Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

Analisis Perbandingan Kerangka Hukum untuk Keamanan Siber dan Perlindungan Data antara Vietnam dan Indonesia

Nguyen Minh Tri[1], Ho Tran Bao Tram[2]
[1]Faculty of International Relations & Communications, Ho Chi Minh City University of Foreign Languages – Information Technology, Vietnam.
[2]Faculty of Law, Nguyen Tat Thanh University, Vietnam

Corresponding author: Nguyen Minh Tri
Email: trinm@huflit.edu.vn

Abstract
This study examines the comparative legal frameworks governing cybersecurity and personal data protection in Vietnam and Indonesia within the context of rapid digital transformation in Southeast Asia. Previous studies on cybersecurity governance in ASEAN have mainly focused on regulatory implementation and digital security issues, while paying limited attention to how differences in governance philosophy shape cybersecurity regulation and enforcement across countries with contrasting political systems. Addressing this gap, the study compares Vietnam's centralized, security-oriented governance model with Indonesia's more decentralized, rights-based regulatory approach, influenced by international standards such as the European Union's General Data Protection Regulation (GDPR). This research employs a normative legal research approach combined with comparative legal analysis. Primary data consist of laws, decrees, and government regulations related to cybersecurity and personal data protection in both countries. In contrast, secondary data include academic literature, policy reports, and international publications on digital governance in Southeast Asia. The data are analyzed qualitatively to identify differences in regulatory structures, institutional arrangements, enforcement mechanisms, and policy orientations. The findings reveal that Vietnam prioritizes national security, political stability, and strong state control over cyberspace. In contrast, Indonesia emphasizes personal data protection, digital economic integration, and regulatory alignment with international norms despite fragmented institutional coordination. This study argues that cybersecurity governance in Southeast Asia is shaped not only by technological challenges but also by broader state philosophies concerning sovereignty, authority, and citizen rights in the digital era. The study contributes theoretically to comparative digital governance research by introducing a governance-philosophy perspective for understanding cybersecurity regulation in emerging digital states.

Keywords: *Legal Framework; Cybersecurity; Data Protection; Vietnam; Indonesia*

Abstrak
Studi ini meneliti kerangka hukum komparatif yang mengatur keamanan siber dan perlindungan data pribadi di Vietnam dan Indonesia dalam konteks transformasi digital yang cepat di Asia Tenggara. Studi sebelumnya tentang tata kelola keamanan siber di ASEAN sebagian besar berfokus pada implementasi peraturan dan isu keamanan digital, sementara hanya sedikit memperhatikan bagaimana perbedaan filosofi tata kelola membentuk regulasi dan penegakan keamanan siber di berbagai negara dengan sistem politik yang berbeda. Untuk mengatasi kesenjangan ini, studi ini membandingkan model tata kelola terpusat dan berorientasi keamanan Vietnam dengan pendekatan regulasi berbasis hak yang lebih terdesentralisasi di Indonesia, yang dipengaruhi oleh standar internasional seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa. Penelitian ini menggunakan pendekatan penelitian hukum normatif yang dikombinasikan dengan analisis hukum komparatif. Data primer terdiri dari undang-undang, dekrit, dan peraturan pemerintah yang berkaitan dengan keamanan siber dan perlindungan data pribadi di kedua negara. Sebaliknya, data sekunder mencakup literatur akademis, laporan kebijakan, dan publikasi internasional tentang tata kelola digital di Asia Tenggara. Data dianalisis secara kualitatif untuk mengidentifikasi perbedaan dalam struktur regulasi, pengaturan kelembagaan, mekanisme penegakan hukum, dan orientasi kebijakan. Temuan menunjukkan bahwa Vietnam memprioritaskan keamanan nasional, stabilitas politik, dan kontrol negara yang kuat atas dunia maya. Sebaliknya, Indonesia menekankan perlindungan data pribadi, integrasi ekonomi digital, dan keselarasan regulasi dengan norma internasional meskipun koordinasi kelembagaan masih terfragmentasi. Studi ini berpendapat bahwa tata kelola keamanan siber di Asia Tenggara dibentuk tidak hanya oleh tantangan teknologi tetapi juga oleh filosofi negara yang lebih luas mengenai kedaulatan, otoritas, dan hak warga negara di era digital. Studi ini memberikan kontribusi teoritis

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

pada penelitian tata kelola digital komparatif dengan memperkenalkan perspektif filosofi tata kelola untuk memahami regulasi keamanan siber di negara-negara digital yang sedang berkembang.

Kata Kunci: Kerangka Hukum; Keamanan Siber; Perlindungan Data; Vietnam; Indonesia

Pendahuluan

Asia Tenggara saat ini sedang mengalami transformasi digital struktural, yang membentuk kembali seluruh ekosistem ekonomi dan sosial negara-negara anggotanya. Dengan lokasi geostrategisnya yang krusial, kawasan ini mencapai tingkat penetrasi internet sebesar 80% pada tahun 2022, meletakkan fondasi yang kokoh untuk ekonomi digital yang mencapai sekitar US$100 miliar pada tahun 2023 (Ha & Chuah, 2023; L. Q. T. Tran et al., 2022). Namun, di samping manfaat ekonomi yang sangat besar ini, peningkatan tingkat digitalisasi juga menjadikan kawasan ini sebagai target utama jaringan kejahatan siber dan kampanye spionase yang disponsori negara. Analisis menunjukkan bahwa dari tahun 2021 hingga 2022, kejahatan siber di Asia Tenggara mencatat peningkatan dramatis sebesar 82% (Prawiyogi & Alwiyah, 2023). Dalam konteks yang lebih luas ini, Vietnam dan Indonesia, sebagai dua negara dengan ekonomi yang paling cepat mengalami digitalisasi dan populasi terbesar, secara konsisten termasuk di antara negara-negara yang paling banyak menjadi target.

Lanskap geopolitik di Asia Tenggara semakin memperumit tantangan keamanan siber. Meningkatnya ketegangan geopolitik, khususnya aktivitas kelompok peretas yang terkait dengan kekuatan besar, telah menimbulkan tantangan eksistensial terhadap kedaulatan nasional. Laporan menunjukkan bahwa serangan siber yang terkait dengan Tiongkok yang menargetkan negara-negara Asia Tenggara meningkat sebesar 20% pada akhir tahun 2022 dibandingkan tahun sebelumnya (Antoniuk, 2024; Kelliher, 2024). Targetnya meluas melampaui pemerasan finansial hingga mencakup infiltrasi server pemerintah untuk mencuri informasi email sensitif, yang secara langsung mengancam keamanan nasional negara-negara seperti Vietnam, Indonesia, Malaysia, dan Thailand (UNCDF, 2021). Menghadapi ancaman non-tradisional ini, negara-negara Asia Tenggara terpaksa meninggalkan pendekatan regulasi mereka yang longgar sebelumnya dan membangun kerangka hukum keamanan siber yang lebih proaktif, kuat, dan komprehensif.

Vietnam dan Indonesia, meskipun memiliki tujuan bersama untuk melindungi keamanan siber dan mempromosikan ekonomi digital, menerapkan pendekatan hukum dan struktur tata kelola yang menunjukkan perbedaan mendasar. Kerangka hukum Vietnam ditandai dengan pendekatan manajemen yang sangat terpusat, yang sangat menekankan keamanan nasional, perlindungan rezim, dan pengendalian aliran informasi (B. Tran, 2024). Indonesia, di sisi lain, mengambil pendekatan yang lebih terdesentralisasi, berupaya meniru standar internasional seperti GDPR Uni Eropa untuk mempromosikan kepercayaan perdagangan dan melindungi privasi individu, meskipun masih terdapat kesenjangan serius dalam penegakan praktis (Alfath & Cahya, 2024; Awaluddin, 2025).

Menganalisis konvergensi dan divergensi dalam kebijakan keamanan siber dan perlindungan data antara dua ekonomi utama ASEAN ini tidak hanya memberikan gambaran komprehensif tentang lingkungan hukum regional, tetapi juga menjelaskan dampak luas kebijakan-kebijakan ini terhadap daya saing nasional inti, arus investasi asing langsung (FDI), dan integrasi regional. Studi ini meneliti mekanisme hukum Vietnam dan Indonesia, serta mengusulkan arah strategis bagi kedua negara untuk mengoptimalkan keseimbangan antara kebutuhan utama keamanan nasional dan tujuan pembangunan berkelanjutan dari ekonomi yang sangat terdigitalisasi.

Meskipun studi mengenai keamanan siber dan perlindungan data di Asia Tenggara terus berkembang, sebagian besar penelitian sebelumnya masih berfokus pada aspek teknis regulasi, efektivitas kebijakan, atau isu perlindungan privasi digital secara umum. Penelitian yang membandingkan bagaimana filosofi tata kelola negara membentuk hubungan antara negara, pasar digital, dan hak-hak warga negara dalam regulasi keamanan siber masih relatif terbatas, khususnya dalam konteks Vietnam dan Indonesia sebagai dua negara dengan sistem politik dan model pembangunan digital yang berbeda. Dalam literatur tata kelola digital, pendekatan keamanan siber sering dipahami melalui ketegangan antara model *state-centric digital sovereignty* (Nguyen et al., 2025; Prokopyshyn & Trushkina, 2025) yang menempatkan stabilitas politik dan kontrol negara sebagai prioritas utama, dan model *rights-based digital governance* (Ballanca, 2025; Bandemer et al., 2026) yang lebih menekankan perlindungan hak individu, privasi data, serta integrasi ekonomi digital global. Perbedaan orientasi ini memengaruhi bagaimana negara mengatur arus data, mengontrol platform digital, membangun hubungan dengan perusahaan teknologi, serta mendefinisikan batas antara keamanan nasional dan kebebasan sipil.

Berdasarkan konteks tersebut, penelitian ini

Public Knowledge / Volume 3 Issue 2
▪ DOI 10.62771/pk. V3i2.34

berupaya menjawab pertanyaan utama: bagaimana perbedaan filosofi tata kelola digital di Vietnam dan Indonesia membentuk kerangka hukum keamanan siber dan perlindungan data, serta bagaimana implikasinya terhadap relasi antara negara, pasar digital, dan warga negara? Dengan menggunakan pendekatan hukum komparatif, penelitian ini tidak hanya mengidentifikasi perbedaan regulasi formal, tetapi juga menganalisis bagaimana orientasi politik dan model tata kelola negara memengaruhi mekanisme pengawasan digital, perlindungan privasi, serta integrasi ekonomi digital di kedua negara. Penelitian ini juga menggunakan perspektif regulatory fragmentation dan institutional capacity untuk menjelaskan efektivitas tata kelola keamanan siber di negara berkembang.

Metode

Penelitian ini menggunakan pendekatan penelitian hukum normatif dengan metode analisis komparatif untuk mengkaji perbedaan dan persamaan kerangka hukum keamanan siber dan perlindungan data antara Vietnam dan Indonesia. Penelitian hukum normatif berfokus pada norma-norma preskriptif yang menentukan bagaimana individu seharusnya berperilaku sesuai dengan standar hukum yang telah ditetapkan. Pendekatan ini mengisolasi norma-norma hukum dari pengaruh non-hukum, sehingga memberikan kerangka kerja yang jelas untuk memahami kewajiban dan hak-hak hukum (Christian, 2019). Hukum perbandingan melibatkan analisis dan perbandingan sistem hukum untuk memahami perbedaan dan persamaannya. Disiplin ilmu ini sangat penting untuk mengidentifikasi bagaimana norma-norma hukum ditransplantasikan dan diadaptasi antar yurisdiksi, suatu proses yang dikenal sebagai transplantasi hukum (Roger, 2018). Penelitian hukum normatif (Putri, 2026) berfokus pada analisis terhadap norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, serta literatur akademik yang relevan dengan topik penelitian.

Data yang digunakan dalam penelitian ini merupakan data primer dan sekunder (Petticrew & Roberts, 2006; Sobieraj & Baker, 2021). Sumber data dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh dari dokumen hukum resmi kedua negara, termasuk undang-undang, peraturan pemerintah, dekrit, dan kebijakan nasional terkait keamanan siber dan perlindungan data, seperti Undang-Undang Keamanan Siber Vietnam 2018 dan 2025, Undang-Undang Perlindungan Data Pribadi Vietnam 2025/2026, Undang-Undang Informasi dan Transaksi Elektronik Indonesia, PP No. 71 Tahun 2019, serta Undang-Undang Perlindungan Data Pribadi Indonesia Tahun 2022. Seluruh dokumen diperoleh melalui portal resmi pemerintah, basis data legislasi nasional, dan publikasi lembaga negara terkait. Data sekunder diperoleh dari artikel jurnal ilmiah bereputasi, buku akademik, laporan lembaga internasional, policy brief, serta publikasi institusi penelitian yang membahas keamanan siber, tata kelola digital, dan perlindungan data di Asia Tenggara. Sumber sekunder dipilih berdasarkan relevansi topik, kredibilitas akademik, serta keterbaruan publikasi.

Validasi data dilakukan melalui teknik triangulasi sumber (source triangulation), yaitu dengan membandingkan isi regulasi resmi dengan analisis akademik, laporan internasional, dan kajian kebijakan dari berbagai institusi (Carter et al., 2014; Schlunegger et al., 2024). Selain itu, penelitian juga menerapkan "cross-country comparative analysis" (Von Knebel, 2023) antara dokumen hukum Vietnam dan Indonesia untuk memastikan konsistensi interpretasi terhadap norma hukum, mekanisme penegakan, serta implementasi kebijakan keamanan siber di kedua negara. Pendekatan ini digunakan untuk meningkatkan validitas analisis dan mengurangi bias interpretatif dalam penelitian hukum komparatif. Data dianalisis menggunakan metode analisis kualitatif-deskriptif (Atkinson & Delamont, 2010) dengan pendekatan perbandingan hukum (Sacco, 1991) untuk mengidentifikasi karakteristik regulasi, mekanisme penegakan hukum, serta implikasi kebijakan dari sistem tata kelola keamanan siber di Vietnam dan Indonesia.

Hasil dan Pembahsan

A. Kerangka Hukum untuk Keamanan Siber dan Perlindungan Data di Vietnam

Sistem hukum Vietnam untuk keamanan siber dan tata kelola data dibangun di atas filosofi legislatif yang jelas: ruang siber merupakan bagian yang tak terpisahkan dari wilayah nasional, dan oleh karena itu, stabilitas politik dan keamanan nasional harus menjadi prioritas utama (B. Tran, 2024). Pergeseran dari peraturan administratif semata ke sistem hukum yang sangat dapat ditegakkan telah dipromosikan secara kuat dalam beberapa tahun terakhir, menciptakan jaringan peraturan yang ketat bagi semua entitas yang berpartisipasi dalam interaksi digital di Vietnam.

Strategi Pengendalian yang Komprehensif dan Terpusat

Di Vietnam, perkembangan pesat teknologi informasi dalam beberapa tahun terakhir telah menciptakan kebutuhan mendesak bagi lembaga-lembaga manajemen negara untuk membangun kerangka hukum yang kuat guna mengatur dan memastikan keamanan

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

dan ketertiban sosial di lingkungan daring. Berangkat dari kebutuhan ini, pada sidang ke-5 Majelis Nasional ke-14 pada tanggal 12 Juni 2018, Undang-Undang Keamanan Siber Tahun 2018 disahkan dan resmi berlaku pada tanggal 1 Januari 2019. Undang-Undang Keamanan Siber Tahun 2018 memuat ketentuan-ketentuan yang pada dasarnya memenuhi tujuan untuk memastikan keamanan dan integritas aktivitas di dunia maya; menciptakan dasar hukum yang kuat untuk mencegah, mendeteksi, menghentikan, dan menangani tindakan yang melanggar keamanan siber dan memengaruhi hak dan kepentingan sah individu, lembaga, dan organisasi. Undang-undang ini terdiri dari 7 bab dan 43 pasal yang mengatur kegiatan yang berkaitan dengan perlindungan keamanan nasional dan memastikan ketertiban dan keamanan sosial di dunia maya; serta tanggung jawab lembaga, organisasi, dan individu terkait.

Dengan tujuan untuk memastikan keamanan dan integritas aktivitas di dunia maya, beberapa ketentuan dasar Undang-Undang Keamanan Siber yang dapat kita sebutkan antara lain: Para pembuat undang-undang telah mencantumkan tindakan terlarang terkait keamanan siber dalam Pasal 8 dan undang-undang khusus dalam Bab III tentang pencegahan dan penanganan tindakan yang melanggar keamanan siber. Lebih lanjut, untuk memastikan pencegahan dan penghapusan pelanggaran keamanan siber yang disebutkan di atas secara efektif, Undang-Undang ini menetapkan langkah-langkah untuk melindungi keamanan siber dan langkah-langkah untuk menangani pelanggaran undang-undang tentang keamanan siber dalam Pasal 5 dan 9. Menurut Pasal 9, siapa pun yang melanggar ketentuan Undang-Undang tentang Keamanan Siber, tergantung pada sifat dan tingkat keparahan pelanggaran, akan dikenakan tindakan disiplin, sanksi administratif, atau penuntutan pidana; jika terjadi kerugian, ganti rugi harus dibayarkan sesuai dengan hukum. Pada tanggal 3 Februari 2020, Pemerintah mengeluarkan Keputusan 15/2020/ND-CP yang menetapkan sanksi administratif untuk pelanggaran di bidang layanan pos, telekomunikasi, frekuensi radio, teknologi informasi, dan transaksi elektronik (diubah dan ditambah dengan Keputusan 14/2022/ND-CP dan Keputusan 211/2025/ND-CP). KUHP 2015 (diubah dan ditambah pada tahun 2017, 2024, dan 2025) juga memuat ketentuan tentang tindak pidana penyediaan atau penggunaan informasi secara ilegal pada jaringan komputer dan jaringan telekomunikasi. Oleh karena itu, siapa pun yang mengunggah informasi ke jaringan komputer atau jaringan telekomunikasi yang melanggar hukum, menimbulkan opini publik negatif, atau berdampak negatif terhadap keamanan, ketertiban, dan keselamatan sosial dapat dituntut atas kejahatan penyediaan atau penggunaan informasi secara ilegal di jaringan komputer dan jaringan telekomunikasi sebagaimana diatur dalam Pasal 288.

Internet, khususnya jejaring sosial, secara bertahap memainkan peran yang semakin penting dan memiliki pengaruh besar pada kehidupan sosial. Hingga saat ini, setelah bertahun-tahun diimplementasikan, Undang-Undang Keamanan Siber, bersama dengan peraturan hukum terkait lainnya, telah berkontribusi dalam menjaga dan memastikan keselamatan dan ketertiban sosial di dunia maya di negara kita. Bertujuan untuk melindungi keamanan nasional dan memastikan ketertiban dan keselamatan sosial di dunia maya, dengan fokus pada kepentingan nasional dan kepentingan rakyat, Undang-Undang Keamanan Siber 2025 dibangun berdasarkan konsolidasi Undang-Undang Keamanan Informasi 2015 dan Undang-Undang Keamanan Siber 2018. Undang-Undang Keamanan Siber 2025 disahkan oleh Majelis Nasional ke-15 Republik Sosialis Vietnam pada sesi ke-10 pada tanggal 10 Desember 2025, dan akan mulai berlaku pada tanggal 1 Juli 2026. Berdasarkan Undang-Undang Keamanan Siber 2018, Undang-Undang 2025 terdiri dari 8 bab dan 45 pasal; undang-undang ini mengatur keamanan siber, perlindungan keamanan siber, serta hak, kewajiban, dan tanggung jawab lembaga, organisasi, dan individu terkait.

Secara konseptual, perkembangan kerangka hukum keamanan siber Vietnam menunjukkan kecenderungan menuju model *state-centric digital sovereignty* (Prokopyshyn & Trushkina, 2025), yaitu pendekatan tata kelola digital yang menempatkan negara sebagai aktor utama dalam mengendalikan arus informasi, infrastruktur data, dan stabilitas politik di ruang siber. Dalam model ini, keamanan siber tidak dipahami semata sebagai perlindungan teknis terhadap serangan digital, tetapi juga sebagai instrumen untuk mempertahankan legitimasi politik, ketertiban sosial, dan kontrol ideologis negara. Oleh karena itu, regulasi seperti kewajiban verifikasi identitas pengguna, lokalisasi data, serta kewajiban platform digital untuk menyerahkan informasi pengguna mencerminkan perluasan kapasitas pengawasan negara ke dalam ruang digital masyarakat sipil.

Pendekatan tersebut juga memperlihatkan bagaimana relasi antara negara, pasar digital, dan warga negara di Vietnam dibangun melalui logika keamanan nasional. Platform digital asing tidak diposisikan sebagai aktor independen, melainkan sebagai entitas yang wajib tunduk pada otoritas negara dan mendukung agenda stabilitas politik domestik. Dalam konteks ini, ruang digital diperlakukan sebagai perpanjangan dari wilayah kedaulatan negara (*digital territoriality*), sehingga kontrol terhadap data dan

Public Knowledge / Volume 3 Issue 2
▪ DOI 10.62771/pk. V3i2.34

informasi menjadi bagian dari strategi pertahanan nasional (Prakosa et al., 2026; Zhang & Morris, 2023). Konsekuensinya, perlindungan terhadap privasi individu dan kebebasan berekspresi sering kali berada di bawah prioritas keamanan politik dan ketertiban sosial.

Beberapa aspek progresif dari Undang-Undang Keamanan Siber tahun 2025

Selain mempertahankan peraturan dasar yang telah diterapkan secara konsisten selama periode sebelumnya, Undang-Undang Keamanan Siber 2025 telah direvisi dan ditambah oleh para pembuat undang-undang dengan banyak poin baru dibandingkan dengan Undang-Undang Keamanan Siber 2018, yang sepenuhnya sesuai dengan konteks transformasi digital global saat ini. Beberapa poin baru yang penting dalam Undang-Undang ini meliputi: mendefinisikan secara jelas lembaga utama untuk pengelolaan keamanan siber oleh negara (Kementerian Keamanan Publik); menambahkan peraturan baru dalam konteks kecerdasan buatan dan teknologi baru; memperkuat perlindungan data (terutama data pribadi) dalam konteks baru; meningkatkan tanggung jawab penyedia layanan jaringan; meningkatkan peraturan tentang pencegahan dan pemberantasan pelecehan anak di dunia maya; mencegah konflik informasi di dunia maya; dan memperluas kerja sama internasional.

Dengan tetap menjunjung tinggi prinsip pengamanan nasional, kegiatan keamanan siber berada di bawah kepemimpinan Partai Komunis Vietnam. Prinsip "Di bawah kepemimpinan Partai Komunis Vietnam; pengelolaan terpadu oleh Negara; memobilisasi kekuatan gabungan sistem politik dan seluruh bangsa; mempromosikan peran inti pasukan keamanan siber khusus," sebagaimana diatur dalam Pasal 2, Ayat 4 Undang-Undang Keamanan Siber 2025, berfungsi sebagai prinsip panduan dalam seluruh legislasi keamanan siber selama bertahun-tahun. Prinsip penting lainnya yang diatur dalam Pasal 4 Ayat ini adalah: "Menerapkan langkah-langkah untuk melindungi ruang siber nasional; secara proaktif mencegah, mendeteksi, menghentikan, dan memerangi semua aktivitas di ruang siber yang melanggar keamanan nasional, ketertiban dan keselamatan sosial, serta hak dan kepentingan sah lembaga, organisasi, dan individu; menangani pelanggaran hukum keamanan siber dengan cepat dan tegas."

Untuk mengkonkretkan prinsip-prinsip di atas, para pembuat undang-undang telah mencantumkan tindakan-tindakan terlarang terkait keamanan siber dalam Pasal 7 Undang-Undang ini dan ketentuan-ketentuan rinci dalam Bab III tentang Pencegahan dan Penanganan Tindakan yang Melanggar Keamanan Siber. Mewarisi dan mengembangkan ketentuan-ketentuan Undang-Undang Keamanan Siber 2018, Pasal 7 Undang-Undang Keamanan Siber 2025 menetapkan tindakan-tindakan terlarang terkait keamanan siber. Dengan demikian, Ayat 1 Pasal 7 melarang pengunggahan dan penyebaran informasi dengan isi sebagai berikut di internet:

(i) Propaganda yang menentang Republik Sosialis Vietnam (propaganda yang mendistorsi dan mencemarkan nama baik pemerintah rakyat; perang psikologis, hasutan untuk perang agresi, perpecahan, kebencian antar kelompok etnis, agama dan masyarakat dari berbagai negara; menghina bangsa, bendera nasional, lambang nasional, lagu kebangsaan, tokoh-tokoh besar, pemimpin, orang terkenal, pahlawan nasional);

(ii) Memutarbalikkan sejarah, menyangkal pencapaian revolusioner, merusak persatuan nasional, menghina agama, melakukan diskriminasi berdasarkan jenis kelamin, dan diskriminasi ras;

(iii) Memalsukan, memfitnah, menyebarkan informasi palsu, melanggar martabat, kehormatan, dan reputasi orang lain, atau menyebabkan kerusakan pada hak dan kepentingan sah lembaga, organisasi, dan individu lain;

(iv) Menyebarkan informasi palsu yang menyebabkan kepanikan publik, merusak kegiatan sosial-ekonomi, menghambat operasi normal lembaga negara atau pejabat publik, melanggar hak dan kepentingan sah lembaga, organisasi, dan individu lain; memalsukan atau menyebarkan informasi palsu tentang produk, barang, uang, obligasi, surat utang, obligasi pemerintah, cek, dan dokumen berharga lainnya; memalsukan atau menyebarkan informasi palsu di bidang keuangan, perbankan, e-commerce, pemasaran multi-level, dan sekuritas.

Pasal 7 ayat 2 mengatur larangan tindakan di dunia maya, dengan tindakan-tindakan yang berkaitan dengan keamanan nasional seperti: (i) Mengorganisir, mengoperasikan, bersekongkol, menghasut, menyuap, menipu, membujuk, melatih, atau menginstruksikan orang untuk menentang Republik Sosialis Vietnam; (ii) Menghasut, menyerukan, memobilisasi, menghasut, mengancam, menyebabkan perpecahan, melakukan kegiatan bersenjata atau menggunakan kekerasan untuk menentang pemerintah rakyat; menyerukan, memobilisasi, menghasut, mengancam, atau membujuk sejumlah besar orang untuk menyebabkan keresahan, melawan petugas penegak hukum, menghalangi kegiatan lembaga dan organisasi, menyebabkan ketidakstabilan dalam keamanan dan ketertiban; ...

Dengan demikian, Undang-Undang Keamanan Siber 2025 terus menegaskan orientasi legislatif yang menempatkan perlindungan keamanan nasional sebagai pusat pengelolaan dunia maya. Undang-undang keamanan siber bertujuan tidak hanya untuk

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

melindungi keamanan politik tetapi juga untuk berkontribusi dalam menjaga ketertiban sosial, keamanan, dan kegiatan ekonomi di dunia maya.

*Regulasi baru ditambahkan dalam konteks kecerdasan buatan dan teknologi bar*u. Pasal 2, Ayat 7 Undang-Undang Keamanan Siber 2025 melarang tindakan-tindakan tertentu di dunia maya. Secara khusus, undang-undang ini melarang penggunaan kecerdasan buatan atau teknologi baru untuk memalsukan video, gambar, atau suara orang lain yang melanggar hukum; dan pembuatan, pengunggahan, dan penyebaran informasi sebagaimana diatur dalam Pasal 1 Ayat ini. Undang-Undang Keamanan Siber 2025 melengkapi dan memperbarui daftar tindakan terlarang untuk melawan perkembangan teknologi baru, terutama AI, IoT, dan metode serangan siber yang canggih. Tujuannya adalah untuk melindungi keamanan nasional, privasi individu, serta keamanan dan transparansi lingkungan daring. Secara khusus, undang-undang ini melarang pemalsuan menggunakan AI (deepfake, suara AI, gambar AI). Perluasan daftar perilaku terlarang dalam Undang-Undang Keamanan Siber 2025 menunjukkan fokus Negara pada perlindungan privasi, aset data, keamanan nasional, dan keselamatan warganya. Pada saat yang sama, Undang-Undang ini secara akurat mencerminkan realitas baru di mana AI, IoT, dan kejahatan siber lintas batas menimbulkan tantangan yang belum pernah terjadi sebelumnya (Huynh, 2025). Mengingat bahwa dunia maya menjadi alat potensial untuk penipuan atau pelanggaran privasi, penambahan peraturan ini tepat waktu dan diperlukan untuk mencegah organisasi dan individu menyalahgunakan kecerdasan buatan untuk melakukan kegiatan ilegal.

Dari perspektif tata kelola teknologi, perluasan regulasi terhadap kecerdasan buatan dan deepfake menunjukkan bahwa Vietnam tidak hanya merespons ancaman teknis, tetapi juga berupaya mengantisipasi potensi disrupsi terhadap otoritas informasi negara. Hal ini memperlihatkan kecenderungan menuju model *preventive digital governance* (Andita et al., 2025; Garcia, 2016), di mana negara mengambil posisi proaktif untuk mengendalikan teknologi baru sebelum teknologi tersebut berkembang menjadi ruang yang sulit diawasi secara politik maupun sosial. Dengan demikian, regulasi AI di Vietnam memiliki dimensi keamanan politik yang lebih dominan dibandingkan pendekatan etika teknologi atau perlindungan hak digital sebagaimana berkembang di banyak negara demokratis liberal.

Penguatan perlindungan data (khususnya data pribadi) dalam konteks baru. Data pribadi adalah data digital atau informasi dalam bentuk lain yang mengidentifikasi atau membantu mengidentifikasi orang tertentu, termasuk data pribadi dasar dan data pribadi sensitif (Pasal 1, Ayat 2, Undang-Undang Perlindungan Data Pribadi, 2026). Meskipun Undang-Undang Perlindungan Data Pribadi telah disahkan, cakupan perlindungan perlu diperluas untuk mencakup data organisasi, data sistem, dan data dalam perjalanan. Penambahan peraturan keamanan data pada Undang-Undang Keamanan Siber sangat penting untuk mencegah pengambilalihan, penggunaan, eksploitasi, atau penghancuran data tanpa izin; dan untuk mencegah bencana tak terduga yang secara langsung memengaruhi keamanan nasional dan ketertiban sosial (Minh, 2025). Undang-Undang Keamanan Siber 2018 juga membahas masalah data, tetapi hanya secara terfragmentasi dan tidak spesifik. Undang-Undang Keamanan Siber 2025 telah lebih lanjut menetapkan peraturan tentang memastikan keamanan data dalam Pasal 26, yang meliputi: Mengembangkan kebijakan dan menetapkan prosedur untuk memastikan keamanan data; Menerapkan langkah-langkah, standar, dan peraturan teknis sebagaimana diatur dalam undang-undang tentang keamanan siber; Menggunakan kriptografi dan kriptografi sipil untuk memastikan keamanan data (Komite Sandi Pemerintah bertanggung jawab untuk mengatur implementasi peraturan hukum tentang penggunaan kriptografi untuk melindungi informasi yang diklasifikasikan sebagai rahasia negara yang disimpan dan dipertukarkan di dunia maya); Menerapkan mekanisme untuk kontrol ketat terhadap personel yang terlibat langsung dalam pemrosesan data; Melakukan pemeriksaan dan penilaian risiko secara berkala untuk mendeteksi, mencegah, dan segera menangani ancaman terhadap keamanan data; Memeriksa dan mengevaluasi transfer data lintas batas.

Memperkuat tanggung jawab penyedia layanan jaringan. Pasal 25 ayat 2 tentang Keamanan Informasi Jaringan dalam Undang-Undang Keamanan Siber 2025 menetapkan bahwa perusahaan domestik dan asing yang menyediakan layanan pada jaringan telekomunikasi, internet, dan layanan nilai tambah di dunia maya di Vietnam memiliki tanggung jawab sebagai berikut:

(i) Memverifikasi informasi ketika pengguna mendaftarkan akun digital; melindungi informasi dan akun pengguna; memberikan informasi pengguna kepada pasukan perlindungan keamanan siber khusus di bawah Kementerian Keamanan Publik paling lambat 24 jam sejak permintaan tertulis atau email, telepon, atau bentuk pertukaran terkonfirmasi lainnya untuk melayani verifikasi, investigasi, dan penanganan pelanggaran hukum tentang keamanan siber; dalam kasus darurat yang mengancam keamanan nasional atau nyawa manusia, permintaan informasi harus dilakukan paling lambat 3 jam;

(ii) Mencegah penyebaran informasi, menghapus informasi, dan menghapus layanan dan

Public Knowledge / Volume 3 Issue 2
▪ DOI 10.62771/pk. V3i2.34

aplikasi yang berisi konten yang melanggar ketentuan Undang-Undang ini paling lambat 24 jam sejak permintaan dari pasukan keamanan siber khusus Kementerian Keamanan Publik, dan menyimpan log sistem untuk keperluan verifikasi, investigasi, dan penanganan pelanggaran hukum keamanan siber dalam waktu yang ditentukan oleh undang-undang; dalam kasus mendesak yang mengancam keamanan nasional, permintaan untuk mencegah dan menghapus informasi harus dilakukan paling lambat 6 jam.

Dibandingkan dengan ketentuan dalam Pasal 26 tentang Penjaminan Keamanan Informasi di Ruang Siber dalam Undang-Undang Keamanan Siber 2018, Undang-Undang 2025 meningkatkan kelayakan dan efektivitas penegakan hukum dengan menetapkan tenggat waktu yang jelas. Dengan demikian, jangka waktu spesifik bagi bisnis domestik dan asing yang menyediakan layanan di jaringan telekomunikasi, internet, dan layanan nilai tambah di ruang siber di Vietnam untuk memenuhi tanggung jawab mereka dalam memberikan informasi pengguna kepada pasukan keamanan siber khusus ditetapkan (24 jam dalam kasus normal; 3 jam dalam kasus darurat). Lebih lanjut, terkait pencegahan penyebaran informasi, penghapusan informasi, dan penghapusan layanan dan aplikasi dengan konten yang melanggar, Undang-Undang 2025 menambahkan kasus darurat yang mengancam keamanan nasional, yang mengharuskan pencegahan dan penghapusan informasi dalam waktu maksimal 6 jam (selain jangka waktu normal 24 jam). Peraturan ini bertujuan untuk memperkuat mekanisme respons cepat terhadap ancaman terhadap keamanan nasional.

Mencegah dan memerangi pelecehan anak di dunia maya. Pasal 16 Undang-Undang Keamanan Siber 2026 menetapkan bahwa anak-anak memiliki hak untuk mengakses informasi, berpartisipasi dalam kegiatan sosial, bermain, dan memiliki privasi pribadi serta hak-hak lainnya yang dilindungi di dunia maya sebagaimana diatur oleh hukum. Undang-undang ini juga memastikan tanggung jawab pemilik sistem informasi dan bisnis yang menyediakan layanan pada jaringan telekomunikasi, internet, dan layanan bernilai tambah di dunia maya; oleh karena itu, pihak-pihak terkait memiliki tanggung jawab untuk mengontrol isi informasi pada sistem informasi atau pada layanan yang disediakan oleh bisnis untuk mencegah bahaya bagi anak-anak atau pelecehan terhadap anak-anak atau pelanggaran hak-hak anak; untuk mencegah penyebaran dan penghapusan informasi yang berbahaya bagi anak-anak atau melecehkan anak-anak atau melanggar hak-hak anak; …Secara khusus, Undang-Undang 2025 menambahkan ketentuan yang mewajibkan orang tua atau wali, sebagaimana diatur oleh hukum perdata, untuk mendaftarkan akun anak-anak yang menggunakan layanan bernilai tambah di internet menggunakan informasi mereka sendiri dan bertanggung jawab untuk memantau dan mengelola konten yang diakses, diunggah, dan dibagikan anak-anak di platform layanan tersebut.

Mencegah konflik informasi di dunia maya. Undang-Undang Keamanan Siber 2025 menambahkan Pasal 22, yang mengatur pencegahan konflik informasi di dunia maya, termasuk pemantauan, deteksi, peringatan, identifikasi sumber, pemblokiran, penghapusan, penyangkalan, panduan opini publik, perbaikan, sanksi, dan langkah-langkah lain untuk menghilangkan konflik informasi di dunia maya. Klausul 1 Pasal 22 dengan jelas menetapkan bahwa "Konflik informasi terjadi ketika dua atau lebih organisasi domestik dan asing menggunakan teknologi dan teknik informasi untuk merugikan informasi dan sistem informasi di dunia maya, yang memengaruhi keamanan nasional, ketertiban sosial, dan keselamatan."

Memperluas kerja sama internasional. Undang-Undang Keamanan Siber 2025 juga membantu memperkuat kerja sama keamanan dan melindungi lingkungan digital antara Vietnam dan negara-negara lain. Undang-Undang Keamanan Siber 2025 berfungsi sebagai jembatan untuk mengimplementasikan Konvensi Perserikatan Bangsa-Bangsa tentang Kejahatan Siber 2025 (Konvensi Hanoi). Undang-undang ini telah menambahkan banyak mekanisme untuk koordinasi internasional, langkah-langkah untuk mendukung investigasi lintas batas, dan penanganan kejahatan teknologi tinggi. Hal ini membantu Vietnam secara bertahap menstandarisasi kerangka hukumnya sesuai dengan praktik internasional. Pada saat yang sama, hal ini memperkuat kemampuan untuk memastikan keamanan dan melindungi pasar ekonomi digital, serta mekanisme untuk menyelesaikan konflik, pelanggaran, sengketa, dan pemulihan aset yang diperoleh melalui cara ilegal (Khong, 2026). Isi kerja sama internasional di bidang keamanan siber secara khusus diatur dalam Pasal 6 Undang-Undang Keamanan Siber 2025.

B. Kerangka Hukum untuk Keamanan Siber dan Perlindungan Data di Indonesia

Berbeda dengan sistem top-down, berorientasi keamanan, dan berorientasi manajemen di Vietnam, kerangka hukum Indonesia untuk keamanan siber dan perlindungan data bersifat reaktif, berupaya meminjam dan mengasimilasi standar Barat, khususnya GDPR. Namun, upaya ini saat ini terhambat oleh kurangnya koordinasi antar sektor, anggaran investasi yang terbatas, dan konflik wewenang di antara lembaga-lembaga politik.

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

Undang-Undang ITE dan Matriks Operasional berdasarkan Peraturan Pemerintah No. 71 (PP 71)

Selama beberapa dekade, fondasi keamanan siber di Indonesia bergantung pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang diberlakukan pada tahun 2008 dan kemudian diamandemen pada tahun 2016 dan 2024 (Awaluddin, 2025). Meskipun berfungsi sebagai dasar hukum awal melawan kejahatan siber, UU ITE memiliki reputasi buruk di kalangan analis hukum karena mengandung "pasal karet" yang ambigu (DLA Piper, 2025). Ketentuan-ketentuan ini sering ditafsirkan secara sewenang-wenang oleh pemerintah untuk menyensor atau menghukum kebebasan berbicara daring. Terutama, putusan Mahkamah Konstitusi Indonesia pada Oktober 2021 menegaskan kekuasaan sah pemerintah untuk sepenuhnya memblokir akses internet warga negara selama periode kerusuhan sosial, sebuah tindakan yang menuai kritik keras dari kelompok advokasi privasi (Rodriguez, 2021).

Dalam hal manajemen infrastruktur elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 (PP 71) menguraikan kewajiban operasional Penyedia Sistem Elektronik (PSK) (ITIF, 2025). Perbedaan terbesar antara PP 71 dan peraturan Vietnam adalah pemisahan yang jelas antara dua sektor: PSK Publik dan PSK Swasta. Peraturan ini melonggarkan persyaratan lokalisasi data dengan mengizinkan organisasi swasta (PSK Swasta, termasuk perusahaan teknologi multinasional) untuk bebas menyimpan dan memproses data di luar perbatasan Indonesia, kecuali untuk sektor-sektor sensitif tertentu seperti jasa keuangan. Sebaliknya, instansi pemerintah dan sektor publik diwajibkan untuk sepenuhnya melokalisasi data untuk melindungi kedaulatan nasional (AHP, 2019).

Meskipun tampaknya penempatan server lebih fleksibel, PP 71 menetapkan matriks administratif yang sangat kompleks untuk aliran data. Bisnis asing diharuskan mendaftar ke Kementerian Komunikasi dan Informatika (KTI) sebelum diizinkan untuk menyediakan layanan (ITIF, 2025). Untuk transfer data lintas batas, perusahaan tidak hanya harus mendapatkan persetujuan tertulis eksplisit dalam bahasa Indonesia dari subjek data, tetapi juga menyerahkan laporan terperinci kepada KTI baik sebelum maupun sesudah transfer, yang menciptakan hambatan administratif yang secara signifikan memperlambat pengembangan produk (ROUSE, 2025). Lebih serius lagi, PP 71 berisi peraturan yang sangat mengganggu: memaksa PSK Swasta untuk membangun mekanisme untuk menyediakan akses "pintu belakang" ke sistem dan data elektronik mereka bagi lembaga penegak hukum. Persyaratan ini secara langsung bertentangan dengan struktur enkripsi ujung-ke-ujung dari banyak platform internasional, menciptakan kerentanan keamanan yang berisiko yang dapat dieksploitasi oleh peretas.

Undang-Undang PDP 2022 dan Dampak Transisinya

Peristiwa legislatif paling signifikan di Indonesia dalam dekade terakhir adalah pengesahan Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022, disingkat PDP), yang secara resmi mengakhiri fase pengelolaan data terdesentralisasi di berbagai sektor. Dengan masa transisi dua tahun dan implementasi penuh yang dijadwalkan pada Oktober 2024, undang-undang ini dirancang berdasarkan prinsip-prinsip inti GDPR Eropa, meningkatkan standar privasi warga negara Indonesia ke tingkat internasional. PDP memiliki cakupan ekstrateritorial, mencakup semua entitas, terlepas dari apakah mereka berlokasi di dalam atau di luar perbatasan Indonesia, selama aktivitas pengolahan data mereka menghasilkan konsekuensi hukum di dalam negeri atau memengaruhi warga negara Indonesia yang tinggal di luar negeri. Undang-undang ini secara jelas mendefinisikan konsep Data Pribadi, Pengendali Data, dan Pengolah Data, sekaligus melindungi hak-hak mendasar subjek data seperti hak untuk mengakses, hak untuk mengoreksi, hak untuk dilupakan, dan terutama hak untuk menolak keputusan yang dibuat sepenuhnya berdasarkan pengolahan otomatis. Untuk transfer data lintas batas, tidak seperti mekanisme TIA berbasis risiko di Vietnam, PDP Indonesia menetapkan sistem perlindungan bertingkat yang lebih konservatif. Untuk mentransfer data keluar dari Indonesia, Pengendali Data harus menunjukkan bahwa negara penerima memiliki sistem hukum perlindungan data yang setara atau lebih unggul dari Indonesia (Kecukupan Perlindungan). Jika ambang batas ini tidak terpenuhi, organisasi harus menetapkan pengamanan yang mengikat sesuai standar (Pengamanan yang Tepat). Jika kedua kondisi di atas gagal, metode terakhir dan paling berisiko adalah memperoleh persetujuan eksplisit dari setiap subjek data untuk transaksi spesifik tersebut.

Perubahan Hukum Terkait DPO dan Beban pada Usaha Kecil dan Menengah

Salah satu aspek yang paling kontroversial dan mengganggu dalam implementasi UU PDP di Indonesia adalah ketentuan mengenai pengangkatan Petugas Perlindungan Data (PKP). Awalnya, Pasal 53 UU tersebut dirancang dengan konsesi kepada sektor swasta, yang menetapkan bahwa pengangkatan PKP hanya wajib jika suatu organisasi memenuhi ketiga kriteria kumulatif: (1) mengolah data untuk kepentingan umum; (2) melakukan pemantauan secara teratur dan sistematis dalam skala besar; dan (3) mengolah data sensitif atau kriminal dalam skala besar.

Public Knowledge / Volume 3 Issue 2
▪ DOI 10.62771/pk. V3i2.34

Struktur "dan" ini berarti bahwa sebagian besar organisasi bisnis biasa dibebaskan dari kewajiban PKP.

Namun, pada Juli 2025, Mahkamah Konstitusi Indonesia mengeluarkan putusan penting (Keputusan No. 151/PUU-XXII/2024), yang sepenuhnya merestrukturisasi lanskap kepatuhan. Mahkamah memutuskan bahwa kata "dan" dalam Pasal 53 tidak konstitusional dan harus diartikan sebagai "dan/atau" (kriteria alternatif). Putusan ini mencerminkan sikap tegas pengadilan bahwa data pribadi adalah hak mendasar dan tidak dapat diperlakukan sebagai komoditas komersial semata. Konsekuensi dari putusan ini adalah penurunan ambang batas wajib secara langsung, memaksa puluhan ribu organisasi, termasuk Usaha Mikro, Kecil, dan Menengah—yang sudah sangat kekurangan personel yang berpengetahuan di bidang keamanan siber—untuk menunjuk seorang DPO jika mereka secara tidak sengaja memenuhi salah satu dari tiga kriteria tersebut. Perubahan mendadak ini menciptakan hambatan finansial dan struktural yang besar, mengancam kapasitas kepatuhan ekonomi digital Indonesia.

Sanksi Pidana dan Administratif Ganda serta Kerentanan Administrasi Sistem

Berbeda dengan pendekatan Vietnam yang menangani pelanggaran dengan denda administratif besar-besaran terhadap bisnis, sistem hukum Indonesia menerapkan model sanksi ganda, yang secara jelas memisahkan tanggung jawab administratif dan pidana. Secara administratif, UU PDP memberi wewenang kepada otoritas pengawas untuk menerapkan tindakan yang meningkat, mulai dari peringatan tertulis dan perintah untuk menangguhkan sementara kegiatan pengolahan data dan memaksa penghancuran data, hingga pengenaan denda administratif. Denda ini dapat mencapai maksimum 2% dari total pendapatan atau pemasukan tahunan organisasi yang melakukan pelanggaran (ITIF, 2025).

Dari sudut pandang kriminal, hukum secara langsung menargetkan individu dan peretas dengan hukuman penjara yang sangat berat. Mengumpulkan atau menggunakan data secara ilegal dengan sengaja dapat berujung pada hukuman penjara 5 tahun dan denda hingga 5 miliar rupiah. Mendistribusikan atau mengungkapkan data secara ilegal dapat berujung pada hukuman penjara 4 tahun dan denda 4 miliar rupiah. Terutama, membuat profil data pribadi palsu untuk keuntungan dapat berujung pada hukuman penjara 6 tahun dan denda 6 miliar rupiah. Jika suatu organisasi bisnis terbukti membantu dan bersekongkol dalam tindakan kriminal ini, organisasi tersebut tidak hanya menghadapi denda sepuluh kali lebih besar daripada individu, tetapi juga asetnya disita, izin usahanya dicabut, diwajibkan membayar ganti rugi, dan dapat dibubarkan secara permanen. Namun, kesempurnaan peraturan ini di atas kertas dibayangi oleh ketidakmampuan untuk menegakkannya secara efektif. Hambatan terbesar dalam sistem perlindungan data di Indonesia adalah tidak adanya Otoritas Perlindungan Data yang independen. Meskipun PDP 2022 mengamanatkan pembentukannya, lembaga ini baru berdiri pada tahun 2025. Pemantauan hukum saat ini untuk sementara dipercayakan kepada Direktorat Pengawasan Ruang Digital di bawah Kementerian Komunikasi dan Teknologi Digital (KPM), sebuah lembaga yang kurang independen dan berwenang untuk menangani pelanggaran antar kementerian atau insiden yang berkaitan dengan pemerintah.

Krisis tata kelola semakin terlihat jelas di bidang keamanan siber. BSSN, yang dibentuk untuk mengkoordinasikan keamanan siber berdasarkan Peraturan Presiden No. 47/2023, beroperasi dengan anggaran yang sangat minim, hanya sebesar 0,02% dari PDB Indonesia (Alfath & Cahya, 2024). Konsekuensi buruk dari fragmentasi dan kurangnya investasi ini ditunjukkan oleh serangan ransomware yang melumpuhkan Pusat Data Nasional (PDN) pada 20 Juni 2024 (Heryadi et al., 2024). Serangan tersebut melumpuhkan sistem 210 instansi pemerintah, memaksa prosedur imigrasi kembali ke proses manual, dan mengungkap kurangnya sistem komando terpadu. Instansi sipil beroperasi sepenuhnya secara independen dan tidak mampu terhubung dengan kemampuan perang siber yang unggul dari Tentara Nasional Indonesia (TNI-Satsiber), sehingga menciptakan kerusakan struktural yang serius dalam respons krisis nasional (Shives & Fatahillah, 2026).

Secara konseptual, kondisi tata kelola keamanan siber di Indonesia mencerminkan fenomena *regulatory fragmentation* (Joseph et al., 2025; Xu, 2024), yaitu situasi ketika kewenangan regulasi, pengawasan, dan penegakan tersebar di berbagai lembaga tanpa mekanisme koordinasi yang kuat. Dalam konteks Indonesia, kewenangan terkait keamanan siber, perlindungan data, pengawasan platform digital, dan investigasi kejahatan siber terbagi antara Kementerian Komunikasi dan Digital, BSSN, kepolisian, lembaga intelijen, serta institusi pertahanan. Fragmentasi ini menciptakan tumpang tindih kewenangan, lambatnya respons krisis, dan ketidakjelasan struktur komando dalam menghadapi ancaman siber berskala nasional. Serangan ransomware terhadap Pusat Data Nasional pada tahun 2024 memperlihatkan bagaimana lemahnya integrasi kelembagaan dapat mengurangi efektivitas respons negara terhadap krisis digital.

Dari perspektif *institutional capacity theory* (Cars et al., 2018; Harun & Kamase, 2012; Polk, 2011), permasalahan keamanan siber Indonesia tidak semata disebabkan oleh kekurangan regulasi, tetapi juga oleh keterbatasan kapasitas institusional negara dalam

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

mengimplementasikan regulasi secara konsisten. Meskipun Indonesia telah mengadopsi Undang-Undang Perlindungan Data Pribadi yang relatif progresif dan terinspirasi oleh GDPR, efektivitas implementasinya masih terhambat oleh keterbatasan sumber daya, rendahnya koordinasi antar lembaga, keterlambatan pembentukan otoritas perlindungan data independen, serta ketergantungan pada mekanisme administratif yang kompleks. Dalam kerangka *governance failure* (Jessop, 2009; Paruchuri et al., 2024; Peters, 2015), kondisi ini menunjukkan adanya kesenjangan antara ambisi regulatif negara dan kapasitas birokrasi untuk menjalankan tata kelola digital secara efektif. Akibatnya, sistem hukum yang secara normatif terlihat modern belum sepenuhnya mampu menghasilkan perlindungan data dan keamanan siber yang kuat dalam praktik.

C. Kerangka Hukum Vietnam dan Indonesia

Membandingkan kerangka hukum Vietnam dan Indonesia tidak hanya menyoroti perbedaan dalam teknik legislatif tetapi juga mengungkapkan perspektif filosofis yang mendalam tentang peran negara dalam ekonomi digital dan hak-hak warga negara.

Perbedaan dalam Struktur Pemerintahan dan Filsafat Legislatif

Perbandingan antara Vietnam dan Indonesia menunjukkan adanya perbedaan mendasar dalam struktur tata kelola dan filosofi legislasi terkait ruang siber serta perlindungan data. Di Vietnam, filosofi legislasi sistemik memandang ruang siber sebagai medan strategis untuk mempertahankan kedaulatan nasional. Oleh karena itu, keamanan nasional, stabilitas rezim, dan pengendalian sosial ditempatkan sebagai prioritas utama dalam regulasi digital. Pendekatan ini mencerminkan kuatnya otoritas negara dalam mengelola dan mengawasi ruang siber. Sebaliknya, Indonesia cenderung memandang ruang siber sebagai lingkungan ekonomi digital yang perlu diatur untuk membangun kepercayaan publik dalam ekosistem digital. Dalam konteks ini, kerangka hukum Indonesia berusaha menyeimbangkan antara perlindungan privasi warga negara—yang sebagian mengacu pada standar Eropa—dan kebutuhan untuk mendukung integrasi ekonomi global serta kerja sama internasional.

Dari sisi kerangka hukum data, Vietnam menunjukkan proses evolusi regulasi yang relatif cepat. Sistem hukum berkembang dari regulasi berbasis peraturan pemerintah, seperti Dekrit 13 tentang Perlindungan Data Pribadi, menuju pembentukan undang-undang yang lebih komprehensif, seperti Undang-Undang Data 2025 dan Undang-Undang Perlindungan Data Pribadi 2025/2026. Dalam proses ini, beberapa hak yang dianggap berisiko, seperti hak portabilitas data, cenderung dibatasi atau dihilangkan demi menjaga kontrol negara terhadap arus data. Di sisi lain, Indonesia memilih pendekatan yang berbeda dengan mengadopsi satu undang-undang utama yang bersifat komprehensif, yaitu Undang-Undang Perlindungan Data Pribadi 2022. Namun, implementasi undang-undang ini menghadapi tantangan karena keterlambatan dalam penyusunan dan pengesahan peraturan pelaksana yang lebih rinci.

Perbedaan juga terlihat dalam struktur kelembagaan pengelolaan data dan keamanan siber. Di Vietnam, kekuasaan pengawasan terpusat secara kuat pada Departemen A05 di bawah Kementerian Keamanan Publik, sementara lembaga militer seperti Kementerian Pertahanan Nasional dan lembaga sipil seperti Kementerian Informasi dan Komunikasi berperan sebagai institusi pendukung. Dalam sistem ini, tidak terdapat konsep otoritas perlindungan data independen (independent Data Protection Authority/DPA). Sebaliknya, di Indonesia, pembentukan DPA independen sebenarnya telah diamanatkan oleh undang-undang, meskipun hingga saat ini lembaga tersebut belum sepenuhnya terbentuk. Sementara itu, kewenangan pengelolaan ruang siber masih tersebar di antara beberapa lembaga, termasuk Kementerian Komunikasi dan Digital sebagai lembaga sipil serta Badan Siber dan Sandi Negara (BSSN) sebagai lembaga keamanan siber, sementara peran militer relatif terpisah dari upaya pengelolaan sipil.

Selain itu, terdapat perbedaan penting terkait kewajiban penunjukan Data Protection Officer (DPO). Di Vietnam, tidak terdapat kewajiban universal bagi perusahaan untuk membentuk struktur DPO yang independen. Kepatuhan terhadap regulasi perlindungan data lebih banyak didasarkan pada mekanisme penilaian risiko internal, seperti Transfer Impact Assessment (TIA) dan Data Protection Impact Assessment (DPIA). Sebaliknya, Indonesia menetapkan kewajiban yang lebih ketat. Sebagian besar organisasi, termasuk perusahaan skala kecil dan menengah, diwajibkan menunjuk DPO. Kewajiban ini semakin diperkuat setelah adanya perubahan interpretasi hukum melalui putusan Mahkamah Konstitusi pada tahun 2025 yang mengubah penggunaan frasa “dan/atau”, sehingga memperluas cakupan organisasi yang wajib mematuhi ketentuan tersebut.

Struktur Kelembagaan dan Kapasitas Penegakan Siber

Di Vietnam, aktor utama yang memiliki kewenangan dalam keamanan siber dan perlindungan data adalah Kementerian Keamanan Publik (Ministry of Public Security/MPS), khususnya melalui

Public Knowledge / Volume 3 Issue 2
▪ DOI 10.62771/pk. V3i2.34

Departemen Keamanan Siber dan Pencegahan Kejahatan Teknologi Tinggi (A05). Lembaga ini berperan sebagai otoritas utama dalam pengawasan ruang siber, investigasi kejahatan siber, pengawasan platform digital, serta penegakan hukum terkait keamanan nasional di ruang digital. Selain itu, Kementerian Informasi dan Komunikasi (MIC) memiliki fungsi regulatif dan teknis dalam pengelolaan infrastruktur telekomunikasi, media digital, dan tata kelola internet. Pemerintah Vietnam juga melibatkan Kementerian Pertahanan Nasional dalam aspek pertahanan siber strategis dan perlindungan terhadap ancaman siber yang berkaitan dengan keamanan nasional. Dalam konteks perlindungan data, perusahaan penyedia layanan digital dan platform teknologi diwajibkan menjalankan kewajiban kepatuhan seperti lokalisasi data, verifikasi identitas pengguna, serta kerja sama dengan otoritas negara.

Sementara itu, di Indonesia, aktor utama dalam keamanan siber adalah Badan Siber dan Sandi Negara (BSSN), yang bertanggung jawab dalam koordinasi keamanan siber nasional, mitigasi serangan siber, perlindungan infrastruktur digital strategis, dan pengembangan kapasitas pertahanan siber nasional (Chotimah, 2019; Haryanto & Sutra, 2023). Kementerian Komunikasi dan Digital (Komdigi) memiliki kewenangan dalam regulasi sistem elektronik, pengawasan platform digital, pemutusan akses terhadap konten ilegal, serta implementasi kebijakan perlindungan data pribadi (Maulana et al., 2026; Nethan & Situbuana, 2025). Selain itu, aparat penegak hukum seperti Kepolisian Republik Indonesia melalui Direktorat Tindak Pidana Siber berperan dalam investigasi dan penindakan kejahatan siber. Tentara Nasional Indonesia (TNI), khususnya unit siber pertahanan, memiliki kemampuan dalam menghadapi ancaman siber yang berkaitan dengan pertahanan negara dan keamanan strategis (Anissa & Djuyandi, 2021; Oktavia & Martini, 2016). Di sektor non-pemerintah, perusahaan teknologi, penyelenggara sistem elektronik, dan Data Protection Officer (DPO) juga menjadi aktor penting dalam implementasi kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi serta perlindungan data pengguna (Ajiraga, 2026; Suleiman et al., 2022).

Perbedaan mendasar antara kedua negara terletak pada struktur koordinasi kelembagaan. Vietnam menerapkan model yang lebih terpusat dengan dominasi aparat keamanan negara, sedangkan Indonesia menggunakan pendekatan yang lebih terfragmentasi dan multi-aktor, dengan pembagian kewenangan antara lembaga sipil, regulator digital, aparat penegak hukum, dan institusi pertahanan.

Strategi Manajemen Data dan Hambatan Ekonomi

Pendekatan terhadap kebijakan lokalisasi data di kedua negara tersebut jelas menggambarkan konflik antara tujuan pengendalian administratif dan kebutuhan liberalisasi perdagangan digital. Secara strategis, lokalisasi data digunakan sebagai senjata geoekonomi untuk mengurangi ketergantungan pada negara adidaya teknologi, tetapi efek sampingnya seringkali menghambat inovasi. Di Indonesia, kebijakan PP 71 awalnya diharapkan dapat mengurangi tekanan pada sektor swasta dengan membebaskan penyimpanan domestik. Namun, alih-alih membuka peluang, kebijakan tersebut justru menciptakan labirin prosedur administratif. Persyaratan bagi bisnis untuk melaporkan informasi rinci kepada KTT sebelum dan sesudah konversi data, bersama dengan kewajiban untuk memberikan kode sumber atau "pintu belakang" kepada pemerintah, menciptakan hambatan teknis non-tarif yang mahal. Analisis ekonomi kuantitatif menunjukkan bahwa pembatasan data di masa lalu Indonesia telah menyebabkan kerusakan makroekonomi yang serius: penurunan output perdagangan sebesar 9,1%, penurunan produktivitas tenaga kerja sebesar 3,7%, dan peningkatan harga pasar konsumen sebesar 1,9% karena biaya kepatuhan yang langsung dibebankan kepada pengguna akhir. Selain itu, perusahaan teknologi multinasional, khususnya dari AS, terpaksa menarik sumber daya teknis yang berharga dari pusat Penelitian & Pengembangan mereka untuk berinvestasi dalam infrastruktur guna memenuhi kebutuhan Indonesia yang terfragmentasi, sehingga melemahkan daya saing global dalam kecerdasan buatan dan komputasi awan. Sebaliknya, Vietnam menggunakan perangkat hukum seperti pisau bedah yang tajam, secara langsung menargetkan yurisdiksi atas informasi warga negara. Dekrit 53 menetapkan mekanisme "pemicu" yang cerdas di mana perusahaan asing diancam harus membangun pusat data yang mahal di Vietnam jika mereka berani menentang perintah sensor konten dari Departemen A05. Lebih lanjut, Dekrit 147 mendorong batas kendali hingga ekstrem dengan memaksa platform dengan lebih dari 100.000 kunjungan untuk mengumpulkan dan membagikan informasi identifikasi pengguna, serta memelihara server yang berlokasi di Vietnam. Mekanisme kendali ganda ini menjadikan Vietnam salah satu lingkungan operasi paling kompleks di dunia untuk platform kebebasan berbicara. Campur tangan ini tidak hanya menciptakan lingkungan sensor diri yang sangat mengakar dalam media daring tetapi juga menghambat integrasi data bebas dalam Kerangka Ekonomi Digital ASEAN. Meskipun sistem Penilaian TIA Vietnam—yang memungkinkan transfer data berdasarkan deklarasi mandiri dan pasca-audit—dianggap lebih ramah terhadap komputasi awan daripada sistem pra-otorisasi Indonesia, lanskap hukum secara keseluruhan masih memberikan tekanan signifikan pada investor teknologi. Misalnya, startup

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

fintech yang berbasis di Vietnam yang ingin memperluas pembayaran elektroniknya ke wilayah tersebut akan terjebak dalam matriks kepatuhan: mereka harus menerapkan TIA Vietnam, memenuhi standar DPIA Singapura, mematuhi pengecualian penyimpanan PP 71 Indonesia, dan menghadapi sistem DPIA Thailand yang masih baru, yang mengakibatkan pengurasan modal operasional yang substansial.

Mekanisme Sanksi dan Sensor

Perbandingan antara Vietnam dan Indonesia juga memperlihatkan perbedaan yang signifikan dalam tingkat ketegasan mekanisme sanksi serta praktik pengawasan terhadap ruang digital. Dari sisi sanksi finansial administratif, Vietnam menunjukkan pendekatan yang jauh lebih keras. Dalam rancangan regulasi terbaru mengenai sanksi administrasi di bidang siber, pemerintah Vietnam mengusulkan denda maksimum hingga 5% dari total pendapatan tahunan perusahaan di Vietnam untuk pelanggaran serius. Bahkan untuk pelanggaran yang bersifat prosedural, sanksi tetap dapat mencapai 1 miliar VND, yang menunjukkan pendekatan penegakan hukum yang sangat ketat. Sebaliknya, di Indonesia batas maksimum denda administratif dalam Undang-Undang Perlindungan Data Pribadi 2022 ditetapkan sebesar 2% dari total pendapatan atau keuntungan tahunan perusahaan. Selain sanksi finansial, pemerintah Indonesia juga dapat menjatuhkan sanksi tambahan seperti penghentian sementara kegiatan usaha atau bahkan penutupan perusahaan.

Perbedaan lain terlihat dalam pengaturan tanggung jawab pidana. Di Vietnam, undang-undang perlindungan data tidak secara spesifik mengatur sanksi pidana bagi pelanggaran data pribadi. Apabila suatu pelanggaran dikategorikan sebagai tindak kejahatan siber, maka penanganannya akan dirujuk pada Pasal 286 Kitab Undang-Undang Hukum Pidana, yang mengatur kejahatan terkait penggunaan jaringan komputer dan telekomunikasi. Sebaliknya, Indonesia mengatur tanggung jawab pidana secara lebih eksplisit dalam PDP 2022. Individu yang dengan sengaja melakukan pelanggaran serius terhadap perlindungan data pribadi dapat dijatuhi hukuman 4 hingga 6 tahun penjara serta denda antara 4 hingga 6 miliar rupiah. Apabila pelanggaran tersebut dilakukan oleh organisasi atau perusahaan, maka denda yang dikenakan dapat mencapai sepuluh kali lipat dari sanksi yang dijatuhkan kepada individu.

Dalam hal kewenangan pemerintah untuk meminta penghapusan konten digital, kedua negara juga menunjukkan pendekatan yang cukup kuat, meskipun dengan mekanisme yang berbeda. Di Vietnam, platform digital diwajibkan untuk menghapus konten dalam waktu 24 jam setelah menerima permintaan resmi dari pemerintah, serta harus menanggapi pengaduan pengguna dalam waktu 48 jam. Kegagalan mematuhi ketentuan ini dapat berujung pada sanksi berat, termasuk pemutusan akses layanan di dalam wilayah Vietnam. Sementara itu, di Indonesia pemerintah mengandalkan UU ITE sebagai dasar hukum untuk memblokir atau menurunkan konten yang dianggap melanggar hukum. Dalam situasi tertentu, terutama ketika terjadi kerusuhan atau konflik sosial, pemerintah bahkan dapat menerapkan pembatasan atau pemutusan akses internet pada tingkat wilayah tertentu sebagai langkah pengendalian keamanan.

Selain itu, perbedaan juga terlihat dalam tingkat intervensi negara terhadap ruang privat pengguna internet. Di Vietnam, Dekrit 147 mewajibkan semua akun media sosial untuk diverifikasi menggunakan nomor identitas nasional atau nomor telepon domestik, sehingga identitas pengguna dapat dilacak dengan mudah oleh otoritas. Pemerintah juga memiliki kewenangan untuk meminta akses terhadap data identitas pengguna kapan pun diperlukan dalam rangka penegakan hukum atau keamanan nasional. Di sisi lain, di Indonesia pemerintah mewajibkan penyelenggara sistem elektronik untuk menyediakan akses khusus atau "backdoor" ke dalam sistem mereka guna mendukung kegiatan pengawasan dan penegakan hukum. Ketentuan ini diatur dalam PP 71 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang memberikan dasar hukum bagi pemerintah untuk memperoleh akses terhadap data elektronik ketika diperlukan.

Penerapan sanksi terhadap serangan siber yang berasal dari luar wilayah negara menghadapi tantangan yurisdiksi, terutama karena pelaku, server, maupun infrastruktur digital sering berada di negara yang berbeda. Dalam konteks Vietnam dan Indonesia, mekanisme penegakan hukum terhadap serangan lintas batas umumnya dilakukan melalui kombinasi pendekatan hukum nasional, kerja sama internasional, dan koordinasi antar lembaga keamanan siber.

Di Vietnam, Undang-Undang Keamanan Siber memberikan kewenangan kepada negara untuk meminta platform digital asing bekerja sama dalam penghapusan konten, penyerahan data pengguna, serta pemblokiran akses terhadap layanan yang dianggap mengancam keamanan nasional. Pemerintah juga dapat menerapkan sanksi administratif terhadap perusahaan asing yang beroperasi di Vietnam apabila tidak memenuhi kewajiban lokalisasi data, verifikasi identitas pengguna, atau permintaan penegakan hukum. Dalam kasus serangan siber lintas negara, Vietnam mengandalkan kerja sama internasional melalui mekanisme bantuan hukum timbal balik (mutual legal assistance), kerja sama kepolisian internasional, serta koordinasi keamanan siber regional ASEAN dan konvensi internasional terkait kejahatan siber (Chi,

2018; Phuong, 2023).

Sementara itu, di Indonesia, Undang-Undang Perlindungan Data Pribadi 2022 dan UU ITE memiliki cakupan ekstrateritorial, sehingga secara hukum dapat diterapkan terhadap pelaku atau perusahaan asing yang aktivitas digitalnya berdampak pada warga negara Indonesia. Namun, implementasi sanksi terhadap pelaku di luar negeri tetap bergantung pada kerja sama internasional, seperti ekstradisi, pertukaran informasi intelijen siber, dan koordinasi melalui INTERPOL atau forum keamanan siber regional. Pemerintah Indonesia juga dapat menjatuhkan sanksi administratif terhadap platform digital asing, termasuk pemblokiran akses layanan atau pembatasan operasional apabila perusahaan tidak mematuhi regulasi nasional (Bahtiar, 2025; Harsya, 2025; Sumaragatha & Evangelista, 2025).

Meskipun demikian, baik Vietnam maupun Indonesia masih menghadapi keterbatasan dalam penegakan hukum lintas batas, terutama terkait perbedaan yurisdiksi hukum, kurangnya harmonisasi regulasi internasional, keterbatasan kapasitas investigasi digital forensik, serta ketergantungan pada kerja sama negara lain. Oleh karena itu, efektivitas penerapan sanksi terhadap serangan siber internasional tidak hanya bergantung pada kekuatan regulasi domestik, tetapi juga pada kapasitas diplomasi digital dan kerja sama keamanan siber internasional.

D. Pelajaran Strategis untuk Indonesia dari Vietnam

Secara lebih luas, perbandingan antara Vietnam dan Indonesia menunjukkan bahwa regulasi keamanan siber dan perlindungan data bukanlah instrumen hukum yang netral secara politik, melainkan produk dari relasi kekuasaan yang berbeda dalam tata kelola digital. Dalam perspektif *power and governance theory* (Chhotray & Stoker, 2009; Griffin, 2012; Haus, 2018), regulasi digital mencerminkan bagaimana negara mendefinisikan distribusi otoritas antara pemerintah, pasar digital, dan warga negara dalam ruang siber. Vietnam merepresentasikan model *state power dominance* (Jessop, 2007; John, 2019; Migdal et al., 1994), di mana negara mempertahankan posisi hegemonik dalam mengendalikan arus informasi, infrastruktur data, dan aktivitas platform digital. Dalam model ini, regulasi keamanan siber berfungsi tidak hanya sebagai instrumen perlindungan teknis, tetapi juga sebagai mekanisme reproduksi stabilitas politik dan legitimasi negara. Oleh karena itu, praktik seperti lokalisasi data, verifikasi identitas pengguna, dan kewajiban kerja sama platform digital dengan aparat keamanan mencerminkan perluasan kapasitas pengawasan negara ke dalam ruang digital Masyarakat.

Sebaliknya, Indonesia menunjukkan pola tata kelola yang lebih bersifat negosiatif antara kepentingan negara, pasar, dan hak-hak warga negara (Ningtyas, 2023; Siswantoro, 2026). Adopsi prinsip-prinsip perlindungan data yang terinspirasi GDPR memperlihatkan adanya tekanan global pasar digital dan kebutuhan integrasi ekonomi internasional yang memengaruhi pembentukan regulasi nasional. Namun, pada saat yang sama, negara tetap mempertahankan instrumen kontrol melalui mekanisme pemblokiran platform, pengawasan konten, dan akses terhadap data elektronik. Kondisi ini menunjukkan bahwa regulasi digital di Indonesia berkembang melalui kompromi antara logika keamanan negara, tuntutan pasar digital global, dan narasi perlindungan hak individu (Ambardi et al., 2025; Anwar & Nepri, 2025). Dengan demikian, studi ini memperlihatkan bahwa regulasi keamanan siber di Asia Tenggara pada dasarnya merupakan arena politik yang memperlihatkan negosiasi kekuasaan antara aktor negara, perusahaan teknologi, dan masyarakat digital.

Perbedaan-perbedaan ini dapat memberikan pelajaran yang berbeda bagi kedua negara. Pertama, atasi krisis tata kelola dengan Sistem Komando Siber terpadu. Jika ada satu hal yang perlu dipelajari pemerintah Indonesia dari Vietnam, itu adalah efektivitas sistem komando terpusat. Runtuhnya PDN akibat serangan ransomware mengungkap kelemahan fatal Indonesia: perpecahan antara BSSN yang kekurangan dana, kekuasaan Kementerian Digital (MOCD) yang terbatas, dan TNI yang tidak bergerak. Indonesia perlu membangun struktur kekuasaan yang mirip dengan "Pusat Koordinasi Keamanan Siber Nasional" (NCCC), atau membentuk Satuan Tugas Pertahanan Siber Gabungan (JCDTF). Model ini, mirip dengan kekuasaan eksekutif yang luas yang dimiliki Departemen A05 di Vietnam, akan mengintegrasikan kemampuan sipil dan sumber daya perang siber militer secara erat, memastikan respons terpadu dan cepat terhadap bencana tingkat nasional sambil mempertahankan kendali sipil.

Kedua, kecepatan dan ketegasan proses transisi hukum. Para pembuat undang-undang Vietnam telah menunjukkan kecepatan yang luar biasa dalam mengisi celah legislatif. Dari penerbitan dekrit tanggap cepat (Dekrit 53, 13, 147) hingga pengesahan undang-undang berskala besar (UU Data, UU PDP 2025/2026), proses ini telah berlangsung terus-menerus, konsisten, dan tegas. Sebaliknya, stagnasi Indonesia setelah adopsi UU PDP 2022, yang dibuktikan dengan kegagalannya untuk membentuk DPA yang independen dan berstatus hukum selama bertahun-tahun, dan gangguan dari putusan retrospektif Mahkamah Konstitusional tentang standar DPO, telah menciptakan lingkungan operasional yang berisiko dan tidak dapat diprediksi bagi bisnis. Indonesia perlu secara signifikan meningkatkan kapasitas penegakannya dan mempersingkat proses implementasi dokumen sub-

Public Knowledge / Volume 3 Issue 2
DOI 10.62771/pk. V3i2.34

hukum.

Ketiga, mengganti hambatan administratif dengan mekanisme Penilaian Dampak. Sistem perizinan dan pelaporan yang rumit dari KTI setiap kali bisnis ingin mentransfer data lintas batas berdasarkan PP 71 saat ini menghambat alur kerja teknologi secara real-time. Indonesia dapat belajar dari pendekatan Vietnam dalam mengelola data lintas batas melalui basis deklarasi mandiri menggunakan dokumen TIA. Mekanisme ini mentransfer tanggung jawab penilaian risiko kepada bisnis, dengan lembaga pemerintah hanya berperan sebagai peninjau pasca-audit, alih-alih menciptakan pos pemeriksaan yang menghambat arus digital.

Kesimpulan

Pengembangan dan penyempurnaan kerangka hukum untuk keamanan siber dan perlindungan data di Vietnam dan Indonesia melukiskan dua gambaran yang sangat kontras tentang tata kelola digital, yang sangat mencerminkan kondisi historis, struktur politik, dan ambisi ekonomi masing-masing negara di abad ke-21.

Vietnam telah memilih jalur kontrol maksimal, memandang dunia maya sebagai medan pertempuran hidup dan mati untuk keamanan nasional. Dengan menerapkan alat penegakan hukum yang keras seperti lokalisasi data bersyarat, penegakan verifikasi identitas di dunia nyata yang ketat, penghapusan anonimitas di media sosial, dan pemusatan kekuasaan absolut pada aparat keamanan (Kementerian Keamanan Publik), Vietnam membangun "benteng digital" yang kokoh. Pendekatan ini memungkinkan negara untuk segera menetralisir ancaman terhadap ketidakstabilan politik, tetapi pada saat yang sama menciptakan hambatan besar pada kebebasan berbicara dan meningkatkan biaya kepatuhan yang sangat besar bagi ekosistem inovasi global, yang berisiko menghambat aliran investasi asing langsung (FDI) teknologi tinggi.

Sebaliknya, Indonesia mengejar model legislatif yang lebih komprehensif, berupaya untuk selaras dengan standar Eropa tertinggi untuk memaksimalkan hak-hak individu dan mempromosikan ekonomi digital yang terbuka dan transparan. Namun, tujuan teoritis yang ambisius ini menghadapi hambatan signifikan dalam implementasinya. Sistem tata kelola keamanan siber yang sangat terfragmentasi, anggaran investasi yang menipis, ketiadaan pemimpin strategis yang terpadu (dicontohkan oleh keterlambatan pembentukan PDO independen dan kegagalan sistem PDN dalam mengatasi malware), dan perubahan peraturan yang tidak konsisten terkait personel perlindungan data telah membuat hukum-hukum canggih negara ini tidak berguna dalam praktiknya.

Tidak ada model yang benar-benar sempurna di era digital, dengan risiko non-tradisional yang selalu berubah. Masa depan kemakmuran digital di Asia Tenggara akan bergantung pada kemampuan kedua negara untuk saling belajar. Indonesia harus memperkuat disiplin penegakan hukumnya, memusatkan sistem pertahanan keamanan sibernya, dan menghubungkan kekuatan sipil dan militer untuk mencegah bencana infrastruktur yang dahsyat. Dengan mencapai keseimbangan yang tepat antara pertahanan keamanan siber yang kuat, penghormatan terhadap privasi warga negara, dan arus bebas data ekonomi lintas batas, baik Vietnam maupun Indonesia dapat dengan mantap membangun posisi kepemimpinan dalam membentuk era digital yang berkembang pesat di kawasan ASEAN.

Secara teoretis, penelitian ini berkontribusi pada pengembangan studi comparative digital governance dengan menunjukkan bahwa regulasi keamanan siber dan perlindungan data di negara berkembang tidak bersifat netral secara teknis, tetapi dibentuk oleh filosofi tata kelola negara, distribusi kekuasaan politik, dan kapasitas institusional masing-masing negara. Studi ini memperluas diskusi mengenai state-centric digital sovereignty, regulatory fragmentation, dan institutional capacity dalam konteks Asia Tenggara, khususnya melalui perbandingan antara model kontrol negara yang terpusat di Vietnam dan model tata kelola multi-aktor yang lebih terfragmentasi di Indonesia. Dari sisi kebijakan, hasil penelitian menunjukkan pentingnya membangun keseimbangan antara keamanan nasional, perlindungan hak digital warga negara, dan kebutuhan integrasi ekonomi digital global. Indonesia perlu memperkuat koordinasi kelembagaan dan kapasitas penegakan keamanan siber, sementara Vietnam menghadapi tantangan untuk meningkatkan transparansi regulasi dan perlindungan hak privasi agar tetap menarik bagi ekosistem ekonomi digital internasional. Untuk penelitian selanjutnya, studi ini membuka peluang analisis lebih lanjut mengenai implementasi empiris regulasi keamanan siber, respons masyarakat sipil terhadap pengawasan digital negara, serta perbandingan tata kelola keamanan siber di negara-negara ASEAN lainnya dalam menghadapi perkembangan kecerdasan buatan, big data, dan ancaman siber lintas batas.

UCAPAN TERIMA KASIH

Penulis ingin menyampaikan rasa terima kasih yang tulus kepada Ibu Ho Tran Bao Tram, LL.M, atas penelitian kolaboratifnya dan atas pemberian perspektif komprehensif tentang hukum Vietnam. Kami juga berterima kasih kepada Pemimpin Redaksi Dr. Yusa Djuyandi, S.IP., M.SI., atas bantuannya

dalam menyunting versi bahasa Indonesia, karena bahasa utama penulis bukanlah bahasa Indonesia..

Referensi

AHP. (2019, October 25). Government Relaxes Data Localisation Requirement. Assegaf Hamzah & Partners. https://www.ahp.id/client-update-25-october-2019/

Ajiraga, H. (2026). Peran dan Tanggungjawab Data Protection Officer dalam Pelaksanaan Perlindungan Data Pribadi. Asas Wa Tandhim: Jurnal Hukum, Pendidikan Dan Sosial Keagamaan, 5(1), 261–290. https://doi.org/10.47200/awtjhpsa.v5i1.3209

Alfath, T. P., & Cahya, W. (2024). Bridging the Gap Between Policy and Practice: Evaluating Indonesia's Cybersecurity Regulatory Framework (2020–2023). Data: Journal of Information Systems and Management, 2(1), 14–24.

Ambardi, K., Widhyharto, D. S., Madya, S. H., & Wibawanto, G. R. (2025). Masyarakat Digital: Teknologi Kekuasaan dan Kekuasaan Teknologi. UGM PRESS.

Andita, B. P., Yitawati, K., & Haryani, A. T. (2025). Legal Protection for Indonesian Migrant Workers Against Online Scam–Based Human Trafficking. Potret Pemikiran, 29(2), 268–281. https://doi.org/10.30984/pp.v29i2.4139

Anissa, Y. N., & Djuyandi, Y. (2021). Analisis Pemenuhan Kebutuhan Minimum Essential Froce (MEF) Dalam Pengadaan Alat Utama Sistem Senjata (Alutsista) Tentara Nasional Indonesia (TNI). Scripta: Jurnal Ilmiah Mahasiswa, 3(1), 34–55. https://doi.org/10.33019/scripta.v3i1.115

Antoniuk, D. (2024, March 19). China-linked hackers target governments and more in Southeast Asia with new backdoors. The Record from Recorded Future News. https://therecord.media/earth-krahang-china-linked-espionage-group-new-backdoors

Anwar, S., & Nepri, J. E. (2025). Harmonisasi Hukum Digital: Tantangan Global dan Strategi Adaptif Indonesia dalam Era Kedaulatan Siber. Hutanasyah : Jurnal Hukum Tata Negara, 4(1), 69–88. https://doi.org/10.37092/hutanasyah.v4i1.1297

Atkinson, P., & Delamont, S. (2010). SAGE Qualitative Research Methods. SAGE Publications, Inc. https://doi.org/10.4135/9780857028211

Awaluddin. (2025). The Existence of Law Number 27 Of 2022 Concerning Personal Data Protection in Protecting Citizens' Privacy Rights. Indonesian Research Journal in Legal Studies, 4(2), 54–60. https://doi.org/10.31934/irjils.v4i2.8717

Bahtiar, M. Y. (2025). Kebijakan dan Regulasi Ekonomi Digital di Indonesia: Analisis Regulasi Otoritas Jasa Keuangan, Bank Indonesia, Kementerian Komunikasi dan Digital, Pajak Digital, serta Perlindungan Data dan Keamanan Siber. Journal of Economics, Management, and Accounting, 1(1), 268–275. https://doi.org/10.65310/avm33948

Ballanca, E. (2025). Between ethics and algorithms: Protecting rights in the digital era. Journal of Modern Science, 64(4), 387–402. https://doi.org/10.13166/jms/215775

Bandemer, S., Daßler, B., Rittberger, B., Weiss, M., & Will, K. (2026). Rule-takers or rule-makers? How regional hubs design digital governance frameworks. Globalizations, 1–23. https://doi.org/10.1080/14747731.2026.2653368

Cars, G., Healey, P., Madanipour, A., & Magalhães, C. S. de (Eds.). (2018). Urban governance, institutional capacity and social milieux. Routledge, Taylor & Francis Group.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. Oncology Nursing Forum, 41(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Chhotray, V., & Stoker, G. (2009). Governance: From Theory to Practice. In V. Chhotray & G. Stoker, Governance Theory and Practice (pp. 214–247). Palgrave Macmillan UK. https://doi.org/10.1057/9780230583344_10

Chi N. N. (2018). International cooporation in criminal procedure to meet the requirement of globalization trend and international intergration. VNU Journal of Science: Legal Studies, 34(2), 1–13. https://doi.org/10.25073/2588-1167/vnuls.4158

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 10(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Christian, J. B. C. (2019). Transplante jurídico = Legal trasplant. EUNOMÍA. Revista En Cultura de La Legalidad, 262–275. https://doi.org/10.20318/eunomia.2019.5032

DLA Piper. (2025, January 20). Data protection laws in Indonesia. DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=law&c=ID

Garcia, D. (2016). Future arms, technologies, and international law: Preventive security governance. European Journal of International Security, 1(1), 94–111. https://doi.org/10.1017/eis.2015.7

Griffin, L. (2012). Where is Power in Governance? Why Geography Matters in the Theory of Governance. Political Studies Review, 10(2), 208–220. https://doi.org/10.1111/j.1478-9302.2012.00260.x

Ha, H., & Chuah, C. K. P. (2023). Digital economy in Southeast Asia: Challenges, opportunities and future development. Southeast Asia: A Multidisciplinary Journal, 23(1), 19–35. https://doi.org/10.1108/SEAMJ-02-2023-0023

Harsya, R. M. K. (2025). Tinjauan Yuridis terhadap Tanggung Jawab Platform Digital atas Konten Ilegal Menurut Hukum Indonesia. Sanskara Hukum dan HAM, 4(01), 276–286. https://doi.org/https://doi.org/10.58812%2Fshh.v4.i01

Harun, H., & Kamase, H. P. (2012). Accounting Change and Institutional Capacity: The Case of a Provincial Government in Indonesia. Australasian Accounting, Business and Finance Journal, 6(2), 35–50.

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. Global Political Studies Journal, 7(1), 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141

Haus, M. (2018). Governance and power. In H. Heinelt (Ed.), Handbook on Participatory Governance. Edward Elgar Publishing. https://doi.org/10.4337/9781785364358.00009

Heryadi, D., Rizaldi, R., Rahmadhani, T. P., Miranti, F. D., & Juliastica, F. (2024). Indonesia's Role as A Cyber Protector in the Southeast Asia Region. Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity, 10(1), 169–187. https://doi.org/10.33172/jp.v10i1.13097

Huynh T. H. (2025, December 12). Beberapa poin baru penting dari Undang-Undang Keamanan Siber yang telah diamandemen dan disahkan pada Sidang ke-10 Majelis Nasional ke-15. Universitas Kepolisian Rakyat. https://dhcsnd.edu.vn/mot-so-diem-moi-cot-loi-cua-luat-an-ninh-mang-sua-doi-duoc-thong-qua-tai-ky-hop-thu-10-quoc-hoi-khoa-xv

ITIF. (2025). Indonesia's Data Localization Regulation. Information Technology and Innovation Foundation. https://itif.org/publications/2025/06/09/indonesia-data-localization-regulation/

Jessop, B. (2007). State Power. Polity.

Jessop, B. (2009). From Governance to Governance Failure and from Multi-level Governance to Multi-scalar Meta-governance. In B. Arts, A. Lagendijk, & H. V. Houtum (Eds.), The Disoriented State: Shifts in Governmentality, Territoriality and Governance (Vol. 49, pp. 79–98). Springer Netherlands. https://doi.org/10.1007/978-1-4020-9480-4_4

John, F. M. (2019). Domination, State Power, and Political Repression. In P. T. Bushnell, V. Shlapentokh, C. Vanderpool, J. Sundram, P. T. Bushnell, V. Shlapentokh, C. K. Vanderpool, & J. Sundram (Eds.), State Organized Terror: The Case of Violent Internal Repression (1st ed.). Routledge. https://doi.org/10.4324/9780429307447

Joseph, K., Lowry, M., & Volkova, E. (2025). Regulatory Fragmentation. The Journal of Finance, 80(2), 1081–1126. https://doi.org/10.1111/jofi.13423

Kelliher, F. (2024, January 3). China data leak spotlights cyber-spying across Southeast Asia. Nikkei Asia. https://asia.nikkei.com/politics/international-relations/china-data-leak-spotlights-cyber-spying-across-southeast-asia

Khong V. H. (2026, February 19). Hukum Keamanan Siber 2025: Dampak pada Bisnis Teknologi dan Pasar Ekonomi Digital. Jurnal Hukum. https://phaply.net.vn/luat-an-ninh-mang-2025-nhung-tac-dong-toi-doanh-nghiep-cong-nghe-va-thi-truong-kinh-te-so-a261078.html

Maulana, A., Ikhsan, W., & Soetijoni, I. K. (2026). Otoritas Kementerian Komunikasi dan Digitalisasi dalam Pemblokiran Aplikasi dan Situs Judi Daring Menurut Undang-Undang ITE. Al-Zayn : Jurnal Ilmu Sosial & Hukum, 4(2), 42–54. https://doi.org/10.61104/alz.v4i2.4244

Migdal, J. S., Kohli, A., & Shue, V. (1994). State Power and Social Forces: Domination and Transformation in the Third World. Cambridge University Press.

Minh Q. (2025, November 16). Undang-Undang Keamanan Siber Terkonsolidasi: "Perisai digital" Vietnam yang sangat diperlukan di era transformasi digital. Jurnal Elektronik

Pengadilan Rakyat. https://tapchitoaan.vn/luat-an-ninh-mang-hop-nhat-%22la-chan-so%22-khong-the-thieu-cua-viet-nam-trong-ky-nguyen-chuyen-doi-so14439.html

Nethan, & Situbuana, T. H. (2025). Implementasi Fungsi Perlindungan Kementerian Komunikasi Dan Digital Dalam Menjamin Perlindungan Data Pribadi Warga Negara Indonesia. Kertha Semaya: Journal Ilmu Hukum, 13(10), 2339–2349. https://doi.org/10.24843/KS.2025.v13.i10.p14

Nguyen, T.-D., Research fellow at the Institute of State and Law, Vietnam Academy of Social Sciences., Nguyen, L.-G., & Deputy Director General at the Institute of State and Law, Vietnam Academy of Social Sciences. (2025). Responsive Centralism: The Political and Regulatory Landscape of Vietnam's Digital Transformation. Contemporary Southeast Asia, 47(3), 353–382. https://doi.org/10.1355/cs47-3a

Ningtyas, V. A. A. (2023). Netralitas Aparatur Sipil Negara Dalam Pemilu Antara Hak Politik dan Kewajiban Untuk Melaksanakan Tata Kelola Pemerintahan yang Baik. Binamulia Hukum, 10(1), 15–30. https://doi.org/10.37893/jbh.v10i1.374

Oktavia, F., & Martini, S. (2016). Besar Risiko Kejadian Hipertensi Berdasarkan Faktor Perilaku Pada Tentara Nasional Indonesia (TNI). Media Kesehatan Masyarakat Indonesia, 12(3), 127–136. https://doi.org/10.30597/mkmi.v12i3.1067

Paruchuri, S., Hoempler, E. A., Cowen, A. P., Cannella, A. A., & Nahm, P. I. (2024). Governance Failure and Governance Under Failure: Reviewing the Role of Directors in Organizational Misconduct. Journal of Management, 50(6), 2237–2265. https://doi.org/10.1177/01492063231225420

Peters, B. G. (2015). State failure, governance failure and policy failure: Exploring the linkages. Public Policy and Administration, 30(3–4), 261–276. https://doi.org/10.1177/0952076715581540

Petticrew, M., & Roberts, H. (2006). Systematic Reviews in the Social Sciences. Wiley. https://doi.org/10.1002/9780470754887

Phuong, N. T. (2023). Enhancing international cooperation in investigating cybercrimes that threaten national security. Journal of State Management, (333), 86–90. https://doi.org/10.59394/qlnn.333.2023.658

Polk, M. (2011). Institutional Capacity-building in Urban Planning and Policy-making for Sustainable Development: Success or Failure? Planning Practice and Research, 26(2), 185–206. https://doi.org/10.1080/02697459.2011.560461

Prakosa, T., Dadang A.R, D., & Hartono, D. (2026). Transformation of Territorial Security in the Digital Era: A Case Study of Sebatik Island as a Border Space Facing Cyber Threats. Indonesian Journal of Interdisciplinary Research in Science and Technology, 4(1), 15–32. https://doi.org/10.55927/marcopolo.v4i1.2

Prawiyogi, A. G. & Alwiyah. (2023). Southeast Asia's Cyber Security Strategy: Multilateralism or Self-help. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 4(2), 119–127. https://doi.org/10.34306/itsdi.v4i2.581

Prokopyshyn, O., & Trushkina, N. (2025). The Geopolitics Of Cybersecurity: A Comparative Analysis Of National Strategies For Digital Sovereignty. Politics & Security, 12(2), 59–71. https://doi.org/10.54658/ps.28153324.2025.12.2.pp.59-71

Putri, W. (2026). Normative Legal Research Methodology from the Experts' Perspective: A Comparative Analysis of Concepts and Approaches. Archipel: Journal of Indonesian Interdisciplinary Studies, 1(6), 12–25. https://doi.org/10.65739/archipel.v1i6.34

Rodriguez, K. (2021, November 23). Indonesian Court Allows Internet Blocking During Unrest, Tightening Law Enforcement Control Over Users' Communications and Data | Electronic Frontier Foundation. Electronic Frontier Foundatio. https://www.eff.org/deeplinks/2021/11/indonesian-court-allows-internet-blocking-during-unrest-tightening-law-enforcement

Roger, M. A. (2018). Comparación jurídica desde el sur global genealogía de un proyecto crítico. THEMIS Revista de Derecho, (73), 131–145. https://doi.org/10.18800/themis.201801.011

ROUSE. (2025, February 9). Data Localisation and Transfer Issues in Southeast Asia: What Businesses Need to Know. Rouse Network. https://rouse.com/insights/news/2025/data-localisation-and-transfer-issues-in-southeast-asia-what-businesses-need-to-know/

Sacco, R. (1991). Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II). The American Journal of Comparative Law, 39(1), 1. https://doi.org/10.2307/840669

Schlunegger, M. C., Zumstein-Shaha, M., & Palm, R. (2024). Methodologic and Data-Analysis Triangulation in Case Studies: A Scoping Review. Western Journal of Nursing Research, 46(8), 611–622.

https://doi.org/10.1177/01939459241263011

Shives, T., & Fatahillah, F. (2026). A Comprehensive Cyber Defense Framework for the Indonesian National Armed Forces: Bridging Governance Gaps for National and ASEAN Cyber Resilience. International Conference on Cyber Warfare and Security, 21(1), 751–758. https://doi.org/10.34190/iccws.21.1.4553

Siswantoro, M. I. (2026). Hubungan Negara Dan Warga Negara Dalam Sistem Demokrasi Indonesia. Jurnal Pendidikan Dewantara: Media Komunikasi, Kreasi Dan Inovasi Ilmiah Pendidikan, 12(1), 122–135. https://doi.org/10.55933/jpd.v12i1.1161

Sobieraj, D. M., & Baker, W. L. (2021). Research and scholarly methods: Systematic reviews. JACCP: Journal of The American College of Clinical Pharmacy, 4(7), 849–854. https://doi.org/10.1002/jac5.1440

Suleiman, A., Audrine, P., & Dewaranu, T. (2022). Pengaturan Bersama dalam Perlindungan Data Pribadi: Potensi Peran Asosiasi Industri sebagai Organisasi Regulator Mandiri (0 ed.). Center for Indonesian Policy Studies. https://doi.org/10.35497/555906

Sumaragatha, I. G. B. S., & Evangelista, B. (2025). Tinjauan Hukum Terhadap Pengaturan Penanaman Modal Asing Pada Sektor E-Commerce Di Indonesia: Legal Review of Foreign Investment Regulations in the E-Commerce Sector in Indonesia. Ganec Swara, 19(4), 1561–1567. https://doi.org/10.59896/gara.v19i4.425

Tran, B. (2024). Vietnam Strengthens Cyber Capabilities for Political Stability, National Defence, and Socio-economic Development. ISEAS Perspective, 2024(78).

Tran, L. Q. T., Phan, D. T., & Nguyen, M. T. (2022). Digital Economy: A Comparative Study in ASEAN. Theory, Methodology, Practice, 18(2), 83–92. https://doi.org/10.18096/TMP.2022.02.05

UNCDF. (2021). The role of cybersecurity and data security in the digital economy. UN Capital Development Fund.

Undang-Undang Perlindungan Data Pribadi, Pub. L. No. 91/2025/QH15 (2026).

Von Knebel, M. (2023). Cross-country comparative analysis and case study of institutions for future generations. Futures, 151, 103181. https://doi.org/10.1016/j.futures.2023.103181

Xu, H. (2024). Regulatory fragmentation and internal control weaknesses. Journal of Accounting and Public Policy, 44, 107191. https://doi.org/10.1016/j.jaccpubpol.2024.107191

Zhang, C., & Morris, C. (2023). Borders, bordering and sovereignty in digital space. Territory, Politics, Governance, 11(6), 1051–1058. https://doi.org/10.1080/21622671.2023.2216737