Arsitektur Global Kedaulatan Digital

Judul: Arsitektur Global Kedaulatan Digital: Analisis Komparatif Model Sensor dan Kontrol Internet pada Tahun 2025

Penulis: NOX

Abstrak:
Artikel ini mengeksplorasi evolusi praktik sensor dan kontrol internet di negara-negara kunci pada tahun 2025. Analisis didasarkan pada pendekatan komparatif yang mengidentifikasi tiga model dominan: otoriter-berdaulat (Tiongkok, Rusia, Iran, Korea Utara), liberal-regulasi (AS, UE, Israel), dan hibrida (Turki, Mesir, dan beberapa negara di Asia, Afrika, dan Amerika Latin). Dinyatakan bahwa pada tahun 2025, konsep "internet berdaulat" telah bertransformasi dari sebuah ide teoretis menjadi arsitektur tekno-hukum konkret yang diimplementasikan oleh sejumlah negara. Fokusnya adalah pada instrumen teknologi (DPI, AI), kerangka hukum, dan tujuan geopolitik di balik pembatasan tersebut. Artikel ini menyimpulkan dengan menguatnya fragmentasi internet global ("Splinternet") dan pembentukan ekosistem digital yang tangguh yang diatur oleh aturannya sendiri.

Kata kunci: sensor internet, kedaulatan digital, 2025, Deep Packet Inspection (DPI), kecerdasan buatan, regulasi, hak asasi manusia, keamanan siber.

Pendahuluan
Pada tahun 2025, internet telah berhenti menjadi ruang global yang menyatu seperti yang dibayangkan pada awal kelahirannya. Didorong oleh ketegangan geopolitik, kekhawatiran keamanan nasional, dan keinginan untuk kedaulatan budaya, berbagai model kontrol nasional dan regional atas ranah informasi digital telah muncul. Istilah "sensor" telah berevolusi untuk mencakup tidak hanya pemblokiran konten, tetapi juga sistem moderasi preemtif yang kompleks, tekanan legislatif pada platform, manipulasi lalu lintas, dan disinformasi yang ditargetkan.

Tujuan artikel ini adalah untuk melakukan analisis komparatif model kontrol internet di kekuatan global besar, mengidentifikasi kesamaan dan perbedaan mendasarnya, serta menilai dampaknya terhadap hak-hak sipil, ekonomi digital, dan stabilitas internasional.

1. Metodologi
Penelitian ini didasarkan pada analisis komparatif kualitatif. Negara dipilih berdasarkan pengaruhnya terhadap kebijakan digital global dan perwakilan dari berbagai model kontrol. Sumbernya meliputi:
• Akta legislatif nasional (undang-undang tentang "internet berdaulat", perlindungan data, anti-ekstremisme);

• Laporan dari organisasi internasional (Freedom House, RSF, Access Now);
• Laporan teknis oleh perusahaan keamanan siber (Citizen Lab, Palo Alto Networks);
• Pernyataan publik oleh pejabat pemerintah dan regulator.

2. Analisis Komparatif Model Kontrol Internet

2.1. Model Kedaulatan Digital Otoriter

Tiongkok:
Pada tahun 2025, Great Firewall of China (GFW) telah berevolusi menjadi sistem komprehensif untuk mengelola masyarakat digital yang disebut "Social Credit 2.0". Pemblokiran berbasis DPI telah dilengkapi dengan algoritma AI prediktif yang mampu mengidentifikasi dan menekan diskusi "yang tidak diinginkan" pada tahap awal. Semua platform global besar telah digantikan dengan alternatif domestik (WeChat, Douyin, Baidu) yang berada di bawah kendali penuh negara. Mengekspor model ini—terutama ke negara-negara Afrika dan Asia melalui Inisiatif Sabuk dan Jalan—telah menjadi instrumen soft power yang kunci.

Rusia:
Implementasi undang-undang "internet berdaulat" (2019) telah selesai. Pada tahun 2025, Sistem Penamaan Domain Nasional (DNS) beroperasi, memungkinkan isolasi segmen internet Rusia (Runet) dari jaringan global ketika diperlukan. DPI secara aktif digunakan untuk menekan VPN dan lalu lintas terenkripsi. Target utama sensor adalah kritik terhadap otoritas, operasi militer, konten LGBTQ+, dan media independen. Dasar hukumnya termasuk undang-undang tentang "berita palsu", "agen asing", dan "ekstremisme".

Iran:
Model Iran menggabungkan kontrol teknis dengan represi yang keras. Negara ini mempertahankan salah satu sistem penyaringan konten paling maju di dunia, yang mampu memblokir messenger (Telegram, WhatsApp) dan media sosial secara dinamis selama protes. Pada tahun 2025, identifikasi pengguna wajib diperlukan untuk mengakses Wi-Fi dan membeli kartu SIM. Throttling (pelambatan) bandwidth internet ke tingkat yang sangat rendah biasa dilakukan selama kerusuhan.

Korea Utara:
Tetap menjadi tolok ukur kontrol total. Intranet Kwangmyong sepenuhnya terisolasi dari internet global. Akses ke internet internasional terbatas pada elite yang sempit. Konten dibatasi pada propaganda negara, materi ideologis, dan informasi ilmiah yang sangat terbatas.

2.2. Model Liberal-Regulasi (AS, UE, Israel)

Amerika Serikat (AS):
Sensor pemerintah tradisional tidak ada, tetapi sistem regulasi swasta dan publik yang kompleks telah muncul. Di bawah tekanan publik dan pengawasan oleh FCC dan FTC, platform utama (Meta, X, Google) telah mengencangkan kebijakan moderasi terkait ujaran kebencian, disinformasi, dan hasutan. Debat sentral tahun 2025 berkisar sekitar Bagian 230, undang-undang yang memberikan kekebalan kepada platform untuk konten yang dibuat pengguna. Seruan untuk mencabut atau mengubahnya mendorong platform untuk secara proaktif melakukan sensor untuk menghindari risiko hukum. Dengan demikian, sensor secara efektif didelegasikan kepada korporasi swasta.

Uni Eropa (UE):
UE telah mengembangkan kerangka regulasi paling maju di dunia, yang pada dasarnya menetapkan standar global. Sensor bersifat tidak langsung, ditegakkan melalui kepatuhan ketat terhadap undang-undang:
• GDPR: Memblokir situs yang melanggar persyaratan perlindungan data;
• Digital Services Act (DSA): Platform wajib menghapus konten ilegal (misalnya, terorisme, ujaran kebencian) dengan cepat di bawah ancaman denda besar;
• Digital Markets Act (DMA): Menargetkan platform monopoli.
UE tidak terlibat dalam pemblokiran tingkat negara tetapi menciptakan lingkungan hukum di mana ketidakpatuhan menyebabkan pengusiran de facto dari pasar.

Israel:
Israel menyajikan kasus unik dari model liberal-regulasi dengan penekanan kuat pada keamanan nasional. Sebagai demokrasi berteknologi tinggi, Israel umumnya menganut prinsip internet terbuka. Namun, di tengah konflik dan ancaman keamanan yang berlangsung, sensor diterapkan secara selektif dan atas dasar hukum yang kuat.
• Kerangka hukum: Instrumen utama adalah sensor militer, yang diwarisi dari era pendirian negara. Semua media dan outlet online harus menyerahkan materi terkait keamanan untuk ditinjau terlebih dahulu oleh Biro Sensor Militer. Pada tahun 2025, prinsip ini telah disesuaikan untuk era digital.
• Teknologi dan praktik: Otoritas dapat meminta ISP dan platform media sosial untuk menghapus konten yang dianggap mengancam keamanan nasional atau menghasut kekerasan. Keputusan ini sering ditantang di Mahkamah Agung, yang berfungsi sebagai penyeimbang penting. Selama eskalasi militer, sensor mengintensifkan, dan platform menghadapi tekanan yang semakin besar untuk mematuhi. Tidak seperti rezim otoriter, Israel mempertahankan masyarakat sipil dan pers bebas yang hidup yang menantang keputusan sensor, membuat prosesnya lebih transparan.

2.3. Model Hibrida (Turki, Mesir, Asia, Afrika, Amerika Latin)

Turki:
Mempertahankan salah satu daftar blokir konten terbesar di dunia di bawah undang-undang yang melindungi kepentingan negara dan ketertiban umum. Undang-Undang No. 5651 diperkuat pada tahun 2025, memungkinkan regulator BTK untuk memblokir konten apa pun dalam empat jam tanpa perintah pengadilan. Undang-Undang No. 7416 menekan platform untuk menunjuk

perwakilan lokal dan mematuhi arahan negara, dengan throttling yang digunakan secara progresif hingga gangguan layanan penuh.

Mesir:
Menggunakan lisensi telekomunikasi sebagai alat kontrol. Pemblokiran VPN dan aplikasi terenkripsi (seperti Signal) adalah praktik standar. Selama ketegangan politik, pemadaman internet nasional dapat terjadi. Undang-undang kejahatan siber memberikan kekuasaan luas untuk memblokir situs dan memantau warga.

Asia (India dan Vietnam):
India mempraktikkan pemadaman internet regional rutin dengan dalih keselamatan publik. Undang-undang TI memberikan pemerintah kekuasaan pemblokiran yang luas. Vietnam mencerminkan model Tiongkok, mewajibkan perusahaan teknologi untuk menyimpan data pengguna secara lokal, membagikannya atas permintaan, dan menghapus konten dalam 24 jam.

Afrika:
Pemerintah di Ethiopia, Uganda, dan Zimbabwe semakin sering menggunakan pemadaman internet selama pemilihan dan protes. Teknologi dan model kontrol Tiongkok—sering kali digabungkan dengan infrastruktur Huawei dan ZTE—semakin berpengaruh.

Amerika Latin:
Pada tahun 2025, kawasan ini menunjukkan tren campuran, sebagian besar sesuai dengan model hibrida dengan variasi yang signifikan.

• **Brasil:**
Sebagai ekonomi terbesar di kawasan, Brasil berusaha menyeimbangkan kebebasan berekspresi dengan memerangi disinformasi dan kejahatan siber. Marco Civil da Internet yang terinspirasi UE tetap menjadi landasan regulasi. Namun, semakin banyak perintah pengadilan untuk memblokir messenger populer (seperti WhatsApp dan Telegram) karena menolak memberikan data pengguna atau membatasi berita palsu telah memicu debat. Sensor sering kali ditargetkan dan bersifat sementara tetapi frekuensinya semakin meningkat.

• **Venezuela & Nikaragua:**
Bergerak menuju model otoriter. Pemerintah menggunakan alat teknis untuk memblokir situs berita independen dan platform media sosial, terutama selama gejolak politik. Conatec Venezuela (Pusat Kontrol Ruang Cyber Nasional) mengoordinasikan sensor. Undang-undang kejahatan siber yang keras mengkriminalkan kritik online terhadap pemerintah.

• **Kuba:**
Mendekati kontrol negara penuh. Meskipun akses internet telah meluas pada tahun 2025, akses tetap mahal dan sangat diatur. Monopoli telekom negara ETECSA memungkinkan penyaringan

konten dan pengawasan pengguna. Kritik pemerintah dan akses media independen secara rutin diblokir.

3. Diskusi dan Kesimpulan

Pada tahun 2025, dunia telah beralih dari internet yang menyatu menjadi kumpulan ranah digital nasional dan regional yang terfragmentasi—Splinternet. Tren utama termasuk:

• **Kecanggihan teknologi:**

Pemblokiran konten sederhana telah memberi jalan kepada sistem berbasis DPI dan AI yang mampu melakukan moderasi prediktif dan penekanan alat penyelamatan (circumvention) yang tepat.

• **Kamuflase hukum:**

Sensor semakin dibenarkan melalui anti-ekstremisme, perlindungan data (UE), atau kedaulatan dan keamanan (Rusia, Tiongkok, Israel), memberikannya legitimasi yang dipersepsikan di arena internasional.

• **Privatisasi sensor:**

Di demokrasi liberal (AS, UE), peran penyensor telah beralih dari negara ke perusahaan, yang dipaksa untuk mengikuti mandat regulasi di bawah ancaman hukuman. Israel mempertahankan sensor negara, tetapi dalam konteks keamanan yang sempit dan dengan pengawasan yudisial.

• **Dimensi geopolitik:**

Dua model global sedang bersaing: pendekatan regulasi AS–UE (berdasarkan hak dan norma pasar) vs. model Tiongkok–Rusia (kontrol dan isolasi negara). Negara-negara hibrida—terutama di Amerika Latin—mengadopsi elemen dari keduanya, tergantung pada keadaan politik.

Bahayanya terletak pada penciptaan gelembung informasi yang persisten, meningkatnya otoritarianisme, dan berkurangnya pertukaran pengetahuan lintas batas. Perjuangan antara keterbukaan dan keamanan nasional, seperti yang ditunjukkan kasus Israel, adalah kontradiksi sentral yang membentuk masa depan internet.

Lampiran: DPI dan Penyadapan Sertifikat (Certificate Interception)

Deep Packet Inspection (DPI) adalah teknologi analisis lalu lintas yang memungkinkan penyedia atau aktor negara tidak hanya melihat ke mana Anda terhubung tetapi juga memeriksa isi sebenarnya dari paket data. Ini mengungkapkan perilaku pengguna—menonton video, menggunakan VPN, berkirim pesan, mengakses Tor, dll.

Dalam praktiknya, DPI memungkinkan:

• Pemblokiran atau throttling layanan tertentu;
• Penghindaran anonimitas VPN atau Tor;
• Pengawasan perilaku online;
• Sensor massal—bahkan dalam lalu lintas terenkripsi.

Ancaman terberat terletak pada pelemahan kepercayaan terhadap teknologi internet fundamental. Di banyak negara, dengan dalih memerangi terorisme, melindungi anak-anak, menegakkan sanksi, atau motif serupa, pemerintah memaksa ISP untuk mengimplementasikan DPI dan memperkenalkan Otoritas Sertifikat (Certificate Authorities/CAs) mereka sendiri. CA ini dapat menerbitkan sertifikat HTTPS palsu—pengguna tidak akan menyadarinya, peramban tidak akan memperingatkan, dan lalu lintas melewati simpul yang dikendalikan.
Koneksi tetap terlihat "aman", tetapi pemerintah dapat secara legal membaca, merekam, dan memodifikasi lalu lintas—tanpa peretasan—dengan membajak infrastruktur kepercayaan. Ini dikenal sebagai penyadapan sertifikat (certificate interception) dan, dikombinasikan dengan DPI, membentuk sistem intrusi yang legal.
Mekanisme seperti itu melanggar netralitas jaringan, privasi, dan gagasan dasar dari komunikasi yang aman. Ketika negara menggantikan kepercayaan—ia tidak lagi melindungi. Ia mengontrol.

Referensi:

• Deibert, R. (2024). The Great Firewall 2.0: AI and the Future of Internet Control. MIT Press.
• Freedom House. (2025). Freedom on the Net 2025: The Global Drive to Control Cyberspace.
• European Commission. (2024). First Annual Report on the Implementation of the Digital Services Act.
• Soldatov, A., & Borogan, I. (2023). The Red Web: The Struggle for Russia's Digital Sovereignty. HarperCollins.
• Reporters Without Borders (RSF). (2025). World Press Freedom Index 2025: The Oligarchy of Truth.
• Zuboff, S. (2023). The Age of Surveillance Capitalism. PublicAffairs.
• Cohen, M., & Leybovich, G. (2024). Digital Democracy under Siege: Security, Censorship and Civil Liberties in Israel. Tel Aviv University Press.
• Americas Quarterly. (2025). Digital Authoritarianism in Latin America: The New Normal?
• Carrasco, E., & Silva, L. (2024). Internet Governance in Brazil: Between Marco Civil and the Shadow of Disinformation. São Paulo University Press.