

**PENGENDALIAN DATA PRIBADI DAN RUANG SIBER OLEH
PLATFORM DIGITAL BIG DATA GLOBAL TERKAIT KEDAULATAN
DIGITAL INDONESIA**

Yokotani, A. Cery Kurnia, Wirazilmustaan, Reko Dwi Salfutra
Fakultas Hukum Universitas Bangka Belitung
andicery@gmail.com

Abstract

The development of global digital technology has brought significant challenges to Indonesia's digital sovereignty, especially regarding the control of personal data and cyberspace. Foreign digital platforms that dominate use in Indonesia process citizens' data massively through big data mechanisms, often outside the jurisdiction of national law. This dependence poses risks to personal data protection, national security, and state control over digital infrastructure. This study uses normative legal methods with a legislative and conceptual approach to examine the role of national regulations, such as Law Number 27 of 2022 concerning Personal Data Protection, in strengthening the state's position. The results of the study show that strengthening regulations, developing local technology, community digital literacy, and international cooperation are key strategies to uphold Indonesia's digital sovereignty. Without concrete and comprehensive steps, control over data and digital space will continue to be in the hands of foreign entities, which can weaken the nation's independence in the digital era.

Keywords: *Personal Data, Cyber, Big Data, Digital Sovereignty*

Ringkasan

Perkembangan teknologi digital global telah membawa tantangan signifikan terhadap kedaulatan digital Indonesia, terutama terkait pengendalian data pribadi dan ruang siber. Platform digital asing yang mendominasi penggunaan di Indonesia memproses data warga negara secara masif melalui mekanisme *big data*, sering kali di luar yurisdiksi hukum nasional. Ketergantungan ini menimbulkan risiko terhadap perlindungan data pribadi, keamanan nasional, dan kendali negara atas infrastruktur digital. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual untuk mengkaji peran regulasi nasional, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dalam memperkuat posisi negara. Hasil kajian menunjukkan bahwa penguatan regulasi, pengembangan teknologi lokal, literasi digital masyarakat, dan kerja sama internasional menjadi strategi kunci untuk menegaskan kedaulatan digital Indonesia. Tanpa langkah konkret dan menyeluruh, kontrol atas data dan ruang digital akan terus berada di tangan entitas asing, yang dapat melemahkan kemandirian bangsa di era digital.

Kata Kunci: Data Pribadi, Siber, Big Data, Kedaulatan Digital



A. Pendahuluan

Insiden serangan siber yang menargetkan Indonesia telah menunjukkan eskalasi dari tahun ke tahun. Pusat Operasi Keamanan Siber Nasional BSSN telah mengamati fenomena ini. Dalam konteks upaya pelanggaran data yang terjadi antara Januari dan Agustus 2020, 190 juta serangan siber yang mengejutkan didokumentasikan, di samping 36.771 akun data yang dikompromikan di berbagai sektor, terutama termasuk domain keuangan. Insiden serangan siber yang tercatat telah menunjukkan peningkatan lima kali lipat dibandingkan dengan tahun 2019. Dalam lanskap teknologi digital kontemporer, kejahatan siber tidak hanya mampu melanggar keamanan data dan informasi pribadi tetapi juga mengganggu usaha ekonomi dan komersial, membahayakan infrastruktur, dan berpotensi menimbulkan ancaman terhadap stabilitas keamanan nasional. Tren eskalasi berlanjut hingga tahun 2021 (Falkner, 2024).

Kaspersky, organisasi keamanan siber yang mapan, menunjukkan bahwa 40% konsumen

di kawasan Asia Pasifik telah berurusan dengan situasi yang melibatkan pelanggaran data pribadi yang dimulai oleh pihak yang tidak disetujui (Falkner, 2024). Sebagaimana yang tertuang dalam Peraturan Presiden 28/2021, Pasal (2) dan (3), BSSN ditetapkan sebagai lembaga yang bertugas membantu Presiden (Pemerintah) dalam hal keamanan siber. Lembaga ini bertugas merumuskan standar dan melakukan pengawasan, mengingatkan aktivitas digital warga negara tidak lepas dari pengelolaan data pribadi. Pemanfaatan data pribadi memerlukan kerangka tata kelola yang kuat dan akuntabel. Regulasi yang komprehensif, ketat, dan tegas menjadi keharusan. Bersamaan dengan itu, kesiapan sumber daya manusia yang cerdas, tangguh, dan adaptif juga sangat dibutuhkan.

Laporan dari *We Are Social* memprediksikan bahwa jumlah pengguna internet di seluruh dunia akan tumbuh hingga 5 miliar pada tahun 2023. Dalam konteks Indonesia, angka ini mencapai 212,9 juta. Individu-individu ini disebut sebagai netizen. Kekhawatiran yang

cukup besar muncul dari sifat dunia maya yang tidak terbatas. *Platform* digital yang paling banyak digunakan oleh netizen Indonesia sebagian besar berasal dari luar negeri. Indonesia, sebagai sebuah negara, memiliki ciri khas yang luas (Jansen, 2024). Penegakan kontrol teritorial dan kedaulatan fisik dari Sabang sampai Merauke, serta dari Pulau Miangas sampai Pulau Rote, menimbulkan tantangan yang cukup besar. Negara kepulauan ini terdiri dari lebih dari 17.000 pulau yang dikelilingi oleh lautan yang luas. Penyatuan, pelestarian, dan penegakan kedaulatan fisik di seluruh daratan, perairan, dan ruang udara Indonesia memerlukan upaya yang sangat besar dari para pendiri negara hingga saat ini. Lebih jauh, masalah kedaulatan dalam domain digital, yang dapat diakses dari lokasi mana pun, juga menghadirkan tantangan yang tidak kalah berat (Jansen, 2024).

Konstitusi, sebagaimana yang diuraikan dalam Pasal 33 Undang-Undang Dasar 1945, menyatakan bahwa "Bumi, air, dan kekayaan alam yang terkandung di dalamnya dikuasai oleh negara dan

dipergunakan untuk sebesar-besar kemakmuran rakyat." Meskipun demikian, pelestarian sumber daya tersebut tidak hanya memerlukan kerangka regulasi dan pengawasan fisik, tetapi juga pengawasan negara yang cermat, suatu tugas yang telah terbukti rumit dan berat. Meskipun telah mencapai 78 tahun kedaulatan, tujuan yang diuraikan dalam Pasal 33 belum sepenuhnya terwujud dengan baik. Munculnya era digital telah menghadirkan tantangan baru, khususnya yang menyangkut keamanan data pribadi, di mana insiden pelanggaran dan serangan siber telah melonjak frekuensinya karena karakter lanskap digital yang tidak terbatas (Hafid *et al.*, 2023).

Di era digital saat ini, data pribadi telah menjadi komoditas bernilai tinggi yang dimanfaatkan oleh berbagai *Platform* digital global. Pengumpulan dan pengolahan data dalam skala besar (*big data*) oleh perusahaan-perusahaan teknologi multinasional menciptakan tantangan serius bagi kedaulatan digital suatu negara, termasuk Indonesia. Ketergantungan terhadap *Platform* masing membuat data warga negara

Indonesia tersimpan dan dikelola di luar yurisdiksi nasional, sehingga berpotensi mengancam perlindungan data pribadi, keamanan nasional, dan kendali negara atas ruang sibernya sendiri (Fratini, 2024).

Meskipun Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai bentuk penguatan regulasi, pengawasan terhadap pengendalian data oleh entitas global masih lemah. Dalam konteks ini, kedaulatan digital Indonesia dipertaruhkan apabila tidak ada kebijakan tegas yang membatasi dominasi *Platform* digital asing dalam mengakses dan memanfaatkan data masyarakat Indonesia.

Keterkaitan yang ditimbulkan oleh infrastruktur digital telah membentuk jaringan global di mana komputer, dan sebagai perluasannya, individu, saling terhubung secara sosial, ekonomi, dan politik. Transformasi ini telah memfasilitasi migrasi berbagai aktivitas dari ranah nyata ke ranah digital, yang mengakibatkan penambahan waktu yang dialokasikan untuk dunia maya, yang kini telah menjadi komponen

penting dari keberadaan yang sebenarnya. Dalam kerangka ini, bentuk kekuasaan baru yang disebut instrumen arianisme berfungsi secara asimetris melalui *Platform* global. Perilaku digital individu diubah menjadi data penting oleh perusahaan teknologi, yang kemudian mengkomodifikasi data ini sebagai aset ekonomi yang berharga (Bakhtiar, 2023). Zaman kapitalisme pengawasan ini telah menempatkan individu dalam kondisi yang rentan, karena informasi digital pribadi mereka diatur dan diproses oleh perusahaan multinasional untuk tujuan kapitalis, dengan Google menjadi ilustrasi yang menonjol.

Kapitalisme pengawasan merupakan perwujudan kontemporer dari keserakahan intrinsik kapitalisme, di mana penekanannya telah beralih dari dominasi sumber daya keuangan dan tanah ke hegemoni atas data dan dunia maya. Tujuan utamanya tetap tidak berubah: untuk secara efektif menjalankan kendali atas kehidupan individu. Transisi ini telah membuat penegakan undang-undang kejahatan dunia maya semakin rumit, karena data yang

diperlukan untuk pembuktian hukum sering kali tersebar dan diatur oleh perusahaan yang beroperasi di bawah kerangka hukum nasional yang berbeda, sehingga menghambat akses penegakan hukum (Fauzi, 2024). Lebih jauh lagi, pemanfaatan teknologi digital terhubung erat dengan dilema politik dan hukum, yang selanjutnya memperkeruh upaya untuk mencapai kedaulatan digital dan menerapkan hukum secara efektif dalam konteks tantangan yang muncul ini.

Penggunaan *Platform* teknologi digital asing berarti menyerahkan dan mempercayakan data warga negara pengguna teknologi tersebut untuk dipantau dan diolah oleh perusahaan asing tersebut, sekaligus tunduk pada hukum negara asal perusahaan tersebut. Oleh karena itu, kemandirian teknologi sangat penting bagi negara besar seperti Indonesia. Tanpa itu, kedaulatan digital yang terkait dengan kepentingan negara sulit dicapai.

Dampak dari lemahnya kedaulatan digital dan penegakan hukum di dunia maya bisa jadi mandul. Konten dan tindakan yang

jelas-jelas merupakan kejahatan dunia maya tidak bisa dihukum karena sulitnya mengakses data pelaku atau karena pelakunya berada di negara lain. Sudah saatnya kedaulatan digital diperkuat. Caranya, selain dengan mengkaji ulang regulasi, juga harus banyak menggalakkan kerja sama dengan negara lain yang memiliki masalah yang sama. Tujuannya, agar penegak hukum bisa mengakses data yang dikuasai perusahaan global dengan mudah. Selain itu, perlu juga dikembangkan teknologi digital yang mandiri agar data benar-benar diolah dan ditempatkan di dalam negeri.

B. Metode Penelitian

Penelitian ini menggunakan metode hukum normatif, yaitu suatu proses untuk menemukan kaidah hukum, asas hukum, atau doktrin hukum guna menjawab permasalahan hukum yang dihadapi. Untuk mendapatkan jawaban dan menyelesaikan permasalahan hukum dari penelitian ini, digunakan pendekatan pemecahan masalah yaitu pendekatan perundang-undangan dan pendekatan konseptual.

C. Pembahasan

Di era digital saat ini, data pribadi telah menjadi komoditas strategis yang memiliki nilai ekonomi dan geopolitik tinggi. Perusahaan-perusahaan teknologi global seperti Google, Meta, Amazon, Microsoft, dan lainnya berperan dominan dalam mengumpulkan, memproses, dan mengeksploitasi data pribadi pengguna di berbagai negara, termasuk Indonesia. Aktivitas ini melibatkan pemrosesan data dalam jumlah besar (*big data*) yang dikumpulkan melalui *Platform* digital seperti media sosial, mesin pencari, aplikasi layanan daring, dan perangkat *Internet of Things* (IoT) (Hafid, 2023). Dominasi ini menyebabkan terjadinya *data colonialism*, yaitu praktik di mana perusahaan asing mengeksploitasi data dari suatu negara untuk kepentingan korporasi tanpa adanya pengembalian manfaat yang setara bagi negara asal data. Dalam konteks Indonesia, hal ini memperlihatkan lemahnya kontrol atas arus data yang keluar masuk dari dan ke dalam wilayah hukum nasional, serta menciptakan ketergantungan

terhadap infrastruktur dan layanan digital global (Yuniarti, 2020).

Kedaulatan digital adalah konsep bahwa suatu negara memiliki hak dan kontrol penuh atas data, infrastruktur digital, serta regulasi ruang siber dalam yurisdiksi nasionalnya. Dalam praktiknya, kedaulatan digital mencakup perlindungan data pribadi warga negara, kontrol terhadap infrastruktur digital (server, jaringan, pusat data), serta kemampuan negara untuk menetapkan aturan main di ruang digital. Namun, dominasi *Platform* digital asing mengancam kedaulatan ini. Sebagai contoh, data pribadi warga Indonesia disimpan di luar negeri, diproses dengan algoritma asing, dan digunakan untuk kepentingan yang tidak sepenuhnya transparan atau sesuai dengan kepentingan nasional. Ketergantungan pada *Platform* seperti WhatsApp, Facebook, TikTok, dan Google menjadikan negara kehilangan otonomi dalam menentukan arah transformasi digital yang inklusif dan berdaulat (Yehizkia, 2024).

Lebih lanjut, dalam situasi tertentu, negara bahkan tidak memiliki akses terhadap data tersebut tanpa melalui prosedur internasional yang rumit. Hal ini tidak hanya mengganggu perlindungan hak-hak digital warga negara, tetapi juga membahayakan keamanan nasional jika data strategis jatuh ke tangan pihak yang tidak berkepentingan. Pemerintah Indonesia telah berupaya mengatasi masalah ini melalui regulasi, antara lain dengan disahkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini menjadi tonggak penting dalam membangun sistem hukum perlindungan data yang komprehensif dan memberikan landasan hukum bagi individu atas hak atas privasi dan kendali terhadap data pribadinya (Rasji, 2024).

UU PDP juga mengatur tentang kewajiban penyelenggara sistem elektronik (PSE) dalam menjaga keamanan data, termasuk kewajiban penempatan pusat data (*data localization*) untuk data strategis. Regulasi ini merupakan langkah afirmatif dalam menegakkan

kedaulatan data, walaupun tantangan implementasi masih besar, terutama dari sisi teknis, sumber daya manusia, dan kepatuhan *Platform* asing terhadap peraturan nasional (Rizal, 2023). Selain Undang-Undang Perlindungan Data Pribadi, Indonesia juga menerapkan beberapa kebijakan pendukung, seperti Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mengatur klasifikasi data dan kewajiban PSE untuk menjaga keamanannya. Namun demikian, regulasi ini masih menghadapi kendala karena sebagian besar PSE asing tetap beroperasi tanpa menempatkan server di Indonesia, atau bahkan tidak mendaftarkan diri sesuai ketentuan.

Salah satu masalah utama dalam pengendalian ruang siber oleh negara adalah keterbatasan yurisdiksi terhadap perusahaan digital multinasional. *Platform* global sering kali beroperasi lintas negara tanpa kehadiran fisik yang jelas di Indonesia, sehingga menyulitkan proses penegakan hukum. Hal ini diperparah oleh posisi tawar negara berkembang yang lemah terhadap

raksasa digital yang memiliki kekuatan ekonomi dan politik besar. Dalam konteks ini, Indonesia membutuhkan pendekatan multilateral dan kerja sama internasional untuk mendorong kepatuhan korporasi global terhadap norma dan aturan nasional. Salah satu pendekatan adalah melalui partisipasi aktif dalam forum internasional seperti G20 *Digital Economy Working Group*, ASEAN *Digital Ministers Meeting* (ADGMIN), dan kerja sama bilateral dalam bidang perlindungan data dan keamanan siber (Ainul, 2025).

Selain itu, penguatan lembaga pengawas data seperti Otoritas Pelindung Data Pribadi (yang dirancang dalam UU PDP) menjadi sangat penting untuk menjamin adanya mekanisme pengawasan dan sanksi yang efektif terhadap pelanggaran yang dilakukan oleh penyelenggara sistem, baik lokal maupun asing. Pengendalian data pribadi tidak hanya bersifat regulatif, tetapi juga teknologis. Indonesia perlu mendorong pengembangan infrastruktur digital nasional seperti pusat data dalam negeri, sistem

enkripsi lokal, dan *Platform* digital buatan dalam negeri. Pembangunan cloud lokal seperti yang dilakukan oleh Telkom melalui *Neucentrix*, serta rencana pembangunan pusat data oleh pemerintah di beberapa lokasi strategis, adalah langkah awal yang patut diapresiasi.

Selain itu, diperlukan dukungan terhadap *startup* dan inovator digital lokal agar mampu bersaing dengan layanan global, terutama dalam hal aplikasi komunikasi, pembayaran digital, media sosial, dan *e-commerce*. Tanpa keberadaan alternatif lokal yang kuat, masyarakat akan tetap tergantung pada *Platform* asing, yang pada akhirnya memperlemah kedaulatan digital bangsa (Bokolo, 2025).

Transformasi digital yang berdaulat juga membutuhkan penguatan literasi digital masyarakat. Warga negara harus memiliki pemahaman tentang pentingnya perlindungan data, risiko pelanggaran privasi, dan bagaimana menggunakan teknologi secara aman dan bertanggung jawab. Ini akan membangun ketahanan digital dari bawah dan memperkuat posisi negara

dalam menghadapi tekanan global. Pengendalian ruang siber dan data pribadi perlu dimasukkan secara eksplisit dalam strategi nasional, termasuk dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN), kebijakan keamanan nasional, serta diplomasi luar negeri. Kedaulatan digital bukan sekadar isu teknis, tetapi juga menyangkut ideologi, kedaulatan hukum, dan keadilan sosial (Nainggolan, 2023).

Dalam strategi keamanan siber nasional, perlu ada sinergi antara sektor publik, swasta, dan masyarakat sipil dalam menjaga ruang siber yang aman, terbuka, dan inklusif. Pengembangan talenta digital, pusat riset keamanan siber, serta kolaborasi dengan negara mitra dapat memperkuat posisi Indonesia dalam menghadapi dominasi *big data* global.

Indonesia juga dapat belajar dari pendekatan negara-negara seperti Uni Eropa yang menetapkan *General Data Protection Regulation* (GDPR) sebagai model perlindungan data global yang bersifat mengikat bagi semua entitas yang memproses data

warga Eropa, termasuk perusahaan asing. Strategi semacam ini dapat menginspirasi penguatan instrumen hukum Indonesia agar lebih berani dalam menegakkan prinsip kedaulatan digital (Dewi, 2024).

D. Penutup

Pengendalian data pribadi dan ruang siber oleh *Platform* digital *big data* global telah menimbulkan tantangan serius bagi kedaulatan digital Indonesia. Ketergantungan terhadap layanan asing, lemahnya yurisdiksi hukum terhadap entitas global, serta kurangnya infrastruktur dan inovasi lokal menjadi hambatan utama dalam memastikan kendali negara atas data warganya. Meski pemerintah telah merespons melalui regulasi seperti Undang-Undang Perlindungan Data Pribadi, implementasi yang kuat dan kolaboratif masih sangat dibutuhkan. Untuk menjaga kedaulatan digital secara utuh, Indonesia harus memperkuat regulasi, teknologi, literasi digital, serta mendorong kemandirian digital nasional secara menyeluruh.

DAFTAR PUSTAKA

- Ainul, A. A., Asbullah, K., Nugraha, F., & Kunci, K. (2025). Aplikasi Domestik Sebagai Instrumen Kedaulatan Digital Dan Keamanan Nasional: Studi Strategis Atas Pendekatan Tiongkok. *JIMR: Journal Of International Multidisciplinary Research JIMR*, 4(01), 21–36. <https://doi.org/10.62668/jimr.v4i01.934>
- Bakhtiar Darmawan, A., Saadah, K., & Putu Arya Aditia Utama, dan I. (2023). Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google. *Jurnal Hubungan Internasional*, 16(1), 211–228.
- Bokolo, A. Jnr. (2025). Implementing Digital Sovereignty to Accelerate Smarter Mobility Solutions in Local Communities. *Smart Cities*, 8(4), 106. <https://doi.org/10.3390/smartcities8040106>
- Dewi, D. P., & Nugroho, B. Y. (2024). The Influencing Factor of Big Data Adoption for Indonesia Open Government. *Journal La Sociale*, 5(3), 701–711. <https://doi.org/10.37899/journal-la-sociale.v5i3.1151>
- Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. In *Journal of European Public Policy* (Vol. 31, Issue 8, pp. 2099–2120). Routledge. <https://doi.org/10.1080/13501763.2024.2358984>
- Fauzi, E., Citra, H., Marwenny, E., & Alfitrianti, N. (2024). Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty. *JIEE: Jurnal Ilmiah Ekotrans & Erudisi*, 4(1), 149–157.
- 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>
- Hafid, M., Firjatullah, F. Z., Pamungkaz, B. W., Magister, P. S., Hukum, I., Wijaya, U., & Surabaya, K. (2023). Tantangan Menghadapi Kejahatan Cyber dalam

- Kehidupan Bermasyarakat dan Bernegara. *Jurnal Pendidikan Tambusai*, 7(2), 9548–9556.
- Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4). <https://doi.org/10.1016/j.giq.2023.101862>
- Nainggolan, B. (2023). Legal Dynamics in the Digital Era: Navigating the Impact of Digital Transformation on Indonesian Society. *Law Development Journal*, 1, 714–728.
- Rasji dan Muhammad Yogi Septiyan Priyono. (2024). Tantangan Terhadap Privasi Dan Kebebasan Berpendapat Di Indonesia Pada Era Digital: Analisis Pandangan Filsafat Hukum. *Rewang Rencang: Jurnal Hukum Lex Generalis*, 5(10), 1–9.
- Rizal, M., & Setyoningsih, E. V. (2023). Perlindungan Konsumen dalam Pemanfaatan Big Data oleh Pelaku Bisnis di Indonesia: Tinjauan Terhadap Regulasi dan Implementasi Praktik Bisnis. *Jurnal Penegakan Hukum Dan Keadilan*, 4(1), 75–85. <https://doi.org/10.18196/jphk.v4i1.15189>
- Yehizkia, B., Kristalia, Y., & Wibisono, I. W. (2024). Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital. *Jurnal Jukim*, 3(2), 83–93. <https://doi.org/10.56127/jukim.v3i02>
- Yuniarti, S., & Herawati, D. E. (2020). Analisis Hukum Kedaulatan Digital Indonesia. *Pandecta*, 15(2), 154–166. <https://doi.org/10.15294/pandecta.v15i2.18293>