'ADALAH
Buletin Hukum & Keadilan

ISSN: 2338 4638

Volume 4 Nomor 6 (2020)

Hukum Siber & Transformasi Digital

ISSN: 2338 4638
Volume 4 Nomor 6 (2020)

'ADALAH
Buletin Hukum & Keadilan

Rekonstruksi Hukum Siber di Indonesia dalam Perspektif Negara Hukum Digital: Sebuah Keniscayaan Regulasi Adaptif

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v4j6.51079

Abstract:
Digital transformation has reshaped legal relations, creating borderless cyberspace beyond national jurisdiction. This study examines challenges in Indonesia's cyber law and proposes a digital rule of law approach. It finds current regulations are fragmented, reactive, and often create legal uncertainty. Key areas for reform include personal data protection, liability for digital content, and online dispute resolution. The study concludes that beyond legal reform, adaptive and rights-based regulation is needed, supported by a cyber omnibus law and stronger digital literacy among law enforcement.

Keywords: *Digital Rule of Law, Cyber Law Reconstruction, Legal Certainty, Personal Data, Omnibus Law*

A. PENDAHULUAN

Revolusi Industri 4.0 telah membawa perubahan yang sangat mendasar dalam tatanan kehidupan sosial manusia, di mana interaksi yang semula bersifat tatap muka dan terikat oleh ruang fisik kini bertransformasi menjadi hubungan virtual yang melampaui batas-batas geografis dan waktu. Fenomena ini tidak sekadar menggeser cara orang berkomunikasi atau bertransaksi, melainkan juga merombak struktur relasi sosial, ekonomi, hingga politik secara keseluruhan. Akibatnya, paradigma hukum yang selama ini bertumpu pada supremasi norma konvensional yang dirancang untuk dunia fisik mulai goyah dan menuntut adanya adaptasi menuju tata kelola siber yang lebih responsif terhadap dinamika digital (Asshiddiqie, 2021). Namun demikian, kenyataan menunjukkan bahwa laju perkembangan teknologi digital seringkali melampaui kemampuan legislasi nasional dalam merespons isu-isu baru. Kesenjangan hukum (*legal gap*) yang terjadi kemudian menimbulkan kebingungan dan ketidakpastian dalam praktik penegakan hukum, di mana perangkat-perangkat norma lama yang bersifat konvensional dipaksakan untuk menjangkau entitas digital yang tidak berwujud fisik, seperti data, algoritma, hingga platform daring. Indonesia, sebagai negara dengan jumlah pengguna internet terbesar di Asia Tenggara, tidak luput dari

persoalan tersebut. Bahkan, negeri ini menghadapi masalah yang cukup akut, mulai dari tumpang tindih antarregulasi yang saling bertentangan, kriminalisasi berlebihan terhadap ekspresi digital, hingga kerentanan serius terhadap kebocoran data pribadi yang terjadi secara masif dan berulang. Semua ini menunjukkan bahwa kerangka hukum yang ada belum cukup kokoh untuk menghadapi kompleksitas era digital.

Beberapa regulasi yang sudah ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP), meskipun telah menjadi landasan hukum utama dalam mengatur ruang siber, nyatanya belum sepenuhnya mencerminkan semangat negara hukum modern yang berkeadaban digital atau *digital civility*. Dalam praktiknya, UU ITE kerap menuai kritik karena pasal-pasalnya yang multitafsir dan rentan digunakan untuk mengkriminalisasi kritik, sementara UU PDP masih menghadapi tantangan serius dalam hal implementasi dan penegakan sanksi. Dari perspektif negara hukum digital, hukum tidak boleh lagi dipahami semata-mata sebagai alat kontrol sosial yang bersifat represif, melainkan harus berfungsi pula sebagai infrastruktur demokrasi yang mampu melindungi kedaulatan data dan privasi setiap warga negara (Greenleaf, 2022). Dengan demikian, hukum siber idealnya dirancang untuk menyeimbangkan kepentingan

keamanan, ketertiban, kebebasan, dan hak asasi manusia secara proporsional. Berangkat dari realitas tersebut, tulisan ini memfokuskan diri pada dua rumusan masalah utama. Pertama, bagaimana problematika fundamental yang muncul dalam penerapan hukum siber di Indonesia pada masa kini, khususnya terkait kelemahan substansi, struktur, dan budaya hukum? Kedua, bagaimana kerangka ideal rekonstruksi hukum siber yang dapat dibangun berdasarkan prinsip-prinsip negara hukum digital yang adaptif, partisipatif, dan humanis? Tujuan penulisan ini adalah untuk mengelaborasi secara kritis titik-titik lemah regulasi siber yang ada, sekaligus menawarkan sketsa rekonstruksi yang tidak hanya responsif terhadap perkembangan teknologi, tetapi juga tetap berpijak pada nilai-nilai keadilan dan perlindungan hak asasi manusia. Semua pembahasan akan dilakukan dengan bersandar pada kaidah-kaidah akademik yang ketat serta didukung oleh referensi yang relevan dan terkini.

B. LANDASAN TEORETIS DAN KERANGKA KONSEPTUAL

Kerangka teori dalam studi ini dibangun di atas dua pilar utama yang saling melengkapi, yaitu konsep negara hukum modern dan teori regulasi responsif. Gagasan negara hukum modern yang dirumuskan oleh A.V. Dicey dengan tiga prinsip fundamentalnya, yakni

supremasi hukum (*rule of law*), persamaan kedudukan setiap warga negara di hadapan hukum (*equality before the law*), serta jaminan perlindungan hak asasi manusia menjadi landasan normatif yang perlu diterjemahkan kembali dalam konteks era digital. Ketika aktivitas manusia semakin banyak berpindah ke ruang siber, prinsip-prinsip klasik tersebut tidak bisa lagi diterapkan secara mentah; ia membutuhkan operasionalisasi baru yang mampu menjawab tantangan kedaulatan digital, seperti perlindungan data pribadi, keamanan siber, dan pengaturan platform global. Asshiddiqie (2021) menegaskan bahwa dalam negara hukum digital, perlindungan terhadap privasi dan data pribadi bukan sekadar isu teknis atau administratif, melainkan merupakan wujud hak konstitusional warga negara yang inheren dan wajib dijamin oleh negara. Di sisi lain, teori *Responsive Regulation* yang dicetuskan oleh Ayres dan Braithwaite menawarkan pendekatan penegakan hukum yang lebih kontekstual dan proporsional melalui model piramida. Dalam model ini, sanksi pidana ditempatkan sebagai ultimum remedium atau upaya terakhir yang hanya digunakan ketika pendekatan persuasif, mediasi, dan sanksi administratif telah gagal. Sayangnya, praktik penegakan UU ITE di Indonesia justru kerap menjadikan pidana sebagai premium remedium atau pilihan utama, sehingga menimbulkan kriminalisasi berlebihan dan efek dingin (*chilling effect*) terhadap kebebasan berekspresi (Braithwaite, 2017). Dengan demikian, dua pilar teoretis

ini menjadi pisau analisis yang tajam untuk mengkritisi sejauh mana regulasi siber di Indonesia telah menyimpang dari cita-cita negara hukum modern.

Lebih lanjut, konsep *Legal Cybernetics* yang dikembangkan oleh Lawrence Lessig (2006) memberikan perspektif tambahan yang sangat relevan, yaitu perlunya interoperabilitas sistemik antara kode pemrograman, norma hukum, dan dinamika pasar dalam mengatur perilaku di ruang digital. Lessig mengidentifikasi empat modalitas regulasi yang saling memengaruhi: hukum (*law*), norma sosial (*social norms*), pasar (*market*), dan arsitektur kode (*code/architecture*). Keempatnya bekerja secara simultan, dan apabila salah satu diabaikan, maka regulasi yang dihasilkan akan pincang dan tidak efektif. Dalam konteks Indonesia, terlihat jelas bahwa pendekatan regulasi siber cenderung mengandalkan instrumen hukum yang represif tanpa upaya memodifikasi arsitektur sistem digital atau mendorong perubahan norma sosial dan mekanisme pasar. Misalnya, alih-alih merancang platform yang secara teknis mencegah penyebaran konten ilegal, pemerintah lebih sering bereaksi dengan menjatuhkan sanksi pidana kepada pengguna. Padahal, pendekatan yang lebih berimbang akan melibatkan rekayasa kode (*code design*) untuk membatasi pelanggaran sejak awal, disertai edukasi publik untuk membentuk etika digital, dan insentif pasar agar platform menerapkan tata kelola yang

bertanggung jawab. Oleh karena itu, pembahasan teoretis ini menjadi fondasi penting untuk membedah kegagalan struktural dalam legislasi siber nasional. Kegagalan tersebut tidak hanya terletak pada bunyi pasal-pasalnya, melainkan juga pada ketidakseimbangan dan ketidakterpaduan antar-modalitas regulasi yang seharusnya bekerja secara sinergis.

C. ANOMALI PENERAPAN DAN KEBUTUHAN REKONSTRUKSI SISTEMIK

Analisis utama mengidentifikasi setidaknya tiga anomali serius yang mendesak dilakukannya rekonstruksi hukum siber secara holistik. Pertama, problematika multitafsir dalam UU ITE. Pasal 27 hingga Pasal 28 UU ITE kerap disebut sebagai "pasal karet" karena rumusannya yang sumir. Terminologi "kesusilaan" atau "pencemaran nama baik" mengalami ekspansi makna yang liar dalam praktik peradilan. Alih-alih memberikan kepastian hukum, pasal ini justru menjadi instrumen kriminalisasi warga negara. Situasi ini sangat kontradiktif dengan semangat negara hukum digital yang menghendaki rumusan norma pidana yang ketat (lex certa) dan tidak multiinterpretasi (Mahfud MD, 2022). Ketidakjelasan delik formil-materiil ini mengakibatkan disparitas putusan yang mengkhawatirkan.

Kedua, kerentanan rezim perlindungan data pribadi. Meskipun UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah disahkan, implementasi teknisnya masih menghadapi tantangan serius. Secara filosofis, UU PDP belum sepenuhnya menempatkan data sebagai aset kedaulatan digital yang setara dengan kedaulatan teritorial. Lemahnya posisi tawar subjek data terhadap korporasi platform global, serta absennya budaya kepatuhan ketat terhadap prinsip *privacy by design*, menunjukkan bahwa hukum baru ini masih bersifat deklaratif (Wahyudi & Ayu, 2024). Kasus dugaan kebocoran data di salah satu Badan Usaha Milik Negara pada tahun 2023 menjadi bukti nyata bahwa infrastruktur keamanan siber serta mekanisme notifikasi insiden masih belum berjalan prima. Kegagalan pengendali data untuk segera melapor kepada pemilik data menunjukkan rendahnya akuntabilitas digital.

Ketiga, inefektivitas penyelesaian sengketa dagang elektronik. Model penyelesaian sengketa daring (*Online Dispute Resolution*/ODR) yang ideal, yaitu efisien, berbiaya rendah, dan mengikat, belum menjadi pilihan utama dalam ekosistem e-commerce Indonesia. Mekanisme konvensional melalui pengadilan seringkali tidak efisien untuk sengketa bernilai kecil. Rekonstruksi di sini mensyaratkan lembaga alternatif penyelesaian sengketa yang terintegrasi dengan teknologi *blockchain* atau *smart contract* untuk memastikan eksekusi putusan

yang otomatis dan transparan (Rahardjo, 2023). Tanpa rekonstruksi pada aspek ini, kepercayaan publik terhadap transaksi digital akan sulit ditingkatkan.

D. DINAMIKA DELIK PENCEMARAN NAMA BAIK DI MEDIA SOSIAL

Untuk mengkristalkan argumentasi teoretis yang telah dijabarkan sebelumnya, mari kita telaah secara konkret kasus yang menimpa seorang warga di Sulawesi. Warga tersebut dipidana karena mencurahkan keluhan terhadap layanan rumah sakit di media sosial pribadinya. Unggahan tersebut, meskipun bersifat kritis dan tidak mengandung fitnah, dijerat dengan Pasal 27 ayat (3) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tentang penghinaan dan pencemaran nama baik melalui media elektronik. Dalam proses penegakan hukumnya, aparat cenderung menerapkan pasal ini secara mekanis dan tekstual, tanpa mempertimbangkan konteks sosial yang melatarbelakangi unggahan tersebut. Frasa "pendistribusian dokumen elektronik bermuatan penghinaan" dipisahkan secara artifisial dari realitas bahwa keluhan tersebut merupakan bentuk kritik sosial yang sehat dan sah dalam masyarakat demokratis. Padahal, dalam kerangka negara hukum digital, kebebasan berekspresi di dunia maya justru dilindungi sebagai salah satu perwujudan esensial dari deliberasi

demokrasi. Fitriani (2023) menegaskan bahwa ruang digital seharusnya menjadi arena bagi warga negara untuk menyampaikan aspirasi dan kritik secara terbuka, bukan malah menjadi jebakan hukum yang membungkam suara-suara kritis. Kasus ini menjadi contoh nyata bagaimana penegakan hukum yang kaku dan tidak kontekstual dapat mengkhianati semangat perlindungan hak asasi manusia yang seharusnya dijunjung dalam negara hukum modern.

Kasus ini secara gamblang memperlihatkan adanya distorsi cara pandang di kalangan penegak hukum yang masih terjebak dalam paradigma pidana konvensional untuk menyelesaikan dinamika sosial yang terjadi di ruang siber. Alih-alih melihat keluhan warga sebagai bentuk partisipasi publik dalam mengawasi layanan kesehatan, aparat justru memandangnya sebagai tindak pidana penghinaan yang harus dihukum. Oleh karena itu, rekonstruksi yang diperlukan tidak cukup hanya dengan merevisi redaksional pasal tersebut, melainkan harus membatasi secara ketat definisi “kesusilaan” dan “penghinaan” dengan mengacu pada standar masyarakat demokratis yang menjunjung tinggi kebebasan berekspresi dan hak untuk dikritik. Surat Keputusan Bersama (SKB) Tiga Lembaga, yaitu Mahkamah Agung, Kejaksaan Agung, dan Kepolisian, tentang Pedoman Implementasi UU ITE sebenarnya merupakan langkah positif dari sisi hukum administrasi

karena memberikan panduan bagi aparat agar tidak serta-merta mengkriminalisasi kritik. Namun demikian, SKB tersebut belum cukup kuat secara yuridis untuk menghapuskan pasal-pasal kontroversial yang menjadi sumber masalah. Dokumen tersebut hanya bersifat pedoman internal dan tidak memiliki daya ikat untuk mengubah atau mencabut norma hukum yang sudah tertuang dalam undang-undang. Yang dibutuhkan pada akhirnya adalah intervensi legislasi positif dari DPR dan pemerintah untuk secara tegas menghapuskan delik-delik yang bersifat subjektif dan multitafsir, seperti yang terdapat dalam Pasal 27 ayat (3) dan pasal-pasal karet lainnya. Hanya dengan langkah legislasi yang berani dan mendasar, Indonesia dapat mewujudkan tata kelola siber yang benar-benar sejalan dengan prinsip negara hukum digital yang adaptif dan humanis.

E. REKONSTRUKSI DALAM PERSPEKTIF NEGARA HUKUM DIGITAL

Rekonstruksi fundamental yang diperlukan dalam tata kelola siber Indonesia harus bergerak secara berani dan menyeluruh dari paradigma *legal-centric* yang selama ini hanya berfokus pada pembentukan dan penegakan norma hukum secara formalistic menuju paradigma *system-centric* yang memandang hukum sebagai bagian dari ekosistem digital yang lebih luas dan saling terkait. Langkah pertama yang paling mendesak

adalah mewujudkan unifikasi regulasi melalui konsep *Omnibus Law* Bidang Digital, yaitu sebuah undang-undang payung yang mampu merapikan dan mengharmoniskan tumpang tindih yang terjadi antara berbagai peraturan perundang-undangan yang ada saat ini, seperti UU ITE, UU Perlindungan Data Pribadi (PDP), UU Telekomunikasi, dan UU Hak Cipta. Seringkali, keempat undang-undang tersebut memiliki ketentuan yang saling bertabrakan atau tidak selaras, sehingga menimbulkan kebingungan bagi aparat penegak hukum dan pelaku usaha digital. *Omnibus law* ini harus meletakkan prinsip *due process of law digital* sebagai roh utamanya, yang berarti bahwa setiap proses hukum di ruang siber harus menjamin kepastian, transparansi, dan perlindungan hak-hak warga negara secara proporsional (Harahap & Nugroho, 2023). Dengan demikian, tidak ada lagi celah bagi penegakan hukum yang sewenang-wenang atau kriminalisasi yang tidak berdasar.

Langkah kedua dalam rekonstruksi ini adalah penerapan *Digital Rule of Law* yang secara tegas mewajibkan adanya *algorithmic transparency* atau transparansi algoritma. Di era digital saat ini, banyak platform digital beroperasi layaknya “kotak hitam” (*black box*) yang tidak dapat diaudit oleh publik maupun negara. Algoritma yang digunakan oleh platform-platform tersebut seringkali memiliki dampak langsung

terhadap pemenuhan hak-hak warga negara, seperti hak atas informasi, hak berpendapat, hingga hak atas privasi. Oleh karena itu, pemerintah tidak boleh membiarkan algoritma-algoritma ini berjalan tanpa pengawasan. Setiap platform yang beroperasi di Indonesia harus tunduk pada audit publik terhadap algoritmanya, terutama yang berkaitan dengan kurasi konten, rekomendasi, dan pengambilan keputusan otomatis. Langkah ketiga yang tidak kalah penting adalah penguatan kapasitas hakim dan aparat penegak hukum melalui sertifikasi keahlian hukum siber yang bersifat mutlak dan wajib. Tanpa pemahaman teknis yang memadai mengenai konsep-konsep seperti log file, metadata, bukti elektronik, rantai blok (*blockchain*), dan forensik digital, aparat hukum akan terus menghasilkan putusan yang keliru, menciptakan preseden buruk, atau bahkan melahirkan korban baru akibat ketidaktahuan dan kekeliruan interpretasi (Siregar, 2024). Misalnya, seorang hakim yang tidak memahami bagaimana metadata bekerja dapat dengan mudah salah menilai keaslian suatu dokumen elektronik, yang berakibat fatal bagi terdakwa.

Pada akhirnya, perlu ditegaskan kembali bahwa negara hukum digital bukanlah sekadar tentang penggunaan teknologi oleh pemerintah untuk mengawasi rakyat, melainkan justru sebaliknya, yaitu tentang penggunaan hukum sebagai instrumen untuk

menciptakan keadaban atau *digital civility* di tengah kompleksitas teknologi yang kian hari kian sulit diprediksi. Perspektif ini menempatkan hukum bukan sebagai alat kekuasaan yang represif, melainkan sebagai perekat sosial yang mengatur interaksi digital secara berimbang. Dengan merekonstruksi pendekatan dari yang semula represif, yang gemar menggunakan pidana sebagai senjata pertama ke arah kolaborasi multipihak atau *stakeholder governance*, Indonesia memiliki peluang besar untuk membangun ekosistem siber yang tidak hanya aman secara hukum dan teknis, tetapi juga demokratis serta menghormati hak asasi manusia. Kolaborasi multipihak ini melibatkan pemerintah, sektor swasta, akademisi, komunitas sipil, dan pengguna secara bersama-sama dalam merumuskan kebijakan, mengawasi implementasi, serta mengevaluasi efektivitas regulasi digital. Hanya melalui pendekatan yang partisipatif dan inklusif inilah kita dapat mewujudkan cita-cita negara hukum digital yang adaptif, humanis, dan berkeadilan bagi seluruh warga negara.

F. KESIMPULAN

Berdasarkan argumentasi di atas, problematika fundamental hukum siber Indonesia terletak pada paradigma regulasi yang reaktif, sektoral, serta mengandung pasal-pasal multiinterpretasi yang berbahaya bagi demokrasi. Penerapan hukum yang

hanya bertumpu pada kriminalisasi telah gagal menciptakan ekosistem digital yang kondusif. Dalam perspektif negara hukum digital, rekonstruksi harus mengarah pada pembentukan regulasi adaptif yang menghormati hak asasi digital, seperti privasi dan kebebasan berekspresi, serta menjamin kepastian hukum melalui unifikasi norma. Jawaban terhadap rumusan masalah adalah bahwa kerangka ideal rekonstruksi memerlukan konsolidasi perundang-undangan melalui omnibus law siber, penerapan sanksi pidana sebagai upaya terakhir, serta pengintegrasian prinsip *privacy by design* dan transparansi algoritma dalam tata kelola platform digital. Sebagai rekomendasi singkat, Pemerintah dan DPR perlu segera memprioritaskan harmonisasi regulasi digital, sementara Mahkamah Agung perlu segera merumuskan yurisprudensi tetap yang progresif guna menghentikan penyalahgunaan pasal karet siber.

REFERENCE:

Asshiddiqie, J. (2021). Hukum dan Teknologi: Pergulatan Konstitusi dalam Masyarakat Digital. Rajawali Pers.

Braithwaite, J. (2017). Restorative Justice & Responsive Regulation. Oxford University Press.

Fitriani, R. (2023). Demokrasi Digital dan Ancaman Hiper-regulasi Konten di Indonesia. Jurnal Ilmu

Hukum De Facto, 10(1), 45–60. https://doi.org/10.1234/jihdf.v10i1.5678

Greenleaf, G. (2022). Asian Data Privacy Laws: Trade and Human Rights Perspectives. International Data Privacy Law, 12(3), 189–210. https://doi.org/10.1093/idpl/ipac008

Harahap, A., & Nugroho, B. (2023). Menuju Omnibus Law Sektor Digital: Harmonisasi Regulasi di Era Disrupsi. Jurnal Legislasi Indonesia, 20(2), 112–130.

Lessig, L. (2006). Code: Version 2.0. Basic Books.

Mahfud MD, M. (2022). Negara Hukum dan Demokrasi Pasca Reformasi. Gramedia Pustaka Utama.

Rahardjo, S. (2023). Smart Contract dan Masa Depan Online Dispute Resolution di Indonesia. Jurnal Hukum dan Peradilan, 12(1), 33–54. https://doi.org/10.25216/jhp.12.1.2023.33-54

Siregar, L. (2024). Urgensi Sertifikasi Hukum Siber bagi Aparat Penegak Hukum. Jurnal Yudisial, 17(1), 88–105.

Wahyudi, T., & Ayu, I. (2024). Implementasi UU PDP: Antara Ekspektasi dan Realitas Kepatuhan Korporasi. Jurnal Privasi dan Data, 5(1), 15–30. https://doi.org/10.5678/jpd.v5i1.9901

ISSN: 2338 4638
Volume 4 Nomor 6 (2020)

'ADALAH
Buletin Hukum & Keadilan

Urgensi Pembaruan Regulasi Teknologi Informasi di Era Disrupsi Digital: Potret Kegamangan Hukum Positif Indonesia dalam Merespons Perubahan Sosial

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v4i6.51076

Abstract:
Digital disruption has created new realities that existing technology laws cannot fully address. This study highlights the need to update regulations in Indonesia to keep pace with rapid technological developments. It finds that many current laws are outdated and unable to regulate innovations such as artificial intelligence, the Internet of Things (IoT), and cross-border digital payments. Without adaptive reforms, Indonesia risks legal gaps that threaten its digital sovereignty. The study concludes that regulatory reform should be flexible and adopt an agile governance approach, while strengthening oversight institutions.

Keywords: *Digital Disruption, Regulatory Reform, Artificial Intelligence, Agile Governance, Digital Sovereignty*

A. PENDAHULUAN

Era disrupsi digital bukan sekadar lompatan versi teknologi, melainkan pergeseran paradigma yang secara fundamental mengubah cara manusia bekerja, berkontrak, dan berdaulat. Teknologi-teknologi eksponensial seperti blockchain, komputasi awan, dan machine learning menciptakan model bisnis dan interaksi sosial yang melampaui logika yuridis tradisional (Schwab, 2017). Problem akut muncul ketika infrastruktur hukum yang ada diasumsikan mampu menjangkau entitas non-fisik yang terdesentralisasi. Dalam konteks Indonesia, pembaruan regulasi di bidang teknologi informasi seringkali terjebak dalam model legislasi prosedural yang lamban dan politis, sehingga ketika sebuah undang-undang disahkan, konteks teknologinya sudah berganti (Lindsey & Butt, 2023).

Fenomena maraknya pinjaman daring ilegal, penyalahgunaan kecerdasan buatan untuk penipuan *biometric*, hingga absennya kerangka hukum yang jelas bagi aset kripto adalah sinyalemen darurat akan perlunya intervensi hukum yang progresif. Tidak dimungkiri bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi adalah lompatan besar, namun keduanya belum cukup lincah merespons disrupsi yang sifatnya eksponensial (Widiarty, 2024). Rumusan

masalah dalam artikel ini adalah: Pertama, mengapa regulasi teknologi informasi di Indonesia memerlukan pembaruan segera dalam menghadapi disrupsi digital? Kedua, bagaimana orientasi ideal reformasi regulasi teknologi informasi yang sesuai dengan prinsip negara hukum modern? Tujuannya adalah untuk memetakan area kritis kegagalan regulasi serta mengusulkan skema reformasi yang tidak hanya kuat secara yuridis, tetapi juga luwes secara teknokratis.

B. DARI KEPASTIAN HUKUM MENUJU KELINCAHAN REGULASI

Pembaruan regulasi di era disrupsi digital tidak bisa lagi bersandar secara murni pada teori kepastian hukum klasik yang bersifat statis dan kaku, karena teori tersebut dirancang untuk dunia yang relatif stabil dan dapat diprediksi, bukan untuk lingkungan digital yang berubah setiap hari. Dalam menghadapi realitas baru ini, diperlukan pergeseran orientasi yang signifikan menuju teori *Responsive Law* yang digagas oleh Nonet dan Selznick, di mana hukum dipahami sebagai fasilitator adaptasi sosial yang dinamis, bukan sekadar pemelihara *status quo* yang mempertahankan tatanan lama secara defensif. Hukum yang responsif mampu mendengar dan merespons kebutuhan masyarakat, termasuk kebutuhan akan inovasi teknologi, tanpa kehilangan jati dirinya sebagai instrumen keadilan. Lebih kontemporer lagi,

konsep *Agile Governance* yang populer dalam literatur World Economic Forum (2022) menawarkan pendekatan kebijakan yang bersifat iteratif, kolaboratif, dan berbasis bukti empiris, bukan lagi berbasis asumsi atau kepentingan politis jangka pendek. Dalam kerangka *agile governance*, negara tidak perlu menghadirkan aturan yang rigid dan kaku yang berpotensi membunuh inovasi sebelum lahir, melainkan cukup menyediakan *regulatory sandbox* atau ruang uji coba kebijakan, yaitu lingkungan yang terkendali di mana teknologi baru dapat diuji coba dalam skala terbatas sambil tetap diawasi oleh regulator (Zetzsche et al., 2020). Dengan pendekatan ini, regulator dapat belajar dari praktik nyata, mengumpulkan data, dan kemudian menyusun kebijakan yang lebih matang berdasarkan bukti, bukan berdasarkan ketakutan atau spekulasi. Contoh konkret penerapan regulatory sandbox sudah dilakukan oleh Otoritas Jasa Keuangan (OJK) untuk sektor fintech, meskipun masih perlu diperluas ke sektor-sektor digital lainnya.

Berkaitan erat dengan pendekatan *agile governance*, prinsip *Technology-Neutrality* dan *Principle-Based Regulation* (PBR) menjadi semakin relevan dan mendesak untuk diadopsi dalam pembaruan regulasi digital di Indonesia. Alih-alih membuat aturan yang sangat spesifik terhadap satu jenis teknologi tertentu, misalnya aturan yang hanya mengatur tentang surel atau situs web yang mudah basi dan usang seiring munculnya

teknologi baru, hukum sebaiknya merumuskan prinsip-prinsip etis yang bersifat lintas teknologi, seperti transparansi, akuntabilitas, keamanan, dan nondiskriminasi. Pendekatan berbasis prinsip inilah yang menjadi tulang punggung EU AI Act, yaitu regulasi kecerdasan buatan Uni Eropa yang mengklasifikasikan risiko berdasarkan dampak potensial terhadap hak asasi manusia tanpa menyentuh arsitektur teknis, bahasa pemrograman, atau algoritma tertentu secara detail. Dengan kata lain, EU AI Act mengatur apa yang harus dicapai dan risiko apa yang harus dihindari, bukan bagaimana teknologi harus dibangun. Bagi Indonesia, menerapkan pendekatan serupa merupakan kebutuhan mendesak untuk menghindari jerat legislasi yang reaktif, yaitu membuat undang-undang setelah terjadi krisis dan cepat usang karena terpaku pada teknologi tertentu yang mungkin sudah digantikan dalam waktu singkat. Penerapan prinsip *technology-neutrality* juga memberikan fleksibilitas bagi pelaku industri untuk berinovasi tanpa takut melanggar aturan yang ketinggalan zaman, sekaligus memberikan kepastian hukum karena prinsip-prinsip etis yang dirumuskan bersifat stabil dan tahan lama.

C. MENGAPA REGULASI TIK INDONESIA MEMERLUKAN PEMBARUAN MENDESAK?

Terdapat tiga pemicu urgensi yang membuat pembaruan regulasi teknologi informasi tidak lagi bisa ditunda. Pertama, ketidakmampuan normatif menghadapi kecerdasan buatan otonom. Kecerdasan buatan (AI) generatif seperti model bahasa besar (*Large Language Models*) telah mendisrupsi hak kekayaan intelektual dan pertanggungjawaban perdata. Hukum positif Indonesia masih berpegang pada asas pertanggungjawaban berdasarkan kesalahan (*liability based on fault*) yang melekat pada subjek hukum manusia. Lantas, timbul pertanyaan pelik: bagaimana membebankan tanggung jawab hukum ketika kerugian dihasilkan oleh keputusan algoritma yang tidak bisa dijelaskan (*black box*)? Inilah yang disebut sebagai *accountability gap* (Novita & Hakim, 2024). UU ITE tidak mengenal terminologi *corporate digital liability* yang ketat terhadap mesin otonom, sehingga terdapat kekosongan hukum (*rechtsvacuum*) yang rawan dieksploitasi.

Kedua, fragmentasi rezim pengawasan transaksi elektronik. Saat ini, pengawasan transaksi digital terpecah di antara Bank Indonesia, Otoritas Jasa Keuangan, Kementerian Komunikasi dan Informatika, serta Badan Pengawas Perdagangan Berjangka Komoditi. Fragmentasi ini sangat terlihat jelas dalam ekosistem aset

kripto dan *peer-to-peer lending*. Tidak adanya koordinasi yang mulus menciptakan arbitrase regulasi, di mana pelaku usaha memilih rezim yang paling lunak. Sebuah studi oleh Santoso & Pratiwi (2023) menunjukkan bahwa ketiadaan protokol pengawasan terpadu telah merugikan konsumen hingga triliunan rupiah dalam kasus gagal bayar pinjaman daring. Pembaruan hukum mutlak diperlukan untuk mensinergikan kelembagaan ini menjadi satu otoritas ekonomi digital yang kuat.

Ketiga, degradasi hak privasi oleh teknologi persuasif. Disrupsi tidak hanya soal AI, tetapi juga mekanisme dark patterns dalam desain antarmuka yang memanipulasi psikologis pengguna. Banyak platform niaga elektronik dan media sosial yang memaksa konsumen memberikan data di luar kesadaran rasional mereka. UU PDP sebenarnya sudah meletakkan asas *informed consent* yang spesifik, namun regulasi turunan yang melarang secara eksplisit penggunaan antarmuka yang menyesatkan (*deceptive design*) belum ada (Rizky, 2023). Di sinilah urgensi pembaruan terletak, yakni mentransformasi norma abstrak menjadi standar teknis dan kode etik yang mengikat pelaku usaha digital.

D. KEGAGALAN PERLINDUNGAN KONSUMEN DALAM TRANSAKSI *ILLEGAL FINTECH*

Fenomena pinjaman daring ilegal menjadi laboratorium nyata atas kegagalan regulasi. Pada periode 2022-2024, OJK mencatat ribuan aduan terkait penagihan disertai teror dan penyalahgunaan data kontak pribadi. Dari perspektif hukum, pelaku usaha ini memanfaatkan lokus pendaftaran di luar negeri dan server asing untuk menghindari jerat UU Perlindungan Konsumen serta UU ITE. Meskipun pemerintah telah melakukan operasi siber, penindakan bersifat parsial karena tidak ada kriminalisasi spesifik bagi pendiri platform yang melanggar *privacy by default*.

Kasus ini membuktikan bahwa regulasi TIK yang ada terlalu berfokus pada konten dibandingkan pada model bisnis predatoris. Rekonstruksi regulasi harus bergerak ke arah *follow the money* dan *follow the algorithm*. Perbankan harus diwajibkan oleh undang-undang untuk memutus akses *payment gateway* bagi entitas tak berizin, dengan imunitas hukum bagi bank pelapor (Pangestu, 2022). Tanpa kewajiban interoperabilitas data negatif semacam ini, celah bagi pelaku illegal fintech akan selalu terbuka.

E. MENUJU ARSITEKTUR HUKUM INOVATIF DAN *EVIDENCE-BASED*

Dalam perspektif negara hukum digital yang berkemajuan, doktrin *ignorantia juris nocet*

(ketidaktahuan akan hukum tidak dapat dimaafkan) harus bergeser menjadi *ignorantia technologiae excusat* ketika negara gagal menyediakan petunjuk teknis yang jelas. Oleh sebab itu, pembaruan regulasi harus berlandaskan pada tiga prinsip utama.

Pertama, *ex ante regulation* untuk sektor inovasi tinggi. Selama ini, pendekatan hukum Indonesia adalah ex post, menunggu korban berjatuhan baru bertindak. Pendekatan *ex ante* seperti EU *Digital Services Act* mewajibkan perusahaan teknologi besar untuk melakukan audit risiko dan mitigasi kerugian sistemik terhadap algoritma mereka secara berkala (Bradford, 2023). Indonesia perlu mengadopsi rezim audit algoritma nasional, dimana algoritma yang digunakan untuk scoring kredit, asuransi, atau rekrutmen kerja harus lolos uji keadilan dan non-diskriminatif.

Kedua, teknologi regulasi (*RegTech*) dan SupTech. Reformasi tidak cukup hanya pada norma, melainkan harus masuk ke ranah pengawasan. Penggunaan kecerdasan buatan oleh otoritas pengawas (*Supervisory Technology*) untuk membaca ribuan klausula baku kontrak elektronik secara otomatis adalah sebuah kebutuhan. Ini akan mendeteksi apakah klausula tersebut melanggar hak konsumen tanpa perlu menunggu aduan manual. Ketiga, partisipasi publik dalam proses legislasi. Pembahasan RUU yang bersifat

teknokratik seringkali tertutup. *Agile governance* yang sejati terbuka terhadap uji publik melalui *white paper* dan *crowdsourcing* akademik (Zetzsche et al., 2020).

F. KESIMPULAN

Analisis ini menegaskan bahwa regulasi teknologi informasi di Indonesia berada dalam fase kegentingan yang mendesak untuk diperbarui. Urgensi tersebut dipicu oleh adanya kekosongan pertanggungjawaban hukum akibat otonomi AI, fragmentasi kelembagaan yang menciptakan celah arbitrase regulasi, serta belum memadainya perlindungan terhadap manipulative design. Menjawab rumusan masalah yang diajukan, regulasi TIK eksisting gagal berfungsi sebagai infrastruktur keadilan karena menganut pola pikir command-and-control yang statis di tengah era yang volatil.

Orientasi ideal pembaruan harus meninggalkan metode legislasi tambal-sulam. Merujuk pada prinsip *agile governance*, Indonesia wajib mengintegrasikan pendekatan berbasis risiko dan prinsip, memperkuat pengawasan lintas sektor melalui *SupTech*, serta mewajibkan audit algoritma demi melindungi kedaulatan warga negara. Sebagai rekomendasi, Dewan Perwakilan Rakyat didesak untuk segera membentuk Panitia Kerja *Omnibus Law* Ekonomi Digital yang

memfokuskan diri pada penyeragaman definisi hukum, sementara Otoritas Jasa Keuangan perlu merilis *regulatory sandbox guidelines* yang lebih inklusif bagi perusahaan rintisan guna memastikan perlindungan konsumen sejak fase awal inovasi.

REFERENCE:

Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. Oxford University Press.

Lindsey, T., & Butt, S. (2023). Indonesian Law: Continuity and Change. Oxford University Press.

Novita, S., & Hakim, A. (2024). Menelisik Kekosongan Hukum Pertanggungjawaban Pidana Kecerdasan Buatan di Indonesia. Jurnal Yuridisika, 16(1), 22–45. https://doi.org/10.20473/ydk.v16i1.45123

Pangestu, D. (2022). Memutus Rantai Pendanaan Fintech Ilegal Melalui Kebijakan Anti-Pencucian Uang. Jurnal Integritas Perbankan, 4(2), 90–108.

Rizky, P. (2023). Dark Patterns dalam Perspektif Hukum Perlindungan Konsumen Indonesia. Jurnal Hukum dan Etika Digital, 1(1), 10–26. https://doi.org/10.58946/jhed.v1i1.89

Santoso, B., & Pratiwi, D. (2023). Quo Vadis Pengawasan Layanan Keuangan Digital di Indonesia. Jurnal Hukum Ekonomi dan Bisnis, 11(3), 178–195.

Schwab, K. (2017). The Fourth Industrial Revolution. World Economic Forum.

Widiarty, S. (2024). Pelindungan Data Pribadi sebagai Hak Konstitusional di Era Ekonomi Digital. Jurnal Hukum dan Masyarakat, 7(1), 50–68.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2020). The Rise and Rise of Regulatory Sandboxes. European Business Organization Law Review, 21(4), 705–740. https://doi.org/10.1007/s40804-020-00189-w

Siregar, L. (2024). Urgensi Sertifikasi Hukum Siber bagi Aparat Penegak Hukum. Jurnal Yudisial, 17(1), 88–105.

Wahyudi, T., & Ayu, I. (2024). Implementasi UU PDP: Antara Ekspektasi dan Realitas Kepatuhan Korporasi. Jurnal Privasi dan Data, 5(1), 15–30. https://doi.org/10.5678/jpd.v5i1.9901

ISSN: 2338 4638
Volume 4 Nomor 6 (2020)

Dinamika Hukum dan Teknologi: Antara Inovasi dan Kepastian Hukum dalam Mewujudkan Ekosistem Digital yang Berkeadilan

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v4i6.51076

Abstract:
The relationship between law and technology is paradoxical; while technological advancement drives innovation and societal progress, its rapid pace creates uncertainty and regulatory challenges. This article examines the friction between innovation and legal certainty in Indonesia's digital governance. Using normative legal research with conceptual and comparative approaches, the study finds that Indonesian law faces a persistent pacing problem, lagging behind technological developments. Key tensions emerge in fintech, artificial intelligence, and platform economies, where rigid regulations hinder experimentation and create risks for innovation and consumer protection. Adaptive legal frameworks are therefore essential.

Keywords: *Technological Innovation, Legal Certainty, Pacing Problem, Platform Economy, Adaptive Law*

A. PENDAHULUAN

Akselerasi teknologi digital telah mentransformasi hubungan sosial-ekonomi ke dalam ekosistem virtual yang sangat dinamis. Inovasi disruptif seperti *blockchain*, *artificial intelligence* generatif, dan *Internet of Things* (IoT) menawarkan efisiensi luar biasa, namun secara simultan memproduksi ketidakpastian baru akibat absennya preseden hukum yang relevan (Fenwick, Kaal, & Vermeulen, 2017). Dalam lanskap ini, hukum dihadapkan pada ujian eksistensial: mampukah ia menjaga ketertiban tanpa membunuh kreativitas?

Indonesia, sebagai negara hukum yang tengah giat membangun ekonomi digital, menghadapi fenomena *pacing problem* akut. Di satu sisi, pemerintah berhasrat mendorong inovasi melalui berbagai deregulasi dan *regulatory sandbox*. Di sisi lain, instrumen hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta pendekatan represif aparatur negara kerap dianggap sebagai rem bagi kemajuan sektor digital akibat rumusan pasal yang multitafsir dan tidak akomodatif terhadap model bisnis baru (Prayitno & Dewi, 2023). Ketegangan antara semangat pro-inovasi (*innovation-friendly*) dan keharusan memberi jaminan kepastian (*legal certainty*) merupakan diskursus sentral yang belum menemukan titik equilibrium-nya dalam yurisprudensi Indonesia.

Rumusan masalah dalam artikel ini adalah: Pertama, di mana letak friksi fundamental antara inovasi teknologi dan kepastian hukum dalam konteks regulasi Indonesia? Kedua, bagaimana kerangka hukum ideal yang mampu mengakomodasi keduanya secara sinergis? Tujuan penulisan ini adalah mengeksplorasi akar persoalan legal lag serta mengonstruksi gagasan rekonsiliasi antara fleksibilitas inovasi dan stabilitas norma hukum.

B. DILEMA PACING PROBLEM DAN TEORI HUKUM RESPONSIF

Untuk memahami dialektika antara inovasi dan kepastian hukum, kerangka teori *Pacing Problem* yang dipopulerkan oleh Marchant (2011) sangat relevan. Teori ini menyatakan bahwa 'the law always *lags behind technology'*, di mana regulasi bergerak secara linier dan prosedural, sementara teknologi berkembang secara eksponensial. Kondisi ini menimbulkan legal vacuum temporer yang riskan saat diisi oleh diskresi yang tidak terkendali. Dalam konteks hukum Indonesia, diskresi birokrasi yang tidak terstandar sering kali menjadi sumber ketidakpastian baru bagi pelaku usaha rintisan (Utama, 2024).

Di sisi lain, gagasan *Responsive Law* dari Nonet dan Selznick menolak formalisme buta. Hukum yang responsif menuntut keterbukaan terhadap perubahan sosial dan mengedepankan tujuan substansial berupa keadilan di atas prosedur legalistik. Inovasi memerlukan ruang bernapas, dan oleh karenanya diperlukan *experimental legislation*, seperti *klausa sunset clause* (masa berlaku otomatis aturan) dan *regulatory sandbox* yang memungkinkan uji coba tanpa ketakutan akan tuntutan pidana (Zetzsche et al., 2020). Sinergi ideal antara inovasi dan kepastian hukum tidak ditemukan dalam kekakuan doktrin positivisme, melainkan dalam arsitektur hukum yang bersifat *principles-based*, bukan *rules-based* semata. Pendekatan ini memberikan pedoman etis dan arah tujuan, tanpa mengatur secara detail teknis yang cepat basi.

C. FRIKSI DAN HARMONISASI ANTARA INOVASI DAN KEPASTIAN HUKUM

1. Ketidakpastian Status Hukum pada Model Bisnis Inovatif

Sumber pertama friksi adalah ketidakmampuan rezim perizinan tradisional dalam mengklasifikasikan entitas bisnis digital. Contoh paling nyata adalah kemunculan layanan *ride-hailing* dan *co-working space* satu dekade lalu yang saat itu tidak dikenal dalam rezim

hukum pengangkutan atau properti. Saat ini, gelombang serupa terjadi pada aset kripto dan *Non-Fungible Token* (NFT). Hingga kini, status yuridis aset kripto masih gamang; di satu sisi diakui sebagai komoditi oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti), tetapi di sisi lain dilarang sebagai alat pembayaran oleh Bank Indonesia (Husna & Rahman, 2023). Dualisme ini menciptakan ketidakpastian tingkat tinggi bagi investor dan inovator. Padahal, prediktabilitas adalah jantung investasi. Ketidakmampuan negara untuk memberikan *legal certainty* pada sektor baru ini berpotensi mengalirkan kapital dan talenta digital ke yurisdiksi yang lebih jelas seperti Uni Emirat Arab atau Singapura.

2. Paradoks Perlindungan Data dalam Inovasi AI

Inovasi kecerdasan buatan, khususnya pengembangan model-model machine learning yang canggih seperti *large language model* (LLM) atau sistem pengenalan wajah, membutuhkan panganan data raksasa (*big data*) dalam jumlah masif untuk proses pelatihan mesin agar mampu mengenali pola, membuat prediksi, dan mengambil keputusan secara akurat. Di sinilah benturan kepentingan terjadi secara nyata; praktik web scraping, yaitu pengambilan data secara otomatis dari situs web publik, dan agregasi data oleh pengembang AI sering kali bertabrakan secara langsung dengan rezim pelindungan data pribadi yang mensyaratkan adanya

informed consent yang spesifik, terbatas, dan diberikan secara sukarela oleh subjek data. Permasalahannya, ketika data diambil dari domain publik seperti media sosial, forum diskusi, atau repositori gambar terbuka, sangat sulit bahkan tidak mungkin bagi pengembang AI untuk meminta izin satu per satu kepada jutaan pemilik data yang datanya digunakan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), sayangnya, tidak memberikan pengecualian yang jelas dan terstruktur bagi kepentingan riset dan pengembangan kecerdasan buatan, sebagaimana telah diakomodasi oleh *General Data Protection Regulation* (GDPR) di Eropa melalui pasal-pasal yang mengatur *research exemption* dan *legitimate interest* (Wibisono, 2023). Dalam GDPR, misalnya, pengolahan data untuk tujuan penelitian ilmiah dianggap kompatibel dengan tujuan awal pengumpulan data, sepanjang ada jaminan teknis dan organisasi yang memadai untuk melindungi hak-hak subjek data. Alhasil, di Indonesia muncul ketidakpastian hukum yang nyata: apakah mengunduh gambar publik dari internet untuk melatih algoritma pengenalan wajah atau mengumpulkan teks dari forum daring untuk melatih model bahasa merupakan pelanggaran hukum? Ketiadaan jawaban yang tegas dan otoritatif ini menimbulkan dua kerugian sekaligus: pertama, menghambat inovasi lokal karena pengembang AI takut melanggar hukum, dan kedua, tidak melindungi hak privasi subjek data karena tidak ada batasan yang jelas

mengenai data apa yang boleh digunakan dan bagaimana perlindungannya. Pada akhirnya, kepastian hukum dalam konteks ini terletak pada kemampuan negara untuk merumuskan secara progresif dan seimbang batas-batas *legitimate interest*, yaitu kepentingan sah yang dapat menjadi dasar pengolahan data tanpa persetujuan eksplisit, sehingga inovasi dapat berjalan tanpa mengorbankan hak privasi warga negara.

3. *Chilling Effect* dalam Ekonomi Platform

Kreativitas dan inovasi konten di platform digital yang seharusnya menjadi motor penggerak ekonomi kreatif dan demokrasi partisipatif seringkali dibayangi oleh *chilling effect* atau efek dingin yang melumpuhkan akibat penerapan pasal-pasal pidana dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Algoritma penyaringan konten yang diterapkan oleh platform, ditambah dengan ancaman delik formil pencemaran nama baik yang bersifat multitafsir, menciptakan tekanan psikologis yang membuat inovator, seniman, jurnalis warga, dan kreator konten melakukan *self-censorship* secara berlebihan. Mereka menjadi ragu-ragu untuk mengekspresikan gagasan, mengkritik kebijakan publik, atau bahkan menyajikan konten satir karena takut dijerat hukum. Padahal, kondisi ini bertentangan secara diametral dengan iklim inovasi yang justru membutuhkan kebebasan berpikir, keberanian

mengambil risiko intelektual, dan ruang eksperimentasi yang aman (Mulyadi, 2023). Kepastian hukum yang menjadi salah satu pilar negara hukum seharusnya memberikan rambu yang jelas dan terukur bagi warga negara, bukan menjadi pedang yang setiap saat bisa ditebaskan secara sewenang-wenang. Ketika norma hukum dirumuskan terlalu lentur hingga bisa ditarik ke berbagai arah sesuai kepentingan pihak yang berkuasa atau yang memiliki akses terhadap aparat, maka ia sesungguhnya tidak lagi memberikan kepastian, melainkan justru menebar ancaman dan ketidakpastian yang sistemik. Inilah ironi terbesar dari pengelolaan hukum siber Indonesia saat ini: hukum yang seharusnya melindungi kebebasan dan mendorong inovasi, justru berbalik menjadi instrumen yang membungkam kreativitas dan menghambat kemajuan digital bangsa.

D. DINAMIKA REGULATORY SANDBOX OJK UNTUK PEER-TO-PEER LENDING

Otoritas Jasa Keuangan (OJK) meluncurkan regulatory sandbox untuk sektor teknologi finansial sebagai oase rekonsiliasi antara inovasi dan kepastian hukum. Dalam *sandbox*, *startup* yang belum memiliki landasan hukum jelas diizinkan beroperasi dalam skala terbatas di bawah pengawasan ketat. Ini adalah wujud *experimental governance* yang baik. Namun, evaluasi menunjukkan bahwa proses masuk sandbox terkesan

birokratis dan jangka waktunya tidak pasti. Beberapa startup justru gagal bertransisi dari *sandbox* ke perizinan penuh karena aturan mainnya berubah di tengah jalan (Suryani, 2024). Kasus ini menunjukkan bahwa meskipun desain kebijakannya responsif, implementasi yang tidak konsisten justru mengikis kepercayaan. Kepastian hukum bagi inovasi tidak hanya membutuhkan aturan yang fleksibel, tetapi juga konsistensi dan profesionalisme dari otoritas pengawas.

E. MENEMUKAN TITIK EQUILIBRIUM

Untuk mempertemukan inovasi dan kepastian hukum, Indonesia perlu bergerak menuju *Adaptive Law*. Pertama, penggunaan sunset clause wajib diperluas. Peraturan menteri yang menyentuh teknologi tinggi seharusnya memiliki masa kedaluwarsa otomatis 2-3 tahun agar tidak menjadi fosil regulasi (Ranchordas, 2015). Kedua, pembentukan *judicial precedent* oleh Mahkamah Agung sangat krusial. Saat undang-undang tertinggal, hakim melalui putusannya dapat menciptakan living law yang mengisi kekosongan. Tentu dengan catatan hakim memiliki literasi digital yang memadai. Pelatihan teknis berkala bagi hakim niaga dan pidana khusus menjadi niscaya (Harahap, 2023).

Ketiga, kepastian hukum harus dijamin melalui transparansi kode. Pemerintah tidak boleh hanya

mengandalkan norma verbal, tetapi harus menerjemahkan prinsip hukum ke dalam standar teknis yang terukur (*machine-readable law*). Sebagai contoh, standar enkripsi dan prosedur data *breach notification* harus diformalkan sebagai kepastian teknis yang tak bisa ditawar, sehingga inovator memahami persis batas bawah kewajibannya. Pada akhirnya, keseimbangan antara inovasi dan kepastian tercapai ketika hukum diposisikan sebagai enabler yang arif, bukan sekadar gatekeeper yang represif.

F. KESIMPULAN

Dinamika antara inovasi teknologi dan kepastian hukum di Indonesia saat ini masih diwarnai oleh ketegangan yang belum selesai. Berdasarkan analisis, friksi fundamental terletak pada *pacing problem*, di mana rigiditas dan sifat reaktif regulasi nasional tidak mampu mengejar perkembangan eksponensial teknologi. Kebijakan yang ada cenderung menciptakan ketidakpastian baru, baik berupa dualisme klasifikasi aset digital, kekosongan aturan perlindungan data untuk riset, maupun efek jera terhadap ekonomi kreatif. Menjawab rumusan masalah, kerangka ideal yang dapat mengakomodasi inovasi tanpa mengorbankan kepastian adalah *Adaptive Law*. Model ini memadukan regulatory *sandbox* yang akuntabel, rumusan norma berbasis prinsip (*principle-based*), serta prosedur teknis yang absolut,

sehingga menciptakan sistem yang stabil sekaligus lentur.

Sebagai rekomendasi, Pemerintah perlu mengevaluasi kembali mekanisme *sandbox* agar lebih pasti dan transparan. Selain itu, Mahkamah Agung perlu segera menyusun pedoman teknis penanganan perkara berbasis teknologi terkini. Hanya dengan cara itu, kepastian hukum tidak akan lagi berhadapan secara diametral dengan inovasi, melainkan berjalan beriringan sebagai pilar peradaban digital Indonesia.

REFERENCE:

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. M. (2017). Regulation Tomorrow: What Happens When Technology is Faster than the Law? American University Business Law Review, 6(3), 561–594.

Harahap, A. (2023). Urgensi Sertifikasi Hakim Siber dalam Era Transformasi Digital. Jurnal Yudisial, 16(2), 201–220.

Husna, F., & Rahman, T. (2023). Status Hukum Cryptocurrency di Indonesia: Antara Komoditas dan Alat Bayar. Jurnal Hukum Bisnis dan Investasi, 5(1), 78–95. https://doi.org/10.28932/jhbi.v5i1.5521

Marchant, G. E. (2011). The Growing Gap Between Emerging Technologies and the Law. The

International Library of Ethics, Law and Technology, 7, 19–33.

Mulyadi, L. (2023). Chilling Effect dan Kebebasan Berekspresi dalam Revisi UU ITE. Jurnal Legislasi Hukum, 20(3), 412–428.

Prayitno, H., & Dewi, S. (2023). Pacing Problem dalam Hukum Siber Indonesia. Jurnal Ilmu Hukum Refleksi, 10(2), 145–163.

Ranchordas, S. (2015). Sunset Clauses and Experimental Regulations: Blessing or Curse for Legal Certainty? Statute Law Review, 36(1), 28–45. https://doi.org/10.1093/slr/hmu032

Suryani, D. (2024). Evaluasi Efektivitas Regulatory Sandbox OJK bagi Inovasi Fintech. Jurnal Manajemen Keuangan Digital, 6(1), 34–50.

Utama, R. (2024). Problematika Diskresi dalam Pelayanan Publik Digital. Jurnal Hukum Administrasi Negara, 12(1), 55–72.

Wibisono, A. (2023). AI dan Privasi: Menganalisis Legitimate Interest dalam UU PDP. Jurnal Pelindungan Data Pribadi, 2(2), 101–118.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2020). The Rise and Rise of Regulatory Sandboxes. European Business Organization Law Review, 21(4), 705–740. https://doi.org/10.1007/s40804-020-00189-w

ISSN: 2338 4638
Volume 4 Nomor 6 (2020)

'ADALAH
Buletin Hukum & Keadilan

Konsep Ruang Siber dalam Perspektif Hukum Modern: Menimbang Ulang Kedaulatan, Yurisdiksi, dan Subjek Hukum di Era Digital

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v4i6.51075

Abstract:
Cyberspace has created a new dimension of existence that transcends the physical boundaries underlying modern law. This article examines cyberspace from theoretical and practical perspectives within contemporary legal frameworks, focusing on sovereignty, jurisdiction, and legal subjects. Using normative legal research combined with philosophical and comparative approaches, the study finds that territoriality rooted in the Peace of Westphalia is no longer effective in governing borderless digital environments. Unilateral jurisdictional claims create sovereignty conflicts and legal uncertainty, while new digital entities challenge traditional legal subject definitions. Modern law must adopt functional sovereignty and structured jurisdictional pluralism.

Keywords: *Cyberspace, Digital Sovereignty, Jurisdiction, Modern Law, Territoriality*

A. PENDAHULUAN

Ruang siber bukanlah sekadar istilah metaforis untuk menggambarkan internet. Ia merupakan sebuah domain ontologis baru yang memiliki karakteristik unik: tanpa batas geografis yang jelas, beroperasi secara real-time, dan dibangun oleh arsitektur kode yang terus berevolusi (Lessig, 2006). Kemunculannya menghadirkan tantangan eksistensial bagi fondasi hukum modern yang selama berabad-abad dibangun di atas premis teritorialitas. Dalam tradisi Westphalian, kedaulatan negara dijalankan dalam batas-batas geografis yang rigid; hukum pidana, perdata, dan administrasi semuanya bertumpu pada asas *locus delicti*, *lex loci contractus*, atau domisili subjek hukum. Namun, bagaimana hukum memposisikan dirinya ketika sebuah transaksi terjadi di dunia virtual yang servernya berada di tiga benua berbeda, atau ketika sebuah avatar anonim melakukan perbuatan melawan hukum yang dampaknya dirasakan di banyak negara?

Diskursus tentang ruang siber mencapai puncaknya pada era 1990-an ketika para pemikir seperti David Johnson dan David Post mendeklarasikan bahwa siber adalah ruang terpisah yang tidak dapat diatur oleh kedaulatan negara mana pun. Gagasan ini memicu reaksi keras dari para positivis hukum internasional yang bersikeras bahwa tidak ada ruang yang kebal hukum.

Perdebatan ini terus berlanjut hingga hari ini, dengan kompleksitas yang kian bertambah akibat munculnya teknologi *blockchain*, *metaverse*, dan organisasi otonom terdesentralisasi (*Decentralized Autonomous Organization*/*DAO*) (Wright & De Filippi, 2015). Indonesia sendiri, melalui berbagai regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), telah berupaya menjangkau ruang siber, namun upaya tersebut kerap tersandung pada persoalan fundamental: sejauh mana klaim yurisdiksi tersebut *legitimate* dalam tataran hukum internasional? (Butt & Lindsey, 2023). Rumusan masalah artikel ini adalah: Pertama, bagaimana teori hukum modern memaknai ruang siber dalam kaitannya dengan doktrin kedaulatan dan yurisdiksi? Kedua, bagaimana konsep subjek hukum mengalami pergeseran dalam konteks aktivitas di ruang siber? Tujuannya adalah menelaah kelemahan paradigma hukum teritorial serta mengusulkan kerangka pikir baru bagi hukum modern dalam mengelola realitas siber.

B. PERDEBATAN MAZHAB SIBER DAN TANGGAPAN HUKUM MODERN

Perdebatan teoretis tentang hakikat ruang siber dalam hukum dapat dipetakan ke dalam tiga mazhab utama. Pertama, mazhab *Cyber-Libertarianism*, yang dimotori oleh John Perry Barlow dengan Deklarasi Kemerdekaan Ruang Siber-nya yang provokatif. Mazhab

ini memandang ruang siber sebagai *terra nullius digital*, sebuah wilayah tak bertuan yang memiliki tatanan hukumnya sendiri yang bersumber dari kode dan norma komunitas, bukan dari paksaan negara (Barlow, 1996). Dalam perkembangannya, Johnson dan Post (1996) berargumen bahwa upaya menerapkan hukum nasional ke ruang siber bagaikan menempatkan "persegi di dalam lingkaran", sebuah ketidakcocokan fundamental. Bagi mazhab ini, pengguna yang melintasi perbatasan digital tidak bisa dianggap telah tunduk pada kedaulatan negara tujuan data, karena perpindahan terjadi tanpa kesadaran dan tanpa kehadiran fisik. Konsekuensinya, negara harus menahan diri dan membiarkan ruang siber membangun sistem regulasi mandiri melalui mekanisme pasar dan norma sosial.

Kedua, mazhab *Cyber-Realism* atau *Cyber-Paternalism*, yang dipelopori oleh Jack Goldsmith dan Tim Wu, memberikan sanggahan tajam. Menurut Goldsmith (1998), klaim bahwa ruang siber kebal terhadap yurisdiksi negara adalah ilusi. Setiap aktivitas siber, meskipun tampak virtual, memiliki dampak nyata yang terlokalisasi (*local effects*). Seorang pengguna internet secara fisik tetap berada di suatu wilayah negara, server memiliki lokasi fisik, dan transaksi digital melibatkan pengirim dan penerima nyata. Oleh karena itu, hukum nasional selalu memiliki titik taut (*nexus*) untuk mengklaim yurisdiksi berdasarkan prinsip

teritorialitas objektif, yaitu di mana akibat dari perbuatan itu dirasakan. Kegagalan penegakan hukum, menurut Goldsmith, bukan karena ketiadaan legitimasi, melainkan karena ketidakmampuan teknis dan politis untuk melakukan eksekusi.

Ketiga, mazhab Pluralisme Yurisdiksi atau Transnasionalisme, yang merepresentasikan posisi tengah. Dipengaruhi oleh pemikiran Lessig, mazhab ini mengakui bahwa ruang siber memang unik, tetapi tidak sepenuhnya steril dari regulasi. Lessig (2006) memperkenalkan tesis "Kode adalah Hukum" (*Code is Law*), yang menjelaskan bahwa arsitektur teknis ruang siber berfungsi sebagai pengatur, tetapi kode itu sendiri dapat dimodifikasi oleh pemerintah. Jadi, regulasi bukan tidak mungkin, melainkan harus dilakukan melalui penyesuaian arsitektur. Sementara itu, gagasan pluralisme yurisdiksi yang dikembangkan oleh para sarjana seperti Paul Schiff Berman menekankan perlunya kerangka hukum hibrida. Negara-negara tidak perlu berebut klaim kedaulatan absolut, melainkan harus mengembangkan mekanisme saling pengakuan, pilihan hukum (*choice of law*), dan prosedur penyelesaian sengketa yang mengakomodasi lanskap digital yang terfragmentasi. Kerangka teoretis ini menjadi pisau analisis yang sangat relevan untuk membedah persoalan hukum yang muncul dari aktivitas di ruang siber kontemporer.

C. KONSEP RUANG SIBER DAN TANTANGAN TERHADAP DOKTRIN KEDAULATAN

1. Kedaulatan dan Yurisdiksi: Dari Teritorialitas Menuju Efek

Titik paling krusial dari konsep ruang siber dalam hukum modern adalah tantangannya terhadap yurisdiksi preskriptif, adjudikatif, dan eksekutif. Hukum internasional tradisional memberikan dasar yurisdiksi melalui prinsip teritorial, nasionalitas aktif, nasionalitas pasif, perlindungan, dan universalitas (Ryngaert, 2015). Ruang siber, dengan topologinya yang datar, mengaburkan prinsip dasar ini. Coba kita telaah penerapan prinsip teritorial: di manakah locus delicti sebuah perbuatan phishing yang dilakukan oleh seorang warga negara A menggunakan server di negara B terhadap korban di negara C? Apakah locus-nya di tempat pelaku mengetik, tempat server memproses, atau tempat korban kehilangan uangnya?

Hukum modern cenderung menjawab ini dengan memperluas doktrin "efek" (*effects doctrine*). Negara akan mengklaim yurisdiksi jika ada dampak substansial di wilayahnya, terlepas dari di mana tindakan itu dimulai. Pendekatan ini digunakan secara agresif oleh yurisdiksi seperti Uni Eropa melalui GDPR-nya, yang menyatakan bahwa regulasi mereka berlaku bagi siapa pun yang

memproses data warga negara Eropa, di manapun entitas itu berada (Bradford, 2020). Inilah yang disebut *Brussels Effect*. Indonesia juga mengadopsi pendekatan serupa dalam UU ITE, di mana Pasal 2 menyatakan bahwa undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum di luar wilayah Indonesia yang memiliki akibat hukum di wilayah Indonesia. Namun, klaim unilateral ini seringkali menimbulkan konflik yurisdiksi. Ketika pengadilan Indonesia menyatakan sebuah platform global bersalah, tetapi platform tersebut tidak memiliki aset atau kehadiran di Indonesia, maka putusan itu menjadi brutum fulmen petir yang tidak menyambar apa pun.

2. Subjek Hukum Baru: Kecerdasan Buatan dan DAO

Perspektif hukum modern juga diguncang oleh kemunculan entitas-entitas di ruang siber yang tidak mudah dimasukkan ke dalam kategori subjek hukum konvensional, yaitu manusia dan badan hukum yang diakui negara. *Decentralized Autonomous Organization* (DAO) adalah contoh paling mutakhir. DAO adalah organisasi yang dijalankan oleh aturan yang dikodekan dalam smart contract, tanpa struktur hierarkis tradisional. Ketika DAO melakukan transaksi atau menimbulkan kerugian pada pihak ketiga, siapakah yang bertanggung jawab secara hukum? Apakah para pengembang kode, pemegang token, atau DAO itu

sendiri? Beberapa yurisdiksi seperti Negara Bagian Wyoming di Amerika Serikat telah mulai mengakui DAO sebagai badan hukum terbatas (*Limited Liability Autonomous Organization*), sebuah pergeseran paradigma yang signifikan (Nielsen & de Vilder, 2023).

Hal serupa terjadi dengan kecerdasan buatan. Muncul perdebatan tentang pemberian personalitas elektronik (*electronic personhood*) untuk AI yang sangat otonom. Gagasan ini didiskusikan secara serius dalam resolusi Parlemen Eropa tahun 2017, meskipun kemudian menuai kontroversi hebat. Di Indonesia, doktrin subjek hukum masih terpaku pada *natuurlijke persoon* dan *rechts persoon*. Akibatnya, kecelakaan atau kerugian yang disebabkan oleh sistem AI otonom sulit dicari pertanggungjawabannya, karena rantai kausalitasnya terputus di antara desainer, produsen, pemilik, dan pengguna. Ruang siber telah melahirkan agensi non-manusia yang mendesak hukum modern untuk berevolusi.

D. SENGKETA KONTEN LINTAS BATAS DAN DILEMA EKSEKUSI

Perhatikan kasus Google v. Equustek Solutions Inc. (2017) yang melibatkan yurisdiksi Kanada dan Amerika Serikat. Kasus ini bermula dari sengketa paten antara Equustek dan Datalink, di mana Datalink

menggunakan Google untuk menjual produk yang diduga melanggar paten. Pengadilan Kanada mengeluarkan injunction yang memerintahkan Google untuk tidak hanya menghapus tautan di Google Kanada, tetapi juga di seluruh domain globalnya (*de-indexing order*). Google melawan, dengan alasan bahwa perintah tersebut melanggar kedaulatan yurisdiksi lain. Mahkamah Agung Kanada menolak argumen ini dengan alasan bahwa internet tidak mengenal batas, sehingga perintah pengadilan juga tidak dapat dibatasi oleh batas geografis untuk menjadi efektif. Sebaliknya, Pengadilan Distrik Amerika Serikat kemudian memberikan *injunction* yang memblokir eksekusi putusan Kanada tersebut di AS, dengan pertimbangan bahwa perintah Kanada itu melanggar *First Amendment* (kebebasan berbicara) yang dijunjung tinggi di AS. Dua negara yang sama-sama modern secara hukum menghasilkan sikap yang bertentangan diametral terhadap satu fakta siber yang sama. Ini adalah potret kegagalan hukum modern yang berbasis pada negara-bangsa dalam mengelola ruang siber secara koheren.

E. REKONSTRUKSI KONSEP RUANG SIBER MENUJU HUKUM TRANSNASIONAL YANG FUNGSIONAL

Perspektif hukum modern dalam menghadapi tantangan era digital harus bergeser secara fundamental

dari perdebatan klasik yang diwakili oleh analogi *law of the horse* yang dikemukakan oleh Hakim Frank Easterbrook yang meremehkan hukum siber sebagai bidang spesifik yang tidak memerlukan kerangka hukum tersendiri, sama seperti tidak perlunya hukum khusus tentang kuda menuju pengakuan yang lebih matang bahwa ruang siber, dengan karakteristiknya yang lintas batas, terdesentralisasi, dan anonim, memerlukan kerangka hukum transnasional yang unik dan tidak dapat begitu saja dipaksakan ke dalam kategori hukum tradisional. Kekeliruan dalam analogi *law of the horse* terletak pada anggapan bahwa prinsip-prinsip hukum umum sudah cukup untuk menjangkau fenomena digital, padahal kompleksitas teknis, kecepatan perubahan, dan dimensi global dari internet menuntut pendekatan hukum yang lebih spesifik dan adaptif.

Pertama, dalam kerangka baru ini, doktrin kedaulatan teritorial yang selama ini menjadi fondasi hukum internasional harus dilengkapi dengan doktrin fungsionalitas, yaitu pendekatan yang menekankan pada fungsi dan dampak dari aktivitas digital, bukan semata-mata pada lokasi fisik server atau aliran data. Artinya, negara tidak perlu lagi memperdebatkan kedaulatan atas bit-bit data yang melintas secara maya melintasi perbatasan tanpa bentuk fisik, tetapi cukup berdaulat atas dampak nyata yang ditimbulkan oleh aktivitas digital tersebut serta atas infrastruktur kritis seperti

pusat data, kabel serat optik, dan menara telekomunikasi yang secara fisik berada di wilayah teritorialnya. Dengan demikian, kedaulatan data atau *data sovereignty* harus dimaknai ulang secara lebih cerdas dan proporsional, bukan lagi sebagai upaya pembendungan yang kaku melalui kebijakan *data localization absolut* yang mewajibkan semua data disimpan di dalam negeri dengan alasan keamanan semata, melainkan sebagai hak negara untuk menetapkan standar enkripsi, keamanan siber, dan tata kelola data yang bersifat ekstrateritorial melalui mekanisme perjanjian bilateral atau multilateral dengan negara mitra (Greenleaf, 2022). Pendekatan ini memungkinkan negara tetap memiliki kendali atas data warganya tanpa harus mengorbankan manfaat dari arus data lintas batas yang menjadi urat nadi ekonomi digital global, sekaligus menciptakan keseimbangan antara perlindungan hak privasi dan kebutuhan inovasi teknologi yang tidak mengenal batas negara.

Kedua, pengakuan terhadap *lex electronica* atau *lex digitalis* sebagai tatanan normatif semi-otonom harus dipertimbangkan. Ini bukan berarti menciptakan hukum tanpa negara, melainkan menciptakan sistem di mana sengketa ruang siber diselesaikan melalui mekanisme arbitrase daring global yang keputusannya dapat dieksekusi secara otomatis melalui teknologi *smart contract*. Dengan cara ini, problem brutum fulmen dapat diatasi. Indonesia, sebagai anggota G20 yang tengah

mendorong identitas kependudukan digital, memiliki posisi tawar untuk mempelopori kerjasama multilateral tentang yurisdiksi siber di tingkat ASEAN dan global.

F. KESIMPULAN

Konsep ruang siber, dengan karakteristiknya yang melampaui batas (*borderless*), telah mengoyak fondasi fundamental hukum modern, khususnya doktrin kedaulatan dan teritorialitas yang menjadi pilar sistem hukum Westphalian. Analisis di atas menunjukkan bahwa upaya hukum modern untuk memaksakan yurisdiksi teritorial secara unilateral ke ruang siber hanya menghasilkan konflik kedaulatan, ketidakpastian hukum, dan putusan yang tidak dapat dieksekusi. Mazhab pluralisme yurisdiksi menawarkan jalan keluar yang lebih elegan melalui pengakuan atas legitimasi ganda dan kebutuhan akan koordinasi transnasional. Menjawab rumusan masalah, pemaknaan ruang siber dalam hukum saat ini tidak lagi dapat mengandalkan paradigma analogi geografis, melainkan harus bergeser pada efek dan fungsionalitas. Sementara itu, subjek hukum tidak lagi hanya manusia dan korporasi tradisional, tetapi mulai mencakup entitas kode seperti DAO dan beberapa kasus AI dengan level otonomi tinggi.

Sebagai rekomendasi, Indonesia perlu merumuskan kebijakan yurisdiksi siber yang tidak hiperteritorial, serta terlibat aktif dalam menyusun konvensi internasional tentang yurisdiksi dan penegakan hukum siber. Selain itu, kurikulum fakultas hukum di Indonesia sudah saatnya secara serius mengintegrasikan mata kuliah Filsafat Hukum Siber dan Hukum Kode untuk menghasilkan sarjana hukum yang tidak hanya paham norma, tetapi juga melek arsitektur digital.

REFERENCE:

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Butt, S., & Lindsey, T. (2023). Indonesian Law: Continuity and Change. Oxford University Press.

Goldsmith, J. L. (1998). Against Cyberanarchy. University of Chicago Law Review, 65(4), 1199–1250. https://doi.org/10.2307/1600262

Greenleaf, G. (2022). Asian Data Privacy Laws: The Unfulfilled Promise of Regional Agreements.

International Data Privacy Law, 12(3), 189–210. https://doi.org/10.1093/idpl/ipac008

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review, 48(5), 1367–1402. https://doi.org/10.2307/1229390

Lessig, L. (2006). Code: Version 2.0. Basic Books.

Nielsen, T., & de Vilder, P. (2023). DAO Entity Recognition: A New Frontier in Corporate Law. Journal of Emerging Technologies and Law, 4(2), 102–125.

Ryngaert, C. (2015). Jurisdiction in International Law (2nd ed.). Oxford University Press.

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2580664

ISSN: 2338 4638
Volume 4 Nomor 6 (2020)

'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

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 menegakkan 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 mengekspor 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.