayaran digital, serta standar keamanan siber justru ditentukan oleh badan-badan internasional seperti *Internet Engineering Task Force* (IETF), *International Organization for Standardization* (ISO), atau bahkan oleh perusahaan-perusahaan teknologi raksasa global seperti Google, Apple, Microsoft, dan Meta. Dalam konteks ini, Indonesia lebih sering berperan sebagai pengguna atau pengadopsi standar (*standard taker*) yang pasif daripada

sebagai pembuat standar (*standard maker*) yang aktif dan memiliki pengaruh dalam merumuskan norma teknis yang akan mengatur perilaku di ruang siber. Ironisnya, sebagaimana diingatkan oleh *Lawrence Lessig* dalam karyanya yang seminal *Code: Version 2.0*, kemampuan untuk menentukan arsitektur teknis sesungguhnya adalah kemampuan untuk mengatur, karena kode pemrograman dan protokol teknis berfungsi sebagai hukum yang mengatur apa yang mungkin dan tidak mungkin dilakukan oleh pengguna di ruang digital. Ketika standar keamanan siber, misalnya standar enkripsi end-to-end atau protokol autentikasi, ditentukan sepihak oleh pihak asing tanpa melibatkan kepentingan nasional Indonesia, maka ruang bagi kebijakan hukum yang berdaulat menjadi sangat terbatas. Akibatnya, setiap upaya pemerintah untuk mengatur keamanan data, melindungi privasi warga negara, atau menegakkan hukum siber seringkali berbenturan dengan arsitektur teknis yang sudah dirancang oleh pihak lain, sehingga kebijakan hukum Indonesia menjadi sekadar tempelan atau patch yang tidak mampu mengubah realitas fundamental yang sudah ditetapkan oleh standar global. Contoh konkretnya adalah kesulitan aparat penegak hukum Indonesia dalam meminta akses terhadap data pengguna yang dienkripsi oleh platform asing, atau ketidakmampuan regulator untuk memaksa perubahan algoritma rekomendasi yang dianggap merugikan masyarakat, karena standar teknisnya sudah

ditetapkan di luar kendali Indonesia. Oleh karena itu, salah satu agenda strategis dalam rekonstruksi hukum siber nasional adalah membangun kapasitas diplomasi teknis dan partisipasi aktif dalam forum-forum standardisasi internasional, sehingga Indonesia tidak hanya menjadi objek dari regulasi global, melainkan juga subjek yang turut menentukan arah perkembangan arsitektur teknis dunia digital.

D. KEBIJAKAN PENDAFTARAN PSE LINGKUP PRIVAT SEBAGAI AKSI DEFENSIF KEDAULATAN

Pada Juli 2022, Kementerian Komunikasi dan Informatika (Kominfo) mengambil langkah kontroversial dengan memblokir sementara sejumlah platform digital global, termasuk PayPal, Steam, dan Dota 2, karena tidak memenuhi kewajiban pendaftaran sebagai Penyelenggara Sistem Elektronik (PSE) Lingkup Privat. Kebijakan ini merupakan implementasi dari Peraturan Pemerintah Nomor 71 Tahun 2019 dan Peraturan Menteri Kominfo Nomor 5 Tahun 2020, yang mewajibkan setiap PSE, termasuk yang beroperasi lintas batas, untuk mendaftarkan diri dan memberikan akses kepada otoritas Indonesia untuk melakukan pengawasan konten serta pemutusan akses terhadap konten ilegal.

Kasus ini adalah potret terang dari upaya negara mempertahankan kedaulatan hukumnya di ruang digital. Pemerintah Indonesia, melalui instrumen hukum

domestik, mencoba memaksa korporasi global untuk tunduk pada yurisdiksinya. Namun, dibalik ketegasan tersebut, terlihat juga kelemahan mendasar. Pemblokiran hanya berlangsung singkat dan segera dicabut setelah perusahaan yang bersangkutan mendaftar. Tidak ada negosiasi ulang yang secara fundamental mengubah relasi kuasa; platform global tetap beroperasi dengan model bisnis yang sama, hanya saja kini mereka "terdaftar" secara administratif. Beberapa platform bahkan mendaftar dengan komitmen minimal, tanpa kehadiran fisik atau perwakilan hukum yang kuat di Indonesia (Hidayat, 2023).

Studi kasus ini menunjukkan bahwa penegakan kedaulatan secara unilateral dan konfrontatif cenderung bersifat simbolik dan rentan terhadap kompromi pragmatis. Negara tidak dapat memblokir terlalu banyak platform vital tanpa menimbulkan gejolak sosial dan ekonomi di dalam negeri. Oleh karena itu, kedaulatan hukum nasional dalam konteks ini lebih tepat dipahami sebagai arena negosiasi yang berkelanjutan, bukan sekadar perintah satu arah.

E. MENUJU KEDAULATAN FUNGSIONAL DAN KOLABORASI MULTILATERAL

Mempertahankan kedaulatan hukum di era digital tidak mungkin dilakukan dengan cara isolasi atau proteksionisme digital total. Sebaliknya, yang diperlukan

adalah pergeseran strategi dari kedaulatan teritorial yang absolut menuju kedaulatan fungsional yang cerdas. Kedaulatan fungsional berarti negara fokus mengontrol aspek-aspek strategis yang benar-benar esensial, seperti keamanan data pribadi warga negara, keamanan siber nasional, dan pengenaan pajak atas nilai ekonomi yang dihasilkan di dalam negeri, tanpa harus mengontrol seluruh spektrum aktivitas digital.

Pertama, Indonesia harus membangun infrastruktur komputasi awan nasional yang mumpuni untuk data-data pemerintahan yang sensitif, sehingga ketergantungan terhadap penyedia asing dapat dikurangi secara bertahap. Kedua, penguatan kapasitas teknis dari regulator sangat krusial. Kominfo, OJK, dan Bank Indonesia harus memiliki auditor forensik digital yang setara dengan kemampuan tim keamanan perusahaan besar agar dapat melakukan pengawasan yang efektif. Ketiga, diplomasi hukum multilateral harus menjadi prioritas. Indonesia perlu mengambil peran aktif dalam forum ASEAN dan PBB untuk merumuskan konvensi tentang yurisdiksi digital yang menghormati kesetaraan kedaulatan. Model interoperabilitas seperti *Cross-Border Privacy Rules* (CBPR) bisa menjadi rujukan awal agar standar perlindungan data Indonesia diakui setara dengan standar negara lain, sehingga ketundukan pada *Brussels Effect* tidak bersifat hierarkis tetapi resiprokal (Greenleaf, 2022).

F. KESIMPULAN

Berdasarkan pembahasan di atas, digitalisasi menghadirkan tantangan multidimensi terhadap kedaulatan hukum nasional. Tantangan pertama adalah ekstrateritorialitas yang melemahkan penegakan hukum domestik karena subjek regulasi berada di luar jangkauan fisik negara. Tantangan kedua adalah munculnya *quasi-sovereign* dalam wujud platform digital global yang menjalankan fungsi legislasi, yudikasi, dan eksekusi privat atas ruang publik komunikasi warga negara. Tantangan ketiga adalah ketergantungan struktural pada infrastruktur dan standar teknis asing yang mereduksi ruang bagi kebijakan yang otonom. Menjawab rumusan masalah, digitalisasi tidak menghapus kedaulatan hukum nasional, tetapi secara fundamental mengubah cara kedaulatan itu dioperasikan; dari monopoli absolut menjadi kewenangan yang harus terus-menerus diperjuangkan melalui negosiasi teknis, komersial, dan diplomatik.

Sebagai sintesis dari seluruh pembahasan yang telah diuraikan, strategi yang direkomendasikan untuk memperkuat kedaulatan hukum Indonesia di era digital mencakup tiga pilar utama yang saling terkait dan harus dijalankan secara simultan. Pertama, pembangunan infrastruktur data nasional yang berdaulat, yang tidak hanya berarti membangun pusat data fisik di dalam negeri, tetapi juga mencakup pengembangan sistem

enkripsi nasional, protokol keamanan siber yang mandiri, serta kebijakan tata kelola data yang memastikan bahwa data strategis warga negara dan kepentingan nasional tidak sepenuhnya bergantung pada infrastruktur asing. Kedua, penguatan kapasitas teknis aparatur pengawas secara menyeluruh dan berkelanjutan, yang meliputi rekrutmen ahli keamanan siber, pembentukan laboratorium forensik digital yang modern, pengembangan program sertifikasi hukum siber bagi hakim, jaksa, dan penyidik, serta penyediaan anggaran yang memadai untuk riset dan pengembangan di bidang regulasi digital. Ketiga, diplomasi aktif dan terarah untuk membentuk rezim yurisdiksi digital yang multipolar dan adil, di mana Indonesia tidak lagi sekadar menerima standar dan aturan yang dibuat oleh negara maju atau korporasi global, melainkan turut berpartisipasi secara setara dalam forum-forum internasional seperti *Internet Governance Forum (IGF)*, *International Telecommunication Union (ITU)*, *ASEAN Digital Ministers Meeting*, dan berbagai perundingan perdagangan digital. Hanya dengan mengintegrasikan ketiga pilar strategis ini secara konsisten dan berani, Indonesia dapat menjadi subjek yang berdaulat penuh dalam ekosistem digital global, bukan sekadar objek pasif yang menerima dampak dari revolusi digital yang digerakkan oleh kepentingan asing. Kedaulatan hukum digital bukanlah sekadar wacana akademis, melainkan sebuah keniscayaan bagi negara yang ingin melindungi

hak-hak warganya, mendorong inovasi lokal, dan berdiri sejajar dengan bangsa-bangsa lain dalam menentukan masa depan tata kelola dunia maya.

REFERENCE:

- Besson, S. (2011). Sovereignty, International Law and Democracy. *European Journal of International Law*, 22(2), 373–387. <https://doi.org/10.1093/ejil/chr019>
- Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.
- DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.
- Douek, E. (2022). Content Moderation as Administration. *Harvard Law Review*, 136(2), 526–609.
- Greenleaf, G. (2022). Global Convergence of Data Privacy Standards and Asia: The Unfinished Agenda. *International Data Privacy Law*, 12(3), 189–210. <https://doi.org/10.1093/idpl/ipac008>
- Hidayat, M. (2023). Pendaftaran PSE Lingkup Privat dan Ambivalensi Kedaulatan Digital Indonesia. *Jurnal Hukum dan Teknologi Nusantara*, 4(1), 67–85.

- Klonick, K. (2018). *The New Governors: The People, Rules, and Processes Governing Online Speech*. *Harvard Law Review*, 131(6), 1598–1670.
- Kusumawardhani, A. (2023). *Mutual Legal Assistance dalam Penegakan Hukum Siber Lintas Batas: Studi Kasus Indonesia*. *Jurnal Hukum Internasional Indonesia*, 20(2), 230–250.
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Mueller, M. (2020). *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Polity Press.
- Pratiwi, N., & Nugroho, S. (2023). *Kedaulatan Data dan Cloud Act: Perlindungan Data Pemerintah di Era Komputasi Awan*. *Jurnal Ketahanan Informasi*, 5(2), 112–130.
- Safitri, R. (2023). *Platform Governance dan Kebebasan Berpendapat di Indonesia: Ruang Hampa Pengawasan*. *Jurnal Ilmu Hukum, Demokrasi, dan Teknologi*, 1(1), 40–58.