BAB VI

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan secara komprehensif pada bab-bab sebelumnya, dengan mengacu pada rumusan masalah yang diajukan dalam penelitian ini, maka dapat ditarik kesimpulan sebagai berikut:

1. Pengaturan hukum terkait pengelolaan big data dalam menghadapi ancaman keamanan siber di Indonesia saat ini masih bersifat fragmentatif dan tersebar dalam berbagai peraturan perundang-undangan yang belum terintegrasi secara koheren. Fragmentasi regulasi yang terjadi menimbulkan berbagai problematika normatif berupa tumpang tindih kewenangan, kekosongan hukum, serta inkonsistensi pengaturan antar berbagai instrumen hukum yang mengatur aspek-aspek pengelolaan data dan keamanan siber. Kondisi demikian mengakibatkan ketidakpastian hukum yang berimplikasi pada lemahnya penegakan kedaulatan digital Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi tonggak penting sebagai *lex generalis* dalam pengaturan pelindungan data pribadi, namun masih terkendala oleh belum tersedianya Peraturan Pemerintah pelaksana yang masih dalam tahap harmonisasi serta belum terbentuknya Lembaga Pelindungan Data Pribadi sebagai otoritas pengawas independen. Kerangka hukum yang ada meliputi UU PDP, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi

dan Transaksi Elektronik (perubahan UU ITE), serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, namun belum terdapat undang-undang yang secara spesifik mengatur keamanan dan ketahanan siber secara komprehensif. Kondisi ini menempatkan Indonesia dalam keadaan *vacuum of norm* di bidang keamanan siber. Pengaturan yang ada juga masih bersifat reaktif-represif dengan pendekatan *ultimum remedium* yang hanya mengatasi permasalahan setelah insiden terjadi, belum mengadopsi pendekatan proaktif-preventif berbasis risiko. Ketiadaan undang-undang keamanan dan ketahanan siber yang komprehensif menyebabkan kekosongan payung hukum dalam penanganan ancaman siber secara sistematis. Kehadiran Konvensi Hanoi dapat menjadi dasar normatif bagi harmonisasi kebijakan nasional terkait kejahatan siber.

2. Penegakan kedaulatan digital Indonesia terhadap ancaman keamanan siber menghadapi tantangan multidimensional yang mencakup aspek kelembagaan, infrastruktur, dan transfer data lintas batas. Dari aspek kelembagaan, BSSN telah menyusun Strategi Keamanan Siber Nasional dengan lima nilai dasar (kedaulatan, kemandirian, keamanan, kebersamaan, dan adaptif), namun koordinasi antar lembaga masih menghadapi hambatan dan ketiadaan Lembaga Pelindungan Data Pribadi mengakibatkan penegakan sanksi administratif UU PDP belum dapat berjalan efektif. Dari aspek infrastruktur, pembangunan Pusat Data Nasional (PDN) sebagai upaya konsolidasi data pemerintah mengalami berbagai kendala dengan dari empat lokasi yang direncanakan (Cikarang,

Batam, Balikpapan, Labuan Bajo) baru satu yang dalam tahap Pembangunan. Dari aspek transfer data lintas batas, Pasal 56 UU PDP mengatur mekanisme *adequacy* namun belum mengakomodasi mekanisme internasional seperti Klausul Kontraktual Standar (*Standard Contractual Clauses*/SCC), dan Aturan Perusahaan yang Mengikat (*Binding Corporate Rules*/BCR), sehingga menciptakan area abu-abu dalam praktik transfer data.

3. Model pengaturan hukum yang ideal untuk mengelola dan melindungi big data dari ancaman keamanan siber dalam menegakkan kedaulatan digital di Indonesia adalah model pengaturan yang bersifat *integratif-komprehensif* dengan pendekatan *proaktif-transformatif-progresif* berbasis risiko. Model ini memerlukan arsitektur regulasi yang koheren mencakup tiga tingkatan: *pertama*, undang-undang sebagai payung hukum utama meliputi UU PDP sebagai *lex generalis* pelindungan data dan Undang-Undang Keamanan dan Ketahanan Siber (UU KKS) yang perlu segera dibentuk; *kedua*, peraturan pelaksana berupa Peraturan Pemerintah dan Peraturan Presiden yang mengatur ketentuan teknis implementasi; dan *ketiga*, regulasi sektoral yang diharmonisasi untuk menghilangkan fragmentasi dan inkonsistensi normatif. Model pengaturan ini memerlukan penguatan kelembagaan melalui pembentukan Lembaga Pelindungan Data Pribadi yang independen dan penguatan kewenangan BSSN dalam koordinasi keamanan siber nasional, pengembangan infrastruktur digital nasional termasuk PDN dengan pendekatan ekosistem kolaboratif yang melibatkan sektor swasta, pembangunan kapasitas SDM

melalui program pelatihan dan sertifikasi di bidang keamanan siber dan pelindungan data, serta penguatan literasi digital masyarakat melalui empat pilar (Kecakapan Digital, Etika Digital, Budaya Digital, dan Keamanan Digital). Implementasi model pengaturan dilakukan secara bertahap melalui tiga fase: tahap persiapan regulasi dan pembangunan kapasitas kelembagaan (tahun 1-2), tahap implementasi bertahap dengan *grace period* (tahun 2-4), dan tahap implementasi penuh dengan evaluasi berkelanjutan (tahun 4-5 dan seterusnya), dengan mengadopsi praktik terbaik internasional seperti *EU Cyber Resilience Act* dan kerangka *Data Free Flow with Trust* (DFFT) yang disesuaikan dengan konteks kebutuhan nasional Indonesia.

B. Saran

Berdasarkan kesimpulan yang telah diuraikan di atas, peneliti menyampaikan saran-saran sebagai berikut:

1. Kepada Pemerintah dan Dewan Perwakilan Rakyat (DPR) disarankan untuk mempercepat pengesahan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) yang telah masuk dalam Program Legislasi Nasional (Prolegnas) Prioritas 2025 sebagai payung hukum komprehensif dalam penanganan ancaman keamanan siber. RUU KKS hendaknya memuat substansi yang mencakup reposisi kelembagaan dengan penguatan kewenangan BSSN, pengaturan tata kelola keamanan infrastruktur informasi vital, kewajiban pelaporan insiden siber, standar keamanan produk dengan elemen

digital, serta pengaturan sanksi yang proporsional. Kepada Kementerian Hukum dan HAM serta Kementerian Komunikasi dan Digital disarankan untuk segera menyelesaikan proses harmonisasi dan pengesahan Peraturan Pemerintah pelaksana UU PDP yang telah melampaui tenggat waktu, dengan memastikan substansi PP mencakup pengaturan yang lebih rinci mengenai pemrosesan big data, standar keamanan teknis, mekanisme transfer data lintas batas termasuk adopsi instrumen internasional seperti *Standard Contractual Clauses* dan *Binding Corporate Rules*, serta prosedur pemberitahuan kebocoran data (*data breach notification*). Kepada kementerian dan lembaga sektoral disarankan untuk melakukan *review* dan harmonisasi seluruh regulasi sektoral yang berkaitan dengan pengelolaan data agar selaras dengan prinsip-prinsip UU PDP sebagai *lex generalis*, sehingga tercipta kerangka hukum yang koheren dan tidak menimbulkan kebingungan dalam implementasi *data protection compliance*.

2. Kepada Presiden disarankan untuk segera menerbitkan Peraturan Presiden tentang Pembentukan Lembaga Pelindungan Data Pribadi sebagaimana diamanatkan UU PDP, mengingat keterlambatan pembentukan lembaga ini telah melewati batas waktu maksimal Oktober 2024 dan mengakibatkan penegakan sanksi administratif UU PDP tidak dapat berjalan efektif. Lembaga Pelindungan Data Pribadi hendaknya dibentuk sebagai lembaga independen dengan kewenangan yang memadai dalam pengawasan, penyelidikan, dan penegakan hukum, serta didukung dengan sumber daya yang mencukupi.

Kepada BSSN disarankan untuk memperkuat koordinasi keamanan siber nasional melalui konsep *Collaborative Security* dengan melibatkan seluruh pemangku kepentingan termasuk kementerian/lembaga, sektor swasta, akademisi, dan masyarakat sipil, serta memperluas pembentukan dan penguatan jaringan Tim Tanggap Insiden Siber (TTIS/CSIRT) di berbagai tingkatan. Kepada Kementerian Komunikasi dan Digital disarankan untuk mengakselerasi pembangunan dan operasionalisasi Pusat Data Nasional (PDN) dengan pendekatan ekosistem kolaboratif yang melibatkan sektor swasta, memastikan standar keamanan Tier-IV terpenuhi, serta menyiapkan mekanisme *disaster recovery* yang handal untuk menghindari terulangnya insiden seperti serangan *ransomware* terhadap PDNS Surabaya. Dalam konteks transfer data lintas batas, disarankan agar Pemerintah menyusun protokol khusus dan daftar negara yang memenuhi kriteria kesetaraan pelindungan data (*adequacy decision*) sebagaimana dipraktikkan Uni Eropa, serta memastikan setiap perjanjian internasional yang melibatkan transfer data tetap menghormati prinsip kedaulatan digital dan ketentuan UU PDP.

3. Kepada Pemerintah disarankan untuk mengadopsi pendekatan implementasi bertahap (*phased approach*) dengan peta jalan yang jelas mencakup tahap persiapan regulasi dan kapasitas kelembagaan, tahap implementasi bertahap dengan mekanisme *grace period* bagi pemangku kepentingan untuk melakukan penyesuaian, serta tahap implementasi penuh dengan evaluasi berkelanjutan. Mekanisme *grace period* perlu disertai dengan program pendampingan dan

insentif bagi pelaku usaha terutama UMKM dalam memenuhi standar pelindungan data dan keamanan siber. Kepada BSSN dan Kementerian Komunikasi dan Digital disarankan untuk memperluas program pengembangan kapasitas SDM di bidang keamanan siber dan pelindungan data melalui pelatihan, sertifikasi, dan pembentukan Lembaga Sertifikasi Profesi (LSP) yang terakreditasi, dengan target menghasilkan tenaga profesional DPO/PPDP dan ahli keamanan siber yang kompeten untuk memenuhi kebutuhan industri. Program Literasi Digital Nasional perlu ditingkatkan intensitas dan jangkauannya dengan fokus pada empat pilar (Kecakapan Digital, Etika Digital, Budaya Digital, dan Keamanan Digital), termasuk integrasi literasi digital ke dalam kurikulum pendidikan formal dan perluasan akses di wilayah 3T (Terdepan, Terpencil, dan Tertinggal). Dalam jangka panjang, disarankan untuk mengembangkan industri teknologi keamanan siber dalam negeri melalui kemandirian kriptografi nasional dan inovasi teknologi lokal guna mengurangi ketergantungan pada platform dan infrastruktur digital asing, serta aktif berpartisipasi dalam forum-forum internasional untuk mengadopsi praktik terbaik global dan memperkuat posisi Indonesia dalam tata kelola keamanan siber internasional.