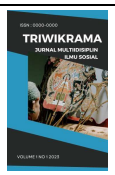
Triwikrama: Jurnal Ilmu Sosial
Volume 9 No. 9 Tahun 2025
E-ISSN: 2988-1986
Open Access:



REDEFINISI KEDAULATAN DI ERA DIGITAL: KEAMANAN SIBER, TATA KELOLA DATA, DAN OTONOMI REGIONAL DI ASIA TENGGARA

Naila Aulia Amin[1], Atika Puspita Marzaman[2]
[1,2]Departemen Ilmu Hubungan Internasional,Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Makassar, Indonesia

ARTICLEINFO

Article history:
Received: Juni 2025
Revised: Juni 2025
Accepted: Juni 2025
Available online

Korespondensi: Email:
[1]nailaauliaamiin@gmail.com
[2]tika.marzaman@gmail.com

Abstrak

Era digital telah membawa perubahan *signifikan* terhadap konsep kedaulatan konvensional, di mana batasan geografis tidak lagi menjadi penghalang bagi aliran informasi dan data. Kedaulatan digital muncul sebagai respons terhadap tantangan ini, menekankan pentingnya penguasaan data, infrastruktur teknologi, dan keamanan siber. Di kawasan Asia Tenggara, tantangan ini semakin kompleks akibat disparitas kapasitas teknologi dan regulasi di antara negara-negara anggotanya, serta ketergantungan yang tinggi pada perusahaan teknologi asing. Ancaman dari serangan siber dan manipulasi informasi juga semakin meningkat, yang dapat merusak stabilitas politik dan sosial. Meskipun ASEAN telah meluncurkan beberapa inisiatif untuk membangun kerangka kerja digital yang terkoordinasi, implementasinya masih menghadapi banyak hambatan, termasuk perbedaan kepentingan politik dan kapasitas teknis antarnegara. Oleh karena itu, diperlukan upaya nyata untuk meningkatkan kapasitas digital, harmonisasi regulasi, dan edukasi masyarakat tentang kedaulatan digital. Dengan pendekatan kolaboratif dan komprehensif, kedaulatan digital dapat menjadi agenda bersama yang menjamin masa depan kawasan Asia Tenggara di era digital.

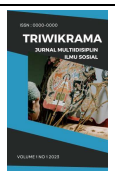
Kata Kunci: Kedaulatan Digital, Keamanan Siber, Tata Kelola Data, Otonomi Regional, Asia Tenggara

Abstract

The digital era has brought significant changes to the conventional concept of sovereignty, where geographical boundaries are no longer a barrier to the flow of information and data. Digital sovereignty has emerged as a response to these challenges, emphasizing the importance of data control, technological infrastructure, and cybersecurity. In Southeast Asia, these challenges are further complicated by disparities in technological capacity and regulation among member countries, as well as a high dependence on foreign technology companies. The threats from cyberattacks and information manipulation are also increasing, potentially undermining political and social stability. Although ASEAN has launched several initiatives to establish a coordinated digital governance framework, implementation still faces numerous obstacles, including differing political interests and technical capacities among countries. Therefore, there is a pressing need for concrete efforts to enhance digital capacity, harmonize regulations, and educate the public about digital sovereignty. With a collaborative and comprehensive approach, digital sovereignty can become a shared agenda that ensures the future of Southeast Asia in the digital era.

Keywords: *Digital Sovereignty, Cybersecurity, Data Governance, Regional Autonomy, Southeast Asia*

Triwikrama: Jurnal Ilmu Sosial
Volume 9 No. 9 Tahun 2025
E-ISSN: 2988-1986
Open Access:



1. PENDAHULUAN

Era digital telah memunculkan tantangan signifikan yang belum pernah terjadi sebelumnya terhadap konsep kedaulatan konvensional. Kemunculan ruang siber (cyberspace) dan aliran data yang melintasi batas-batas negara dengan sangat masif telah menciptakan domain baru yang tidak terikat oleh batasan geografis tradisional. Hal ini menyebabkan penerapan prinsip-prinsip kedaulatan klasik semakin bergeser. Internet, sebagai infrastruktur global yang menghubungkan miliaran perangkat dan pengguna di seluruh dunia, telah menciptakan realitas baru di mana informasi mengalir secara instan melampaui batas-batas negara tanpa perlu melewati mekanisme pemeriksaan fisik maupun kontrol perbatasan formal.

Tantangan kedaulatan semakin diperumit dengan munculnya *Big Tech* yang memiliki jangkauan dan pengaruh yang melampaui yurisdiksi nasional. Perusahaan seperti Google, Meta, Amazon, dan TikTok tidak hanya mengoperasikan infrastruktur digital yang tersebar di seluruh dunia, tetapi juga memiliki kekuatan ekonomi yang dalam beberapa kasus melebihi PDB dari banyak negara berdaulat. Keamanan siber (*cybersecurity*) muncul sebagai dimensi baru dalam pertahanan nasional dan kedaulatan di era digital, sementara kemampuan platform global untuk membentuk opini publik dan mempengaruhi wacana politik nasional melalui algoritma dan penargetan konten menimbulkan kekhawatiran tentang kedaulatan informasi dan otonomi politik.

Asia Tenggara telah menjadi salah satu wilayah yang paling menarik dan strategis untuk mengkaji dinamika kedaulatan digital pada era kontemporer. Dengan populasi lebih dari 650 juta jiwa dan pertumbuhan ekonomi digital yang pesat, kawasan ini merepresentasikan laboratorium empiris untuk memahami bagaimana negara-negara dengan kondisi sosial-ekonomi, sistem politik, dan kapasitas teknologi yang beragam menavigasi tantangan dan peluang era digital. Posisi geopolitik Asia Tenggara yang berada di antara kekuatan besar Amerika Serikat dan China, semakin menekankan pentingnya wilayah ini untuk studi tentang kedaulatan digital.

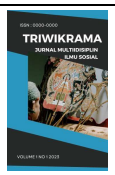
Kajian tentang kedaulatan digital di Asia Tenggara tidak hanya penting untuk memahami dinamika regional, tetapi juga memberikan wawasan berharga tentang tantangan yang dihadapi oleh ekonomi berkembang di seluruh dunia dalam menyeimbangkan manfaat dari integrasi digital global dengan kepentingan kedaulatan nasional.

2. KAJIAN TEORITIS

2.1 Konsep Kedaulatan Westphalia dan Fondasi Teoritis

Konsep kedaulatan yang kita kenal saat ini memiliki akar historis yang dalam, berasal dari Perjanjian Westphalia tahun 1648 yang telah membentuk dasar sistem negara modern selama berabad-abad (Krasner, 1999). Perjanjian ini melahirkan prinsip yang kemudian menjadi fondasi bagi hubungan internasional modern, di mana setiap negara diakui memiliki otoritas eksklusif atas wilayah geografisnya dengan batas-batas yang jelas dan terdefinisi. Tidak hanya demikian, prinsip ini telah menjadi norma dalam hukum internasional dengan menetapkan bahwa negara lain tidak memiliki hak untuk mencampuri urusan internal suatu negara berdaulat.

Kedaulatan dalam pengertian Westphalia ini dapat dipahami melalui tiga pilar utama yang saling terkait dan memperkuat satu sama lain. Pertama, prinsip integritas teritorial menegaskan pentingnya batas-batas fisik negara yang diakui secara internasional dan tidak dapat dilanggar oleh kekuatan eksternal. Kedua, prinsip non-intervensi menjamin bahwa



setiap negara memiliki hak untuk menentukan nasibnya sendiri tanpa campur tangan dari negara lain. Ketiga, prinsip kesetaraan hukum mengakui bahwa semua negara berdaulat memiliki kedudukan yang setara dalam hukum internasional, terlepas dari ukuran, kekuatan ekonomi, atau pengaruh politiknya.

Konsep kedaulatan tradisional ini sangat terikat dengan dimensi teritorial fisik, di mana pemerintah nasional memiliki wewenang tertinggi untuk membuat dan menegakkan hukum dalam batas-batas negara mereka. Pandangan ini telah mendominasi pemikiran tentang negara dan hubungan internasional selama berabad-abad, meskipun ada pengamatan bahwa beberapa aspek dari "mitos Westphalia" telah disederhanakan dalam diskursus kontemporer (Osiander, 2001).

2.2 Tantangan Era Digital terhadap Kedaulatan Konvensional

Sifat tanpa batas dari cyberspace telah menjadi tantangan signifikan bagi kedaulatan negara. Informasi dan data mengalir secara bebas melintasi batas-batas negara, mempersulit penerapan yurisdiksi nasional secara efektif (Mueller, 2010). Perkembangan ini telah menciptakan situasi di mana kontrol atas informasi dan data, yang semakin menjadi aset strategis di era digital, tidak lagi sepenuhnya berada di tangan negara.

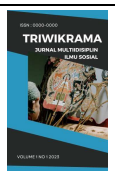
Perkembangan teknologi memungkinkan perusahaan *Big Tech Global* mengumpulkan dan memproses data pengguna dalam skala yang belum pernah terjadi sebelumnya, mengubahnya menjadi wawasan yang berharga dan produk yang dipersonalisasi, bahkan seringkali dengan minim pengawasan dari pemerintah nasional. Serangan siber, baik yang dilakukan oleh aktor negara maupun non-negara, dapat menargetkan infrastruktur kritis, lembaga pemerintah, dan sektor swasta dari jarak jauh, dengan pelaku yang seringkali sulit diidentifikasi. Sifat serangan ini menimbulkan pertanyaan kompleks tentang pertahanan nasional, atribusi, dan akuntabilitas dalam arena internasional (Zuboff, 2019).

Berbagai studi terbaru menunjukkan bahwa media sosial dan platform digital telah menjadi arena baru untuk manipulasi informasi dan kampanye pengaruh. Fenomena ini berpotensi menggerus kepercayaan publik dan merusak demokrasi negara. Untuk mengatasi kekhawatiran ini, banyak negara tengah merefleksikan ulang makna kedaulatan, termasuk bagaimana cara mendefinisikannya, melindunginya, serta menjaganya di tengah dunia yang semakin terkoneksi secara digital dan penuh tantangan baru.

Konsep "kedaulatan digital" *(digital sovereignity)* mulai berkembang sebagai bentuk respons terhadap tantangan yang dihadirkan oleh era digital (Pohle dan Thiel, 2020). Gagasan ini berupaya memperluas pemahaman konvensional tentang kedaulatan, dengan menekankan pentingnya penguasaan atas data, infrastruktur teknologi, serta keamanan siber. Dalam konteks ini, kedaulatan digital menjadi landasan teoritis yang relevan untuk menjelaskan bagaimana negara-negara berusaha menjaga otonomi dan kendali di tengah transformasi digital yang terus berlangsung.

2.3 Konteks Regional Asia Tenggara

Dalam beberapa tahun terakhir, kawasan Asia Tenggara telah mengalami lonjakan pertumbuhan digital yang sangat pesat. Laporan e-Conomy SEA 2021 mengungkapkan bahwa ekonomi digital di kawasan ini mengalami perkembangan luar biasa, yang semakin dipercepat oleh pandemi COVID-19 melalui peningkatan penggunaan layanan digital di berbagai sektor kehidupan (Google, Temasek, dan Bain, 2021). Meluasnya akses internet dan teknologi digital membuat kawasan ini sedang berada di tengah proses transformasi digital yang mendalam, dan menuntut perhatian serius dari para pembuat kebijakan untuk mengantisipasi dampaknya terhadap kedaulatan negara.



Keberagaman sistem politik di Asia Tenggara menambah dimensi yang menarik untuk analisis. Kawasan ini mencakup spektrum kepemerintahan yang beragam mulai dari demokrasi liberal hingga negara otoriter, yang masing-masing memiliki pendekatan tersendiri dalam mengatur ruang digital dan melindungi kedaulatan. Beberapa negara, seperti Singapura, telah mengadopsi pendekatan proaktif dan komprehensif terhadap tata kelola digital, sementara yang lain masih berada pada tahap awal pengembangan kerangka regulasi. Variasi ini menjadi ruang eksploratif untuk analisis perbandingan tentang bagaimana karakteristik politik memengaruhi respons terhadap isu kedaulatan digital.

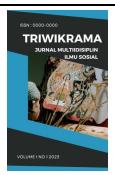
Selain itu, negara-negara ASEAN juga dihadapkan pada tantangan geopolitik yang kompleks, terutama dalam menyikapi persaingan teknologi antara Amerika Serikat dan Tiongkok. Dilema dalam memilih teknologi, membangun infrastruktur digital, dan menjalin kemitraan strategis memiliki dampak besar terhadap kontrol dan kedaulatan nasional masing-masing negara (Tan, 2020).

2.4 Upaya Koordinasi Regional dan Tantangan Implementasi

Dalam beberapa tahun terakhir, ASEAN sebagai badan regional telah menunjukkan kesadaran yang meningkat akan pentingnya koordinasi dalam menghadapi tantangan digital. Inisiatif seperti ASEAN *Data Security Framework* dan Rencana ASEAN *Cybersecurity Cooperation Strategy* menandakan adanya langkah awal menuju pendekatan regional yang lebih terkoordinasi untuk mengatasi tantangan *digital sovereignity*. Meski demikian, implementasi dari inisiatif-inisiatif belum mencapai tingkat pemerataan di seluruh Kawasan. Hal ini mencerminkan adanya disparitas kapasitas dan prioritas di antara negara-negara anggota.

Ketimpangan kapasitas digital yang signifikan di antara negara-negara ASEAN menciptakan hambatan struktural dalam upaya menegakkan kedaulatan digital. Sebagai bukti, Singapura telah memantapkan posisinya sebagai pemimpin regional dalam tata kelola digital berkat kapasitas teknis yang kuat dan kerangka regulasi yang maju. Sebaliknya, negara-negara seperti Myanmar, Laos, dan Kamboja masih menghadapi tantangan mendasar dalam membangun infrastruktur digital serta mengembangkan keahlian teknis yang diperlukan untuk secara efektif menjaga kepentingan digital nasional mereka.

Ketergantungan pada infrastruktur dan teknologi digital asing merupakan kekhawatiran yang meluas di kawasan ini. Banyak negara di Asia Tenggara masih sangat bergantung pada perusahaan teknologi asing, baik dari Barat maupun China, untuk infrastruktur dan layanan digital mereka. Ketergantungan ini menimbulkan pertanyaan tentang otonomi teknologi dan implikasinya terhadap kedaulatan nasional dalam jangka panjang. Burri (2017) mengamati bahwa banyak ekonomi berkembang menghadapi dilema serupa dalam hal regulasi aliran data, keamanan siber, dan tata kelola platform, menjadikan pelajaran dari pengalaman Asia Tenggara relevan secara global dalam memahami tantangan kedaulatan digital di era kontemporer.



3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk memahami transformasi konsep kedaulatan dari dimensi teritorial menuju ranah digital. Penelitian ini bersifat non-empiris dan mengandalkan data sekunder seperti publikasi akademik, dokumen kebijakan, laporan riset, serta informasi yang relevan dari institusi dan organisasi terkait. Data dianalisis menggunakan metode analisis isi tematik, yang bertujuan untuk mengidentifikasi pola-pola gagasan, kecenderungan kebijakan, serta kerangka normatif.

Untuk memperkuat analisis, penelitian ini menggunakan pendekatan studi kasus komparatif terhadap beberapa negara di Asia Tenggara untuk menggambarkan variasi pendekatan dan kapasitas negara-negara dalam menghadapi tantangan kedaulatan digital, baik dari sisi regulasi, keamanan, maupun relasi dengan aktor-aktor global. Studi kasus ini diharapkan dapat memberikan pemahaman kontekstual dan representatif terhadap kompleksitas isu yang dibahas.

4. HASIL DAN PEMBAHASAN

4.1 Transformasi Kedaulatan di Era Digital

4.1.1 Evolusi Konsep Kedaulatan Westphalia

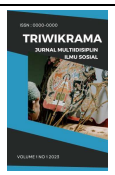
Konsep Konsep kedaulatan Westphalia menghadapi tantangan serius akibat transformasi digital. Kedaulatan negara yang berusia seabad ini memperoleh makna baru dan menjadi perdebatan hangat, akibat disrupsi digital dan teknologi tanpa batas, dominasi oleh perusahaan teknologi global yang kuat, seringkali milik asing, dan pengaruh siber yang merusak oleh negara-negara jahat (Timmers, 2023). Sistem yang dibangun sejak Perjanjian Westphalia 1648 menekankan supremasi teritorial negara, prinsip non-intervensi, dan pengakuan mutual antar negara berdaulat. Prinsip-prinsip ini bekerja dengan baik ketika aktivitas manusia masih terbatas pada ruang fisik yang dapat diidentifikasi secara geografis, namun kini mengalami erosi signifikan dalam era digital.

Revolusi digital mengubah lanskap ini dengan menciptakan ruang baru yang tidak terikat oleh batas geografis tradisional. Internet dan teknologi digital memungkinkan aktivitas ekonomi, sosial, dan politik berlangsung dalam ruang virtual yang dapat diakses dari mana saja di dunia, menciptakan paradoks dalam penerapan konsep kedaulatan berbasis teritorial. Kondisi ini menghasilkan ketegangan antara sistem kedaulatan yang dibangun untuk mengatur aktivitas dalam batas-batas geografis dengan realitas digital yang melampaui batasan fisik tersebut.

4.1.2 Keterbatasan Kedaulatan Berbasis Teritorial Fisik

Kedaulatan tradisional yang berbasis kontrol teritorial fisik menghadapi limitasi ketika mengatur aktivitas digital yang melampaui batas geografis. Kompleksitas ini terlihat jelas dalam skenario sederhana: ketika seseorang di Jakarta mengakses layanan cloud yang servernya berada di Singapura, perusahaan penyedia layanannya berkantor pusat di Amerika Serikat, dan data backup disimpan di Eropa, maka jurisdiksi mana yang berlaku? Pertanyaan ini menjadi semakin rumit karena data dapat berpindah melintasi berbagai yurisdiksi dalam hitungan detik, server dapat berlokasi di negara yang berbeda dari penggunanya, dan layanan digital dapat diakses tanpa mempertimbangkan batas teritorial. Kondisi ini menciptakan kesenjangan mendasar antara konsep kedaulatan tradisional dengan realitas digital kontemporer.

Triwikrama: Jurnal Ilmu Sosial
Volume 9 No. 9 Tahun 2025
E-ISSN: 2988-1986
Open Access:



Karakteristik teknologi digital yang memungkinkan duplikasi dan distribusi informasi secara instan menantang konsep kepemilikan dan kontrol yang menjadi basis kedaulatan teritorial. Sebuah file digital dapat disalin dan disebarkan ke ribuan lokasi dalam waktu bersamaan, membuatnya hampir mustahil untuk mengontrol distribusinya menggunakan pendekatan teritorial tradisional. Lebih lanjut, sifat intangible dari aset digital membuat konsep kepemilikan menjadi lebih kompleks dibandingkan dengan aset fisik yang memiliki lokasi dan keberadaan yang jelas.

4.1.3 Munculnya Domain Siber sebagai Ruang Baru Kedaulatan

Domain siber telah berkembang menjadi ruang baru yang memerlukan konseptualisasi kedaulatan yang berbeda dari pendekatan teritorial tradisional. Produksi data digital telah mengalami percepatan luar biasa dalam beberapa dekade terakhir, dengan semakin banyak proses yang didatifikasi (Glasze et al., 2022). Berbeda dengan ruang fisik yang memiliki batas jelas, ruang siber bersifat virtual, dinamis, dan dapat diakses secara bersamaan oleh multiple aktor dari berbagai lokasi geografis. Dalam ruang fisik, jika suatu wilayah dikuasai oleh satu negara, maka negara lain tidak dapat mengklaim kedaulatan atas wilayah yang sama. Namun dalam ruang siber, multiple aktor dapat beroperasi dalam ruang virtual yang sama secara bersamaan tanpa saling mengganggu secara langsung.

Domain siber memiliki karakteristik paradoksal: bergantung pada infrastruktur fisik namun tidak terikat pada lokasi geografis infrastruktur tersebut. Server yang secara fisik berada di Singapura dapat melayani pengguna di seluruh Asia Tenggara atau bahkan dunia. Data yang tersimpan di server tersebut dapat diakses dari mana saja, menciptakan kompleksitas dalam menentukan yurisdiksi yang berlaku. Hal ini menghasilkan situasi dimana aktivitas dalam ruang siber dapat memiliki dampak langsung terhadap kedaulatan negara meski dilakukan dari luar wilayah teritorialnya. Serangan siber yang diluncurkan dari luar negeri dapat melumpuhkan infrastruktur kritis suatu negara, sementara kampanye disinformasi dapat mempengaruhi proses demokratis tanpa ada pelaku yang secara fisik memasuki wilayah target.

4.1.4 Tantangan Yurisdiksi Lintas Batas dalam Ruang Digital

Tantangan yurisdiksi dalam ruang digital menjadi salah satu isu paling kompleks dalam transformasi kedaulatan kontemporer. Kedaulatan digital adalah konsep populer namun masih berkembang, yang diklaim oleh dan berkaitan dengan berbagai aktor global, dengan naratif yang sering bersaing dan saling tidak konsisten (Fratini et al., 2024). Kompleksitas ini bermula dari kasus sederhana seperti ketika warga negara suatu negara mengakses layanan digital dari perusahaan asing, namun berkembang menjadi dilema hukum yang rumit: hukum mana yang berlaku - hukum negara tempat tinggal pengguna, hukum negara tempat perusahaan beroperasi, atau hukum negara tempat data disimpan?

Kompleksitas bertambah secara eksponensial ketika melibatkan transaksi komersial lintas batas. E-commerce modern memungkinkan konsumen di satu negara membeli produk dari penjual di negara lain melalui platform yang beroperasi di negara ketiga, dengan pembayaran diproses oleh perusahaan fintech di negara keempat. Setiap tahap transaksi dapat tunduk pada hukum yang berbeda, menciptakan ketidakpastian hukum yang signifikan. Situasi menjadi lebih serius ketika menyangkut aktivitas ilegal seperti kejahatan siber, penipuan online, pencurian identitas, atau penyebaran malware yang seringkali melibatkan pelaku yang beroperasi dari satu negara, menyerang target di negara lain, menggunakan infrastruktur di negara ketiga. Mengidentifikasi pelaku, mengumpulkan bukti, dan menerapkan sanksi hukum menjadi sangat sulit dalam kondisi yang melibatkan multiple

yurisdiksi dengan sistem hukum dan tingkat kerjasama internasional yang berbeda-beda.

4.1.5 Redefinisi Kedaulatan dalam Konteks Digital

Transformasi digital telah mendorong redefinisi konsep kedaulatan menjadi tiga dimensi utama yang saling berkaitan: kedaulatan data, kedaulatan teknologi, dan kedaulatan informasi. Ketiga dimensi ini membentuk kerangka kerja baru untuk memahami kedaulatan dalam era digital, masing-masing dengan tantangan dan peluang yang unik.

a. Kedaulatan Data (Data Sovereignty)

Kedaulatan data mengacu pada pengelolaan dan tata kelola informasi sesuai dengan hukum dan protokol negara-bangsa di mana informasi tersebut berada (Reyes-García et al., 2022) Konsep ini menekankan bahwa negara memiliki hak dan tanggung jawab untuk mengatur data yang dihasilkan di wilayahnya atau oleh warga negaranya. Data telah menjadi aset strategis untuk kesejahteraan masyarakat dan daya saing ekonomi. Dalam era ekonomi digital, data bukan hanya byproduct dari aktivitas digital, tetapi menjadi input utama untuk inovasi, pengambilan keputusan, dan penciptaan nilai ekonomi. Warga negara dan organisasi menginginkan penentuan nasib sendiri atas penggunaan data mereka (von Scherenberg et al., 2024).

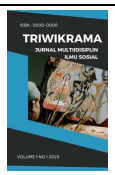
Kedaulatan data mencakup empat aspek penting:

- **Kontrol lokasi penyimpanan data** memberikan negara kemampuan untuk memastikan bahwa data warga negaranya disimpan di wilayah yang tunduk pada hukum nasional. Ini penting untuk perlindungan privasi, keamanan nasional, dan penegakan hukum.
- **Regulasi akses data** memungkinkan negara menetapkan siapa yang dapat mengakses data warga negaranya dan dalam kondisi apa. Hal ini mencakup pembatasan akses untuk perusahaan asing, persyaratan transparansi untuk algoritma yang memproses data pribadi, dan mekanisme consent yang memungkinkan individu mengontrol penggunaan data mereka.
- **Perlindungan privasi** memastikan bahwa data pribadi warga negara dilindungi sesuai dengan standar dan nilai-nilai nasional. Berbagai negara memiliki konsep privasi yang berbeda, yang tercermin dalam undang-undang perlindungan data mereka.
- **Pengaturan transfer data lintas batas** menjadi aspek krusial dalam kedaulatan data. Dalam ekonomi global yang terintegrasi, data seringkali perlu dipindahkan antar negara untuk berbagai keperluan bisnis dan operasional, namun transfer ini harus dilakukan tanpa mengorbankan kedaulatan data negara asal.

b. Kedaulatan Teknologi (Technological Sovereignty)

Kedaulatan teknologi mengacu pada tingkat kemerdekaan nyata yang dicapai dalam bidang sains, teknologi, dan teknik, yang memastikan implementasi kepentingan nasional yang tidak terhambat dalam teknosphere, dengan mempertimbangkan ancaman yang ada dan masa depan (Economic and Political Weekly, 2024). Konsep ini muncul sebagai respons terhadap ketergantungan teknologi yang semakin besar dari banyak negara terhadap beberapa kekuatan teknologi global. Aspirasi terhadap kedaulatan teknologi semakin merasuki perdebatan politik, namun definisi yang ambigu meninggalkan tujuan yang tepat masih menjadi bahan perdebatan akademis (March & Schieferdecker, 2023)).

Kedaulatan teknologi bukan berarti autarki teknologi atau isolasi dari rantai pasokan global. Sebaliknya, ini tentang memiliki kemampuan untuk membuat pilihan teknologi yang independen dan mengurangi risiko ketergantungan yang berlebihan pada satu atau beberāpa supplier. Tiga aspek utama kedaulatan teknologi:



- **Kemandirian infrastruktur digital** melibatkan kemampuan untuk membangun, memelihara, dan mengamankan infrastruktur teknologi informasi dan komunikasi yang kritikal. Infrastruktur ini mencakup jaringan telekomunikasi, pusat data, sistem pembayaran digital, dan platform e-government.
- **Kontrol atas teknologi kritis** yang vital bagi keamanan nasional dan ekonomi. Teknologi seperti artificial intelligence, quantum computing, cybersecurity, dan biotechnology dapat memiliki implikasi strategis yang besar.
- **Pengembangan kapasitas domestik** melalui investasi dalam penelitian, pengembangan, dan inovasi teknologi lokal. Ini melibatkan pembangunan ekosistem inovasi yang mencakup universitas, institusi penelitian, startup teknologi, dan perusahaan teknologi domestik.

c. Kedaulatan Informasi (Information Sovereignty)

Kedaulatan informasi mengacu pada kemampuan negara untuk mengontrol aliran informasi dalam wilayahnya dan melindungi warga negaranya dari informasi yang berpotensi merugikan. Dimensi ini menjadi semakin penting dalam era post-truth dan proliferasi disinformasi yang dapat mempengaruhi stabilitas politik dan sosial. Platform media sosial memungkinkan siapa saja untuk menjadi broadcaster, menciptakan ekosistem informasi yang sangat terdecentralisasi namun juga rentan terhadap manipulasi dan penyalahgunaan.

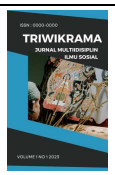
Empat aspek kedaulatan informasi:

- **Kontrol konten digital** melibatkan kemampuan untuk mengatur konten yang dapat diakses oleh warga negara melalui berbagai platform digital, namun harus seimbang dengan prinsip kebebasan berekspresi dan akses informasi.
- **Penanggulangan disinformasi** merupakan tantangan yang sangat kompleks. Disinformasi dapat berupa berita palsu, manipulasi foto atau video (deepfakes), atau kampanye propaganda yang terorganisir dengan dampak yang dapat sangat serius.
- **Perlindungan diskursus publik** penting dalam demokrasi, dimana kualitas debat publik sangat mempengaruhi kualitas keputusan kolektif yang diambil masyarakat. Manipulasi diskursus publik melalui bot, akun palsu, atau kampanye pengaruh terorganisir dapat merusak proses demokratis.
- **Keamanan informasi** mencakup perlindungan informasi sensitif negara dari akses yang tidak sah. Ini melibatkan tidak hanya informasi klasifikasi pemerintah, tetapi juga informasi ekonomi dan teknologi yang strategis.

Ketiga dimensi kedaulatan digital ini saling berkaitan serta membentuk ekosistem yang tidak dapat dipisahkan. Kontrol atas data memerlukan kemandirian teknologi, sementara kedaulatan informasi bergantung pada penguasaan data. Transisi dari kedaulatan teritorial ke digital menuntut kebijakan yang holistik dan adaptif. Negara perlu menyusun regulasi yang mencakup ketiga aspek tersebut tanpa mengorbankan keterbukaan yang penting bagi ekonomi digital global.

Di Asia Tenggara, perbedaan kapasitas digital antar negara menciptakan ketergantungan timbal balik. Negara dengan kapasitas digital lebih maju dapat menjadi pusat regional, sedangkan negara dengan kapasitas terbatas menjadi lebih rentan terhadap dominasi eksternal. Solusi terbaik terletak pada peningkatan kapasitas dalam negeri, diversifikasi mitra teknologi, dan penguatan kerja sama regional guna membangun ekosistem digital yang tangguh dan berdaulat.

Triwikrama: Jurnal Ilmu Sosial
Volume 9 No. 9 Tahun 2025
E-ISSN: 2988-1986
Open Access:



4.2 Ancaman terhadap Digital Sovereignity

Kedaulatan digital dihadapkan pada beragam ancaman yang bersifat kompleks dan melibatkan berbagai aktor dari bermacam dimensi. Ancaman tersebut tidak hanya terbatas pada isu teknis, tetapi juga mencakup ranah ekonomi, politik, dan sosial yang berkesinambungan dan berdampak besar. Di kawasan Asia Tenggara, urgensi isu ini semakin meningkat seiring dengan percepatan transformasi digital, sementara kerentanan dalam berbagai sektor masih menjadi tantangan yang tidak terhindari.

4.2.1 Ancaman dari Aktor Non-Negara

Kekuatan finansial serta jangkauan platform-platform digital menciptakan ketimpangan struktural dalam hubungan antara Perusahaan Teknologi Besar Global (*Big Tech*) dan negara. Sebagai gambaran, nilai kapitalisasi pasar Google melampaui gabungan Produk Domestik Bruto dari beberapa negara di kawasan ini. Sementara itu, Meta secara efektif memonopoli ruang komunikasi digital melalui WhatsApp, Facebook, dan Instagram sebagai platform yang digunakan oleh ratusan juta penduduk Asia Tenggara setiap harinya. Amazon Web Services, di sisi lain, menyediakan layanan komputasi awan yang menjadi fondasi operasional tidak hanya bagi sektor swasta, tetapi juga bagi institusi pemerintahan di sejumlah negara.

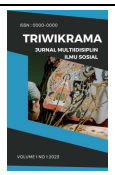
Dominasi *Big Tech* ini menciptakan dilema tersendiri bagi negara-negara di Kawasan Asia Tenggara. Di satu sisi, layanan dan teknologi yang mereka tawarkan berpeluang besar dalam mendorong pertumbuhan ekonomi digital, mempermudah inovasi, dan memperluas akses informasi. Namun di sisi lain, ketergantungan yang tinggi pada platform-platform *Big Tech* menimbulkan kerentanan strategis yang bisa saja dimanfaatkan oleh aktor non-negara untuk kepentingan yang tidak selalu selaras dengan agenda nasional.

Beberapa pemerintah negara Kawasan Asia Tenggara menunjukkan langkah pembatasan akses ke platform media sosial dalam situasi tertentu. Hal ini menunjukkan betapa kompleksnya interdependensi yang terjadi. Upaya negara untuk menegakkan kedaulatannya, seperti dengan menuntut transparansi algoritma atau akses terhadap data pengguna, sering kali berhadapan dengan perlawanan dari *Big Tech*, yang berdalih membela standar global dan perlindungan hak asasi manusia. Ketegangan ini mencerminkan situasi tarik-menarik yang terus berlangsung antara kedaulatan nasional dan tata kelola digital global.

Di Asia Tenggara, algoritma yang diterapkan oleh platform media sosial dan *Search Engine* telah menjadi kekuatan yang tidak terlihat namun sangat berpengaruh dalam membentuk percakapan publik dan arah opini politik. Melalui algoritma inilah ditentukan informasi apa yang muncul di hadapan pengguna, berita mana yang diperlihatkan lebih dulu, dan konten politik mana yang diperkuat atau justru disisihkan. Sering kali, algoritma ini dirancang dengan mempertimbangkan data dan logika yang berasal dari konteks budaya yang berbeda, sehingga kurang mencerminkan nilai-nilai serta kepentingan lokal masyarakat Asia Tenggara.

Dalam kerangka *Surveillance Capitalism,* pengalaman digital individu seperti preferensi pribadi hingga interaksi sosial berubah menjadi komoditas yang dieksploitasi untuk tujuan komersial maupun politik, yang belum tentu selaras dengan kepentingan nasional (Zuboff, 2019). Situasi ini menjadi semakin kompleks karena mayoritas warga Asia Tenggara mengakses informasi dan berita politik melalui platform digital yang dimiliki dan dioperasikan oleh perusahaan asing. Sistem seperti algoritma umpan di Facebook dan Instagram, fitur rekomendasi di YouTube, serta hasil pencarian Google secara bersama-sama menciptakan ekosistem informasi yang sangat menentukan cara publik memahami dan merespons isu-isu sosial serta politik.

Triwikrama: Jurnal Ilmu Sosial
Volume 9 No. 9 Tahun 2025
E-ISSN: 2988-1986
Open Access:



Penelitian menunjukkan bahwa algoritma secara konsisten memprioritaskan konten yang mendorong keterlibatan tinggi, yang sering kali berupa materi provokatif, emosional, atau bersifat memecah belah. Akibatnya, ruang digital kerap memperbesar polarisasi sosial dan politik bahkan dapat memicu ekstremisme. Di sejumlah negara Asia Tenggara, media sosial telah dikaitkan dengan meningkatnya insiden kekerasan komunal, penyebaran ujaran kebencian, dan ketidakstabilan politik yang signifikan.

Platform digital kini menjadi arena baru bagi operasi pengaruh dan manipulasi informasi yang mengancam kedaulatan informasi di negara-negara Asia Tenggara. Perusahaan teknologi besar telah menjelma menjadi penguasa data yang tak terhindarkan bagi pemerintah di era data saat ini (Gu, 2023). Dalam situasi ini, platform asing memiliki kekuatan besar dalam membentuk narasi publik dan memengaruhi dinamika politik demokratis di kawasan.

Lebih dari sekadar penyedia layanan teknologi, platform-platform ini turut membawa sistem nilai yang seringkali tidak sejalan dengan konteks budaya dan politik lokal. Aktor domestik maupun asing memanfaatkan ruang digital ini untuk menyebarkan disinformasi, memengaruhi opini publik, hingga mencampuri proses politik. Rentetan kasus manipulasi pemilu lewat media sosial di berbagai negara Asia Tenggara menjadi bukti nyata kerentanan demokrasi terhadap eksploitasi digital.

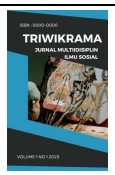
Fenomena "Digital Colonialism" menunjukkan bagaimana dominasi platform asing tidak sekadar mengekstrak nilai ekonomi dari data pengguna di Asia Tenggara, tetapi juga merekayasa cara kita mengonsumsi konten, membentuk preferensi politik, dan bahkan menata ulang identitas sosial melalui algoritma yang dirancang untuk melayani kepentingan bisnis dan geopolitik negara asal platform tersebut..

4.2.2 Ancaman *Cybersecurity*

Ancaman terhadap keamanan digital di Asia Tenggara semakin kompleks, mencakup serangan siber terhadap infrastruktur kritis hingga manipulasi informasi publik. Sepanjang tahun 2023, tercatat lebih dari 420 juta serangan terhadap infrastruktur kritis secara global, yang berarti sekitar 13 serangan setiap detik. Angka ini menunjukkan peningkatan sebesar 30 persen dibandingkan tahun sebelumnya (Security Today, 2024). Serangan semacam ini menyasar sistem vital seperti kelistrikan, telekomunikasi, perbankan, transportasi, dan layanan kesehatan. Karena semakin tingginya keterhubungan antar sistem, serangan terhadap satu sektor berisiko memicu efek domino terhadap sektor lainnya, sehingga mengancam stabilitas ekonomi, sosial, dan keamanan nasional secara menyeluruh.

Dalam konteks geopolitik, ketergantungan pada teknologi asing turut memperbesar risiko keamanan nasional. Dominasi teknologi dapat bertransformasi menjadi kekuatan militer melalui pemanfaatan perangkat canggih, menjadikan ketergantungan tersebut sebagai kerentanan strategis. Dari perspektif ekonomi dan keamanan, prevalensi teknologi asing yang kritis dapat membuka celah terhadap eksploitasi siber yang mengancam kepentingan nasional (ISEAS, 2021).

Konsep perang siber juga telah berkembang menjadi dimensi baru dalam strategi pertahanan. Serangan digital kini digunakan untuk melumpuhkan infrastruktur atau menciptakan kekacauan sosial tanpa perlu keterlibatan militer secara fisik. Serangan ini dapat dilakukan dari jarak jauh dengan biaya rendah, sulit dilacak, dan dapat menimbulkan dampak destruktif yang luas. Oleh karena itu, negara-negara perlu mengembangkan kemampuan pertahanan dan serangan di ranah siber, termasuk pembentukan komando siber, pelatihan sumber daya manusia, dan integrasi aspek siber dalam kebijakan pertahanan nasional.



a. Tantangan Atribusi, Akuntabilitas, dan Manipulasi Informasi

Salah satu hambatan utama dalam keamanan siber adalah kesulitan dalam melakukan atribusi terhadap pelaku serangan. Ruang siber memungkinkan anonimitas dan penyamaran jejak digital, membuat proses pelacakan menjadi sangat kompleks. Pelaku dapat memanfaatkan server proksi, jaringan pribadi virtual, atau teknik penyamaran lain untuk menyembunyikan identitas dan lokasi mereka. Kompleksitas ini menciptakan tantangan hukum dan diplomatik, karena negara korban sering kesulitan membuktikan siapa pelakunya dan dari mana serangan berasal. Hal ini menghambat upaya pertanggungjawaban, penerapan sanksi, atau respons yang proporsional terhadap serangan.

Dalam konteks hukum internasional, prinsip-prinsip seperti kedaulatan dan non-agresi sulit diterapkan di dunia maya. Serangan siber dapat dilakukan oleh aktor negara, kelompok kriminal yang disponsori negara, organisasi teroris, atau individu dengan berbagai motif dan metode. Ketidakjelasan dalam membedakan antara serangan negara dan tindakan kriminal memperumit pengambilan langkah responsif yang tepat.

Selain ancaman teknis, Asia Tenggara juga menghadapi tantangan serius dalam bentuk disinformasi dan manipulasi opini publik. Media sosial telah menjadi medan utama bagi kampanye pengaruh yang dilakukan oleh aktor domestik maupun asing. Platform digital dimanfaatkan untuk menciptakan dan memperkuat narasi tertentu melalui konten terarah, jaringan bot, akun palsu, dan iklan yang ditargetkan secara mikro. Fenomena *astroturfing* atau gerakan buatan yang tampak organik juga digunakan untuk mempengaruhi persepsi publik dan proses politik.

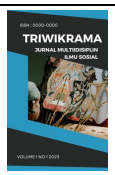
Manipulasi ini menciptakan ancaman terhadap integritas demokrasi, termasuk penyebaran informasi menyesatkan seputar pemilu, polarisasi sosial melalui ruang gema dan gelembung informasi, serta erosi kepercayaan terhadap institusi demokratis melalui teori konspirasi dan narasi palsu. Campur tangan asing dalam bentuk kampanye disinformasi juga memperparah kerentanan demokrasi di kawasan.

b. Surveillance Capitalism* dan Era *Post-Truth

Surveillance Capitalism semakin menggerus kedaulatan informasi. Di Asia Tenggara, data warga dijual sebagai komoditas pasar global tanpa izin yang benar atau imbalan yang adil. Akibatnya, negara kehilangan kendali atas data warganya. Data tersebut dimanfaatkan untuk membangun profil psikologis yang digunakan dalam manipulasi politik, dan keuntungan ekonominya mengalir ke perusahaan multinasional, bukan kembali ke negara asal.

Tantangan yang semakin kompleks pun muncul di era pascakebenaran *(post-truth)*, di mana emosi dan keyakinan pribadi lebih memengaruhi opini publik dibandingkan fakta objektif, sehingga batas antara yang benar dan yang salah menjadi kabur. Arus informasi yang massif, teknologi rekayasa seperti *deepfake*, serta polarisasi politik yang meningkat, berdampak pada proses verifikasi yang semakin sulit. Tidak hanya itu, kepercayaan pada media utama dan otoritas ahli semakin memperlemah daya tahan masyarakat terhadap informasi yang salah *(misinformation*), yang pada akhirnya membahayakan demokrasi dan kohesi sosial.

Dengan demikian, ancaman siber dan informasi tidak hanya sekadar soal teknologi, tetapi juga tantangan strategis yang mengancam keamanan nasional, stabilitas politik, dan kedaulatan digital negara-negara di Asia Tenggara.



4.3 *Governance Data* dan Tantangan Regulasi

4.3.1 Ketimpangan Regulasi dan Standar Perlindungan Data antar Negara ASEAN

Ketimpangan dalam pembangunan regulasi data di antara negara-negara ASEAN mencerminkan secara gamblang perbedaan kapabilitas yang masih membentang di kawasan ini. Singapura, misalnya, telah lama menerapkan *Personal Data Protection Act* (PDPA) yang menyeluruh dan responsif terhadap perkembangan zaman. Sebaliknya, Indonesia baru saja mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, setelah melalui proses panjang yang berlarut-larut. Di sisi lain, negara-negara CLMV (Cambodia, Laos, Myanmar, dan Vietnam) bahkan masih berada pada tahap awal pengembangan digital. Akibatnya, terdapat kesenjangan dalam kesiapan infrastruktur dan kebijakan yang menghambat penyelarasan kebijakan digital di tingkat ASEAN.

Kesenjangan tersebut juga menciptakan ketidakseimbangan dalam pengaruh pembuatan kebijakan regional. Negara dengan kapasitas lebih baik cenderung menjadi pengatur arah, sementara negara dengan kapasitas lebih rendah menjadi pengikut pasif, yang dalam jangka panjang dapat melemahkan rasa kepemilikan bersama atas proyek integrasi digital ASEAN.

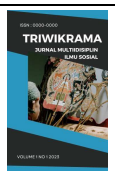
Ketiadaan standar yang seragam antarnegara turut menimbulkan tantangan besar dalam membangun kerja sama yang efektif, baik dalam penegakan hukum maupun dalam penyusunan perjanjian digital lintas batas. Dalam konteks ini, pakar tata kelola data Paul de Hert pernah menyampaikan pandangan yang menggugah: "tanpa kejelasan yurisdiksi dan konsistensi kebijakan, data menjadi warga negara tanpa negara—bergerak bebas tapi tanpa perlindungan yang pasti" (de Hert & Papakonstantinou, 2012).

4.3.2 Ketergantungan pada Infrastruktur Teknologi Asing dan Dilema Kedaulatan

Tantangan yang tampak samar namun memiliki implikasi strategis yang mendalam adalah kenyataan bahwa banyak negara di Asia Tenggara masih sangat bergantung pada infrastruktur teknologi milik pihak asing. Ketergantungan ini terlihat mulai dari penggunaan layanan cloud, sistem perangkat lunak administratif, hingga penyimpanan data kritikal, yang pada umumnya dikendalikan oleh raksasa teknologi global seperti Amazon Web Services, Microsoft, Google, Alibaba, dan Huawei. ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC, 2023) mengungkap bahwa lebih dari 70 persen penyimpanan data digital sektor publik di kawasan ini masih diserahkan kepada entitas asing.

Situasi ini menimbulkan masalah serius dalam konteks yurisdiksi. Ketika data warga negara tersimpan di luar negeri atau berada dalam kendali entitas asing, maka kemampuan negara untuk melindungi dan mengatur data tersebut menjadi terbatas. Instrumen hukum nasional tidak selalu mampu menjangkau perusahaan yang tunduk pada sistem hukum yang berbeda. Di titik inilah dilema kedaulatan digital menemukan bentuk paling nyata, sebuah kondisi di mana negara memiliki kedaulatan penuh secara geografis, namun tidak dalam penguasaan atas data warganya.

Indonesia memberikan contoh nyata atas persoalan ini. Pada tahun 2021, proyek pembangunan pusat data nasional yang melibatkan aktor luar negeri memicu kritik tajam dari berbagai pihak karena dikhawatirkan berisiko terhadap kebocoran data strategis negara. Menyikapi hal tersebut, pemerintah merespons dengan kebijakan yang mewajibkan agar data milik pemerintah disimpan di dalam negeri. Meski ini merupakan langkah afirmatif menuju kemandirian digital, pelaksanaannya di lapangan masih menghadapi banyak tantangan.



Sebagaimana diingatkan oleh Evgeny Morozov, "ketika infrastruktur digital Anda dibangun oleh pihak luar, maka keputusan strategis tentang siapa yang bisa mengakses data, kapan, dan untuk tujuan apa, pada dasarnya telah Anda delegasikan" (Morozov, 2014). Pernyataan ini mempertegas bagaimana ketergantungan pada infrastruktur asing tidak hanya berdampak teknis, tetapi juga menyentuh jantung kedaulatan sebuah negara di era digital.

4.3.3 Hambatan Penegakan dan Transfer Data Lintas Batas

Penegakan hukum di ranah digital merupakan tantangan struktural yang tidak bisa disederhanakan. Dalam praktiknya, pelaku kejahatan siber bisa saja berada di satu negara, memanfaatkan server di negara lain, dan menyerang korban di negara ketiga. Dalam situasi seperti ini, pendekatan penegakan hukum yang berpijak pada batas-batas teritorial negara menjadi tidak lagi relevan. Ketika bukti digital tersebar lintas yurisdiksi dan tiap negara memiliki sistem hukum serta standar yang berbeda, maka koordinasi internasional menjadi sangat krusial. Namun ironisnya, justru pada titik inilah letak salah satu kelemahan utama upaya penegakan hukum global.

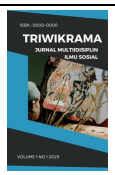
Di kawasan Asia Tenggara, mekanisme konkret untuk penegakan hukum digital antarnegara masih belum terbentuk secara efektif. Meski ASEAN telah memperkenalkan *Model Contractual Clauses* dan *Data Transfer Mechanism*, upaya tersebut sejauh ini masih bersifat normatif dan belum menyentuh tahap implementasi yang substansial. Tanpa adanya penguatan kelembagaan yang nyata serta harmonisasi kerangka hukum di tingkat regional, maka hak-hak digital masyarakat Asia Tenggara akan terus berada dalam posisi yang rentan, dan menggantung di antara kekosongan aturan hukum internasional.

4.4 ASEAN dan *Digital Sovereignity* Regional

4.4.1 Inisiatif Regional ASEAN: Capaian dan Keterbatasan

ASEAN telah meluncurkan sejumlah kebijakan penting sebagai bagian dari upaya membangun fondasi kedaulatan digital yang kolektif. Di antaranya adalah *ASEAN Digital Masterplan 2025, ASEAN Cybersecurity Cooperation Strategy, dan ASEAN Data Management Framework*. Ketiga dokumen ini merepresentasikan kesadaran yang tumbuh di tingkat regional mengenai urgensi tata kelola digital yang terkoordinasi dan terarah. Meskipun demikian, sebagian besar inisiatif tersebut masih disusun dalam bentuk yang tidak mengikat secara hukum. Pendekatan yang digunakan lebih menekankan pada kerangka kerja sukarela atau soft law, sehingga efektivitas implementasinya sangat bergantung pada komitmen masing-masing negara anggota, bukan pada mekanisme penegakan yang jelas dan tegas.

Keterbatasan struktural dalam desain kelembagaan ASEAN turut menjadi penghambat efektivitas berbagai inisiatif digital tersebut. Sebagai organisasi yang mengedepankan prinsip musyawarah dan non-intervensi, ASEAN tidak memiliki otoritas supranasional yang memungkinkan penegakan langsung terhadap kesepakatan digital kolektif. Tidak adanya mekanisme pemantauan, penilaian kinerja, atau sanksi atas ketidakpatuhan membuat implementasi kebijakan digital sangat bergantung pada inisiatif dan kapasitas masing-masing negara anggota. Selain itu, pendekatan berbasis konsensus yang menjadi ciri khas ASEAN sering memperlambat proses pengambilan keputusan, terutama ketika menyangkut isu-isu sensitif seperti pengelolaan data lintas negara, perlindungan privasi, atau keamanan informasi. Hal ini mengurangi daya dorong dari kebijakan regional yang telah dirumuskan dan memperlemah posisi ASEAN dalam menghadapi tekanan dari kekuatan teknologi global.



4.4.2 Fragmentasi Kepentingan dan Kapasitas Digital di Antara Negara ASEAN

Selain tantangan kapasitas yang tidak merata, ASEAN juga dihadapkan pada fragmentasi kepentingan politik serta perbedaan mendasar dalam prinsip tata kelola informasi. Perbedaan ini tampak jelas dalam beragamnya pendekatan negara-negara anggota terhadap isu-isu seperti moderasi konten, penyebaran disinformasi, pengawasan digital, dan kebebasan berekspresi. Di beberapa negara dengan sistem politik yang lebih otoriter, regulasi digital kerap dijadikan alat untuk memperkuat kendali atas ruang publik dan membatasi kritik terhadap pemerintah. Sebaliknya, negara-negara dengan sistem demokratis cenderung menempatkan perlindungan hak-hak digital sebagai prioritas utama.

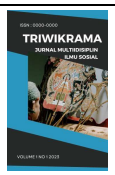
Ketimpangan orientasi ini menyulitkan ASEAN dalam membangun kesepakatan yang kuat untuk merumuskan kebijakan digital bersama. Prinsip non-intervensi yang menjadi salah satu fondasi kerja sama regional turut memperumit upaya harmonisasi regulasi lintas negara. Setiap langkah menuju pembentukan standar perlindungan data bersama atau sistem keamanan siber yang terintegrasi kerap terbentur pada sensitivitas politik dan keengganan negara anggota untuk menyerahkan sebagian kewenangan nasionalnya ke tingkat regional. Akibatnya, meskipun kesadaran akan pentingnya kerja sama ada, jalan menuju integrasi digital yang solid masih penuh dengan tantangan struktural dan politis.

4.4.3 Prospek "*Collective Digital Sovereignty*" ASEAN di Tengah Kompetisi Global

Konsep *Collective Digital Sovereignty* menawarkan pendekatan yang relevan dan strategis bagi negara-negara ASEAN untuk memperkuat posisi negosiasi mereka di tengah tekanan dari kekuatan teknologi global. Pendekatan ini bukan bertujuan menghapus kedaulatan nasional, melainkan membangun mekanisme bersama yang memungkinkan pengelolaan data, teknologi, dan informasi lintas batas secara lebih adil dan terkoordinasi. Dalam kerangka ini, ASEAN dapat mengembangkan bentuk kerja sama yang lentur namun fungsional, dengan fokus pada keterpaduan regulasi, pertukaran informasi terkait ancaman siber, serta fasilitasi transfer data antarnegara yang aman dan saling menguntungkan.

Meski demikian, realisasi gagasan ini memerlukan prasyarat kelembagaan yang kuat. Diperlukan peningkatan kapasitas teknis di negara-negara anggota, pembentukan sistem pemantauan dan evaluasi terhadap pelaksanaan kebijakan digital tingkat regional, serta penyediaan ruang konsultasi teknis yang inklusif dan berkelanjutan. Tanpa penguatan aspek-aspek tersebut, ide mengenai kedaulatan digital kolektif akan tetap berada pada tataran normatif dan belum mampu menjawab tantangan nyata di lapangan.

Dalam konteks dunia yang semakin kompetitif dan didominasi oleh aktor-aktor teknologi besar, kerja sama digital yang erat antarnegara ASEAN bukan sekadar opsi tambahan, melainkan kebutuhan strategis. Jika ASEAN mampu mengatasi hambatan internal dan memperkuat solidaritas kawasan, maka peran geopolitik digitalnya akan menjadi semakin signifikan. Dengan demikian, kedaulatan digital tidak hanya perlu dipahami sebagai isu nasional masing-masing negara, tetapi sebagai agenda bersama yang menentukan masa depan kawasan di era digital.



5. SIMPULAN DAN SARAN

Transformasi era digital telah mengubah secara fundamental konsep kedaulatan yang selama ini kita kenal, di mana batas-batas geografis tidak lagi menjadi penghalang utama bagi aliran informasi dan data. Dalam konteks ini, kedaulatan digital muncul sebagai kebutuhan mendesak yang menekankan pentingnya penguasaan atas data, infrastruktur teknologi, serta keamanan siber. Kawasan Asia Tenggara menghadapi tantangan unik yang cukup kompleks, terutama karena disparitas kapasitas teknologi dan regulasi di antara negara-negara anggotanya. Ketergantungan tinggi pada perusahaan teknologi asing menimbulkan kerentanan strategis yang bisa dimanfaatkan oleh aktor non-negara, sehingga perlindungan dan penguatan kedaulatan digital menjadi suatu keharusan. Selain itu, ancaman keamanan siber semakin nyata dengan meningkatnya serangan terhadap infrastruktur kritis serta manipulasi informasi yang dapat mengganggu stabilitas politik dan sosial kawasan. Meskipun ASEAN telah meluncurkan beberapa inisiatif untuk menjawab tantangan ini, implementasinya masih menghadapi hambatan akibat perbedaan kepentingan politik dan kapasitas teknis antarnegara.

Untuk menghadapi tantangan tersebut, diperlukan upaya nyata dalam meningkatkan kapasitas digital setiap negara di kawasan, termasuk investasi yang serius dalam pengembangan teknologi lokal agar ketergantungan terhadap teknologi asing bisa diminimalisir. Selain itu, penting untuk mendorong harmonisasi regulasi terkait perlindungan data dan keamanan siber di tingkat regional agar tercipta standar yang seragam dan efektif. ASEAN harus berperan aktif sebagai fasilitator dalam dialog dan kerja sama sehingga setiap negara dapat menemukan titik temu yang saling menguntungkan. Masyarakat juga perlu diberikan edukasi yang memadai tentang pentingnya kedaulatan digital dan risiko yang mungkin muncul, sehingga dapat membangun kesadaran kolektif dan ketahanan sosial. Di sisi lain, menjalin kemitraan strategis dengan negara dan lembaga internasional yang memiliki keahlian dan pengalaman di bidang ini juga sangat diperlukan agar ASEAN dapat memperkuat posisi tawarnya dalam percaturan global di era digital. Dengan pendekatan yang holistik dan kolaboratif, kedaulatan digital bukan hanya menjadi isu nasional, melainkan agenda bersama yang mampu menjamin masa depan kawasan Asia Tenggara dalam menghadapi dinamika dunia digital yang terus berkembang.

6. DAFTAR PUSTAKA

Burri, M. (2017). The regulation of data flows through trade agreements. *Georgetown Journal of International Law*, 48, 407-448.

Google, Temasek, & Bain. (2021). *e-Conomy SEA 2021: Roaring 20s - The SEA Digital Decade*. Google.

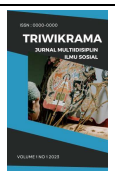
Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton: Princeton University Press.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Osiander, A. (2001). Sovereignty, international relations, and the Westphalian myth. *International Organization*, 55(2), 251-287.

Pohle, J., & Thiel, T. (2020). Digital Sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Tan, S. S. (2020). Consigned to hedge: South-east Asia and America's 'free and open Indo-Pacific' strategy. *International Affairs*, 96(1), 131-148.



Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs.

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(3). https://doi.org/10.1007/s44206-024-00146-7

Economic and Political Weekly. (2024, December 27). Technological Sovereignty. Economic and Political Weekly, 52. https://www.epw.in/journal/2024/52/strategic-affairs/technological-sovereignty.html

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data Sovereignty in Information Systems. Electronic Markets, 34(1). https://doi.org/10.1007/s12525-024-00693-4

Reyes-García, V., Tofighi-Niaki, A., Austin, B. J., Benyei, P., Danielsen, F., Fernández-Llamazares, Á., Sharma, A., Soleymani-Fard, R., & Tengö, M. (2022). Data Sovereignty in community-based environmental monitoring: Toward Equitable Environmental Data Governance. BioScience, 72(8), 714–717. https://doi.org/10.1093/biosci/biac048

March, C., & Schieferdecker, I. (2023). Technological sovereignty as ability, not autarky. International Studies Review, 25(2). https://doi.org/10.1093/isr/viad012

Timmers, P. (2023). Sovereignty in the Digital age. Introduction to Digital Humanism, 571–592. https://doi.org/10.1007/978-3-031-45304-5_36

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2022). Contested spatialities of Digital Sovereignty. Geopolitics, 28(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Hema Nadarajah, A. I. (n.d.). Indonesian government under fire for string of cyber breaches. Asia Pacific Foundation of Canada. https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches

Bank Info Security Asia. (2023). Indonesia hardest hit by cyberattacks in the region. Bank Info Security.

Badan Siber dan Sandi Negara. (2024). Laporan Tahunan Keamanan Siber Indonesia 2024. Jakarta: BSSN.

IndoSec Summit. (2025). The escalating cyber threat in Indonesia: A wake-up call for digital security. IndoSec Summit Report.

Institute of Southeast Asian Studies. (2021). Digital sovereignty viewed from Asia. Directions Blog.

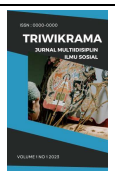
Security Today. (2024). World's critical infrastructure suffered 13 cyber attacks every second in 2023. Security Today.

SOCRadar Cyber Intelligence. (2024). Indonesia threat landscape report 2024. SOCRadar Cyber Intelligence.

Gu, Hongfei. (2023). Data, Big Tech, and the New Concept of Sovereignty. Journal of Chinese Political Science. 29. 10.1007/s11366-023-09855-1.

AJCCBC. (2023). *Cybersecurity Capacity Building in ASEAN: Regional Review*. ASEAN-Japan Cybersecurity Capacity Building Centre.

ASEAN Secretariat. (2021). ASEAN Digital Masterplan 2025. https://asean.org/book/asean-digital-masterplan-2025/



de Hert, P., & Papakonstantinou, V. (2012). *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*. Computer Law & Security Review, 28(2), 130–142.

Morozov, E. (2014). *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs.