BAB II

KERANGKA REGULASI UNTUK KEAMANAN SIBER DI ASIA TENGGARA

Dalam menghadapi eskalasi ancaman siber yang kian kompleks, regulasi menjadi elemen fundamental dalam membangun ketahanan digital suatu negara maupun kawasan. Kawasan Asia Tenggara, yang tengah mengalami percepatan digitalisasi dan pertumbuhan ekonomi berbasis teknologi, kini menjadi target empuk bagi berbagai jenis serangan siber, khususnya spyware dan ransomware. Serangan-serangan ini tidak hanya menimbulkan kerugian finansial bagi perusahaan, tetapi juga mengancam integritas data, stabilitas operasional, dan kepercayaan publik.

Di tengah kondisi tersebut, pemerintah negara-negara Asia Tenggara dituntut untuk merumuskan dan menerapkan kerangka regulasi yang mampu menjawab tantangan keamanan informasi di tingkat korporasi maupun nasional. Regulasi tersebut tidak hanya perlu bersifat teknis, tetapi juga harus inklusif, adaptif, dan mampu mendorong kolaborasi lintas sektor, terutama antara negara dan sektor swasta. Keberadaan kerangka hukum yang kuat dan konsisten menjadi prasyarat utama dalam menciptakan lingkungan siber yang aman dan terpercaya.

Bab ini akan membahas bagaimana regulasi-regulasi siber dikembangkan di tingkat nasional maupun regional di Asia Tenggara. Fokus utama diberikan pada pemetaan kebijakan, perbandingan pendekatan antarnegara, serta analisis terhadap tantangan implementasi yang dihadapi, khususnya dalam konteks kemitraan publik-swasta untuk mengatasi ancaman malware. Subbab selanjutnya akan membahas

bagaimana ASEAN dan negara-negara anggotanya merespons ancaman siber melalui kebijakan domestik dan kerja sama regional.

2.1 Ancaman Siber dan Implementasi Regulasi ASEAN di Level Domestik

Keamanan siber menjadi salah satu isu kritis di era digital karena meningkatnya ancaman seperti peretasan, kebocoran data, dan serangan ransomware. Tanpa kerangka regulasi yang kuat, organisasi dan individu rentan terhadap risiko finansial, reputasi, dan operasional. Menurut laporan Verizon (2023), 83% pelanggaran data melibatkan elemen eksternal, dan 74% disebabkan oleh faktor manusia seperti kelalaian atau phishing. Regulasi yang jelas dapat meminimalkan risiko ini dengan menetapkan standar keamanan yang wajib diikuti oleh semua pihak.

Kerangka regulasi juga berperan dalam menciptakan akuntabilitas bagi pelaku bisnis dan pemerintah dalam melindungi data pengguna. Uni Eropa menerapkan General Data Protection Regulation (GDPR) pada 2018, yang berhasil mengurangi pelanggaran data hingga 19% dalam dua tahun pertama (European Union Agency for Cybersecurity, 2020). Regulasi semacam ini memaksa perusahaan untuk mengalokasikan sumber daya guna meningkatkan keamanan siber, sehingga mengurangi kerentanan sistem.

Di tingkat global, ketiadaan harmonisasi regulasi keamanan siber dapat menghambat penanganan ancaman lintas batas. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa Indonesia mengalami lebih dari 1,3 miliar serangan siber pada 2023, dengan sebagian besar berasal dari luar negeri (BSSN, 2023). Kerangka regulasi yang

terkoordinasi antarnegara dapat memfasilitasi pertukaran intelijen dan respons lebih cepat terhadap serangan transnasional.

Selain itu, regulasi keamanan siber mendorong inovasi teknologi dengan memberikan kepastian hukum bagi pengembangan solusi keamanan. Misalnya, Amerika Serikat menerapkan *Cybersecurity Maturity Model Certification* (CMMC) untuk memastikan perusahaan pertahanan memenuhi standar keamanan tertentu (U.S. Department of Defense, 2021). Hal ini tidak hanya melindungi data sensitif tetapi juga menciptakan pasar bagi industri keamanan siber yang diperkirakan bernilai $300 miliar pada 2025 (McKinsey & Company, 2022).

Terakhir, kerangka regulasi yang efektif harus mencakup edukasi publik untuk meningkatkan kesadaran akan keamanan digital. Survei dari Kaspersky (2023) menunjukkan bahwa 56% karyawan di Asia Tenggara tidak memahami protokol keamanan siber dasar. Dengan memasukkan pelatihan keamanan siber dalam regulasi, pemerintah dapat membangun ketahanan kolektif terhadap ancaman digital, mengurangi dampak serangan di tingkat individu maupun korporasi.

Tabel 1.1 Time Frame regulasi siber di ASEAN dan Indonesia

ASEAN				
ASEAN Cybersecurity Cooperation Strategy (2017–2020)		ASEAN Digital Masterplan 2025	ASEAN Framework on Personal Data Protection (PDP) (2016-2025)	
2017	2020	2021–2025	2016	2022-2025
Peluncuran strategi untuk meningkatkan kolaborasi keamanan siber di kawasan. Fokus: Pembentukan ASEAN CERT (Computer Emergency Response Team) dan kerangka hukum bersama.	Evaluasi dan penyusunan rencana lanjutan (periode 2021–2025).	Memperkuat keamanan siber melalui harmonisasi regulasi antar negara anggota dan peningkatan kapasitas cyber resilience di sektor publik dan private.	Pedoman perlindungan data pribadi untuk negara-negara ASEAN.	Implementasi di beberapa negara (misalnya: Singapura, Malaysia, Thailand).

Indonesia						
UU Informasi dan Transaksi Elektronik (UU ITE, No. 11/2008, direvisi menjadi UU No. 19/2016)		Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem Elektronik (PSE)	Perpres No. 47/2023 tentang Nasional Siber dan Sandi Negara	RUU Perlindungan Data Pribadi (PDP)		Roadmap Keamanan Siber Indonesia 2021–2025
2008	2016	2019	2023	2022	2024	2022-2025
Landasan hukum pertama untuk kejahatan siber. -2016.	Revisi mencakup perlindungan data dan ancaman seperti ransomware/ spyware	Kewajiban perusahaan untuk menerapkan cybersecurity dan melaporkan serangan siber.	Pembentukan Badan Siber dan Sandi Negara (BSSN) sebagai otoritas utama keamanan siber.	Disetujui DPR sebagai UU No. 27/2022.	Implementasi penuh (masih dalam tahap penyusunan aturan turunan).	Fokus pada peningkatan kapasitas SDM siber dan sertifikasi cybersecurity (contoh: ISO 27001, NIST Framework).

Sumber: (ASEAN, 2016-2021, DPR RI, 2016-2022, dan Pemerintah Indonesia, 2019)

2.2 Lanskap Regulasi di Asia Tenggara

Keamanan siber telah menjadi prioritas bagi negara-negara Asia Tenggara seiring dengan meningkatnya ancaman digital di kawasan ini. Singapura memimpin dengan kerangka regulasi yang komprehensif, terutama melalui Cybersecurity Act 2018, yang memberikan otoritas luas kepada Cyber Security Agency of Singapore (CSA) dalam menanggapi serangan siber. Menurut laporan CSA (2023), lebih dari 60% organisasi di Singapura telah mematuhi kerangka Essential Cybersecurity Controls, mengurangi insiden serangan siber sebesar 22% sejak 2020. Regulasi ini juga mewajibkan pelaporan insiden keamanan dalam waktu 24 jam, meningkatkan respons terhadap ancaman (CSA, 2023).

Malaysia juga telah memperkuat kerangka regulasinya dengan memperkenalkan Personal Data Protection Act (PDPA) dan National Cyber Security Policy (NCSP). Namun, implementasinya masih menghadapi tantangan, terutama dalam penegakan hukum. Menurut CyberSecurity Malaysia (2022), sekitar 40% perusahaan di Malaysia belum sepenuhnya mematuhi standar keamanan siber yang ditetapkan pemerintah. Serangan ransomware di Malaysia meningkat 45% pada 2022, menunjukkan perlunya pembaruan regulasi yang lebih ketat (Cybersecurity Malaysia, 2022).

Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada 2022 menjadi langkah penting dalam memperkuat keamanan siber. Namun, Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada 2023, Indonesia

masih mengalami lebih dari 1,3 miliar serangan siber, menjadikannya salah satu negara paling rentan di kawasan (BSSN, 2023). Regulasi seperti Peraturan Presiden No. 82/2022 tentang Perlindungan Infrastruktur Informasi Vital belum sepenuhnya efektif karena kurangnya kesiapan infrastruktur dan sumber daya manusia.

Thailand dan Filipina juga sedang mengembangkan kerangka regulasi keamanan siber yang lebih kuat. Thailand memberlakukan Cybersecurity Act 2019 dan Personal Data Protection Act (PDPA) pada 2022, tetapi implementasinya masih terhambat oleh birokrasi. Sementara itu, Filipina mengandalkan Data Privacy Act of 2012 dan Cybercrime Prevention Act, namun laporan dari National Privacy Commission (NPC) (2023) menunjukkan bahwa hanya 30% lembaga pemerintah yang memenuhi standar keamanan data. Serangan phishing di Filipina meningkat 65% pada 2023, menunjukkan perlunya pembaruan kebijakan (NPC, 2023).

Vietnam dan negara-negara ASEAN lainnya juga sedang berupaya menyelaraskan regulasi keamanan siber dengan standar global. Vietnam menerapkan Law on Cybersecurity pada 2019, yang mewajibkan perusahaan teknologi menyimpan data lokal. Namun, kritik muncul karena aturan ini dianggap terlalu ketat dan menghambat investasi asing (Ministry of Information and Communications Vietnam, 2022). Sementara itu, negara seperti Kamboja dan Laos masih tertinggal dalam pembentukan regulasi khusus keamanan siber, mengandalkan kebijakan umum tanpa penegakan yang kuat. Laporan ASEAN Coordinating Committee on Cybersecurity (2023) menyatakan bahwa hanya 50% negara ASEAN yang memiliki undang-undang

khusus keamanan siber, menunjukkan perlunya harmonisasi kebijakan di tingkat regional.

2.2.1 Perbandingan pendekatan regulasi di antara berbagai negara di Asia Tenggara

Asia Tenggara menunjukkan keragaman pendekatan dalam regulasi keamanan siber, mencerminkan perbedaan tingkat perkembangan digital dan prioritas keamanan nasional. Singapura memimpin dengan kerangka regulasi paling komprehensif melalui Cybersecurity Act 2018 dan Personal Data Protection Act (PDPA), yang mengintegrasikan prinsip-prinsip GDPR Eropa. Menurut Cyber Security Agency of Singapore (2023), pendekatan berbasis risiko ini telah mengurangi insiden siber kritis sebesar 28% sejak 2020. Berbeda dengan negara ASEAN lainnya, Singapura menerapkan sanksi berat hingga 10% pendapatan tahunan perusahaan untuk pelanggaran data (PDPC Singapore, 2023).

Malaysia dan Thailand mengadopsi model hybrid yang menggabungkan unsur-unsur regulasi Barat dengan kebutuhan lokal. Malaysia menerapkan Personal Data Protection Act 2010 yang lebih longgar dibanding Singapura, dengan fokus pada sektor privat. CyberSecurity Malaysia (2023) melaporkan bahwa hanya 45% perusahaan yang sepenuhnya mematuhi regulasi ini. Sementara itu, Thailand memberlakukan PDPA 2022 dan Cybersecurity Act 2019 yang memberikan kewenangan luas kepada pemerintah dalam

mengakses data demi alasan keamanan nasional. Laporan Electronic Transactions Development Agency (2023) menunjukkan bahwa pendekatan ini menimbulkan kekhawatiran di kalangan pelaku bisnis asing.

Indonesia dan Filipina menghadapi tantangan serupa dalam implementasi regulasi karena faktor geografis dan kapasitas kelembagaan. Indonesia baru saja mengesahkan UU Perlindungan Data Pribadi (PDP) 2022 setelah penundaan bertahun-tahun. BSSN (2023) mengakui bahwa implementasinya masih terhambat oleh kurangnya infrastruktur pendukung. Di Filipina, Data Privacy Act 2012 dan Cybercrime Prevention Act belum efektif menangani peningkatan 65% serangan phishing pada 2023 (National Privacy Commission, 2023). Kedua negara ini juga menghadapi kesenjangan besar dalam kesiapan SDM siber dibanding Singapura.

Vietnam dan Myanmar mewakili pendekatan yang lebih restriktif dengan penekanan pada kedaulatan siber. Vietnam menerapkan Law on Cybersecurity 2019 yang mewajibkan perusahaan teknologi menyimpan data lokal dan memberikan akses penuh kepada pemerintah. Ministry of Information and Communications Vietnam (2023) melaporkan bahwa regulasi ini telah mengurangi serangan siber lintas batas sebesar 35%. Namun, Google Transparency Report (2023) mencatat Vietnam sebagai negara dengan permintaan penghapusan konten tertinggi di ASEAN. Myanmar yang sedang dalam transisi politik justru mengalami kemunduran dalam kerangka regulasi

sibernya, dengan peningkatan penyensoran internet sebesar 200% sejak 2021 (Freedom House, 2023).

Perbandingan ini mengungkap tiga model utama di ASEAN: (1) pendekatan berbasis risiko ala Singapura, (2) model hybrid Malaysia-Thailand, dan (3) pendekatan kedaulatan siber Vietnam. ASEAN Cybersecurity Report (2023) menyimpulkan bahwa hanya 4 dari 10 negara anggota yang memiliki undang-undang siber komprehensif. Tantangan utama kawasan ini adalah harmonisasi regulasi mengingat ASEAN Framework on Personal Data Protection (2021) masih bersifat sukarela. Rekomendasi World Economic Forum (2023) menyarankan peningkatan kapasitas kelembagaan dan kolaborasi regional untuk mengatasi disparitas ini.

2.3 Regulasi dan Undang-Undang Utama

2.3.1 Indonesia

Tinjauan Umum Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan landasan hukum pertama di Indonesia yang secara komprehensif mengatur perlindungan data pribadi. UU ini disahkan pada 17 Oktober 2022 setelah melalui proses pembahasan selama lebih dari tujuh tahun, mengisi kekosongan regulasi yang selama ini diatur secara parsial dalam berbagai peraturan sektoral (Kementerian Komunikasi dan Informatika, 2022).

UU PDP mengadopsi prinsip-prinsip umum perlindungan data seperti yang dianut dalam General Data Protection Regulation (GDPR) Uni Eropa, termasuk hak subjek data, kewajiban pengendali data, dan mekanisme penegakan hukum.

Secara substantif, UU PDP mengklasifikasikan data pribadi menjadi dua kategori: data pribadi umum dan data spesifik yang mencakup informasi sensitif seperti data biometrik, genetika, catatan kesehatan, dan keyakinan politik (Pasal 4 UU PDP). Pengolahan data spesifik mendapat pengaturan lebih ketat dan hanya dapat dilakukan berdasarkan persetujuan eksplisit subjek data. Menurut laporan Badan Siber dan Sandi Negara, sekitar 65% pelanggaran data di Indonesia selama 2022-2023 melibatkan data spesifik, menunjukkan urgensi pengaturan khusus ini. UU juga memperkenalkan prinsip accountability yang mewajibkan pengendali data untuk dapat membuktikan kepatuhannya (Pasal 20).

Salah satu aspek inovatif UU PDP adalah pembentukan otoritas independen, yaitu Lembaga Perlindungan Data Pribadi (LPDP), yang berfungsi sebagai pengawas dan penegak hukum (Bab VII UU PDP). Mekanisme ini mengadopsi model otoritas perlindungan data ala GDPR, berbeda dengan pendekatan sebelumnya yang tersebar di berbagai instansi. Studi oleh Pusat Studi Hukum dan Teknologi Universitas Indonesia mengidentifikasi bahwa pembentukan LPDP diperkirakan akan meningkatkan efektivitas penanganan kasus pelanggaran data hingga 40% dibandingkan mekanisme sebelumnya.

Namun, hingga kuartal III 2023, proses pembentukan LPDP masih dalam tahap finalisasi struktur organisasi.

UU PDP juga mengatur sanksi yang cukup berat, baik administratif maupun pidana. Untuk pelanggaran berat seperti pemrosesan data tanpa dasar hukum, dapat dikenakan denda administratif hingga 2% pendapatan tahunan atau Rp50 miliar (Pasal 57), serta sanksi pidana penjara maksimal 6 tahun (Pasal 67). Data dari Indonesian Cyber Security Forum menunjukkan bahwa ancaman sanksi ini telah mendorong 70% perusahaan skala besar untuk memperbarui kebijakan perlindungan datanya dalam tahun pertama pasca pengesahan UU. Namun, implementasi sanksi masih menghadapi tantangan karena belum adanya putusan pengadilan yang menjadi yurisprudensi.

Tantangan utama implementasi UU PDP terletak pada aspek teknis dan kultural. Survei Asosiasi Penyedia Jasa Internet Indonesia mengungkap bahwa hanya 30% UMKM yang memahami kewajiban mereka di bawah UU ini. Selain itu, ketentuan mengenai transfer data lintas batas (Pasal 56) yang mensyaratkan tingkat perlindungan setara menimbulkan kerumitan bagi perusahaan global. Analisis oleh Center for Digital Society Universitas Gadjah Mada merekomendasikan perlunya pedoman teknis (implementing regulations) yang lebih rinci dan program edukasi masif untuk memastikan efektivitas UU ini di semua lapisan masyarakat.

2.3.2 Malaysia

Undang-Undang Perlindungan Data Pribadi 2010 (PDPA) Malaysia merupakan salah satu regulasi pertama di Asia Tenggara yang secara khusus mengatur perlindungan data pribadi. Diberlakukan pada tahun 2013, PDPA mengatur pemrosesan data pribadi baik di sektor komersial maupun non-pemerintah, dengan pengecualian untuk pemerintah federal dan negara bagian (Personal Data Protection Department Malaysia, 2013). Undang-undang ini didasarkan pada sembilan prinsip perlindungan data, termasuk prinsip persetujuan (consent), pengungkapan tujuan (purpose limitation), dan keamanan data (security principle). Namun, berbeda dengan GDPR Uni Eropa, PDPA Malaysia tidak mencakup hak untuk dilupakan (right to be forgotten) dan memiliki cakupan yang lebih terbatas (Wong & Hazlina, 2015).

Salah satu kelemahan utama PDPA 2010 adalah tidak adanya ketentuan yang mengatur pemrosesan data oleh entitas pemerintah. Hal ini menciptakan celah hukum yang signifikan, mengingat instansi pemerintah merupakan pengumpul dan pengolah data pribadi terbesar di Malaysia (Nordin et al., 2018). Studi oleh CyberSecurity Malaysia (2020) menunjukkan bahwa 60% kebocoran data di Malaysia antara tahun 2016-2019 berasal dari sektor publik, tetapi tidak dapat dijerat dengan PDPA. Selain itu, undang-undang ini juga tidak mengatur secara rinci tentang transfer data lintas batas, yang menjadi masalah penting di era ekonomi digital (Ali & Salleh, 2021).

Implementasi PDPA 2010 juga menghadapi tantangan dalam penegakan hukum. Laporan tahunan Personal Data Protection Commissioner (2019) mencatat bahwa hanya 35% dari 1,200 keluhan yang diterima sejak 2013 yang berhasil diselesaikan. Rendahnya angka penegakan ini disebabkan oleh terbatasnya sumber daya dan kewenangan komisioner, yang hanya dapat mengenakan denda administratif maksimal RM500,000 (sekitar Rp1,7 miliar) tanpa sanksi pidana (PDP Commissioner Malaysia, 2020). Bandingkan dengan Singapura yang dalam PDPA-nya menerapkan denda hingga SGD 1 juta (sekitar Rp11 miliar) untuk pelanggaran serius.

Perbandingan dengan perkembangan terbaru regulasi perlindungan data di kawasan menunjukkan bahwa PDPA 2010 sudah tertinggal. Thailand dengan PDPA 2019 dan Indonesia dengan UU PDP 2022 telah mengadopsi pendekatan yang lebih komprehensif, termasuk perlindungan data oleh pemerintah dan pengaturan transfer data internasional (ASEAN Data Protection Forum, 2022). Bahkan Singapura telah merevisi PDPA-nya tiga kali sejak 2012 untuk menyesuaikan dengan perkembangan teknologi. Pakar hukum siber Malaysia, Abu Bakar Munir (2023), merekomendasikan amendemen menyeluruh terhadap PDPA untuk mencakup sektor publik, memperkuat otoritas pengawas, dan menambahkan ketentuan tentang data anak serta kecerdasan buatan.

Meskipun memiliki berbagai keterbatasan, PDPA 2010 tetap menjadi landasan penting dalam perlindungan data pribadi di Malaysia. Survei oleh *Malaysian Digital Association* (2023) menunjukkan bahwa kesadaran

masyarakat tentang hak perlindungan data telah meningkat dari 25% pada 2013 menjadi 65% pada 2023. Namun, untuk tetap relevan, PDPA perlu pembaruan signifikan yang sejalan dengan perkembangan GDPR dan konvensi internasional seperti APEC Cross-Border Privacy Rules. Pembelajaran dari implementasi 10 tahun PDPA Malaysia dapat menjadi bahan pertimbangan berharga bagi negara-negara ASEAN yang sedang mengembangkan kerangka perlindungan data mereka.

2.3.3 Negara Asia Tenggara Lainnya

Singapura memiliki kerangka regulasi perlindungan data pribadi yang matang melalui Personal Data Protection Act (PDPA) 2012, yang diperbarui secara berkala untuk menyesuaikan dengan perkembangan teknologi. PDPA Singapura mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi swasta, dengan pengecualian untuk lembaga pemerintah dan data yang diproses secara pribadi (Personal Data Protection Commission Singapore, 2023). Pembaruan penting pada 2021 memperkenalkan ketentuan tentang data portability dan obligatory data breach notification yang mewajibkan pelaporan dalam 72 jam setelah insiden (PDPC Singapore, 2021). Menurut laporan tahunan PDPC, tingkat kepatuhan perusahaan terhadap PDPA mencapai 78% pada 2022, dengan sektor keuangan dan kesehatan menjadi yang paling patuh (PDPC Singapore, 2022)

Thailand mengadopsi Personal Data Protection Act (PDPA) 2019, yang mulai berlaku penuh pada 1 Juni 2022. Regulasi ini sangat terinspirasi oleh GDPR Uni Eropa, mencakup prinsip lawful basis, hak subjek data (seperti hak menghapus dan hak mengakses data), serta sanksi berat berupa denda administratif hingga 5 juta baht (sekitar Rp2,1 miliar) atau pidana penjara (Digital Economy Promotion Agency Thailand, 2022). Namun, implementasinya menghadapi tantangan karena kurangnya kesiapan UMKM. Survei Electronic Transactions Development Agency (ETDA) 2023 menunjukkan bahwa hanya 35% UMKM Thailand yang memahami kewajiban mereka di bawah PDPA (ETDA, 2023). Otoritas Thailand juga membentuk Personal Data Protection Committee (PDPC) sebagai pengawas, tetapi kapasitasnya masih terbatas dalam menangani pelanggaran lintas sektor.

Filipina memiliki Data Privacy Act (DPA) 2012, yang dikelola oleh National Privacy Commission (NPC). Regulasi ini mencakup prinsip-prinsip dasar perlindungan data tetapi dinilai kurang tegas dalam penegakan hukum. Misalnya, meskipun DPA mengatur sanksi denda hingga 5 juta peso (sekitar Rp1,7 miliar), NPC Annual Report 2022 mencatat hanya 12 kasus yang berakhir dengan sanksi sejak 2016 (NPC Philippines, 2022). Filipina juga menghadapi tantangan serius dalam kebocoran data, dengan peningkatan 65% insiden phishing pada 2023 (Cybercrime Investigation and Coordination Center Philippines, 2023). Selain itu, DPA 2012 tidak secara eksplisit mengatur data localization, sehingga banyak perusahaan asing menyimpan data di luar negeri.

2.4 Tantangan dan Keterbatasan Peraturan Saat Ini

Salah satu tantangan utama dalam regulasi keamanan siber adalah kecepatan perkembangan teknologi yang tidak diimbangi pembaruan hukum. Menurut laporan World Economic Forum (2023), lebih dari 60% negara di Asia Tenggara memiliki undang-undang siber yang belum diperbarui dalam lima tahun terakhir, sementara serangan siber meningkat 300% dalam periode yang sama. Contoh nyata adalah Indonesia, di mana UU ITE 2008 masih menjadi dasar hukum utama meskipun sudah tidak relevan dengan ancaman kontemporer seperti deepfake dan AI-powered cyberattacks (BSSN, 2023). Kesenjangan ini dimanfaatkan pelaku kejahatan untuk mengeksploitasi celah hukum, terutama dalam kasus ransomware yang menargetkan sektor kesehatan selama pandemi (Kaspersky, 2022).

Fragmentasi regulasi antar-yurisdiksi juga menjadi masalah signifikan. Di ASEAN misalnya, hanya Singapura dan Malaysia yang memiliki binding cross-border data sharing agreement, sementara negara lain masih mengandalkan kerangka sukarela (ASEAN Cybersecurity Report, 2023). Kondisi ini menyulitkan penanganan kejahatan siber lintas batas, seperti yang terlihat dalam kasus kebocoran data 279 juta warga Indonesia pada 2021 yang melibatkan server di Amerika Serikat dan Rusia (Privacy Rights Clearinghouse, 2022). Padahal, laporan Interpol (2023) menunjukkan bahwa 80% investigasi siber membutuhkan akses data lintas negara, tetapi hanya 35% yang berhasil karena hambatan hukum.

2.4.1 Mekanisme Penegakan Hukum yang Lemah

Kapasitas penegakan hukum yang terbatas merupakan keterbatasan kritis lainnya. Studi UNODC (2023) mengungkapkan bahwa:

a. 70% lembaga penegak hukum di negara berkembang kekurangan ahli digital forensik.
b. Hanya 20% kasus kejahatan siber yang berujung pada penuntutan, di Indonesia, Bareskrim Polri (2023) mengakui hanya memiliki 120 penyidik siber untuk menangani 1,3 miliar serangan tahunan, dengan rata-rata penyelesaian kasus memakan waktu 9-12 bulan. Ironisnya, anggaran keamanan siber Indonesia hanya 0,1% dari APBN, jauh di bawah standar global 2-4%.

Ketidakjelasan regulasi tentang teknologi baru seperti IoT dan AI semakin memperparah masalah. Microsoft Digital Defense Report (2023) mencatat bahwa 65% perusahaan di Asia Tenggara mengaku kesulitan mematuhi regulasi yang ambigu tentang cloud security dan AI governance. Kasus TikTok di Vietnam menjadi contoh nyata - platform ini dituduh melanggar Cybersecurity Law 2019 karena algoritmanya dianggap membocorkan data pengguna, tetapi tidak ada ketentuan eksplisit yang mengatur hal tersebut (Ministry of Information and Communications Vietnam, 2023).

Terakhir, rendahnya kesadaran regulasi di tingkat UMKM menciptakan weak link dalam ekosistem siber. Data APJII (2023) menunjukkan hanya 15% UMKM Indonesia memiliki protokol keamanan siber dasar. Kemudian sebuah penelitian juga dikemukakan oleh Rinaldi et al. dan Khoirunnisa et al. bahwa UMKM di Indonesia semakin jelas menghadapi tantangan besar dalam kesiapan keamanan digital, baik dari sisi teknis, finansial, maupun kesadaran sumber daya manusianya. 90% pelanggaran data pada UMKM terjadi karena ketidaktahuan regulasi Padahal, UMKM menyumbang 60% serangan ransomware di ASEAN (Kaspersky, 2023). Tanpa pendekatan tiered regulation yang membedakan kewajiban perusahaan besar dan UMKM, seperti model NIST Cybersecurity Framework di AS, efektivitas regulasi akan tetap terbatas (CSIS Indonesia, 2023).

2.4.2 Kurangnya Harmonisasi

Salah satu tantangan utama dalam keamanan siber global adalah tidak adanya standar harmonis yang mengatur perlindungan data dan kejahatan siber lintas negara. Menurut laporan United Nations Conference on Trade and Development (UNCTAD, 2023), dari 194 negara yang disurvei, hanya 58% yang memiliki undang-undang perlindungan data, dan hanya 23% yang mematuhi kerangka kerja internasional seperti Budapest Convention on Cybercrime. Ketidakkonsistenan ini menciptakan celah hukum (legal gaps) yang dimanfaatkan pelaku kejahatan siber untuk menghindari penuntutan.

Sebagai contoh, kasus ransomware yang menargetkan rumah sakit di Jerman pada 2022 ternyata dilakukan melalui server di Belarusia, yang tidak memiliki perjanjian ekstradisi dengan Uni Eropa (Europol, 2023).

Perbedaan definisi kejahatan siber antar-yurisdiksi semakin memperumit penanganan kasus transnasional. Studi Council of Europe (2023) mengungkapkan bahwa:

a. 41% negara mengkategorikan phishing sebagai kejahatan berat
b. 29% menganggapnya sebagai pelanggaran ringan
c. 30% bahkan tidak memiliki ketentuan khusus Kondisi ini jelas terlihat dalam kasus kebocoran data Shopee 2021, di mana perusahaan yang berbasis di Singapura ini hanya dijatuhi denda simbolis SGD 10.000 (Rp110 juta) oleh Personal Data Protection Commission Singapore, sementara jika terjadi di Uni Eropa bisa kena denda hingga 4% omzet global berdasarkan GDPR (PDPC Singapore vs European Commission, 2022).

Mekanisme transfer data lintas batas juga menjadi titik masalah utama. Asia-Pacific Economic Cooperation (APEC, 2023) mencatat bahwa:

a. Hanya 11 dari 21 ekonomi APEC yang menerapkan Cross-Border Privacy Rules (CBPR)
b. 7 negara menerapkan kebijakan data localization ekstrem seperti China dan Rusia akibatnya, perusahaan multinasional seperti

TikTok harus membangun pusat data terpisah di setiap negara, meningkatkan biaya operasional hingga 35% (McKinsey, 2023). Kasus TikTok Vietnam yang dipaksa menyimpan data lokal pada 2023 menunjukkan betapa kebijakan ini dapat menjadi hambatan perdagangan digital (Ministry of Information and Communications Vietnam, 2023).

Ketidakselarasan dalam prosedur investigasi lintas batas memperparah situasi. Laporan Interpol (2023) menunjukkan bahwa:

a. Permintaan bukti elektronik (e-evidence) antar-negara memakan waktu rata-rata 10 bulan.
b. 65% permintaan ditolak karena perbedaan hukum domestik. Contoh nyata adalah kasus penipuan investment scam senilai $600 juta yang melibatkan 30 negara pada 2022. Proses hukum terhambat karena ketiadaan mutual legal assistance treaty (MLAT) antara negara korban dan pelaku.

Solusi parsial melalui kerja sama regional seperti ASEAN Framework on Digital Data Governance ternyata belum efektif. Data ERIA (2023) mengungkap:

a. Hanya 4 dari 10 negara ASEAN yang meratifikasi perjanjian transfer data
b. Mekanisme ASEAN CERT hanya menangani 15% insiden siber lintas batas. Padahal serangan siber di kawasan meningkat 45%

selama 2022-2023 (ASEAN Cybersecurity Report, 2023). Rekomendasi World Economic Forum (2023) menyarankan pembentukan badan arbitrase siber global, namun implementasinya masih jauh dari kenyataan.

2.4.3 Keterbatasan Sumber Daya

Adapun juga Salah satu tantangan utama dalam penegakan hukum siber adalah alokasi anggaran yang tidak memadai. Menurut laporan UNODC (2023), negara-negara berkembang rata-rata hanya mengalokasikan 0,3% dari APBN untuk keamanan siber, jauh di bawah standar internasional sebesar 2-4% yang direkomendasikan ITU (2022). Di Indonesia, BSSN (2023) melaporkan bahwa anggaran keamanan siber hanya Rp1,2 triliun pada 2023, padahal kebutuhan minimal mencapai Rp5 triliun untuk membangun infrastruktur dasar. Keterbatasan ini berdampak langsung pada kapasitas investigasi, di mana 65% kasus kejahatan siber tidak tertangani secara tuntas.

Kurangnya ahli forensik digital yang kompeten memperparah situasi. Data Interpol (2023) menunjukkan rasio yang timpang:

a. 1 ahli forensik digital untuk setiap 2 juta penduduk di Asia Tenggara
b. Bandingkan dengan 1:200.000 di Eropa Barat. Bareskrim Polri (2023) mengakui hanya memiliki 120 penyidik siber yang tersertifikasi, padahal idealnya dibutuhkan minimal 1.000

penyidik untuk menangani 1,3 miliar serangan tahunan di Indonesia. Akibatnya, waktu penyelesaian kasus rata-rata mencapai 9-12 bulan, lima kali lebih lama dari standar G8 High-Tech Crime Committee (Kemenkominfo, 2023).

Ketertinggalan teknologi investigasi menjadi kendala struktural. Studi CSIS Indonesia (2023) menemukan bahwa:

a. 80% kepolisian di daerah masih menggunakan tools digital forensik versi 2015
b. Hanya 3 lab forensik di Indonesia yang memiliki alat dekripsi mutakhir. Kondisi ini kontras dengan perkembangan kejahatan siber di mana 75% kasus pada 2023 sudah menggunakan teknik AI-powered attacks (Kaspersky, 2023). Laporan BSSN menyebutkan bahwa kebocoran data di sektor kesehatan meningkat 300% selama pandemi karena lemahnya sistem deteksi intrusi (BSSN, 2022).

Dependensi pada bantuan asing menunjukkan kerentanan sistem. Microsoft Digital Crimes Unit (2023) mencatat bahwa:

a. 90% investigasi siber di Asia Tenggara memerlukan bantuan vendor teknologi asing
b. 60% kasus bergantung pada peralatan forensik impor. Contoh nyata adalah kasus pembobolan Bank Negara Indonesia 2021 yang penyidikannya membutuhkan bantuan FBI untuk melacak

server di Panama (Kompas, 2021). Padahal, biaya bantuan luar negeri per kasus kompleks bisa mencapai Rp2-5 miliar (Bareskrim, 2022).

Solusi parsial melalui pelatihan belum menjawab akar masalah. Program ASEAN-Singapore Cybersecurity Centre of Excellence hanya mampu melatih 200 ahli per tahun, sementara kebutuhan regional mencapai 50.000 orang (ASEAN Secretariat, 2023). Di tingkat nasional, Kemenkominfo RI (2023) mengaku kesulitan memenuhi target 20.000 SDM siber kompeten pada 2025 karena keterbatasan dana pelatihan. Rekomendasi World Bank (2023) menyarankan alokasi khusus 1% APBN untuk pengembangan SDM siber, tetapi implementasinya masih terhambat birokrasi.

2.5 Inisiatif Kerja Sama Regional

ASEAN telah mengambil peran penting dalam mempromosikan kerjasama keamanan siber melalui berbagai inisiatif regional. Salah satu yang utama adalah ASEAN Cybersecurity Cooperation Strategy (ACCS) 2021-2025, yang bertujuan untuk meningkatkan ketahanan siber kawasan melalui harmonisasi kebijakan, peningkatan kapasitas, dan kerja sama operasional (ASEAN Secretariat, 2021). Strategi ini mencakup lima pilar utama, termasuk pembangunan kapasitas, penelitian dan pengembangan, serta kerja sama dengan sektor swasta. Menurut laporan ASEAN Coordinating Committee on Cybersecurity (ACCC, 2023), implementasi ACCS telah membantu mengurangi insiden siber lintas batas sebesar 15% pada 2022-2023.

Salah satu pencapaian signifikan ASEAN adalah pembentukan ASEAN Computer Emergency Response Team (ASEAN CERT), yang berfungsi sebagai pusat koordinasi untuk menangani insiden siber di kawasan. Laporan ASEAN CERT (2023) menunjukkan bahwa lembaga ini telah menangani lebih dari 5.000 insiden siber pada 2022, dengan tingkat respons rata-rata 48 jam untuk kasus-kasus prioritas. Namun, tantangan tetap ada, termasuk kurangnya sumber daya teknis di beberapa negara anggota seperti Kamboja dan Laos (ERIA, 2023). ASEAN CERT juga aktif berkolaborasi dengan mitra global seperti INTERPOL dan EUROPOL untuk meningkatkan kapasitas investigasi.

Selain itu, ASEAN telah mengembangkan ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) di Bangkok, yang berfokus pada pelatihan dan sertifikasi profesional keamanan siber. Data Japan International Cooperation Agency (JICA, 2023) menunjukkan bahwa pusat ini telah melatih lebih dari 1.200 ahli siber dari negara-negara ASEAN sejak 2019. Program pelatihan mencakup forensik digital, manajemen insiden, dan perlindungan infrastruktur kritis. Namun, evaluasi oleh CSIS Asia (2023) mengungkapkan bahwa hanya 40% lulusan yang kemudian bekerja di lembaga pemerintah, sementara sisanya beralih ke sektor swasta karena insentif finansial yang lebih baik.

ASEAN juga mempromosikan harmonisasi regulasi melalui ASEAN Framework on Personal Data Protection (AFPDP), yang dirancang untuk menyelaraskan standar perlindungan data di kawasan. Meskipun belum mengikat, kerangka kerja ini telah menginspirasi pembaruan undang-undang di beberapa negara

seperti Thailand (PDPA 2019) dan Indonesia (UU PDP 2022) (Asian Business Law Institute, 2023).

Tantangan utama adalah perbedaan tingkat perkembangan regulasi antar negara anggota; misalnya, Singapura dan Malaysia sudah memiliki undang-undang yang matang, sementara Myanmar dan Kamboja masih dalam tahap awal penyusunan (Privacy Laws & Business International Report, 2023).

2.5.1 Pentingnya kemitraan publik-swasta dalam meningkatkan efektivitas peraturan

Kemitraan publik-swasta (*Public-Private Partnership*/PPP) memainkan peran krusial dalam meningkatkan efektivitas regulasi keamanan siber, terutama dalam menghadapi dinamika ancaman digital yang semakin kompleks. Menurut laporan World Economic Forum (2023), 78% serangan siber global menargetkan sektor swasta, sementara kapasitas penanganan oleh pemerintah seringkali terbatas. Kolaborasi ini memungkinkan pembagian sumber daya, pengetahuan, dan teknologi, seperti yang terlihat dalam inisiatif Cyber Threat Intelligence Sharing di Singapura, di mana perusahaan swasta dan badan pemerintah berbagi informasi ancaman secara real-time, mengurangi waktu respons insiden dari 72 jam menjadi 24 jam (Cyber Security Agency of Singapore, 2023).

Sektor swasta seringkali memiliki akses ke teknologi mutakhir dan keahlian teknis yang tidak dimiliki pemerintah. Studi oleh McKinsey &

Company (2023) menunjukkan bahwa 65% inovasi keamanan siber, seperti AI-based threat detection, berasal dari perusahaan teknologi. Di Indonesia, kemitraan antara BSSN dan perusahaan seperti Telkom Indonesia telah meningkatkan kapasitas pemantauan serangan siber nasional, dengan deteksi dini meningkat 40% dalam dua tahun terakhir (BSSN, 2023). Namun, tantangan seperti perbedaan prioritas dan kekhawatiran atas kerahasiaan data sering menghambat kolaborasi yang lebih mendalam (CSIS Indonesia, 2023).

Regulasi yang mendorong kemitraan publik-swasta juga terbukti efektif dalam memperkuat ketahanan siber sektor kritis. Di Amerika Serikat, Cybersecurity and Infrastructure Security Agency (CISA) mengadopsi model Joint Cyber Defense Collaborative (JCDC) yang melibatkan perusahaan seperti Microsoft dan Google. Hasilnya, 60% serangan ransomware berhasil dicegah pada 2022 (CISA, 2023). Di tingkat ASEAN, ASEAN-Singapore Cybersecurity Centre of Excellence menjadi contoh sukses dengan melatih 1.500 ahli siber dari sektor publik dan swasta sejak 2020 (ASEAN Secretariat, 2023).

Namun, implementasi kemitraan antara sektor publik dan swasta dalam konteks keamanan siber memerlukan kerangka regulasi yang jelas dan kuat agar kerja sama tersebut dapat berjalan efektif dan saling menguntungkan. Laporan OECD (2023) mengidentifikasi tiga tantangan utama yang kerap menghambat keberhasilan kolaborasi ini. Pertama, adanya asimetri informasi antara kedua pihak, di mana sekitar 70% perusahaan masih enggan untuk

berbagi data sensitif dengan pemerintah karena kekhawatiran terhadap kerahasiaan dan potensi penyalahgunaan informasi. Kedua, insentif yang tidak seimbang turut menjadi kendala, sebab hanya 30% dari kemitraan yang ada menawarkan insentif finansial yang cukup menarik bagi sektor swasta untuk terlibat secara aktif. Ketiga, tidak adanya standar yang seragam dalam protokol keamanan menyebabkan inkonsistensi dalam pelaksanaan kerja sama, yang pada akhirnya memperlemah efektivitas sistem pertahanan siber secara keseluruhan.

Untuk mengatasi permasalahan tersebut, beberapa solusi telah ditawarkan oleh lembaga internasional. Salah satunya adalah pembentukan zona aman atau *safe harbor* secara hukum bagi perusahaan yang ingin berbagi informasi terkait ancaman siber tanpa takut terkena sanksi hukum. Selain itu, penerapan skema pendanaan bersama juga dinilai efektif, seperti yang telah dilakukan oleh Uni Eropa melalui *NIS Directive 2.0*, yang mendorong kerja sama antar sektor melalui dukungan keuangan dan penguatan kerangka regulasi (European Union Agency for Cybersecurity, 2023).

Ke depan, penguatan kemitraan publik-swasta memerlukan pendekatan yang lebih terstruktur dan sistematis. World Bank (2023) merekomendasikan beberapa langkah strategis untuk mencapai hal ini. Pertama, penting untuk membentuk lembaga koordinasi nasional yang melibatkan perwakilan dari pemerintah dan sektor swasta, sehingga pengambilan kebijakan menjadi lebih inklusif dan responsif terhadap kebutuhan kedua belah pihak. Kedua,

pengembangan platform bersama untuk berbagi informasi ancaman yang dienkripsi dengan protokol keamanan ketat perlu diprioritaskan, guna menciptakan kepercayaan dalam pertukaran data. Ketiga, penyelenggaraan program pelatihan bersama juga sangat penting untuk membangun kapasitas teknis serta memperkuat kepercayaan antara para pelaku kerja sama.

Keberhasilan model semacam ini telah terlihat di Jepang melalui pendirian *Cybersecurity Partnership Council*, yang terbukti mampu menurunkan insiden serangan siber terhadap infrastruktur kritis hingga 35% (JICA, 2023). Keberhasilan ini menunjukkan bahwa kolaborasi publik-swasta memiliki potensi besar untuk menjadi pilar utama dalam strategi ketahanan siber nasional, selama didukung oleh regulasi yang adaptif, transparansi dalam pelaksanaan, serta komitmen politik yang konsisten dari semua pemangku kepentingan.