NASKAH AKADEMIK
RANCANGAN UNDANG-UNDANG
TENTANG
KEAMANAN DAN KETAHANAN SIBER

DIREKTORAT JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA
2025

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Y.M.E. atas karunia dan perkenan-Nya sehingga kami dapat melaksanakan kegiatan Penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber.

Penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber (RUU tentang Keamanan dan Ketahanan Siber) merupakan upaya pemerintah dalam memberikan pelindungan keamanan dan ketahanan siber di era ruang siber dan ekosistem digital yang telah menjadi bagian tak terpisahkan dari kehidupan masyarakat dan penyelenggaraan negara serta memiliki pengaruh signifikan terhadap keamanan nasional, stabilitas ekonomi, kesejahteraan sosial, reputasi negara, dan pelayanan publik. Keamanan Siber merupakan pelindungan terhadap ruang siber dari berbagai ancaman dan serangan yang dapat merusak integritas, kerahasiaan, ketersediaan informasi, atau tindakan yang menyebabkan infrastruktur informasi tidak berfungsi, atau gangguan dalam segala bentuknya.

Regulasi mengenai Keamanan dan Ketahanan Siber telah diatur di berbagai negara dan menjadi bagian dari hukum internasional yang dijadikan rujukan komparatif dalam penyusunan regulasi keamanan dan ketahanan siber nasional Indonesia untuk menghadapi ancaman dan kejahatan siber. Dengan demikian diperlukan legislasi dengan pendekatan komprehensif transformatif sebagai dasar penyelenggaraan keamanan dan ketahanan siber nasional untuk memberikan kepastian dan mengatur berbagai aspek keamanan dan ketahanan siber di Indonesia untuk mendukung pertumbuhan ekonomi, ketertiban umum, dan pelayanan publik, dengan tetap mendorong inovasi teknologi dan pemanfaatannya untuk keunggulan negara.

Berdasarkan Pasal 43 dalam Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 13 Tahun 2022, dinyatakan bahwa setiap Rancangan Undang-Undang harus disertai dengan Naskah Akademik. Diharapkan, Naskah Akademik RUU tentang Keamanan dan Ketahanan Siber dapat menjadi acuan utama dalam penyusunan dan pembahasan Rancangan Undang-Undang.

Direktur Jenderal
Peraturan Perundang-undangan,

Dr. Dhahana Putra

DAFTAR ISI

KATA PENGANTAR ..... **i**

BAB I PENDAHULUAN **1**

A. Latar Belakang 1

B. Identifikasi Masalah 9

C. Tujuan dan Kegunaan Kegiatan Penyusunan Naskah Akademik 10

D. Metode 10

BAB II KAJIAN TEORETIS DAN PRAKTIK EMPIRIK **12**

A. Kajian Teoretis 12

1. Ruang Siber 12

2. Keamanan Siber 15

3. Ketahanan atau Resiliensi Siber 21

4. Ancaman Siber 24

5. Insiden Siber 27

6. Krisis Siber 29

7. Relevansi dengan Keamanan dan Ketahanan Siber 42

B. Kajian terhadap Asas/Prinsip yang Berkaitan dengan Penyusunan Norma 45

1. Asas keamanan dan ketahanan siber 45

2. Prinsip keamanan dan ketahanan siber 53

C. Kajian terhadap Praktik Penyelenggaraan, Kondisi yang Ada, Permasalahan yang Dihadapi Masyarakat, dan Perbandingan dengan Negara Lain. 76

1. Kajian terhadap praktik 76

2. Kondisi yang ada 80

3. Permasalahan yang Dihadapi 84

4. Perbandingan Regulasi dan Kelembagaan dengan Negara Lain 87

5. Perbandingan Regulasi Pelindungan Infrastruktur Informasi Kritikal dengan Negara Lain 118

D. Kajian terhadap Implikasi Penerapan Regulasi 140

E. Kajian terhadap Praktik dan Koordinasi Penyelenggaraan Negara. 149

BAB III EVALUASI DAN ANALISIS PERATURAN PERUNDANG-UNDANGAN **151**

A. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik 151

B. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara 152

C. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber 154
D. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital 155
BAB IV LANDASAN FILOSOFIS, SOSIOLOGIS, YURIDIS 160
A. Landasan Filosofis 160
B. Landasan Sosiologis 163
C. Landasan Yuridis 166
BAB V JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP .....
MATERI MUATAN 168
A. Sasaran 168
B. Arah dan Jangkauan Pengaturan 169
1. Arah Pengaturan 169
2. Jangkauan Pengaturan 169
C. Ruang Lingkup dan Materi Muatan 170
1. Pengaturan Keamanan Siber 170
2. Pengaturan Ketahanan Siber 188
3. Peningkatan Kapasitas SDM 189
4. Peningkatan Kapasitas Teknologi 192
5. Peningkatan Kapasitas Proses Bisnis 195
6. Kerja Sama Internasional 199
7. Peran Pemerintah 202
8. Audit Teknis 203
9. Partisipasi Masyarakat 204
10. Pendanaan 205
11. Penyidikan 207
12. Sanksi Adminstratif 207
13. Ketentuan Pidana 211
14. Ketentuan Penutup 214
BAB VI PENUTUP 217
A. Simpulan 217
B. Saran 219
DAFTAR PUSTAKA 220

BAB I
PENDAHULUAN

A. Latar Belakang

Dalam beberapa dekade terakhir, perkembangan teknologi dan informasi telah membawa perubahan signifikan di berbagai sektor kehidupan, termasuk ekonomi, pertahanan, pemerintahan, dan infrastruktur publik. Digitalisasi ini memungkinkan pertukaran informasi yang lebih cepat dan efisien, meningkatkan produktivitas, serta membuka peluang besar untuk inovasi dan kemajuan di berbagai bidang. Namun, pesatnya perkembangan teknologi tersebut juga membawa tantangan baru, khususnya terkait ancaman terhadap keamanan dan ketahanan siber. Negara-negara di seluruh dunia kini menghadapi ancaman siber yang semakin kompleks dan merusak, mulai dari serangan terhadap Infrastruktur Informasi Kritikal hingga penyalahgunaan data pribadi yang mengancam stabilitas nasional dan privasi masyarakat.

Perkembangan teknologi dan informasi adalah sebuah peluang sekaligus tantangan yang melahirkan perubahan dalam segala aspek kehidupan mulai dari ruang lingkup terkecil yaitu individu, sampai pada ruang yang begitu luas yaitu negara bahkan dunia. Pesatnya kemajuan di bidang teknologi dan informasi juga telah memberikan pengaruh besar terhadap seluruh komponen kehidupan, mulai dari ekonomi, politik, sosial, serta keamanan. Sifat alamiah dari ancaman dan keamanan adalah dinamis, terbukti bahwa ancaman dan keamanan bukanlah hal yang dapat selesai untuk diperbincangkan, di diskusikan dan berhenti untuk diperbaharui. Pada abad ke-21, ancaman yang sering terjadi adalah ancaman yang bersifat tidak terlihat *(intangible)*, misalnya ancaman ideologi berupa terorisme dan radikalisme yang berpengaruh pada keamanan nasional khususnya di Indonesia.

Perubahan bentuk, sifat, dan model dari ancaman tersebut yang kemudian menjadi pemicu bagi setiap negara untuk terus melakukan evaluasi dan pengembangan sistem dan alternatif cara untuk menangkal

ancaman tersebut. Perkembangan teknologi dan informasi di era sekarang ini telah membentuk ruang kehidupan baru untuk manusia saling berinteraksi, ruang tersebut disebut dengan *cyberspace*. Secara singkat *cyberspace* merupakan sebuah tempat maya dimana komunikasi antar pengguna terjadi.[1]Kemunculan dan meningkatnya penggunaan *cyberspace* ini menghadirkan kemudahan bagi para penggunanya untuk berhubungan dengan orang lain, namun hal tersebut juga bersamaan dengan dampak negatif yang berupa ancaman keamanan dari dan untuk individu, organisasi dan pemerintahan.[2]

Presiden RI telah menandatangani Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Diundangkannya Peraturan Presiden tersebut didasari oleh perlu dilakukannya penataan organisasi Badan Siber dan Sandi Negara (BSSN) dalam rangka mewujudkan keamanan, pelindungan, dan kedaulatan siber nasional, serta meningkatkan pertumbuhan ekonomi nasional. Peraturan Presiden tersebut diterbitkan untuk mengoptimalkan pelaksanaan tugas dan fungsi di bidang keamanan siber dan Sandi Negara dalam organisasi BSSN sehingga dapat dilakukan dengan lebih efektif dan efisien. BSSN merupakan lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden. Organisasi dan Tata Kerja BSSN kemudian diatur dalam Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

Badan Siber dan Sandi Negara bukan merupakan lembaga baru namun merupakan transformasi peleburan lembaga keamanan informasi pemerintah yang telah ada sebelumnya, yaitu Lembaga Sandi Negara dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika sebagaimana diatur dalam Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara yang selanjutnya disempurnakan dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan

[1] Makbul Rizki, Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi, Vol. 14 Nomor 1, Politeia: Jurnal Ilmu Politik, 2022, hlm 2.
[2] M. Smith (2015). Research Handbook on International Law and Cyberspace. Massachusetts: Elgar Publishing Limited.

atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara. Dengan dibentuknya Badan Siber dan Sandi Negara maka pelaksanaan seluruh tugas dan fungsi di bidang Persandian di Lembaga Sandi Negara serta pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan dan infrastruktur telekomunikasi yang ada di KemenKominfo dilaksanakan oleh Badan Siber dan Sandi Negara.[3] Perkembangan teknologi yang sangat pesat menjadikan individu saling terhubung satu sama lain untuk dapat berkomunikasi dan berinteraksi tanpa terhalang sekat-sekat geografis negara *(borderless)*.

Perkembangan tersebut menciptakan konsep dunia baru yaitu siber melalui penggunaan jaringan sistem informasi yang diintegrasikan dengan sistem komputasi. Pemanfaatan ruang siber melalui sarana prasarana jaringan internet telah berhasil menciptakan dan mengakselerasi suatu revolusi dalam kehidupan masyarakat secara global baik dalam aspek komputer maupun telekomunikasi. Revolusi tersebut tidak terlepas dari dahsyatnya fungsi yang dimiliki internet dalam hal kemampuan penyiaran di seluruh dunia, mekanisme penyebaran informasi, kemudahan akses, dan media kolaborasi serta interaksi antar pemangku kepentingan (*stakeholders*) di seluruh penjuru dunia. Masifnya aktivitas di ruang siber dalam waktu yang relatif bersamaan secara mutatis mutandis menimbulkan akibat positif maupun negatif bagi masyarakat dunia.

Pemanfaatan ruang siber sebagai pola baru bagi masyarakat dalam beraktivitas merupakan hak asasi yang wajib dilindungi negara. Hal tersebut tercantum dalam konstitusi dalam Pasal 28F dan 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Norma dasar konstitusi tersebut tentu diperlukan diterjemahkan dalam pengaturan lebih lanjut oleh regulasi yang berada di bawahnya secara komprehensif karena konstitusi dalam kacamata ideal hanya

[3] Tentang BSSN | www.bssn.go.id

menggariskan norma hukum dalam bentuk yang singkat. Ketentuan dasar dalam konstitusi secara faktual tidak diejawantahkan peraturan perundang-undangan di bawahnya secara komprehensif. Norma hukum perihal pelindungan masyarakat di ruang siber, khususnya terkait keamanan dan ketahanan siber dalam Undang-Undang masih belum komprehensif dan terintegrasi dengan baik.

Keterbatasan regulasi yang mengatur implementasi amar konstitusi menyebabkan upaya penanganan persoalan keamanan dan ketahanan siber di Indonesia masih menghadapi tantangan kompleks. Kondisi ini semakin diperparah dengan meningkatnya aktivitas kejahatan di ruang siber yang menunjukkan tren eskalatif dari tahun ke tahun. Pada bulan Mei 2023, Bank Syariah Indonesia (BSI) mengalami gangguan layanan yang parah. Gangguan ini disinyalir akibat serangan siber *ransomware* yang mengganggu jaringan layanan perbankan BSI. Layanan BSI sempat lumpuh selama kurang-lebih lima hari, membuat kesal para nasabahnya. Badan Penyelenggara Jaminan Sosial (BPJS) juga mengalami gangguan layanan yang parah pada bulan April 2024. Gangguan ini disinyalir akibat serangan siber yang mengganggu jaringan pelayanan perawatan kesehatan BPJS. Layanan BPJS sempat lumpuh selama kurang-lebih tiga hari. Selain itu, beberapa waktu lalu terjadi insiden siber berupa gangguan pada Pusat Data Nasional Sementara (PDNS) yang dikelola Kementerian Komunikasi dan Informatika pada Juni 2024. Gangguan ini mengakibatkan layanan digital Direktorat Jenderal Imigrasi Kementerian Hukum dan Hak Asasi Manusia tidak berfungsi, serta gangguan pada Layanan Penerimaan Peserta Didik Baru (PPDB) di beberapa daerah sehingga berakibat perlunya perpanjangan waktu pendaftaran.

Tren eskalasi kejahatan siber di Indonesia dari tahun 2022 hingga 2024 menunjukkan peningkatan yang konsisten baik dari sisi volume maupun kompleksitas serangan. Pada tahun 2022, BSSN mencatat lebih dari 1,6 (satu koma enam) miliar anomali trafik siber, menandai maraknya aktivitas *malware* dan *phising* yang menargetkan sektor pemerintahan dan layanan publik. Tahun berikutnya, 2023, jumlah

tersebut tercatat 403 (empat ratus tiga) juta anomali trafik dengan 347 (tiga ratus empat puluh tujuh) dugaan insiden, menegaskan bahwa serangan siber mulai menyentuh infrastruktur penting seperti perbankan dan lembaga layanan sosial. Memasuki tahun 2024, berdasarkan *Lanskap Keamanan Siber* yang dirilis BSSN, ancaman meningkat secara lebih terarah dan terukur dengan 330.527.636 (tiga ratus tiga puluh juta lima ratus dua puluh tujuh enam ratus tiga puluh enam) anomali trafik yang sebagian besar didominasi oleh aktivitas *Mirai Botnet*, 2,48 (dua koma empat puluh depalan) juta aktivitas Advanced Persistent Threat (APT), 514 (lima ratus empat belas) ribu aktivitas *ransomware*, dan lebih dari 26 (dua puluh enam) juta aktivitas phishing. Selain itu, terdapat 241 (dua ratus empat puluh satu) dugaan kebocoran data dan lebih dari 56 (lima puluh enam) juta data *exposure* yang mempengaruhi ratusan *stakeholder* di berbagai sektor.[4] Fakta tersebut menunjukkan bahwa eskalasi ancaman siber di Indonesia tidak hanya bersifat teknis, melainkan juga berdampak sosial dan psikologis, mulai dari terganggunya pelayanan publik, hilangnya data pribadi, hingga menurunnya kepercayaan masyarakat terhadap institusi pemerintah dan swasta. Oleh karena itu, peningkatan kapabilitas keamanan siber nasional, penegakan regulasi yang adaptif, serta penguatan kesadaran digital masyarakat menjadi faktor kunci dalam mewujudkan ketahanan siber yang tangguh dan berkelanjutan.

Serangan yang melibatkan peretasan situs web pemerintah, kebocoran data pribadi, hingga serangan *ransomware* pada institusi publik menjadi contoh nyata dari meningkatnya risiko siber di Indonesia. Hal tersebut mencerminkan rentannya keamanan dan ketahanan siber di Indonesia. Berdasarkan *Global Cyber Security Index*, aspek legal di Indonesia sudah sempurna. Namun demikian untuk implementasi yang lebih efektif diperlukan penguatan dalam kepatuhan terhadap peraturan perundang-undangan.

[4] https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html diakses terkahir pada 24 Februari 2025

Pelindungan hukum sejatinya merupakan hak bagi masyarakat yang terus melekat dimanapun dan kapanpun. Hukum berkewajiban untuk menjamin hak asasi masyarakat agar tidak terdegradasi saat menjalani kesehariannya, termasuk pada saat beraktivitas di ruang siber. Pandangan filosofis tersebut pada kenyataannya berbanding terbalik dengan ranah implementasi. Regulasi sebagai manifestasi Pelindungan hukum masih belum mengatur secara sistematis. Perangkat hukum terkait ruang siber, khususnya keamanan dan ketahanan siber masih bersifat parsial dan sektoral pada berbagai peraturan perundang-undangan. Terlebih, materi muatan yang terkandung dalam masing-masing peraturan perundang-undangan tersebut masih belum komprehensif, sehingga menimbulkan ketidakpastian hukum yang menjadi celah untuk berbagai pelanggaran dan tindak kejahatan (di bidang keamanan dan ketahanan siber) yang sangat merugikan masyarakat.

Reformasi regulasi menjadi sebuah solusi konkret untuk mengatasi berbagai permasalahan terkait ruang siber di tanah air, khususnya terkait keamanan dan ketahanan siber. Kebutuhan mendesak terhadap Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber (RUU KKS) harus segera direalisasikan oleh pemerintah dan DPR. Pemerintah telah mengajukan RUU KKS dalam Prolegnas Jangka Menengah Tahun 2025-2029. Melalui kajian akademik substansi RUU KKS ini, BSSN bersama dengan akademisi dan Kementerian Hukum telah merumuskan konsep dan mengkaji substansi RUU KKS. Kajian ini diarahkan telah menghasilkan konsep awal rancangan naskah akademik maupun konsep awal RUU KKS.

Dalam penyusunan naskah akademik substansi RUU KKS, khususnya pada bagian “kajian terhadap implikasi penerapan sistem baru akan diatur dalam Undang-Undang terhadap aspek kehidupan masyarakat dan dampaknya terhadap aspek beban keuangan negara”, perlu dilakukan dengan menganalisis dampak dari suatu norma dalam RUU KKS untuk memperkirakan biaya yang harus dikeluarkan dan manfaat yang diperoleh dari penerapan RUU KKS. Kajian tersebut

didukung dengan analisis yang menggunakan metode *Regulatory Impact Analysis* (RIA) atau metode *Rule*, *Opportunity*, *Capacity*, *Communication, Interest, Process, and Ideology* (ROCCIPI).

Apabila dalam proses kajian ditemukan berbagai pengaturan terkait keamanan dan ketahanan siber yang telah diatur dalam peraturan perundang-undangan lain, konsep RUU KKS dirancang sebagai regulasi yang melengkapi dan mengisi celah hukum dari kerangka norma yang sudah ada. RUU KKS bertujuan memperkuat koherensi kerangka hukum keamanan siber. Pendekatan ini difokuskan pada penyelarasan pengaturan yang belum tercakup secara optimal dalam regulasi eksisting, sehingga terbentuk sistem hukum yang utuh, terpadu, dan responsif terhadap dinamika ruang siber. Dengan demikian, RUU KKS dapat menjadi fondasi hukum yang komprehensif untuk melindungi hak masyarakat dalam memanfaatkan teknologi digital sekaligus memastikan keamanan dan ketahanan siber Indonesia secara berkelanjutan, tanpa menimbulkan irisan tugas atau kekosongan regulasi.

Dalam upaya mewujudkan fondasi hukum yang utuh dan responsif dalam RUU KKS, penting untuk mengakui bahwa tidak semua elemen dalam ruang siber memiliki bobot strategis yang setara, terutama ketika menyangkut layanan esensial bagi negara dan mempengaruhi kesejahteraan masyarakat. Perbedaan tingkat kritikalitas infrastruktur ini menuntut regulasi khusus yang mempertimbangkan dimensi ancaman yang berpotensi mengganggu stabilitas nasional secara sistemik. Dengan demikian, keberadaan kerangka hukum yang terpadu harus mampu merespons hierarki risiko secara proporsional, di mana pelindungan terhadap komponen kritikal yang jika terganggu dapat mengancam kelangsungan layanan publik, ekonomi, hingga kedaulatan negara menjadi prioritas utama yang tidak bisa disamaratakan dengan pengaturan sistem atau layanan secara umum. Hal ini menjadi landasan krusial untuk memahami mengapa pendekatan keamanan dalam regulasi eksisting belum mengakomodasi karakteristik unik infrastruktur kritikal dalam ekosistem siber.

Infrastruktur Informasi (II) dan Infrastruktur Informasi Kritikal (IIK) tidak dapat disamakan dengan sistem elektronik yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengingat perbedaan mendasar pada konsekuensi disrupsi yang ditimbulkan. Dalam kerangka UU ITE, sistem elektronik didefinisikan sebagai serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik, sementara II merujuk pada jaringan sistem elektronik yang saling terkait dan ketergantungan fungsionalnya bersifat multidimensi. Adapun IIK merupakan kategori khusus yang, apabila mengalami gangguan, berpotensi mengakibatkan dampak luas terhadap kepentingan umum, pelayanan publik, stabilitas pertahanan dan keamanan, serta perekonomian nasional. Ada perbedaan filosofis antara sistem elektronik dengan IIK, UU ITE beroperasi dalam paradigma respons pasca-insiden (*reactive approach*) dengan logika "jika rusak, diperbaiki", sedangkan IIK harus beroperasi dalam prinsip *zero-failure paradigm* yang tidak mengizinkan terjadinya kegagalan, mengingat setiap detik terhentinya operasional berpotensi melumpuhkan layanan vital yang menjadi penopang kehidupan masyarakat dan negara. Sejalan dengan eskalasi ancaman keamanan siber yang telah berevolusi dari tindak kriminal individu menjadi sistematis dan terkoordinasi yang secara strategis menyasar infrastruktur kritikal, pengaturan yang semata-mata berfokus pada aspek transaksi elektronik sebagaimana diamanatkan UU ITE dipandang kurang memadai untuk melindungi sistem yang menjadi fondasi kedaulatan negara.

RUU KKS mengatur IIK secara spesifik mengingat karakteristik unik yang tidak dapat ditangani oleh kerangka regulasi yang ada saat ini. Berbeda dengan UU ITE yang bersifat reaktif, RUU KKS mengadopsi pendekatan proaktif melalui penerapan prinsip *security by design* sejak tahap perencanaan, pemantauan secara *real-time* yang terintegrasi dengan Sistem Deteksi Dini Ancaman Siber Nasional, serta mekanisme

pelaporan insiden yang lebih ketat.

Pengaturan IIK dalam RUU KKS didasarkan pada kebutuhan akan mekanisme penetapan yang objektif, terukur, dan akuntabel, hal yang tidak terpenuhi dalam UU ITE. UU ITE hanya mengacu pada sistem elektronik milik pemerintah atau badan strategis secara umum tanpa kriteria spesifik, sehingga berpotensi menimbulkan ketidakjelasan dalam menentukan prioritas Pelindungan. Sebaliknya, RUU KKS membangun kerangka penetapan IIK melalui asesmen multidimensi yang mempertimbangkan kriteria objektif potensi dampak sistemik terhadap kepentingan nasional, serta risiko ancaman siber strategis. Proses ini melibatkan koordinasi antara BSSN, kementerian terkait, dan pemangku kepentingan sektoral untuk memastikan validasi dan transparansi dalam pengambilan keputusan.

Perbedaan penting lain terletak pada dimensi waktu respons ancaman terhadap sistem elektronik konvensional masih memungkinkan penanganan melalui skema respons pasca-insiden, sementara ancaman terhadap IIK harus diantisipasi secara preventif mengingat waktu respons pasca-insiden terlalu sempit untuk mencegah dampak yang bersifat sistemik dan katastrofik. Tanpa pengaturan khusus yang membedakan IIK dari II biasa, negara akan kehilangan kapasitas untuk mengalokasikan sumber daya keamanan secara proporsional sesuai tingkat kritikalitas, sehingga menciptakan kerentanan yang dapat dieksploitasi oleh pelaku ancaman siber yang semakin kompleks dan terorganisir. Pelindungan IIK memerlukan kerangka hukum yang lebih komprehensif, preskriptif, dan berlapis dibandingkan pengaturan sistem elektronik secara umum. Kerangka hukum ini tidak hanya menjamin ketersediaan layanan kritikal, tetapi juga memperkuat ketahanan nasional dalam menghadapi ancaman siber yang semakin canggih dan berdampak multidimensi.

B. Identifikasi Masalah

1. Permasalahan apa yang dihadapi terkait pembentukan/penyusunan RUU KKS dan bagaimana

permasalahan tersebut dapat diatasi?

2. Mengapa perlu adanya RUU KKS sebagai dasar pemecahan masalah tersebut?
3. Apa yang menjadi pertimbangan landasan filosofis, sosiologis, dan yuridis pembentukan RUU KKS?
4. Bagaimana sasaran, arah dan jangkauan pengaturan serta ruang lingkup materi muatan RUU KKS?

C. Tujuan dan Kegunaan Kegiatan Penyusunan Naskah Akademik

Sesuai dengan ruang lingkup identifikasi masalah yang dikemukakan, tujuan penyusunan Naskah Akademik RUU KKS adalah sebagai berikut :

1. Merumuskan permasalahan yang terkait dengan pembentukan/penyusunan RUU KKS dan cara mengatasi permasalahan tersebut.
2. Merumuskan permasalahan hukum yang dihadapi sebagai alasan pembentukan RUU KKS sebagai dasar hukum penyelesaian atau solusi permasalahan kehidupan berbangsa, bernegara dan bermasyarakat.
3. Merumuskan pertimbangan landasan filosofis, sosiologis, dan yuridis pembentukan RUU KKS.
4. Merumuskan sasaran, arah dan jangkauan pengaturan serta ruang lingkup materi muatan RUU KKS.

Adapun kegunaan penyusunan Naskah Akademik RUU KKS sebagai acuan atau referensi penyusunan dan pembahasan RUU KKS.

D. Metode

Penyusunan Naskah Akademik RUU KKS menggunakan metode yuridis normatif. Metode ini dilakukan dilakukan untuk mengumpulkan data dan informasi terkait perbandingan atau pemahaman mendalam tentang keamanan dan ketahanan siber dengan merujuk pada pengalaman atau praktik yang ada di tempat lain. Hasil kegiatan studi banding dengan melakukan pendekatan penelitian yang melibatkan

pengumpulan data, informasi, dan pengamatan terkait dengan tujuan untuk memperoleh wawasan yang lebih dalam dan pemahaman yang lebih komprehensif. Metode ini digunakan dalam berbagai konteks, termasuk dalam organisasi, pemerintahan, atau sektor lainnya. Kegiatan studi banding melibatkan beberapa tahap, termasuk perencanaan, pelaksanaan, analisis, dan pelaporan. Pada tahap perencanaan, peneliti merancang kerangka kerja penelitian, tujuan, dan metode yang akan digunakan. Selanjutnya data diolah secara kualitatif.

BAB II
KAJIAN TEORETIS DAN PRAKTIK EMPIRIK

A. Kajian Teoretis

1. Ruang Siber

Ruang siber dan ekosistem digital telah menjadi bagian tak terpisahkan dari kehidupan masyarakat dan penyelenggaraan negara serta memiliki pengaruh signifikan terhadap keamanan nasional, stabilitas ekonomi, kesejahteraan sosial, reputasi negara, dan pelayanan publik. Transformasi digital selain memberikan manfaat besar bagi kehidupan manusia juga telah menimbulkan ancaman baru dalam bentuk kejahatan siber, yang kini menjadi ancaman global serius bagi banyak negara, termasuk Indonesia. Dunia siber yang terus berkembang telah menciptakan tantangan baru dalam menjaga keamanan dan kedaulatan nasional, serta memelihara stabilitas ekonomi, pelayanan publik, dan kesejahteraan sosial. Ruang siber *(cyberspace)* mengacu pada dunia virtual yang diciptakan oleh jaringan komputer global, di mana interaksi dan komunikasi digital berlangsung.

Ruang ini beroperasi dalam jaringan sistem-sistem yang terhubung, menggunakan protokol komunikasi seperti *Transmission Control Protocol/Internet Protocol* (TCP/IP), yang memungkinkan pertukaran data dan informasi di seluruh dunia. ruang siber, sejak diperkenalkan oleh William Gibson dalam karyanya *"Neuromancer"* di tahun 1984, telah berkembang pesat dan menjadi medium esensial dalam kehidupan modern, terutama di era digitalisasi global.[5] Ruang siber merupakan lingkungan nonfisik yang memungkinkan aktivitas interaksi digital antar manusia dan sistem. Salah satu karakteristik penting dari ruang siber adalah sifatnya yang "tanpa batas" *(borderless)*, di mana individu dapat terhubung dengan orang lain dan berbagai sistem di

[5] Vangie Beal and Natalie Medleva, "Cyberspace", *Techopedia,* diakses dari https://www.techopedia.com/definition/2493/cyberspace#:~:text=Cyberspace%20refers%20to%20the%20virtual,for%20communication%20and%20data%20exchange., diakses pada 13 Oktober 2024.

seluruh dunia secara digital, tanpa dibatasi oleh lokasi geografis atau ruang fisik.

Selain itu, ruang siber memberikan akses terhadap berbagai aktivitas, termasuk bisnis, media, hiburan, pendidikan, dan lain-lain. Ruang siber dan dunia fisik memiliki beberapa perbedaan mendasar. Ruang siber merupakan lingkungan virtual dan abstrak, dimana interaksi terjadi secara digital melalui jaringan komputer. Interaksi di ruang siber tidak memiliki batasan fisik dan dapat melibatkan siapa saja, di mana saja, selama terhubung dengan internet. Karena sifatnya ini, maka ruang siber sangat fleksibel dan dapat mencakup berbagai aktivitas dari interaksi sosial hingga pertukaran data.

Berbeda dengan ruang siber, dunia fisik menekankan pada basis tempat-tempat nyata dan interaksi fisik. Maka dari itu, interaksi yang terjadi terbatas oleh ruang, waktu, dan geografi sehingga memiliki batasan fisik yang jelas, seperti negara atau kota. Ruang siber terdiri dari berbagai komponen yang mendukung fungsinya sebagai media interaksi digital, antara lain:

a. Kecerdasan Buatan *(Artificial Intelligence/AI)*: Digunakan untuk menciptakan pengalaman pengguna yang dipersonalisasi, seperti rekomendasi konten di platform digital atau *chatbot* otomatis.
b. Komputasi Awan *(Cloud Computing)*: Penyimpanan data yang terdesentralisasi dan diakses melalui internet, memungkinkan kolaborasi dan akses jarak jauh.
c. Keamanan Siber *(Cybersecurity)*: Sistem yang melindungi jaringan dan data dari ancaman siber, seperti serangan malware, peretasan, dan pencurian identitas.
d. *Internet of Things* (IoT): Koneksi antara perangkat fisik dengan internet yang memungkinkan pertukaran data secara *real-time*.

Infrastruktur Informasi Kritikal (IIK) yang bergantung pada ruang siber meliputi sektor penting yang esensial bagi berjalannya

kehidupan sehari-hari, seperti telekomunikasi, energi, keuangan, pemerintah, kesehatan, pertahanan, pangan, dan transportasi. Gangguan pada IIK dapat mengakibatkan dampak serius terhadap stabilitas ekonomi dan keamanan nasional. Ruang siber merupakan entitas yang selalu berkembang, seiring dengan kemajuan teknologi. Pengguna ruang siber bertambah seiring meningkatnya kebutuhan akan komunikasi digital, komputasi awan, dan teknologi berbasis internet lainnya.

Teknologi baru seperti kecerdasan buatan, *quantum computing*, jaringan 5G, dan *augmented reality* (AR) diharapkan akan semakin memperluas cakupan dan potensi ruang siber di masa depan. Ruang siber menawarkan berbagai manfaat, seperti akses ke informasi yang luas dimana pengguna dapat dengan mudah memperoleh informasi dari berbagai sumber secara global, kemudahan dalam hiburan dimana media digital dan *game online* dapat diakses kapan saja dan di mana saja, hingga koneksi global yang semakin luas dimana ruang siber memungkinkan interaksi antarindividu dan komunitas dari berbagai belahan dunia. Akan tetapi, ruang siber juga memiliki beberapa risiko, seperti keamanan data pribadi dimana data pengguna dapat terekspos oleh berbagai ancaman siber, seperti peretasan atau pencurian identitas, serangan terhadap IIK dapat menjadi target serangan siber yang berpotensi mengganggu layanan kritikal, hingga kerentanan terhadap ancaman siber dimana ruang siber dapat menjadi tempat bagi berbagai jenis serangan, mulai dari *malware* hingga serangan *phishing*.

Ruang siber adalah entitas digital yang memungkinkan interaksi dan komunikasi di dunia maya. Peranannya yang semakin penting dalam kehidupan modern menjadikannya ruang yang terus berkembang dan berpotensi memberikan dampak besar bagi individu, bisnis, dan pemerintah. Di sisi lain, risiko yang melekat pada ruang siber, seperti ancaman keamanan, menuntut langkah-langkah pelindungan yang kuat, baik secara individu

maupun sistemik. Regulasi yang kuat dan komprehensif sangat diperlukan untuk menjaga ruang siber khususnya dalam perspektif kedaulatan Indonesia sebagai bangsa dan negara.

2. Keamanan Siber

National Institute of Standards and Technology (NIST) Amerika Serikat memberikan setidaknya 4 (empat) definisi terkait keamanan siber *(Cyber security).* Definisi pertama menekankan pada pencegahan kerusakan, Pelindungan, dan pemulihan sistem komunikasi elektronik serta komputer, yang mencakup pelindungan integritas, ketersediaan, dan kerahasiaan informasi. Dalam hal ini, fokus utama adalah melindungi sistem dan data dari akses tidak sah serta menjaga keandalan dan validitas informasi. Selain itu, konsep seperti nonrepudiation memastikan bahwa pihak yang mengirim dan menerima informasi tidak dapat menyangkal proses komunikasi yang terjadi, menambah lapisan keamanan dalam transaksi digital.

Di sisi lain, definisi kedua hingga keempat memperluas konsep ini dengan memasukkan elemen respons terhadap ancaman, pemulihan sistem setelah serangan, dan pelindungan keseluruhan ruang siber. Definisi kedua melihat keamanan siber sebagai proses melibatkan deteksi, pencegahan, dan penanggulangan serangan siber, yang menunjukkan pentingnya perencanaan dan respons insiden yang terorganisir. Definisi ketiga lebih menekankan pada pelindungan seluruh ruang siber dari serangan, sementara definisi keempat menggabungkan pencegahan kerusakan dan pemulihan informasi serta sistem komunikasi. Meski beragam, semua definisi ini berfokus pada pelindungan data, integritas, dan keberlangsungan sistem dalam menghadapi ancaman digital.[6]

NIST Cybersecurity Framework (CSF) 2.0 merupakan kerangka konseptual yang dikembangkan oleh *National Institute of Standards*

[6] NIST, "Glossary: Cybersecurity", *Computer Security Resource Center CSRC,* diakses dari https://csrc.nist.gov/glossary/term/cybersecurity, diakses pada 13 Oktober 2024.

*and Technology (NIST) se*bagai panduan sistematis untuk mengelola risiko keamanan siber secara terukur, adaptif, dan berorientasi hasil. *Framework* ini berlandaskan pada pendekatan *risk-based* dan *outcome-based,* yang menekankan bahwa keamanan siber harus dikelola berdasarkan pemahaman terhadap risiko aktual yang dihadapi organisasi serta capaian yang ingin diwujudkan, bukan semata melalui pemenuhan administratif. Versi terbaru, yaitu *CSF 2.0* yang diterbitkan pada tahun 2024, merupakan penyempurnaan dari versi 1.1 dengan memperluas cakupan penerapan dari infrastruktur kritikal menuju seluruh sektor pemerintahan, swasta, dan masyarakat digital secara luas. Pembaruan ini mencerminkan pandangan bahwa keamanan siber merupakan bagian integral dari tata kelola organisasi dan ketahanan nasional, bukan sekadar domain teknis yang terpisah.

Secara struktural, CSF 2.0 terdiri atas tiga komponen utama, yaitu *Core, Profiles,* dan *Tiers.* Komponen *Core* menggambarkan hasil yang diharapkan dari upaya pengelolaan risiko siber dan diorganisasikan ke dalam enam fungsi inti, yaitu *Govern, Identify, Protect, Detect, Respond,* dan *Recover.* Fungsi *Govern,* yang merupakan inovasi pada versi 2.0, menegaskan pentingnya aspek tata kelola dalam keamanan siber, termasuk kebijakan, struktur tanggung jawab, serta keterlibatan pimpinan organisasi dalam pengambilan keputusan strategis. Fungsi *Identify* berfokus pada pemahaman konteks, aset, dan eksposur risiko; *Protect* memastikan penerapan mekanisme Pelindungan; *Detect* mengatur kemampuan mendeteksi insiden; *Respond* menitikberatkan pada penanganan insiden; dan *Recover* menekankan kemampuan pemulihan pascakejadian. Setiap fungsi tersebut diuraikan dalam kategori dan subkategori yang menggambarkan hasil konkret yang dapat dicapai, serta dilengkapi dengan *Implementation Examples* dan *Informative References y*ang mengaitkan *framework* ini dengan berbagai standar internasional seperti ISO/IEC 27001, NIST SP 800-53, dan COBIT.

Komponen Profiles memungkinkan organisasi menyesuaikan *framework* dengan kebutuhan dan prioritas masing-masing, melalui pembandingan antara *Current Profile* (kondisi saat ini) dan *Target Profile* (tujuan yang diinginkan), yang selanjutnya digunakan untuk menyusun rencana perbaikan dan mitigasi risiko. Sementara itu, *Tiers* menunjukkan tingkat kematangan penerapan manajemen risiko siber, mulai dari *Partial* hingga *Adaptive,* yang dapat dijadikan tolok ukur kemampuan organisasi dalam mengelola ancaman dan meningkatkan kapasitas adaptif secara berkelanjutan. Konsep-konsep ini mencerminkan siklus peningkatan berkelanjutan (*continuous improvement cycle*) dalam tata kelola keamanan siber.

Framework ini penting dijadikan landasan konseptual bagi penyusunan RUU Keamanan dan Ketahanan Siber (RUU KKS) karena memiliki sejumlah keunggulan normatif dan praktis. Pertama, CSF 2.0 menawarkan kerangka kerja yang terstandar secara internasional, sehingga dapat memperkuat keselarasan kebijakan keamanan siber Indonesia dengan praktik global tanpa mengabaikan konteks nasional. Kedua, *framework* ini menempatkan keamanan siber dalam konteks tata kelola risiko dan pengambilan keputusan strategis, yang sejalan dengan kebutuhan pengaturan kelembagaan keamanan siber di tingkat nasional. Melalui fungsi *Govern*, CSF 2.0 menegaskan bahwa keamanan siber tidak dapat didelegasikan semata kepada unit teknis, tetapi harus menjadi tanggung jawab kolektif yang melibatkan pimpinan, regulator, pelaku industri, dan masyarakat. Ketiga, *framework* ini mendorong pendekatan lintas sektor dan kolaboratif, yang sangat relevan dengan ekosistem keamanan siber Indonesia yang melibatkan beragam pemangku kepentingan. Keempat, prinsip *risk-based approach* dalam CSF 2.0 dapat mendukung perumusan kebijakan yang proporsional dan berbasis risiko, sehingga kebijakan keamanan siber nasional tidak bersifat seragam, tetapi

mempertimbangkan tingkat risiko, kapasitas, dan karakteristik masing-masing sektor.

Lebih lanjut, penerapan prinsip CSF 2.0 dalam RUU KKS dapat memperkuat ketahanan siber nasional (*cyber resilience*) melalui pembangunan sistem keamanan yang adaptif, terukur, dan berkelanjutan. Pendekatan berbasis fungsi dan tata kelola sebagaimana diatur dalam CSF 2.0 juga dapat membantu mewujudkan mekanisme koordinasi antarlembaga yang lebih efektif, mendorong integrasi kebijakan antara aspek pertahanan, penegakan hukum, dan Pelindungan data, serta membangun budaya keamanan siber yang inklusif di seluruh lapisan masyarakat. Dengan mengadopsi kerangka ini, RUU KKS akan memiliki landasan yang kuat untuk mengatur penyelenggaraan keamanan dan ketahanan siber secara menyeluruh, mulai dari aspek kelembagaan, mekanisme koordinasi, manajemen risiko, hingga pemulihan pasca kejadian. Dengan demikian, NIST *Cybersecurity Framework* 2.0 tidak hanya menjadi acuan teknis, tetapi juga dasar konseptual yang mendukung perumusan kebijakan siber nasional yang terukur, adaptif, partisipatif, dan sejalan dengan standar internasional.

Perkembangan teknologi informasi saat ini memberikan dampak yang sangat signifikan terhadap kehidupan manusia, salah satunya dengan hadirnya dunia siber yang mampu menghubungkan masyarakat antara satu dengan lainnya dengan menggunakan jaringan untuk melakukan berbagai macam kegiatan dan tujuan. Dengan terdapatnya dunia siber yang mampu menghubungkan manusia, hal ini memberikan banyak keuntungan dan kemanfaatan yang dapat mempermudah hidup masyarakat. Akan tetapi, kehadiran dunia siber juga memberikan ancaman dan tantangan yang berbahaya dan mengganggu keselamatan manusia. Hal ini tentu membuat masyarakat kerap kali mengkhawatirkan keamanan siber mereka ketika mereka mengakses atau memiliki sesuatu data yang terdapat di dunia

siber.

Hal ini tentu menjadi perhatian sebab sangat tidak mungkin kehidupan manusia saat ini tidak terpengaruh atau terhubung dalam dunia siber. Keamanan siber menjadi aspek yang penting bagi seluruh manusia dalam mengakses dunia siber. Keamanan Siber sendiri merupakan upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial.[7] Kehadiran keamanan siber diperlukan untuk mencegah terjadinya serangan siber yang dapat menyerang *database online* pemerintah yang menyimpan data-data penting negara, seperti data penduduk, keuangan, dan sumber daya alam.[8] selain itu, keamanan siber juga diperlukan agar dapat melindungi masyarakat dan pelaku usaha terhadap kejahatan yang memberikan kerugian dan ancaman yang besar bagi mereka.[9]

Skema kejahatan siber yang semakin berkembang dari tahun ke tahun juga menjadi ancaman tersendiri bagi masyarakat. Para pelaku kejahatan siber terus mencari cara agar dapat mengembangkan cara baru untuk melakukan kejahatan siber. Oleh karena itu, guna menjamin keamanan siber bagi setiap masyarakat, dan untuk mencegah kejahatan siber, setiap individu, kelompok masyarakat, pelaku usaha, para penegak hukum, pemangku kebijakan, serta pemerintah perlu memahami dengan baik dan jelas skema kejahatan siber dan perkembangan kejahatan yang berlaku di dunia siber oleh para penjahat siber ini.[10] Dengan memahami perkembangan kejahatan siber, maka masyarakat akan terhindar dari kejahatan siber dan dapat memberikan keamanan

[7] Pasal 1 Angka 1 Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

[8] Wanda Ayu A., ui.ac.id, "Pentingnya Keamanan Siber Bagi Pertahanan dan Keamanan Nasional", 2017, https://www.ui.ac.id/pentingnya-keamanan-siber-bagi-pertahanan-dan-keamanan-nasional/ diakses pada 11 Oktober 2024.

[9] Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Analisis, dan Perkembangannya", Technology and Economics Law Journal Vol. 2 Nomor 2, 2023, hlm. 300.

[10] Bhavna Arora, "Exploring and Analyzing Internet Crimes and Their Behaviours", Perspectives in Science Vol. 8, 2016, hlm. 540 - 542.

siber dalam mengakses dunia siber.

Selain itu, bagi pemerintah serta pemangku kebijakan memerlukan pengaturan yang komprehensif dalam mewujudkan keamanan siber. Hal ini sejalan dengan teori hukum transformatif yang dikemukakan oleh Guru Besar FH Unpad, Ahmad M. Ramli. Teori tersebut berpandangan bahwa hukum tidak semata berfungsi untuk terciptanya ketertiban, kepastian dan keadilan semata. Akan tetapi, hukum juga berperan sebagai infrastruktur transformasi untuk kekuatan bangsa agar mampu menghadapi perkembangan digital yang tidak dapat dibendung.[11] Dengan menimbang aspek hukum sebagai infrastruktur transformasi digital bagi masyarakat, maka salah satu peran yang dapat dimiliki adalah dengan memberikan pengaturan yang komprehensif terkait keamanan siber, guna mampu menjadi pilar dalam transformasi digital bangsa.

Pengaturan yang komprehensif ini dapat berupa pengaturan terkait kriteria atau standar keamanan siber yang harus dipenuhi setiap Penyelenggara Sistem Elektronik maupun setiap Produk dengan Elemen Digital. Pemerintah juga dapat mengatur ketentuan untuk menanggulangi insiden siber yang telah terjadi, agar tidak semakin parah dan memberikan kerugian bagi pihak yang terdampak. Pengaturan ini dapat termasuk strategi untuk mengatur perangkat teknologi mampu menyimpan atau menempatkan dokumen penting yang digunakan agar disimpan sebagai arsip sesuai dengan standar global, agar dapat mencegah dampak/risiko yang terjadi berupa kehilangan data-data penting akibat terjadinya insiden siber.[12]

[11] Ahmad M. Ramli & Tasya Safiranita, *Hukum Sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital,* Bandung: Refika Aditama, 2022, hlm. 25.
[12] Febyola Indah (et.al), "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka), Jurnal Bidang Penelitian Informatika Vol. 1 Nomor 1, 2022, hlm. 3.

3. Ketahanan atau Resiliensi Siber

Ketahanan atau resiliensi siber dapat diartikan sebagai kemampuan suatu organisasi/sistem untuk bertahan dari adanya serangan siber termasuk memberikan respon, mengatasi dampak serangan dan memulihkan kondisi dengan cepat setelah adanya insiden siber tersebut.[13] Upaya penyelenggaraan pertahanan negara mencakup berbagai langkah strategis dan teknis yang dirancang untuk melindungi Infrastruktur Informasi. Dalam konteks ini, upaya tersebut tidak hanya berfokus pada pencegahan serangan, tetapi juga pada deteksi dini, respons yang cepat, dan pemulihan setelah insiden.

Di Amerika Serikat, Arahan Kebijakan Presiden Nomor 21, yang dikeluarkan oleh Pemerintah Amerika Serikat pada tanggal 12 Februari 2013, menetapkan kebijakan nasional untuk pemerintah Amerika Serikat tentang keamanan dan ketahanan infrastruktur penting.[14] Ketahanan, sebagaimana didefinisikan dalam arahan tersebut, mengacu pada "kemampuan untuk mempersiapkan dan beradaptasi dengan kondisi yang berubah serta untuk bertahan dan pulih dengan cepat dari gangguan". Pengertian ketahanan siber juga dapat dilihat berdasarkan *The NIST Computer Security Resource Center Glossary* yang mendefinisikan *Cyber Resiliency* sebagai *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises in systems that use or are enabled by cyber resources."*[15]

Menurut Faisal Yahya, seorang ahli strategi keamanan siber, *cyber resiliency* atau ketahanan siber adalah kunci untuk menghadapi dinamika ancaman yang intens di era digital saat ini.

---

[13] Universitas Islam Indonsia, "Transformasi Digital dan Resiliensi Siber", dalam Seminar dan Workshop "Yogyakarta Cyber Resilience 2023" yang diselenggarakan di Universitas Islam Indonesia pada 19 Juni 2023, <https://www.uii.ac.id/transformasi-digital-dan-ketahanan-siber/> diakses pada 10 oktober 2024.

[14] The White House Office of the Press Secretary, (2013), "Presidential Policy Directive - Critical Infrastructure Security and Resilience", <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructuresecurity-and-resil> diakses pada 10 Oktober 2024.

[15] *Misael Sousa de Araujo (et.al),* "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance", Applied Sciences, 2024, hlm. 5.

Ia menekankan perlunya manajemen risiko yang terpadu, di mana organisasi harus mampu mengidentifikasi dan mengevaluasi risiko serta menerapkan langkah-langkah keamanan seperti enkripsi dan kontrol akses. Selain itu, Faisal juga menekankan pentingnya memiliki rencana respons terhadap insiden siber untuk menjaga kelangsungan operasional meskipun terjadi gangguan.[16]

Ketahanan Siber dikonsepkan sebagai kondisi dinamis Infrastruktur Informasi untuk mampu bertahan dari Serangan Siber sekaligus menjamin kelangsungan operasionalnya. Berbeda dengan keamanan siber yang lebih berfokus pada upaya pencegahan, ketahanan siber didefinisikan sebagai kemampuan sistem untuk pulih dan beroperasi kembali secara normal pascainsiden atau setelah mengalami gangguan dan/atau Serangan Siber. Pendekatan ini merefleksikan prinsip *cyber resilience* yang menjadi landasan filosofis pengaturan ketahanan siber dalam kerangka kebijakan nasional.

Dalam perspektif kebijakan, ketahanan siber tidak hanya berkaitan dengan kemampuan pemulihan pasca-serangan, melainkan mencakup upaya sistematis untuk memastikan Infrastruktur Informasi tetap beroperasi secara kontinu meskipun menghadapi ancaman dan serangan siber. Ketahanan siber menjadi krusial ketika upaya pencegahan tidak mencukupi atau ketika serangan siber berhasil menembus lapisan keamanan yang ada, sehingga diperlukan kemampuan sistem untuk tetap beroperasi dan segera pulih dari gangguan.

Implementasi ketahanan siber dilaksanakan melalui tiga pilar utama yang saling terkait dan saling memperkuat. Pertama, peningkatan kapasitas sumber daya manusia yang meliputi penyediaan, peningkatan kompetensi, alih teknologi, serta pembentukan budaya kesadaran keamanan informasi. Kedua,

[16] AntaraNews, "Cyber Resiliency" Dinilai Kunci Hadapi Ancaman Siber Yang Kian Intens, 2023, <https://www.antaranews.com/berita/3737610/cyber-resiliency-dinilai-kunci-hadapi-ancaman-siber-yang-kian-intens>, [diakses pada 11/10/2024].

peningkatan kapasitas teknologi yang mencakup penggunaan Produk dengan Elemen Digital yang memenuhi standar keamanan siber, pelaksanaan riset dan pengembangan teknologi, pemanfaatan kecerdasan artifisial, serta penerapan keamanan rantai pasokan. Ketiga, peningkatan kapasitas proses bisnis yang meliputi manajemen risiko keamanan siber, berbagi informasi keamanan siber, penerapan Persandian, pengukuran tingkat kematangan keamanan siber, serta audit dan asesmen keamanan siber.

Melalui tiga pilar ini, ketahanan siber tidak hanya berfokus pada aspek pemulihan data dan perbaikan sistem pasca-serangan, tetapi lebih luas mencakup upaya proaktif untuk membangun sistem yang mampu bertahan, beradaptasi, dan pulih dengan cepat dari gangguan siber. Pendekatan holistik ini memastikan bahwa Infrastruktur Informasi dapat mempertahankan fungsi kritikalnya dalam mendukung pelayanan publik, stabilitas ekonomi, dan keamanan nasional, sekaligus mendorong inovasi teknologi secara bertanggung jawab sesuai dengan prinsip pengembangan ekonomi digital yang menjadi salah satu asas penyelenggaraan keamanan dan ketahanan siber. Dengan demikian, ketahanan siber menjadi fondasi penting dalam membangun ekosistem digital yang aman, resilien, dan tangguh sebagai bagian dari kehadiran negara dalam melindungi kepentingan nasional di ruang siber.

Hukum transformatif berfokus pada bagaimana hukum dapat berperan dalam mengubah perilaku sosial dan menciptakan keadilan dalam konteks yang lebih luas.[17] Dalam hal ini, pendekatan hukum transformatif dapat membantu membangun kerangka hukum yang mendukung pengembangan ketahanan siber di Indonesia. Misalnya, Undang-Undang yang mengatur pelindungan data pribadi dan keamanan informasi dapat menjadi landasan bagi organisasi untuk meningkatkan ketahanan mereka

[17] Ahmad M. Ramli & Tasya Safiranita, *Hukum Sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital,* Op.Cit.

terhadap serangan siber. Kesimpulannya adalah ketahanan siber tidak bisa dipandang sebelah mata dalam konteks transformasi digital saat ini. Baik dari perspektif organisasi maupun individu, membangun ketahanan terhadap ancaman siber adalah langkah krusial untuk memastikan keberlangsungan operasional dan pelindungan data.

4. Ancaman Siber

Seiring dengan perkembangannya, kemajuan teknologi tidak hanya menjadi peluang namun juga memunculkan berbagai ancaman, dimana salah satunya adalah ancaman di bidang siber. Ancaman siber atau *cyber threat* diartikan sebagai tindakan, gangguan, atau pun serangan yang berpotensi merusak atau mempengaruhi sistem dengan menargetkan kerahasiaan, interitas, dan ketersediaan informasi.[18] NIST mendefinisikan *cyber threat* sebagai "Setiap keadaan atau peristiwa yang berpotensi berdampak negatif pada operasi organisasi (termasuk misi, fungsi, citra, atau reputasi), aset organisasi, atau individu melalui sistem informasi, seperti akses tidak sah, perusakan, pengungkapan, modifikasi informasi, dan/atau penolakan layanan, serta potensi sumber ancaman untuk berhasil mengeksploitasi kerentanan tertentu dalam sistem informasi".[19] Dalam arti lain, ancaman siber merupakan potensi bahaya yang dapat menimbulkan kerugian, gangguan, atau serangan terhadap keamanan informasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan data. Ancaman tersebut dapat berasal dari berbagai sumber, baik internal maupun eksternal yang mana mencakup aspek ideologi, politik, ekonomi, dan teknologi.[20]

[18] Ratno Dwi Putra (et.al), "Ancaman Siber Dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)", Jurnal Peperangan Asimetris Universitas Pertahanan, Vol. 4 Nomor2, 2018, hlm. 13.
[19] NIST, "Glossary: Cyber Threat", *Computer Security Resource Center CSRC,* diakses dari https://csrc.nist.gov/glossary/term/cyber_threat, diakses pada 13 Oktober 2024.
[20] *Ibid*.

Ancaman sendiri, menurut Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara, diartikan sebagai setiap upaya, pekerjaan, kegiatan dan tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan kepentingan nasional di berbagai aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan.[21] Ancaman ini dapat dikategorikan berdasarkan target yang terpengaruh. Sumber ancaman siber berasal dari entitas yang memiliki niat untuk melanggar hukum dan norma keamanan informasi, baik untuk keuntungan materi maupun immateri, melalui dunia maya. Sumber tersebut bisa berasal dari dalam maupun luar, termasuk dari intelijen, kekecewaan, investigasi, organisasi ekstremis, hacktivist, kelompok kejahatan terorganisir, serta faktor persaingan dan konflik.

Ancaman siber melibatkan berbagai aspek, seperti ideologi, politik, ekonomi, budaya, dan teknologi, yang berkaitan dengan kehidupan berbangsa dan bernegara, serta kepentingan pribadi. Baik individu maupun organisasi dapat menjadi pelaku ancaman siber. Penetrasi dan kebocoran informasi melalui protokol komunikasi harus diwaspadai, karena apabila tidak diatasi, dapat berujung pada serangan siber yang membahayakan aset informasi. Serangan siber sendiri merupakan tindakan yang bertujuan untuk mengakses, memodifikasi, mencuri, atau merusak sistem informasi.[22] Serangan yang bersifat besar dan intens dapat berdampak signifikan pada pertahanan negara.

Ancaman siber sendiri terdiri dari beragam jenis, yang diantaranya meliputi penipuan (*phishing*), manipulasi psikologis (*social engineering*), serangan enkripsi data (*ransomware*),

[21] Pasal 1 ayat (4) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.
[22] IBM, "Apa yang dimaksud dengan serangan siber?", https://www.ibm.com/id-id/topics/cyber-attack, diakses pada 10 Oktober 2024.

perangkat lunak berbahaya (*malware*), serangan server atau jaringan (serangan DDoS), Serangan *Man in the Middle* yang mencegat komunikasi antara dua pihak yang sah dan mencuri informasi yang sedang ditransmisikan, serangan *zero-day* untuk mengeksploitasi kerentanan perangkat lunak yang belum ditemukan, serangan terhadap identitas, serangan terhadap aplikasi web, serangan terhadap pemerintah dan Infrastruktur Informasi Kritikal, dan serangan terhadap bisnis.[23]

Sehubungan dengan Teori Hukum Transformatif yang dikembangkan oleh Ahmad M. Ramli, dimana teori tersebut berfokus pada perubahan dan adaptasi hukum dalam menghadapi realitas sosial yang dinamis, dengan menekankan pentingnya hukum untuk berfungsi sebagai alat transformasi sosial yang tidak hanya sekedar instrumen penegakan hukum statis semata.[24] Hal ini sangat relevan keterkaitannya dengan konteks ancaman siber dimana teori ini pada dasarnya menekankan perkembangan teknologi informasi dan komunikasi yang dapat mempengaruhi cara hukum beroperasi dan diterapkan.

Ancaman siber menciptakan tantangan baru bagi sistem hukum. Teori hukum transformatif menekankan bahwa hukum harus dapat beradaptasi untuk menangani isu-isu baru seperti pencurian identitas, penipuan *online*, dan serangan terhadap IIK. Oleh karena itu, Undang-Undang yang mengatur keamanan siber harus dirumuskan dengan mempertimbangkan dinamika dan sifat ancaman siber yang terus berubah. Selain itu, dalam konteks ancaman siber, teori hukum transformatif menekankan pula pada pentingnya partisipasi berbagai pihak dalam proses pembentukan hukum. Dalam hal ini, keterlibatan pemerintah, sektor swasta, akademisi, serta masyarakat menjadi sangat penting untuk menghasilkan kebijakan dan regulasi yang lebih komprehensif dan

[23] BPPTIK, "Jenis-Jenis Serangan Siber di Era Digital", 2023. https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital, diakses pada 10 Oktober 2024.
[24] Ahmad M. Ramli dan Tasya Safiranita Ramli, *Hukum sebagai Infrastruktur Transformasi Indonesia*: *Regulasi dan Kebijakan Digital*, Op.Cit.

responsif dalam menghadapi ancaman siber.

5. Insiden Siber

Kejahatan siber memiliki banyak ragam baik yang berada pada level individu, kelompok kecil, maupun kelompok kejahatan terorganisasi yang menyerang dan melakukan kejahatannya secara sistematis. Berikut beberapa contoh kejahatan siber *(cyber crime)* yang menjadi perhatian dalam keamanan siber;

a. *Unauthorized Access to Computer System and Service,* yakni kejahatan yang dilakukan dengan masuk secara ilegal ke dalam sistem jaringan komputer. Modus operasi ini biasanya dilakukan dengan maksud untuk pencurian informasi penting dan rahasia;
b. *Illegal Contents,* yakni memasukan data atau informasi ke internet tentang suatu hal yang tidak benar dan dianggap melanggar hukum atau mengganggu ketertiban publik yang ditujukan kepada individu, kelompok maupun negara;
c. *Data Forgery,* yakni memalsukan data pada dokumen penting yang tersimpan di internet. Kejahatan ini ditujukan pada dokumen yang dimiliki lembaga yang layanannya berbasis web data;
d. *Cyber Sabotage And Extortion,* yakni kejahatan dengan tujuan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer hingga sistem jaringan komputer yang terhubung dengan internet;
e. *Cyber Espionage,* yakni mata-mata terhadap pihak lain melalui fasilitas jaringan internet sebagai media kejahatan. Pada umumnya hal ini dilakukan untuk mendapat dokumen atau data penting pihak tertentu yang tersimpan dalam suatu sistem yang terhubung dengan komputer;
f. *Offense against Intellectual Property,* yakni kejahatan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet;

g. *Carding,* yakni aksi mencuri nomor kartu-kartu penting milik orang lain dan dipergunakan untuk transaksi perdagangan di internet; dan
h. *Cracking,* Kejahatan di internet yang memiliki ruang lingkup lebih luas, mulai dari aksi balas dendam terhadap instansi tertentu hingga pembajakan hak atas kekayaan intelektual dan penghilangan data melalui jaringan internet.[25]

Beberapa insiden kejahatan siber di Indonesia menunjukkan pola yang berulang serta tantangan signifikan yang dihadapi oleh penegak hukum dalam menanganinya. Berikut adalah pola-polanya :[26]

Kasus A : Serangan Enkripsi Canggih

Teknologi yang Digunakan	:	Enkripsi canggih
Tantangan	:	Kesulitan melacak pelaku
Solusi yang Diterapkan	:	Pengembangan alat forensik baru untuk mengatasi teknik enkripsi

Kasus B : Penipuan *Phishing*

Teknologi yang Digunakan	:	Metode *phishing*
Tantangan	:	Kurangnya edukasi publik mengenai risiko *phishing*

[25] Rosy, Afifah Fidina. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber : Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security." *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan* 1.2 (2020): 123-124

[26] Sitanggang, Andri Sahata, Fernanda Darmawan, and Dony Saputra. "Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber." *Jurnal Pendidikan dan Teknologi Indonesia* 4.3 (2024): 81

Solusi yang Diterapkan	:	Kampanye kesadaran siber untuk meningkatkan pemahaman publik tentang bahaya *phishing*

Kasus C : Serangan *Ransomware*

Teknologi yang Digunakan	:	*Ransomware*
Tantangan	:	Koordinasi antar lembaga yang lemah
Solusi yang Diterapkan	:	Pembentukan tim tanggap darurat siber yang terkoordinasi dengan baik

Untuk mengatasi tantangan tersebut, penelitian ini mengusulkan beberapa solusi, antara lain peningkatan kapasitas teknologi melalui investasi dalam alat dan sistem yang lebih canggih, pengembangan program pelatihan serta peningkatan kapasitas sumber daya manusia berkelanjutan bagi penegak hukum dan Penyelenggara Infrastruktur Informasi dan Penyelenggara IIK untuk meningkatkan keterampilan teknis, serta membangun sistem koordinasi yang lebih baik antara berbagai lembaga penegak hukum dan institusi terkait untuk memastikan respon yang lebih cepat dan efisien terhadap insiden kejahatan siber. Selain itu, penguatan kerja sama internasional melalui perjanjian bilateral dan multilateral dapat membantu dalam menangani kejahatan siber yang bersifat lintas negara.[27]

6. Krisis Siber

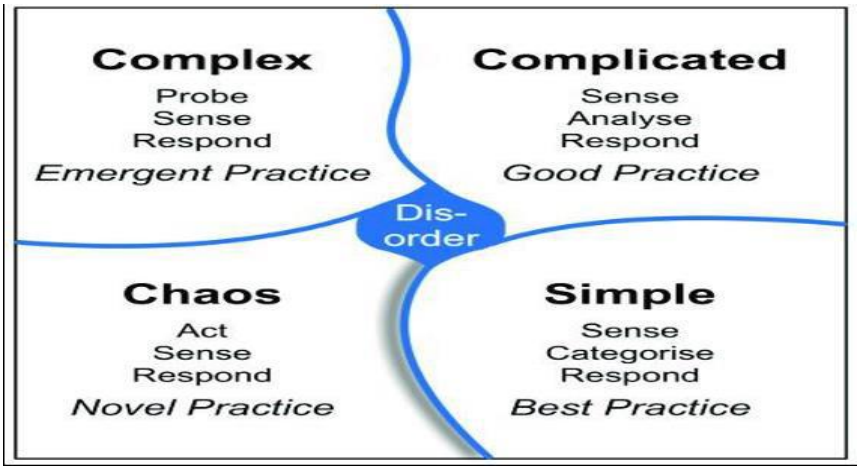
Mengacu dari dampak dan potensi kerusakan yang dapat diakibatkan oleh gangguan dan serangan siber di Indonesia, penanganan krisis siber tentunya berbeda dengan penanganan krisis biasa. Perlu diingat bahwa ruang siber berurusan dengan

[27] *Ibid,* hlm.82

sistem yang kompleks dan adaptif serta dapat berubah dari waktu ke waktu. Maka dari itu, perlu memperhatikan beberapa teori dan konsep di bawah, sebagai berikut:

a. Teori *Cynefin Framework*

Dalam menangani krisis siber, diperlukan sikap dalam menanggapi serangan dan pengetahuan akan lingkungan yang lebih spesifik. Untuk itu, teori *Cynefin Framework* adalah teori yang tepat untuk menjelaskan apa yang harus diwaspadai pimpinan atau *leading sector* dalam memitigasi dan mengendalikan sebuah masalah atau krisis. Teori ini menjelaskan bahwa ada lima kategori masalah yang biasa dihadapi sebuah organisasi. Kelima kategori tersebut adalah *simple, complicated, complex, chaos*, dan *disorder.* Berikut gambar kerangka teori *Cynefin Framework*:



Gambar 1. Teori *Cynefin Framework*

(Sumber: Erik Puik dan Darek Ceglarek, The Quality of a design will not exceed the knowledge of its designer; an analysis based on Axiomatic Information and the *Cynefin Framework.*, 2015)

Berdasarkan gambar di atas, kategori pertama adalah *simple*, dimana situasi dan hubungan sebab akibat sangat jelas atau mudahnya adalah situasi yang sangat sederhana. Biasanya ada satu buah solusi dan pengambilan keputusan bisa dilakukan sangat cepat. Kategori kedua adalah *complicated*, dimana terdapat lebih dari satu solusi akan tetapi masih memiliki sebab akibat yang jelas. Biasanya memerlukan

masukan seorang pakar untuk menyelesaikan masalahnya. Contohnya dapat berupa masalah kalkulasi atau *coding* dalam pengembangan *software*, dimana diperlukannya seorang ahli untuk menyelesaikan masalah. Kategori ketiga adalah *complex*, dimana tidak adanya satu solusi atau jawaban pasti dalam sebuah masalah dan biasanya terjadi secara tiba-tiba. Biasanya terjadi di sebuah sistem yang rumit dan banyak faktor eksternal seperti pasar modal atau sebuah ekosistem. Kategori keempat adalah *chaotic* yakni kondisi yang tidak stabil, dimana sebab dan akibat tidak diketahui dan tidak bisa diselesaikan dengan respon yang murni teoritis. Karena sifatnya yang mendesak, biasanya fokus pada mencari titik stabil untuk mengendalikan situasi. Contohnya adalah serangan teroris 9/11 yang terjadi di New York Amerika Serikat. Reaksi pertama yang harus dikedepankan dalam kondisi ini biasanya fokus pada menyumbat masalah agar tidak merambat ke masalah lain. Kondisi kelima adalah disorder dimana suatu kondisi yang tidak dapat dikategorikan ke empat kondisi yang tersebut.

Melihat dari situasi kondisi ruang siber Indonesia dan berdasarkan penjelasan teori *Cynefin Framework* menunjukkan bahwa kategori ruang siber Indonesia dalam keadaan krisis berada di antara *complex* dan *chaotic*. Dalam kondisi krisis, ruang siber Indonesia akan berpotensi untuk meluas secara nasional, menghadapi situasi yang sangat tidak stabil, terjadi sangat mendadak, dan tidak mungkin diselesaikan dengan satu solusi. Oleh karena itu, melihat dari karakter ruang siber Indonesia berdasarkan teori ini menunjukkan bahwa seluruh pemangku kepentingan harus memiliki kesadaran penuh akan lingkungannya.

Pada dasarnya, ada dua tipe ancaman di dalam ruang siber yang sangat adaptif, yaitu *known risk* atau risiko yang diketahui dan *unknown risk* atau risiko yang tidak diketahui.

Pada praktiknya, ancaman yang terjadi di ruang siber lebih banyak *unknown risk* karena faktanya adalah sekuat apapun sistem ketahanan siber akan selalu berpotensi untuk dieksploitasi. Banyak individu, bisnis, atau bahkan organisasi pemerintahan yang sudah menerapkan sistem pertahanan siber namun masih tetap mampu ditembus. Contohnya terjadi di United Kingdom (UK) yang juga diketahui sebagai salah satu negara dengan kapabilitas siber yang kuat. Pada tahun 2017, serangan *WannaCry* berhasil menembus pertahanan siber mereka dan mengakibatkan terganggunya sistem pelayanan kesehatan mereka. Dengan kata lain, serangan siber dalam di dunia sekarang ini sangat mungkin sekali terjadi walaupun sudah diterapkan sistem pertahanan siber.

Sikap dan reaksi dari pimpinan atau *leading sectors* juga sangat menentukan dalam kondisi krisis. Seperti yang sudah dijelaskan di atas, bahwa dalam kondisi *complex* atau *chaos* pendekatan masalah harus berfokus untuk membatasi atau mengisolasi masalah sehingga permasalahan tidak menyebar ke tempat lain. Disaat yang bersamaan, pimpinan atau leading sectors juga diperlukan untuk lebih adaptif dan fleksibel dalam menangani krisis siber.

b. Tingkatan Krisis Siber

Pengelolaan atau manajemen krisis siber membutuhkan pendekatan multidimensional dan multi-perspektif yang menganalisis dan memberikan pengelompokan berbagai prinsip dan panduan praktik untuk mendorong ketahanan siber dengan mengaplikasikan kapabilitas pengelolaan krisis yang efektif. Dalam memutuskan kondisi serangan krisis siber ini terdapat dua indikator yang perlu dipertimbangkan yakni indikator di ruang siber dan di ruang fisik.

Berdasarkan indikator tersebut, sebelumnya perlu diketahui bahwa terdapat 4 (empat) tingkatan krisis negara

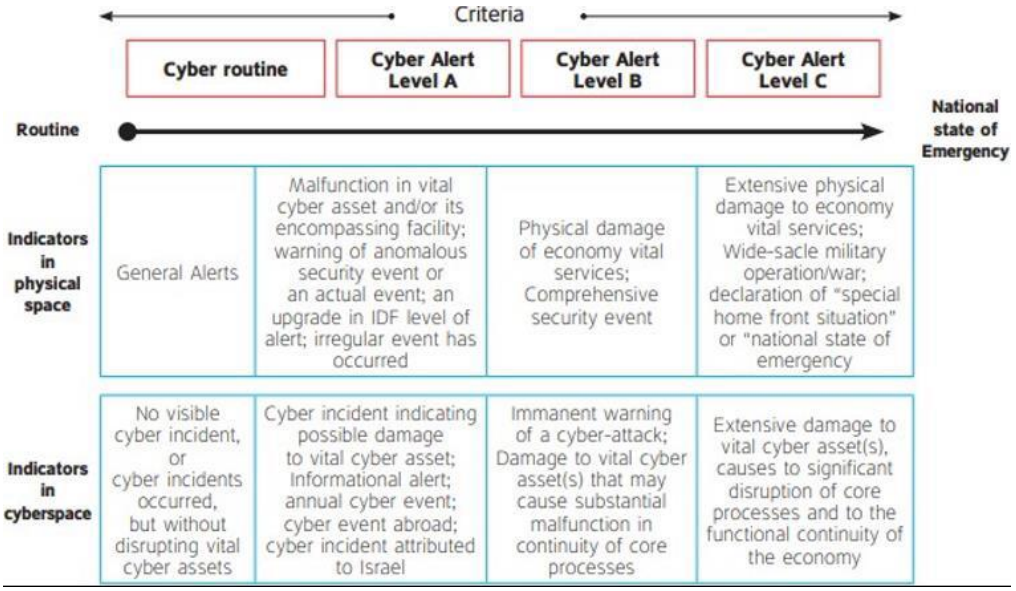
yang dibagi menjadi rutinitas biasa (pertahanan) dan 3 (tiga) tingkat eskalasi kerusakan berdasarkan tingkat yang semakin tinggi, yakni Siaga Tingkat A,B, dan C. Keempat tingkatan ini memiliki lambang warna masing-masing, di mana rutinitas pertahanan biasa siber biasa dilambangkan berwarna hijau, eskalasi Siaga Tingkat A berwarna kuning, lalu Siaga Tingkat B berwarna Merah, dan Siaga Tingkat C berwarna Hitam. Dalam masing-masing tingkatan yang dilambangkan dengan warna ini memiliki alur atau siklus masing-masing yang dipengaruhi lama waktu serangan dan tingkat tekanan yang diberikan, sehingga mampu menggambarkan pola intensitas serangan krisis siber yang terjadi. Pola intensitas krisis siber tersebut dapat dilihat melalui gambar di bawah:

Gambar 2. Pola intensitas krisis siber

Berdasarkan gambar di atas, setiap krisis siber memiliki siklusnya masing-masing, di mana terdapat fase insiden yang semakin meningkat eskalasinya dan berpotensi menjadi krisis yang muncul setelahnya. Fase-fase ini dapat ditentukan dengan sebelumnya mendapatkan informasi terkait sistem kontrol, indikasi yang dideteksi pada data, laporan insiden siber, dan lain-lain. Dalam setiap fase ini selanjutnya memerlukan penanganan lanjutan dari berbagai badan termasuk BSSN dan Tim Tanggap Siber. Secara garis besar, beberapa tingkatan proses yang menggambarkan pola intensitas krisis siber, sebagai berikut:

1) Ketahanan (*Robustness*) yakni masa tidak adanya serangan berarti di ruang siber, di mana pada masa ini informasi di ruang siber secara berkelanjutan dikumpulkan dan bertukar satu sama lain.
2) Deteksi (*Detection*) yakni tahap terdapat penemuan aktivitas tidak biasa pada aset siber vital organisasi dan proses inti karena adanya ancaman atau gangguan aktual, sehingga pada tahap ini diperlukan tanggapan atau respons secepat mungkin.
3) Analisis (*Analysis*) yakni tahap klarifikasi yang komprehensif dan mendalam mengenai sifat kejadian dan memverifikasi bahwa tidak ada pelanggaran atau serangan lebih lanjut, dan menganalisis pengaruhnya terhadap fungsionalitas organisasi, di luar aspek teknologi.
4) Penahanan (*Containment*) yakni tahap memblokir serangan untuk mendapatkan kendali awal dan penyebarannya ke aset siber lainnya, dan menahan kerusakan yang disebabkan dari serangan siber tersebut (baik dampak pada kelangsungan bisnis, reputasi, kerusakan ekonomi). Tahap penahanan ini harus sesuai dengan rencana manajemen krisis organisasi.
5) Eradikasi (*Eradication*) yakni upaya menetralkan komponen serangan sambil berusaha membalikkan atau meminimalkan kerusakan yang telah disebabkan agar tidak kembali terjadi.
6) Pemulihan (*Restoration*) yakni pengembalian kembali kendali ke operasi normal, menyatakan akhir dari krisis siber agar kembali ke rutinitas siber biasa, melakukan penyelidikan dan menggambarkan pelajaran yang didapat, dan menentukan langkah-langkah untuk implementasi kedepannya.

Saat menentukan pola intensitas krisis siber ini baru dilakukan pertimbangan dua indikator untuk menentukan tingkat siaga siber negara. Tingkat siaga siber negara ini membantu dalam menentukan tahapan serangan siber dari biasa hingga krisis negara sehingga bisa menunjukkan langkah maupun tindakan yang perlu dilakukan serta sumber daya yang perlu digunakan dalam mengatasinya. Berikut adalah tingkatan siaga siber negara



Gambar 3. Tingkat Siaga Siber Negara

Berdasarkan gambar di atas, beberapa butir yang bisa digunakan sebagai pertimbangkan yakni:

1) Tingkatan pertama atau rutinitas siber (*cyber routine*) yang menjadi bagian rutinitas pertahanan, yakni situasi atau keadaan biasa, di mana baik dari indikator di ruang siber dan ruang fisik tidak menunjukkan indikasi gangguan fungsi operasional dari aset Infrastruktur Informasi Vital (IIV) yang membutuhkan peningkatan pertahanan besar. Dalam situasi ini, syarat tingkatan siaga tinggi belum terpenuhi.
2) Tingkatan kedua yakni Siaga Tingkat A yakni tergantung situasi yang ada, di mana salah satu indikator mencapai

tingkatan tertentu. Indikator di ruang siber yakni adanya insiden siber yang mengindikasikan adanya kemungkinan gangguan pada fungsi normal aset IIV, adanya penerimaan peringatan aset informasi, atau adanya serangan siber tahunan lokal yang berpotensi meningkatkan ancaman, atau adanya serangan siber yang terjadi di luar negeri. Selanjutnya dari indikator ruang siber yakni adanya mal fungsi (kegagalan pemakaian) pada aset informasi IIV pada situs terkait, adanya peringatan yang jangkauannya cukup luas, adanya peningkatan aktivitas tidak biasa yang bisa menyebabkan kerusakan atau ancaman.

3) Tingkatan ketiga yakni Siaga Tingkat B juga bergantung pada situasi yang akan memenuhi siaga tingkat B jika dalam indikator di ruang siber terdapat peringatan tetap pada serangan siber, kerusakan maupun ancaman pada aset informasi IIV, sehingga memunculkan gangguan nyata pada keberlanjutan proses pertukaran informasi. Dari sisi indikator ruang fisik, terdapat kerusakan fisik pada pelayanan inti perekonomian (seperti listrik, pelayanan kesehatan), atau bahkan operasi militer terbatas.

4) Tingkatan keempat yakni Siaga Tingkat C yang menjadi tingkatan tertinggi kesiagaan negara. Tahap ini terjadi jika terdapat deklarasi atau pernyataan bahwa negara dalam kondisi darurat. Pada indikator di ruang siber, terdapat serangan terus menerus pada aset informasi IIV, yang mendorong adanya gangguan penting pada proses dan keberlangsungan fungsional perekonomian. Lalu pada indikator ruang fisik, terdapat kerusakan fisik yang luas sehingga mengganggu pelayanan terhadap unsur vital perekonomian, operasi perang atau militer jangka luas, adanya deklarasi atau pernyataan “situasi darurat

sipil."

Setelah memutuskan tingkat siaga siber negara ini, menyatakan keadaan darurat atau krisis di ruang siber, yakni tingkat nasional, tingkat sektoral, dan tingkat organisasional. Tingkatan-tingkatan ini menunjukkan skala serangan siber pada masing-masing tingkatan yang diperbandingkan juga dengan keadaan di Indonesia. Mengingat pentingnya pertukaran informasi, dan kecepatan insiden siber terjadi, maka penting bagi tiap tingkatan organisasi mengubah atau memperbaharui kewaspadaan di ruang siber, termasuk terkait pengembangan hukum dan kerja sama sub organisasi yang lain. Berikut merupakan deskripsi tingkatan pernyataan skala keadaan darurat, yakni:

1) Tingkat Nasional, yakni adanya pernyataan dari aktor yang bertanggung jawab di ruang siber untuk menyatakan tingkat siaga siber. Tingkatan ini bisa dinyatakan jika terdapat ancaman atau kondisi yang kemungkinan besar meningkat mencapai tingkat krisis nasional. Selanjutnya suatu sektor dapat menentukan tingkat siaga siber lebih tinggi, namun tidak lebih rendah dari yang ditetapkan sebagai tingkat nasional.

   Dikaitkan dengan rencana penerapan di Indonesia melalui pengaturan tentang manajemen krisis siber nasional, krisis siber di Indonesia ditetapkan jika terdapat eskalasi berdampak luas pada sektor-sektor pemerintahan sehingga mengakibatkan situasi darurat pada keselamatan, keutuhan, dan kedaulatan negara. Aktor yang menyatakan adanya krisis siber nasional adalah Presiden dengan sebelumnya sudah mendapat pertimbangan dari Tim Tanggap Insiden Siber Nasional dan BSSN, yang juga bisa mendapat dukungan badan-badan lain yang dibutuhkan sesuai dengan pengaturan atau ketetapan yang ada. Setelah itu, Presiden akan

membentuk gugus tugas krisis siber nasional dalam menangani permasalahan darurat ini. Bersama dengan instansi terkait, publik dan swasta, gugus tugas akan melakukan tugas seperti mengurangi dampak kerusakan dan risiko, mengumpulkan dan mengamankan bukti penyebab krisis siber nasional, dan lain-lain

2) Tingkat Sektoral, yakni sektor terkait kementerian atau pihak berwenang menyatakan tingkat siaga siber dengan tetap berkoordinasi dengan Direktur Jenderal INCD atau sudah mendapat rekomendasi sebelumnya. Pernyataan ini mengikat semua yang ada dalam organisasi dan tetap berada di bawah tanggung jawab sektoral atau menunjuk organisasi spesifik tertentu. Namun juga terdapat pernyataan tingkat siaga siber di beberapa sektor yang bisa tidak mengikat sektor lainnya, namun kondisi di ruang siber yang ada tetap harus diberitahukan dan ditangani.

   Dikaitkan dengan rencana penerapan di Indonesia melalui pengaturan tentang manajemen krisis siber nasional, maka tahap ini dikategorikan sebagai insiden di level sektoral, dimana insiden siber sudah mengganggu sebagian besar entitas dalam lingkup sektoral seperti administrasi pemerintahan, energi dan sumber daya mineral, transportasi, keuangan, kesehatan, TIK, pangan, pertahanan. Pada tahap ini, Tim Tanggap Sektoral menangani insiden dengan melakukan berbagai langkah seperti mengurangi dampak kerusakan dan risiko, mencegah perluasan dan perulangan kejadian, dan lain-lain. Selanjutnya jika tim tanggap insiden sektoral tidak dapat menangani, maka perlu ada pernyataan peningkatan eskalasi menjadi potensi krisis kepada tim tanggap insiden siber nasional yang tetap perlu berkoordinasi dengan BSSN.

Penanganan insiden siber yang yang terjadi pada entitas di lingkup sektoral terjadi saat ada peristiwa maupun rangkaian peristiwa yang mengancam dan mengganggu aset dan operasional Siber pada salah satu layanan Infrastruktur Informasi Vital, dan menyebabkan terganggunya sistem elektronik publik dan privat sehingga berdampak pada aktivitas ekonomi masyarakat. Dalam tahap ini, tim tanggap insiden siber sektor hanya menyelenggarakan sistem pemantauan situasi, peringatan dini, pelayanan penerimaan laporan dan informasi. Setelah itu, akan dilakukan pelaporan pada instansi atau institusi terkait yang memiliki data elektronik strategis terdampak, lalu selanjutnya penanganan ini menjadi tanggung jawab institusi atau instansi terdampak tersebut. Pada tahap ini BSSN membantu institusi dan instansi terdampak dalam upaya penanggulangan dan pemulihan. Di masa penanganan insiden siber sektor terjadi eskalasi yang berdampak luas pada sektor lain, maka tim tanggap insiden siber sektor berkoordinasi dengan instansi atau institusi terdampak melapor situasi tersebut pada tim tanggap insiden nasional, dimana tim tanggap insiden ini melalui kepala BSSN melaporkan potensi krisis siber nasional kepada Presiden Republik Indonesia.

3) Tingkat Organisasional, yakni pemimpin atau direktur dalam organisasi tersebut yang akan menyatakan tingkat siaga siber dengan tetap berkoordinasi dengan unit siber sektoral atau lembaga berwenang, atau mendapat rekomendasi atau pedoman dari lembaga berwenang. Selanjutnya, pemimpin atau wakil pimpinan organisasi ini bisa mendefinisikan tingkat peringatan siber lebih tinggi yang ditetapkan pada sektor organisasinya berada.

Dikaitkan dengan rencana penerapan di Indonesia melalui pengaturan tentang manajemen krisis siber nasional, insiden siber tingkat organisasional ini termasuk pada insiden siber biasa di lingkup internal organisasi karena merujuk pada serangan siber di internal instansi atau kementerian tertentu saja dan sifatnya sementara. Insiden tahap ini mengganggu pelayanan atau kinerja dari suatu instansi atau organisasi. Maka dari itu, pada tahap ini, tim tanggap siber organisasi bisa melakukan tanggapan insiden untuk menanggulangi insiden siber biasa dengan melakukan berbagai langkah seperti mengurangi dampak kerusakan dan risiko, mencegah perluasan dan pengulangan kejadian insiden siber, dan lain- lain. Jika mencapai tahap tidak dapat ditangani oleh tim tanggap insiden organisasi dan sudah cukup meluas, maka perlu ada peningkatan status menjadi insiden siber tingkat sektoral, dan tetap perlu berkoordinasi dengan BSSN.

c. Alur Manajemen Krisis Siber

Setelah itu, langkah lanjutan dalam manajemen yakni perlu membentuk dan mendefinisikan dokumen kebijakan manajemen krisis dalam hal ini pengaturan tentang Manajemen Krisis Siber yang akan menjadi dasar pedoman dalam pengembangan perencanaan dan implementasi prosedur manajemen krisis siber. Dokumen kebijakan manajemen krisis siber ini akan mengatur mengenai pencegahan, mitigasi, respon insiden, dan evaluasi pembelajaran dari krisis siber. Manajemen krisis siber ini bukan hanya terkait respons insiden siber namun juga proses mengingat peningkatan serangan dan ancaman siber yang berpotensi menyebabkan krisis siber nasional.

Berdasarkan ISO/IEC 27035:2016, terdapat 5 (lima) tahapan dalam manajemen insiden siber yang rentan. Tahapan manajemen insiden siber ini merupakan sebuah siklus berkelanjutan dan perlu dikembangkan secara berkala, yakni:

1) Perencanaan dan persiapan (*plan and prepare*) yakni perencanaan dan persiapan untuk melakukan Pelindungan dalam menghadapi dan mengatasi insiden siber yang berpotensi menjadi krisis siber baik dalam skala organisasi, sektoral, maupun nasional. Persiapan ini dilakukan dengan membentuk kerangka hukum atau kebijakan terkait manajemen insiden keamanan siber maupun krisis siber, membentuk Tim Siap Tanggap seperti: CSIRT (*Computer Security Incident Response Team*), membentuk perencanaan manajemen risiko dan krisis siber, dan lain-lain. Tahap awal ini penting sebagai pencegahan maupun membangun ketahanan ruang siber nasional agar dapat meminimalisir kerusakan tambahan atau meluas.
2) Deteksi dan pelaporan (*detection and reporting*) yakni tahap pemeriksaan dan mengidentifikasi laporan insiden keamanan di ruang siber. Pada tahap ini pihak-pihak tertentu yang mendeteksi dan mengidentifikasi serangan siber harus melaporkan kejadian siber yang bisa meningkat menjadi insiden siber bahkan menjadi krisis siber
3) Penilaian dan keputusan (*assessment and decision*) yakni tahap untuk menilai dan memutuskan insiden terkait bagaimana insiden akan ditangani terutama jika memiliki potensi meluas dan meningkat skalanya. Tahapan ini dilakukan dengan individu maupun organisasi menilai situasi insiden siber yang ada dan memastikan kebenaran peristiwa insiden.

4) Tanggapan (*response*) yakni tahapan menanggapi insiden baik dengan menginvestigasi, menahan, dan menyelesaikan insiden siber tersebut. Dalam tahap tanggapan ini perlu mendefinisikan bantuan teknis dan lainnya yang dibutuhkan bahkan jika pihak ketiga dibutuhkan atau membutuhkan pemberitahuan lanjutan
5) Pembelajaran (*learn*) yakni mengambil pelajaran dari insiden yang ada dengan bukan hanya mengidentifikasi namun juga langkah-langkah yang perlu diambil maupun dipertimbangkan dalam menghadapi serangan siber atau bahkan krisis siber ke depannya

7. Relevansi dengan Keamanan dan Ketahanan Siber

Kajian teoritis yang telah disampaikan di atas mengenai keamanan dan ketahanan siber memiliki relevansi yang sangat signifikan dalam menghadapi tantangan dunia digital saat ini. Keamanan siber *(Cybersecurity)* dan ketahanan siber *(cyber resilience)* adalah dua pilar utama yang saling berkaitan dan menjadi landasan dalam melindungi seluruh aspek interaksi manusia dengan dunia siber. Keduanya sangat penting untuk menjamin pelindungan sistem, data, dan infrastruktur terhadap ancaman yang terus berkembang, baik dari sisi teknis maupun sosial. Perkembangan teknologi informasi yang pesat memang mempermudah akses masyarakat ke berbagai layanan digital, namun juga memunculkan ancaman dan risiko baru yang dapat menimbulkan kerugian besar jika tidak diantisipasi dengan baik.

Keamanan siber mencakup langkah-langkah proaktif untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi dalam dunia digital. Hal ini diperlukan untuk melawan serangan siber yang sering kali bersifat merusak dan meluas, seperti *ransomware*, *phishing*, dan serangan DDoS (*Distributed Denial of Service*). Dalam kaitannya dengan

ketahanan siber, keamanan siber berperan sebagai garis pertahanan pertama untuk mencegah serangan tersebut terjadi. Sebagai contoh, penerapan *firewall*, enkripsi, dan teknologi keamanan lainnya menjadi bagian integral dari upaya Pelindungan ini. Namun, meskipun upaya preventif ini telah diimplementasikan, ancaman siber tetap ada dan terus berkembang, sehingga diperlukan pendekatan yang lebih komprehensif dan berkelanjutan.

Ketahanan siber, di sisi lain, berfokus pada kemampuan suatu sistem atau organisasi untuk bertahan, pulih, dan menyesuaikan diri dengan serangan atau insiden siber yang terjadi. Ketahanan ini menjadi kunci ketika upaya pencegahan tidak cukup, atau serangan siber berhasil menembus lapisan keamanan yang ada. Ketahanan siber memastikan bahwa organisasi tidak hanya mampu mendeteksi dan menanggapi insiden siber secara cepat, tetapi juga mampu memulihkan kondisi operasional mereka dengan segera setelah serangan. Dengan demikian, ketahanan siber bukan hanya soal mencegah serangan, tetapi juga soal bagaimana suatu sistem mampu beradaptasi dan kembali beroperasi normal setelah terkena dampak. Hal ini mencakup aspek pemulihan data, perbaikan sistem, dan evaluasi risiko agar insiden serupa tidak terulang di masa depan.

Dalam hal keamanan dan ketahanan siber, regulasi yang kuat dan adaptif sangat diperlukan untuk menjamin bahwa teknologi yang digunakan oleh masyarakat dan lembaga penting dilindungi dari ancaman siber. Pengaturan ini harus mencakup standar keamanan siber yang jelas bagi penyelenggara sistem elektronik dan pedoman respons yang tepat ketika terjadi insiden. Selain itu, kerangka hukum yang kuat juga membantu membangun kepercayaan masyarakat dalam dunia digital, sehingga transformasi digital dapat berjalan dengan lancar tanpa kekhawatiran berlebih terhadap

potensi ancaman.

Ancaman siber yang semakin kompleks dari tahun ke tahun, seperti yang dijelaskan dalam kajian teoretis, memperlihatkan bahwa para pelaku kejahatan siber terus mengembangkan metode baru untuk meretas, mencuri, atau merusak data dan infrastruktur informasi. Hal ini mencakup serangan yang bersifat teknis, seperti *cracking* dan *ransomware*, hingga serangan manipulatif seperti *phishing* dan *social engineering*. Oleh karena itu, penting bagi setiap elemen masyarakat, seperti individu, pelaku usaha, pemerintah, dan penegak hukum, untuk memahami perkembangan ancaman siber ini dan membekali diri dengan pengetahuan serta teknologi yang memadai. Penelitian mengenai serangan siber yang terjadi di Indonesia menunjukkan bahwa insiden siber tidak hanya mempengaruhi sektor swasta, tetapi juga sektor pemerintahan, di mana *database* sensitif bisa menjadi target.

Kesadaran akan pentingnya ketahanan siber di kalangan lembaga pemerintah dan swasta juga menjadi semakin penting di era transformasi digital yang sedang berlangsung di Indonesia. Konsep ketahanan siber ini sangat erat kaitannya dengan ketahanan organisasi secara keseluruhan, di mana setiap lembaga diharapkan dapat membangun struktur pertahanan yang fleksibel dan mampu beradaptasi terhadap serangan yang tidak terduga. Kesiapan teknologi, kapasitas SDM, dan kerja sama internasional menjadi faktor kunci dalam mewujudkan ketahanan siber yang tangguh dan berkelanjutan. Sektor yang paling rentan terhadap ancaman siber, seperti keuangan, transportasi, energi, dan layanan kesehatan, perlu memprioritaskan langkah-langkah keamanan yang dapat menjamin kelangsungan operasional mereka dalam menghadapi serangan siber yang merusak.

Keamanan dan ketahanan siber adalah dua aspek yang tidak bisa dipisahkan dalam konteks pelindungan di dunia

digital. Keduanya saling melengkapi dan krusial dalam memastikan bahwa masyarakat dapat terus mengakses layanan digital tanpa takut terhadap risiko yang mengintai. Selain itu, peran hukum yang adaptif dan dinamis sangat dibutuhkan dalam membangun kerangka kebijakan yang memungkinkan negara untuk merespons ancaman siber dengan cepat dan efektif. Hal ini tidak hanya akan melindungi keamanan informasi nasional, tetapi juga memperkuat fondasi transformasi digital di Indonesia, menuju masa depan yang lebih aman dan terkendali di dunia siber.

B. Kajian terhadap Asas/Prinsip yang Berkaitan dengan Penyusunan Norma

1. Asas keamanan dan ketahanan siber yaitu:

a. Kedaulatan Negara

Asas kedaulatan negara adalah asas hukum yang menyatakan bahwa suatu negara memiliki kekuasaan tertinggi untuk mengatur dirinya sendiri, tanpa campur tangan dari negara lain. Asas ini merupakan salah satu asas hukum tata negara yang penting, karena menjadi dasar bagi negara untuk menjalankan fungsi dan perannya.[28] Secara keseluruhan, asas kedaulatan negara mengimplikasikan bahwa negara harus memiliki kebebasan dan wewenang untuk menetapkan kebijakan yang memastikan ketahanan fisik dan non-fisiknya, termasuk dalam ruang siber. Negara yang tidak memiliki kendali pengamanan atas ruang siber atau IIK digitalnya berisiko kehilangan kedaulatan terhadap ancaman yang datang dari dunia maya, yang kini menjadi salah satu bidang ancaman terbesar di era digital ini.

[28] Dwiono, Sugeng, et al. "Hukum Tata Negara: Deskripsi dan Tinjauan Kritikal." *CV. Edupedia Publisher,* 2024, hlm. 42

b. Pelindungan dan Kepastian Hukum

Asas pelindungan hukum adalah nilai dasar dari aturan hukum yang sifatnya memberikan pelindungan bagi objek hukum.[29] Asas pelindungan hukum merupakan nilai dasar yang menjadi pondasi dalam penyusunan aturan hukum. Asas ini berfungsi untuk memberikan jaminan pelindungan terhadap objek hukum, baik individu, kelompok, maupun negara, dari ancaman, kerugian, atau penyalahgunaan yang mungkin timbul. Dalam konteks Undang-Undang Keamanan dan Ketahanan Siber, asas pelindungan hukum sangat penting untuk memastikan bahwa seluruh sistem dan infrastruktur siber, yang meliputi data, informasi, dan layanan digital, terlindungi secara efektif.

Keamanan dan ketahanan siber menekankan perencanaan strategis yang proaktif dengan mengintegrasikan keamanan siber ke semua level organisasi, menjadikannya lebih dari sekedar tanggung jawab IT. Pendekatan holistik ini meminimalkan dampak serangan siber terhadap operasional bisnis dan mempertahankan reputasi organisasi. Dengan berfokus pada kesiapan, kemampuan beradaptasi, dan pemulihan yang cepat, organisasi dapat terus beroperasi secara efektif dan aman, bahkan di tengah gangguan dan utamanya memberikan pelindungan. Hal ini menyebabkan pentingnya asas pelindungan dalam Undang-Undang Keamanan dan Ketahanan Siber.

Asas ini juga menuntut agar negara, penyelenggara sistem siber, dan masyarakat berperan aktif dalam menjaga ketahanan siber melalui kebijakan dan tindakan yang memastikan keamanan informasi dan teknologi. Selain itu, asas pelindungan hukum juga berfungsi untuk mengatur hak

[29] Suriaatmadja, Steffi Rifasa Tohir, and Ira Dewi Rachmadiani. "Pelindungan Hukum Terhadap Dokter Umum dalam Melakukan Pelayanan Kesehatan di Masa Pandemi Covid 19 Ditinjau dari UU Wabah Tahun 1984." *Innovative: Journal Of Social Science Research* 4.3 (2024): hlm. 2

dan kewajiban antara penyelenggara sistem siber dengan pengguna, serta memberikan pelindungan hukum terhadap pihak yang dirugikan akibat pelanggaran terhadap ketentuan keamanan siber. Dalam hal terjadi insiden atau pelanggaran, asas Pelindungan hukum mengharuskan adanya mekanisme pemulihan yang cepat dan adil, agar para pihak yang terdampak dapat memperoleh ganti rugi atau pelindungan yang layak sesuai dengan hukum.

Secara keseluruhan, asas pelindungan hukum dalam Undang-Undang Keamanan dan Ketahanan Siber bertujuan untuk menciptakan keseimbangan antara kemajuan teknologi dan Pelindungan hak-hak individu dan masyarakat. Dengan prinsip pelindungan yang kuat, diharapkan Indonesia dapat membangun ekosistem siber yang aman, stabil, dan dapat diandalkan, baik di tingkat nasional maupun internasional. Selain asas pelindungan, dalam Undang-Undang Keamanan dan Ketahanan Siber juga mengandung asas kepastian hukum. Asas kepastian hukum mengandung nilai-nilai yang sangat penting dalam konteks hukum dan keadilan. Asas ini merujuk pada keyakinan bahwa hukum haruslah jelas, dapat dipahami, dan dapat diakses oleh semua warga negara.

Dalam konteks ini, latar belakang pembahasan mengenai nilai-nilai yang tercakup dalam asas kepastian hukum sangat relevan dan perlu untuk dipahami lebih dalam. Salah satu nilai yang tercakup dalam asas kepastian hukum adalah prediktabilitas. Prediktabilitas dalam hukum berarti bahwa individu dapat dengan pasti mengetahui konsekuensi hukum dari tindakan atau perilaku yang mereka lakukan. Dengan adanya prediktabilitas, individu dapat mengambil keputusan yang bijak dan memahami risiko yang mungkin timbul dari tindakan mereka. Hal ini penting untuk menciptakan lingkungan hukum yang stabil dan meminimalkan ketidakpastian.

Selain itu, asas kepastian hukum juga mencakup nilai keadilan. Hukum haruslah diterapkan secara adil dan setiap individu harus tunduk pada hukum tanpa pandang bulu. Keadilan menjadi prinsip yang mendasari pelaksanaan hukum, sehingga setiap warga negara memiliki hak yang sama untuk mendapatkan Pelindungan hukum dan perlakuan yang adil di bawah hukum.[30] Asas kepastian hukum menjadi sangat penting dalam keamanan dan ketahanan siber karena menyediakan kerangka kerja yang jelas dan dapat diprediksi, membantu organisasi, individu, dan pemerintah menghadapi serta mengatasi ancaman keamanan secara efektif.

Dengan kehadiran asas kepastian hukum dalam Undang-Undang Keamanan dan Ketahanan Siber akan memberikan batasan yang lebih jelas terkait batasan perilaku dan perbuatan dalam ruang siber. Selain itu, asas kepastian hukum juga memberikan konsistensi dalam penegakan hukum terhadap pelanggaran maupun kejahatan yang terjadi dalam ruang siber, dikarenakan memiliki parameter yang jelas dan konsisten. Hal lain yang juga dapat diterima manfaatnya dari kehadiran asas kepastian hukum adalah penanggulangan terhadap insiden yang lebih lebih jelas dengan adanya respon dan prosedur dari mulai pelaporan insiden, waktu tanggapan, dan koordinasi antar pemangku kepentingan, yang dapat menjadikan koordinasi dalam pencegahan dan penanggulangan insiden siber menjadi dengan pasti dapat diatasi.

Kerja sama antar *stakeholder* dan pihak-pihak yang memiliki tugas untuk tanggap terhadap insiden siber dapat dengan segera melaksanakan kewajibannya. Asas kepastian hukum dalam Undang-Undang Keamanan dan Ketahanan Siber bertujuan untuk memberikan jaminan bahwa peraturan

[30] Neltje, Jeane, and Indrawieny Panjiyoga. "Nilai-Nilai Yang Tercakup Di Dalam Asas Kepastian Hukum." *Innovative: Journal of Social Science Research* 3.5 (2023): hlm.2

yang mengatur segala aspek terkait keamanan siber, termasuk pelindungan data pribadi, pencegahan dan penanggulangan ancaman siber, serta pemulihan pasca-insiden, dapat dilaksanakan dengan jelas dan tanpa keraguan. Kepastian hukum ini penting untuk memastikan bahwa pihak-pihak yang terlibat dalam sistem siber baik individu, organisasi, maupun negara dapat mengetahui dengan pasti aturan yang berlaku, sehingga dapat mengambil tindakan yang sesuai untuk melindungi infrastruktur dan data mereka.

c. Yurisdiksi Ekstrateritorial

Asas hukum yurisdiksi ekstrateritorial merujuk pada prinsip dalam hukum internasional yang memungkinkan suatu negara untuk menerapkan dan menegakkan hukum nasionalnya terhadap tindakan, individu, atau entitas yang berada di luar wilayah teritorialnya, selama tindakan tersebut memiliki dampak atau hubungan signifikan dengan negara tersebut. Prinsip ini didasarkan pada beberapa dasar hukum, seperti prinsip efek (*effects doctrine*), di mana negara dapat menuntut pelaku jika tindakan mereka menyebabkan kerugian di dalam wilayahnya, prinsip nasionalitas (*active personality principle*) untuk melindungi warga negaranya, atau prinsip Pelindungan (*protective principle*) untuk menjaga kepentingan keamanan nasional.

Dalam konteks keamanan dan ketahanan siber, asas ini menjadi sangat relevan karena sifat ruang siber yang tanpa batas fisik (*borderless*), di mana serangan siber seperti *hacking*, pencurian data, atau penyebaran malware sering kali melintasi batas negara.

Namun, penerapan asas ini harus seimbang dengan prinsip non-intervensi dan kedaulatan negara lain, sering kali memerlukan persetujuan (*consent*) atau kerangka hukum multilateral untuk menghindari konflik yurisdiksi.

Fenomena yurisdiksi ekstrateritorial dicontohkan Amerika Serikat yang menerapkan kekuasaan hukumnya di luar batas wilayahnya. Hal ini semakin kompleks dan penting untuk dipahami. Fenomena digital menunjukan perlunya pendekatan terpadu untuk melihat ekstrateritorialitas sebagai satu kesatuan fenomena dengan berbagai penerapan hukum, bukan sekadar kumpulan masalah terpisah.[31] Dengan cara ini, pembuat kebijakan dan penegak hukum dapat lebih mudah menyelesaikan masalah ekstrateritorialitas sekaligus memahami bagaimana solusi tersebut sejalan dengan prinsip-prinsip hukum yang lebih luas dalam konteks global.[32]

d. Transparansi

Transparansi secara umum berarti publik mengetahui kebijakan pemerintah dan yakin atas niat dan tujuan kebijakan tersebut. Ini bisa dicapai dengan memberi ruang untuk partisipasi pubik dalam pembuatan dan pelaksanaan kebijakan.

Transparansi merupakan prinsip keterbukaan yang memungkinkan publik mengakses informasi tentang proses, keputusan, dan tindakan pemerintah, untuk memastikan akuntabilitas dan kepercayaan. Transparansi mendorong partisipasi publik, mencegah penyalahgunaan wewenang, dan memperkuat kepercayaan masyarakat terhadap negara.

Asas transparansi dalam penyelenggaraan keamanan dan ketahanan siber menjadi landasan esensial untuk memastikan bahwa penyelenggaraan keamanan siber dilakukan secara terbuka, akuntabel, dan inklusif. Hal tersebut diwujudkan dalam mekanisme operasional yang konkret melalui sistem

[31] Anthony J., "What Is Extraterritorial Jurisdiction", Cornell Law Review, Volume 99, Issue 6 September 2014 - Symposium on Extraterritoriality.
[32] *Ibid*

pelaporan, berbagi informasi, audit, dan pengawasan. Transparansi diatur dengan keseimbangan yang tepat antara keterbukaan informasi untuk kepentingan keamanan nasional dengan Pelindungan informasi sensitif, terutama untuk sektor yang terkait dengan intelijen, penegakan hukum, dan pertahanan keamanan negara yang dikecualikan dari beberapa kewajiban berbagi informasi.

Pendekatan yang berbasis transparansi menunjukkan komitmen untuk membangun ekosistem siber yang aman melalui kolaborasi berbagai pemangku kepentingan dengan dasar saling percaya dan pertukaran informasi yang terstruktur, sesuai dengan prinsip tata kelola yang baik (*good governance*).

e. Inovasi Teknologi yang Bertanggung Jawab

Asas inovasi teknologi yang bertanggung jawab menekankan bahwa pengembangan dan penerapan teknologi baru dalam sektor siber harus dilakukan dengan mempertimbangkan dampaknya terhadap keamanan, privasi, dan hak individu. Seiring dengan pesatnya perkembangan teknologi informasi, inovasi harus dijalankan dengan prinsip tanggung jawab untuk mencegah penyalahgunaan atau risiko yang dapat mengancam stabilitas ruang siber dan merugikan masyarakat. Dalam konteks Undang-Undang mengenai Keamanan dan Ketahanan Siber, asas ini mengharuskan semua pihak yang terlibat dalam pengembangan teknologi, baik itu pemerintah, perusahaan teknologi, maupun lembaga riset, untuk berinovasi dengan mengutamakan aspek keamanan dan etika. Inovasi teknologi yang bertanggung jawab juga berarti menciptakan sistem dan aplikasi yang dapat diandalkan, aman dari ancaman siber, serta menghormati hak privasi individu.

f. Pengembangan Ekonomi Digital

Pengembangan ekonomi digital adalah asas yang mendukung pertumbuhan sektor ekonomi yang berbasis pada teknologi informasi dan komunikasi. Dalam era digital yang terus berkembang, ekonomi digital menjadi pilar utama bagi kemajuan ekonomi nasional. Undang-Undang mengenai Keamanan dan Ketahanan Siber harus mengatur tidak hanya aspek keamanan, tetapi juga mendukung kemajuan ekonomi digital dengan memberikan landasan hukum yang aman dan kondusif bagi pelaku ekonomi digital.

Asas ini mencakup pelindungan terhadap ekosistem ekonomi digital, termasuk transaksi elektronik, perdagangan daring, dan pengelolaan data digital, yang menjadi komponen penting dalam perekonomian modern. Dengan memberikan jaminan terhadap keamanan transaksi dan data di dunia maya, asas ini bertujuan untuk menciptakan iklim bisnis yang aman dan menarik bagi para investor dan pelaku usaha, baik di tingkat nasional maupun internasional. Selain itu, pengembangan ekonomi digital yang berbasis pada teknologi yang aman juga akan meningkatkan daya saing Indonesia di kancah global.

g. Penghargaan dan Pelindungan Hak Asasi Manusia

Asas penghargaan dan pelindungan hak asasi manusia menegaskan bahwa dalam pengelolaan keamanan dan ketahanan siber, hak individu harus dihormati dan dilindungi. Hal ini termasuk hak atas privasi, kebebasan berpendapat, dan pelindungan data pribadi. Dalam menghadapi ancaman siber, penting untuk memastikan bahwa langkah keamanan yang diambil tidak mengorbankan hak dasar warga negara. Undang-Undang mengenai Keamanan dan Ketahanan Siber harus memastikan bahwa regulasi yang diterapkan dalam rangka

melindungi sistem siber dan data pribadi tidak melanggar hak asasi manusia. Misalnya, pengumpulan dan pemrosesan data pribadi harus dilakukan dengan prinsip transparansi, keadilan, dan persetujuan yang jelas dari pemilik data.

Dengan asas ini, Indonesia akan tetap menjaga keseimbangan antara keamanan siber dan penghormatan terhadap kebebasan serta hak individu, yang menjadi bagian penting dari prinsip demokrasi dan negara hukum. Asas penghargaan atas hak asasi manusia juga bertujuan untuk menekankan keseimbangan langkah-langkah keamanan dengan pelindungan kebebasan dan hak individu di ranah digital. Asas penghargaan atas hak asasi manusia juga memiliki kaitan dengan pelindungan privasi, guna mencegah kejahatan dengan melindungi hak privasi individu dan mencegah penyalahgunaan informasi pribadi. Selain itu, asas penghargaan atas hak asasi manusia juga memiliki kaitannya dengan kebebasan berpendapat dalam dunia siber, agar regulasi yang ada tidak melanggar kebebasan berbicara setiap orang. Dengan adanya asas penghargaan atas hak asasi manusia dalam Undang-Undang mengenai Keamanan dan Ketahanan Siber maka juga memberikan proses pengadilan yang wajar dalam kasus kejahatan siber.

2. Prinsip keamanan dan ketahanan siber yaitu:

   a. Kedaulatan Siber

      Keamanan siber adalah serangkaian upaya yang terkoordinasi untuk melindungi sistem komputer, baik dari aspek perangkat keras maupun perangkat lunak, dari

berbagai ancaman, gangguan, dan serangan.[33] Keamanan siber juga mencakup Pelindungan informasi serta komponen lain di dalam ruang siber yang menjadi bagian penting dari Infrastruktur Informasi Kritikal suatu negara. Dalam konteks kedaulatan siber, pelindungan ini tidak hanya terbatas pada aspek teknis, tetapi juga terkait dengan hak eksklusif suatu negara untuk mengatur, mengontrol, dan menjaga integritas ruang sibernya sendiri dari intervensi pihak asing. Kedaulatan siber menegaskan bahwa suatu negara memiliki wewenang penuh atas pengelolaan aktivitas digital yang terjadi di dalam yurisdiksinya.

Hal ini meliputi pengawasan terhadap data, jaringan, serta pelindungan terhadap aset digital strategis dari serangan siber yang dapat merugikan kedaulatan dan keamanan nasional. Dalam ranah kedaulatan siber, negara harus mampu memastikan bahwa ancaman eksternal tidak dapat mengganggu sistem kritikal yang mendukung kehidupan masyarakat, ekonomi, maupun pemerintahan. Seiring dengan meningkatnya ketergantungan pada teknologi digital, prinsip kedaulatan siber semakin penting sebagai fondasi untuk menjaga ketahanan negara di tengah pesatnya perkembangan teknologi global. Negara memiliki hak untuk membuat regulasi yang kuat dan sistem pertahanan yang tangguh guna melindungi seluruh elemen digital dari pengaruh dan serangan luar.

Kedaulatan siber memainkan peran strategis dalam keamanan nasional sebuah negara, terutama dalam era globalisasi yang semakin terhubung melalui teknologi informasi. Pertahanan dan keamanan siber bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi

[33] Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Pelindungan Data Pribadi)", *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 13(2), hlm 223.

penting bagi negara, serta melindungi sistem elektronik yang strategis atau kritikal bagi kelangsungan pelayanan publik atau kelangsungan negara sendiri.[34] Kedaulatan siber memegang peranan strategis dalam menjaga stabilitas serta keamanan nasional di tengah pesatnya perkembangan teknologi informasi di era globalisasi. Seiring semakin terhubungnya negara-negara melalui jaringan digital, ancaman siber seperti peretasan, pencurian data, hingga serangan terhadap infrastruktur penting menjadi semakin nyata dan berisiko. Oleh sebab itu, pertahanan dan keamanan siber tidak hanya berfokus pada pelindungan perangkat dan sistem elektronik, tetapi juga mencakup keamanan data sensitif yang penting, baik di sektor publik maupun swasta.

Sasaran utama dari pertahanan siber adalah menjamin kerahasiaan, integritas, dan ketersediaan informasi penting bagi keamanan negara. Ini termasuk usaha untuk mencegah kebocoran data yang dapat disalahgunakan, menjaga agar informasi tetap utuh tanpa dimanipulasi, serta memastikan infrastruktur strategis seperti jaringan listrik, transportasi, komunikasi, dan layanan keuangan tetap berfungsi dengan baik meski dihadapkan pada serangan siber. Selain itu, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut PP PSTE) merupakan dasar hukum yang mengatur keamanan dan pertahanan siber di Indonesia.

UU ITE mengatur bahwa penyelenggara sistem elektronik harus menyelenggarakan sistemnya secara aman, andal, dan

[34] Admin Aptika, "Kebijakan Keamanan dan Pertahanan Siber, Aptika Kominfo, dalam (https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/), diakses pada 23 September 2024.

bertanggung jawab.[35] Sedangkan, PP PSTE memberikan pedoman tentang lima komponen sistem elektronik yang harus dipertahankan, yaitu perangkat keras, perangkat lunak, tenaga ahli, tata kelola, dan pengamanan.[36] Prinsip kedaulatan siber juga telah tercantum dalam Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber (selanjutnya disebut Permenhan 82/2014) yang didalamnya menekankan pentingnya memiliki model pengamanan informasi yang terstruktur, terintegrasi, serta sesuai dengan standar dan panduan yang telah ditetapkan oleh instansi berwenang.[37] Salah satu aspek utama dalam pengamanan siber adalah memastikan kerahasiaan, integritas, dan ketersediaan informasi sejak tahap perancangan, yang menjadi prinsip dasar keamanan informasi. Pertahanan siber mencakup kebijakan, kelembagaan, teknologi, dan infrastruktur pendukung, yang harus didukung oleh Sumber Daya Manusia (selanjutnya disingkat menjadi "SDM/") yang kompeten, memiliki integritas tinggi, dan terjamin keamanannya.[38]

Pelaksanaan pertahanan siber harus dilakukan secara efektif dan efisien melalui penggabungan keamanan fisik dan logis secara terintegrasi, dengan memanfaatkan teknologi terbuka dan produk dalam negeri untuk mendukung kemandirian serta kedaulatan nasional. Zona pengamanan ditetapkan berdasarkan klasifikasi SDM, seperti administrator dan pengguna lainnya, untuk memastikan pelindungan yang tepat. Pengelolaan pertahanan siber juga harus mengacu pada prinsip tata kelola yang menjamin adanya pengawasan

[35] Pasal 15 Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.
[36] Pasal 4 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
[37] BAB III angka 3.2, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.
[38] BAB II angka 2.4, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber

melekat dalam implementasinya, sehingga sistem yang diterapkan aman dan tahan terhadap serangan siber dari pihak lawan. Selain itu, pertahanan siber juga diharapkan mampu menciptakan kondisi yang lebih menguntungkan bagi tindakan ofensif sekaligus mencegah kerugian pada sistem komputer yang tidak diinginkan.

Lebih lanjut, prinsip kedaulatan siber juga menekankan pentingnya kolaborasi antar sektor dalam menjaga keamanan ruang siber. Pemerintah, lembaga keamanan, dan sektor swasta harus bekerja sama dalam membangun sistem keamanan yang tangguh. Keterlibatan sektor swasta sangat diperlukan mengingat peran signifikan mereka dalam mengelola Infrastruktur Informasi Kritikal, seperti layanan telekomunikasi, teknologi informasi, dan *platform online* yang menjadi sasaran potensial serangan siber. Dalam hal ini, pemerintah perlu memastikan adanya regulasi yang mengatur keterlibatan sektor swasta dalam pertahanan siber, termasuk kewajiban melaporkan insiden siber serta berpartisipasi dalam simulasi keamanan siber yang terkoordinasi.

Selain itu, peran aktif SDM dalam bidang siber sangat krusial. Negara harus berinvestasi dalam pengembangan kompetensi SDM di bidang keamanan siber melalui program pendidikan dan pelatihan berkelanjutan. SDM yang terlatih dan memiliki kompetensi tinggi akan menjadi garda terdepan dalam mendeteksi, merespons, dan memitigasi ancaman siber. Keberlanjutan program ini penting untuk menciptakan tenaga profesional yang siap menghadapi dinamika ancaman siber yang terus berkembang. Sebagai penutup, penerapan prinsip kedaulatan siber menjadi aspek krusial dalam menjaga stabilitas dan keamanan nasional, terlebih di tengah meningkatnya kompleksitas ancaman di era digital. Negara harus memastikan bahwa seluruh sistem informasi dan infrastruktur strategis terlindungi dari potensi serangan yang

dapat mengancam kedaulatan dan integritasnya.

Pengelolaan ruang siber yang komprehensif tidak hanya melibatkan aspek teknis, tetapi juga aspek regulasi dan pengawasan yang menyeluruh, memastikan bahwa setiap entitas yang beroperasi di ruang siber mematuhi aturan yang telah ditetapkan. Untuk mencapai tujuan ini, sinergi antara pemerintah, sektor swasta, dan masyarakat sangat penting. Kerja sama lintas sektor diperlukan untuk menciptakan ekosistem digital yang aman dan andal, di mana setiap komponen, mulai dari teknologi hingga SDM, berperan aktif dalam upaya pelindungan terhadap ancaman siber. Investasi dalam pengembangan SDM serta teknologi lokal juga menjadi elemen kunci dalam memastikan kedaulatan digital yang mandiri dan berdaya saing di ranah internasional. Pada akhirnya, kedaulatan siber bukan hanya sebuah prinsip yang melindungi negara dari ancaman siber, tetapi juga merupakan fondasi yang memungkinkan Indonesia memanfaatkan teknologi digital secara maksimal untuk mencapai kemajuan ekonomi, sosial, dan politik. Dengan penerapan yang konsisten dan terstruktur, Indonesia dapat membangun ketahanan nasional yang kokoh di era digital, menjamin keamanan bagi masyarakat, dan tetap kompetitif di tengah persaingan global yang semakin intens.

b. Pelindungan Data Pribadi

Pelindungan data pribadi merupakan komponen penting dalam keamanan dan ketahanan siber, terutama dalam era digital yang semakin kompleks. Dalam konteks penetapan struktur, materi muatan, dan tujuan RUU KKS untuk Indonesia, prinsip pelindungan data pribadi harus diprioritaskan untuk menjaga privasi individu dan mencegah penyalahgunaan informasi. Prinsip pelindungan data pribadi bertujuan untuk menjamin privasi individu serta menjaga

keamanan informasi pribadi yang dikumpulkan, disimpan, dan diproses oleh berbagai entitas. Prinsip ini menekankan bahwa pengumpulan data pribadi harus dilakukan secara sah, transparan, dan sesuai dengan tujuan yang telah disepakati.[39] Setiap penggunaan data pribadi harus sejalan dengan persetujuan pemilik data, serta tidak boleh digunakan untuk kepentingan lain tanpa izin lebih lanjut.[40]

Terdapat 8 (delapan) prinsip dalam mengatur pelindungan data pribadi diantaranya adalah *collection limitation, minimalisasi data, data quality, security safeguard, akurasi, openness, purpose specification,* dan *accountability.*[41] Selain itu, keamanan data pribadi juga harus dipastikan melalui langkah-langkah teknis dan organisasi yang memadai guna mencegah akses yang tidak sah, kebocoran, atau penyalahgunaan.[42] Pengendali Data Pribadi juga diwajibkan untuk memastikan akurasi dan keutuhan data yang dikelola, serta memberikan hak kepada subjek data pribadi untuk mengakses, memperbarui, atau menghapus data mereka sesuai dengan regulasi yang berlaku. Prinsip ini sangat penting dalam era digital, di mana Pelindungan terhadap data pribadi menjadi salah satu kunci dalam menjaga hak privasi individu serta mencegah penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab.

Dalam menjalankan segala aktivitas yang berkaitan dengan pemrosesan data pribadi, penting untuk memperhatikan prinsip yang telah diatur dalam APEC *Privacy*

---

[39] Ahmad M Ramli, "UU Pelindungan Data Pribadi, Big Data, dan Ekonomi Digital", Kompas.com, dalam(https://nasional.kompas.com/read/2022/10/10/09570741/uu-pelindungan-data-pribadi-big-data-dan-ekonomi-digital?page=3), diakses pada 13 Oktober 2024.

[40] *Ibid*.

[41] Willa Wahyuni, "8 Prinsip Hak Privasi dalam Aturan Pelindungan Data Pribadi", HukumOnline.com, dalam (https://www.hukumonline.com/berita/a/8-prinsip-hak-privasi-dalam-aturan-pelindungan-data-pribadi-lt64a2dcec71359/), diakses pada 24 September 2024.

[42] Aptika, "Pentingnya Pelindungan Data Pribadi Di Era Digital", Aptika Kominfo, Dalam (Https://Aptika.Kominfo.Go.Id/2021/10/Pentingnya-Pelindungan-Data-Pribadi-Di-Era-Digital/),Diakses pada 24 September 2024.

Framework. *APEC Privacy Framework* menegaskan bahwa data pribadi harus diperoleh, disimpan, diproses, atau digunakan secara adil ("*fairly*") dan sah ("*lawfully*").[43] Untuk menilai apakah data pribadi tersebut diperoleh secara adil, biasanya dilihat dari metode yang digunakan dalam pengumpulan, penyimpanan, pemrosesan, atau penggunaannya.[44] Pemrosesan data pribadi harus dilakukan secara sah, adil, dan transparan. Hal ini diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menekankan bahwa Pengendali Data Pribadi wajib memiliki dasar hukum yang jelas untuk pengumpulan data pribadi.

Pengendali Data Pribadi harus memberikan informasi yang jelas tentang tujuan pengumpulan data, cara penggunaan data, dan hak-hak subjek data.[45] Selain itu, data pribadi yang dikumpulkan harus relevan dan terbatas hanya pada data yang diperlukan untuk tujuan pemrosesan. Penggunaan data pribadi harus sesuai dengan tujuan yang telah disampaikan kepada subjek data dan tidak boleh digunakan untuk kepentingan lain tanpa izin lebih lanjut. Prinsip *Collection limitation* menekankan bahwa pengumpulan data pribadi harus dibatasi hanya pada data yang diperlukan untuk tujuan yang sah, tanpa pengumpulan berlebihan. Pengendali Data Pribadi harus mematuhi prinsip minimalisasi data, yakni mengumpulkan dan menyimpan data hanya sebatas yang relevan untuk kepentingan pemrosesan, guna mengurangi risiko penyalahgunaan.

Selain itu, *openness* mengharuskan Pengendali Data Pribadi untuk menyediakan informasi yang jelas dan mudah diakses oleh subjek data pribadi terkait dengan cara data

[43] BAB III Bagian III Angka 18, *APEC Privacy Framework*.
[44] Sinta Dewi, "Prinsip-Prinsip Pelindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya", *Jurnal Sosiohumaniora*, 19(3), Nov. 2017, hlm 209.
[45] Wila Wahyuni, "Melihat Prinsip dan Dasar Pemrosesan Data Pribadi", HukumOnline.com, dalam (https://www.hukumonline.com/berita/a/melihat-prinsip-dan-dasar-pemrosesan-data-pribadi-lt64a2df2ad70ce/), diakses pada 24 September 2024 .

mereka dikumpulkan, diproses, dan digunakan, sehingga keterbukaan ini dapat membangun kepercayaan antara subjek dan pengendali data. Prinsip penggunaan data pribadi *purpose specification* mengharuskan bahwa data yang dikelola untuk tujuan tertentu tidak boleh digunakan untuk keperluan lain tanpa persetujuan dari subjek data pribadi. Penggunaan data tersebut harus tetap sesuai dengan maksud pengumpulannya atau terkait langsung dengan tujuan tersebut. Selain itu, prinsip pengungkapan data pribadi menyatakan bahwa data tidak boleh diungkapkan tanpa persetujuan subjek data pribadi kecuali jika pengungkapan itu sesuai dengan tujuan awal pengumpulan data.

Dalam hal keakuratan data pribadi, Pengendali Data Pribadi wajib memastikan bahwa data pribadi yang mereka kelola selalu akurat, lengkap, relevan, tidak menyesatkan, dan terbaru sesuai dengan tujuan pengumpulannya.[46] Data pribadi juga tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan penggunaannya. Oleh karena itu, Pengendali Data Pribadi harus secara berkala mengevaluasi dan menghapus data yang sudah tidak relevan kecuali untuk kepentingan umum. Subjek data pribadi memiliki hak untuk mengakses dan mengoreksi data pribadinya yang dikelola, guna memastikan data tersebut akurat dan mutakhir.[47] Dalam aspek keamanan, Pengendali Data Pribadi harus mengambil langkah-langkah yang memadai untuk melindungi data pribadi dari akses, pemrosesan yang melanggar hukum. Langkah ini harus mempertimbangkan ancaman potensial terhadap data, lokasi penyimpanan, sistem keamanan yang diterapkan, serta tindakan untuk menjamin integritas dan keandalan individu yang memiliki akses ke data tersebut, termasuk memastikan transmisi data yang aman.

[46] Sinta Dewi, *Op.cit,* Hlm 209.
[47] Pasal 6, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

c. Keamanan Nasional

Sebagai sebuah konsep/prinsip, keamanan telah mengalami evolusi pemaknaan yang luas dan berkembang mengikuti perkembangan dinamika perubahan zaman. Secara etimologis, keamanan *(security)* berasal dari bahasa latin *"securus"* (se+cura) yang bermakna terbebas dari bahaya atau terbebas dari ketakutan. Kata ini juga bisa bermakna dari gabungan kata *se* (yang berarti tanpa/*without*) dan *curus* (yang berarti "*uneasiness*"). Bila digabungkan kata ini bermakna *"liberation from uneasiness, or a peaceful situation without any risks or threats",* atau jika diterjemahkan ke dalam bahasa Indonesia yaitu "Pembebasan dari ketidaknyamanan, atau situasi damai tanpa risiko atau ancaman apa pun."[48]

Di Indonesia, prinsip dasar dari keamanan nasional tertuang dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dalam Pasal 30 ayat (2) yang menyatakan bahwa usaha pertahanan dan keamanan negara dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta (Sishankamrata). Sesuai dengan dasar tersebut, kebijakan pertahanan negara tidak dapat ditinjau hanya dari perspektif pertahanan semata, namun dalam pengelolaannya merupakan satu kesatuan konseptual pertahanan dan keamanan yang bulat dan utuh.[49] Dalam definisinya, prinsip Keamanan Nasional (Kamnas) dapat dimaknai baik sebagai kondisi maupun fungsi. Sebagai fungsi, Kamnas akan memproduksi dan menciptakan rasa aman dalam pengertian luas, yang didalamnya tercakup rasa nyaman, damai, tentram, dan tertib.

Kondisi keamanan semacam ini merupakan kebutuhan dasar setiap manusia disamping kesejahteraan. Pemahaman

[48] Anak Agung Banyu Perwita, Hakikat Prinsip dan Tujuan Pertahanan-Keamanan Negara, dalam Tim Propatria Institute, Mencari Format Komprehensif Sistem Pertahanan dan Keamanan Negara, (Jakarta: Propatria, 2006)
[49] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

terhadap makna dan substansi yang terkandung didalamnya akan bervariasi tergantung kepada tata nilai, persepsi, dan kepentingan.[50] Kamnas dalam konteks Indonesia diartikan sebagai kondisi di mana sebuah negara mampu melindungi dan mempertahankan kepentingan nasionalnya dari berbagai ancaman, baik yang datang dari dalam negeri maupun luar negeri. Dalam hal ini, ancaman tersebut tidak hanya meliputi aspek militer, tetapi juga mencakup aspek non-militer seperti politik, ekonomi, sosial budaya, termasuk ancaman siber.[51]

Seiring dengan berkembangnya teknologi dan digitalisasi, ancaman terhadap keamanan nasional kini mencakup ancaman siber yang bisa mempengaruhi kestabilan politik, ekonomi, serta keamanan publik, khususnya ancaman siber dan serangan siber terhadap Infrastruktur Informasi dan Infrastruktur Informasi Kritikal. RUU KKS berfungsi sebagai salah satu mekanisme hukum yang dirancang untuk menangani ancaman ini melalui pendekatan yang menyeluruh dan terkoordinasi. Dalam dunia yang semakin digital, keamanan siber menjadi salah satu elemen penting dari keamanan nasional. Ancaman yang datang dari ruang siber, seperti gangguan, perusakan, atau peretasan terhadap Infrastruktur Informasi dan Infrastruktur Informasi Kritikal, yang berpotensi melemahkan kestabilan negara. Oleh karena itu, RUU ini menempatkan keamanan siber sebagai pilar untuk mempertahankan kedaulatan negara di dunia digital.

RUU ini harus mencerminkan kepentingan nasional Indonesia, yang terdiri dari pelindungan terhadap kedaulatan negara, keamanan publik, dan hak asasi warga negara dalam konteks dunia digital. Negara bertanggung jawab memastikan bahwa infrastruktur informasi digital, data, serta informasi

[50] Dewan Ketahanan Nasional, Sebuah Konsep dan Sistem Keamanan Bagi Bangsa Indonesia, Sekretariat Jenderal Dewan Ketahanan Nasional, 2010, hlm. 44.
[51] *Ibid.*

yang beredar dalam jaringan siber tetap aman dan terjamin. Keamanan nasional dalam hal ini juga mencakup proteksi terhadap data warga negara dari akses yang tidak sah dan penyalahgunaan. Lebih lanjut, berdasarkan Permenhan 82/2014, ada beberapa ancaman siber yang dapat mempengaruhi keamanan nasional. Ancaman siber dapat bersumber dari pelaku negara (*State Actor*) maupun non-negara (*Non-State Actor*), seperti individu, kelompok, atau organisasi yang memiliki niat dan kemampuan untuk merusak sistem elektronik dan informasi. Sumber ancaman ini bisa bersifat internal (dari dalam negeri) maupun eksternal (dari luar negeri). Berikut adalah beberapa sumber ancaman yang diidentifikasi:[52]

1) Kegiatan Intelijen: Upaya pengumpulan informasi secara rahasia oleh negara atau entitas lain yang bertujuan untuk mencuri data strategis.
2) Organisasi Ekstremis dan *Hacktivists*: Kelompok yang melakukan serangan untuk mempromosikan ideologi atau tujuan tertentu, termasuk menyusupi sistem siber nasional.
3) Grup Kejahatan Terorganisir: Sindikat kriminal yang memanfaatkan ruang siber untuk mendapatkan keuntungan finansial atau keuntungan lainnya melalui kejahatan siber.

Kemudian dalam Permenhan ini juga menjelaskan ancaman siber apa saja yang sering terjadi, yang meliputi:

1) *Advanced Persistent Threats* (APT): Serangan siber jangka panjang yang ditargetkan untuk merusak atau mencuri informasi dari sistem strategis suatu negara.
2) *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS): *Serangan* yang menyebabkan sistem atau

[52] Peraturan Menteri Pertahanan (Permenhan) Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

jaringan mengalami kelebihan beban dan akhirnya tidak dapat digunakan, yang berdampak pada kelumpuhan operasional.

3) *Phishing*: Tindakan penipuan yang bertujuan mencuri informasi penting seperti kata sandi atau informasi bank dengan *menggunakan* situs web palsu yang menyerupai situs resmi.
4) *Malware*: Program berbahaya yang dapat menginfeksi sistem komputer, *menghancurkan* data, atau mencuri informasi. Jenis serangan *malware* ini bisa berupa virus, worm, *trojan horse*, *ransomware*, dan lain-lain.
5) *Defacement*: Pengubahan tampilan situs web korban dengan *tujuan* menyebarkan pesan atau menyebabkan kerusakan citra organisasi atau lembaga.
6) Penyusupan Siber: Metode penyusupan ke dalam sistem melalui eksploitasi *kerentanan* yang ada, seperti melalui password yang lemah atau penipuan sosial (*social engineering*).

Selain ancaman harian, serangan siber yang lebih serius dapat terjadi dalam bentuk:[53]

1) Perang Siber (*Cyber War*): Serangan terkoordinasi yang dirancang untuk mengganggu kedaulatan negara melalui siber. Ini bisa melibatkan terorisme siber (*cyber terrorism*) atau spionase siber (*cyber espionage*) yang menargetkan informasi strategis dan keamanan nasional.
2) Gangguan Siber (*Cyber Violence*): Serangan yang tidak disengaja, tetapi tetap dapat menyebabkan kerusakan dan gangguan pada sistem penting negara.

Tugas dan fungsi BSSN yang tercantum dalam Pasal 2 dan Pasal 3 Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara dalam hal ini juga memiliki

[53] *Ibid.*

keterkaitan dengan prinsip keamanan nasional. BSSN sebagai lembaga pemerintah yang bertanggung jawab dalam keamanan siber dan persandian memiliki tugas untuk melindungi ruang siber Indonesia. BSSN memainkan peran kunci dalam mempertahankan keamanan nasional, karena tugas dan fungsinya berkaitan erat dengan pencegahan, mitigasi, dan penanggulangan ancaman siber yang dapat mempengaruhi kedaulatan dan stabilitas nasional. Prinsip keamanan nasional menjadi landasan bagi BSSN dalam melaksanakan tugasnya, termasuk dalam perumusan kebijakan, pelaksanaan operasional, pengelolaan aset, dan pengawasan yang semuanya bertujuan untuk menjaga stabilitas dan keamanan negara dari ancaman siber.

Prinsip Kamnas dalam RUU KKS dapat mengadopsi pendekatan *state-centered security* dan *people-centered security*,[54] di mana *state-centered security* menitikberatkan pada Pelindungan negara, pemerintah, dan Infrastruktur Informasi Kritikal yang mendukung operasional negara. Contohnya, melindungi sistem perbankan, listrik, transportasi, serta lembaga pemerintah dari serangan siber. Sedangkan *people-centered security* berfokus pada Pelindungan individu dan komunitas dari bahaya ancaman siber, termasuk privasi data dan keamanan digital warga negara. Prinsip ini memastikan bahwa masyarakat terlindungi dari ancaman digital yang bisa berdampak pada kehidupan sehari-hari mereka, baik secara sosial maupun ekonomi.

Prinsip Keamanan Nasional dalam RUU KKS untuk Indonesia sangat relevan dalam menghadapi tantangan keamanan siber di era digital ini. RUU ini harus mampu mengintegrasikan berbagai pendekatan, baik yang berfokus pada keamanan negara maupun Pelindungan terhadap warga

[54] Dewan Ketahanan Nasional, *loc.cit.*

negara, melalui pengelolaan ancaman siber yang komprehensif dan inklusif. Sesuai dengan Pasal 30 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, maka negara berkewajiban untuk mengambil peran proaktif dalam menjaga kedaulatan sibernya. Negara harus memiliki strategi yang jelas dan terukur untuk mendeteksi, mencegah, dan menanggapi setiap bentuk ancaman siber.

Hal ini mencakup kemampuan dalam pengembangan infrastruktur keamanan siber yang kokoh, penguatan sistem pertahanan siber, serta pembentukan kerja sama internasional untuk memerangi ancaman siber lintas negara. Selain negara yang berkewajiban untuk hal ini, dalam pasal 30 ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 juga disebutkan bahwa "Tiap-tiap warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara". Dalam konteks keamanan siber, peran masyarakat meliputi peningkatan kesadaran terhadap ancaman siber, menjaga kerahasiaan data pribadi, dan mematuhi standar keamanan dalam penggunaan teknologi informasi.

d. Akuntabilitas dan Transparansi

Prinsip akuntabilitas merujuk pada konsep tanggung jawab yang diemban oleh individu, lembaga, atau organisasi dalam melaksanakan tugas dan fungsinya. Istilah akuntabilitas berasal dari istilah dalam bahasa Inggris *accountability* yang berarti pertanggung jawaban atau keadaan untuk dipertanggungjawabkan atau keadaan untuk diminta pertanggungjawaban.[55] Akuntabilitas *(accountability)* yaitu berfungsinya seluruh komponen penggerak jalannya kegiatan perusahaan, sesuai dengan tugas dan kewenangannya

[55] Putri, B. E. (2014). Penerapan prinsip-prinsip good corporate governance pada PT purnama semesta alamiah. Agora, 2(2), 1351–1355.

masing-masing. Arti dari akuntabel itu sendiri adalah: Pertama, dapat dipertanggung jawabkan, dapat menjawab pada atasan sebagaimana manusia bertanggung jawab kepada Tuhan-Nya atas apa yang telah ia lakukan. Kedua, memiliki kemampuan untuk dipertanggungjawabkan secara eksplisit, dan yang Ketiga, sesuatu yang bisa diperhitungkan atau dipertanggung jawabkan.

Di sisi lain, prinsip transparansi menekankan pentingnya keterbukaan dalam proses pengambilan keputusan, pelaksanaan kebijakan, serta penyampaian informasi kepada publik. Transparansi berarti bahwa segala aktivitas yang dilakukan oleh pemerintah atau lembaga publik dapat diakses, dipantau, dan dipahami oleh masyarakat luas. Informasi yang relevan, seperti prosedur, kebijakan, keputusan, biaya, hingga tanggung jawab, harus disediakan secara lengkap, akurat, dan dapat diakses oleh siapa saja yang berkepentingan. Transparansi bukan sekadar membuka akses terhadap informasi, tetapi juga memastikan bahwa informasi tersebut disajikan dengan jelas, tidak memihak, dan sesuai dengan realitas yang terjadi.[56] Hal ini sangat penting untuk membangun kepercayaan publik, mencegah korupsi, dan memastikan bahwa setiap kebijakan atau keputusan yang diambil oleh pemerintah benar-benar berorientasi pada kepentingan umum.

Transparansi juga mendorong partisipasi aktif dari masyarakat dalam proses pengambilan keputusan karena masyarakat yang mendapatkan informasi yang memadai dapat memberikan umpan balik, mengajukan keberatan, atau menyampaikan aspirasi yang konstruktif. Berdasarkan Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan dijelaskan bahwa sistem pemerintahan yang

[56] Pandji Santoso, *Administrasi Publik: Teori dan Aplikasi Good Governance*, (Bandung: Refika Aditama, 2008)

baik adalah sistem pemerintahan yang mampu mengimplementasikan asas-asas pemerintahan yang baik (asas kepastian hukum, asas kemanfaatan, asas ketidakberpihakan, asas tidak menyalahgunakan kewenangan, asas keterbukaan, asas kepentingan umum, dan asas pelayanan yang baik). Dari penjelasan regulasi tersebut, pemerintah seharusnya mampu mengimplementasikan suatu sistem tata kelola pemerintahan yang baik dalam seluruh rangkaian proses pelaksanaan sistem pemerintahan.

Terkait dengan sistem pemerintahan yang baik atau yang biasa dikenal dengan *good governance*, *United National Development Programme* (UNDP) menjelaskan bahwa dalam sebuah sistem pemerintahan yang baik (*good governance*) terdapat beberapa karakteristik yang di antaranya adalah *participation, rule of law, transparency, responsiveness, consensus orientation, semua warga negara, effectiveness and efficiency, accountability dan strategic vision.*[57] Kedua prinsip ini, akuntabilitas dan transparansi, saling terkait erat dan menjadi fondasi utama dalam menciptakan tata kelola yang baik *(good governance).* Akuntabilitas tanpa transparansi tidak akan efektif, karena tanpa akses terhadap informasi, masyarakat atau pihak yang berwenang tidak dapat menilai dan mengawasi kinerja pemerintah atau lembaga publik secara optimal. Sebaliknya, transparansi tanpa akuntabilitas akan kehilangan esensinya, karena keterbukaan informasi yang tidak diiringi dengan pertanggungjawaban yang jelas hanya akan menjadi formalitas yang tidak bermakna.

Dalam keamanan dan ketahanan siber, prinsip akuntabilitas meliputi setiap pihak yang terlibat dalam pengelolaan keamanan siber, baik itu pemerintah, lembaga

[57] Muhammad Fikri Haikal dan Deasy Mauliana, *"Akuntabilitas dan Transparansi dalam Pelayanan Publik (Studi Kasus Pelayanan E-KTP di Kantor Kecamatan Tallo Kota Makassar)," Jurnal Administrasi Negara,* Vol. 28 Nomor 1 (2022), hlm. 90 -91.

negara, maupun pihak swasta yang diberikan kewenangan, harus mampu mempertanggungjawabkan segala tindakannya, terutama yang berkaitan dengan penanganan ancaman siber, Pelindungan data, dan pemulihan insiden siber. Setiap pihak yang terlibat wajib menjelaskan secara terbuka alasan di balik setiap kebijakan yang diambil, termasuk dalam aspek teknis, seperti kebijakan pelindungan Infrastruktur Informasi dan Infrastruktur Informasi Kritikal termasuk mekanisme deteksi ancaman, serta tindakan mitigasi yang diambil saat terjadi insiden keamanan siber. Pertanggungjawaban ini mencakup penyampaian laporan secara berkala kepada lembaga pengawas yang relevan dan kepada masyarakat, sehingga masyarakat dapat menilai efektivitas kebijakan yang diterapkan. Hal ini sejalan dengan tujuan utama dari keamanan dan ketahanan siber, yaitu melindungi kepentingan publik, ekonomi, dan pertahanan negara dari ancaman digital.

Prinsip transparansi juga harus menjadi bagian kesatuan dalam setiap tahap pengambilan keputusan terkait keamanan siber. Keterbukaan informasi sangat penting, terutama dalam menghadapi ancaman siber yang semakin kompleks dan meluas. Transparansi dalam keamanan siber mencakup penyediaan akses yang jelas dan akurat bagi masyarakat terhadap informasi yang relevan, seperti ancaman yang sedang dihadapi, langkah-langkah yang diambil untuk mengatasi insiden siber, serta kebijakan Pelindungan data yang diterapkan oleh pemerintah dan pihak swasta. Dalam RUU KKS, prinsip ini harus tercermin melalui kewajiban lembaga terkait untuk melakukan koordinasi hasil penanganan Insiden Siber kepada pemangku kepentingan baik internal maupun eksternal, kebijakan keamanan yang diterapkan, serta langkah-langkah mitigasi yang dilakukan.

Lebih lanjut, transparansi dalam kebijakan keamanan siber juga mencakup pemberian informasi yang jelas mengenai

prosedur yang harus diikuti oleh pengguna layanan digital, baik individu maupun organisasi, dalam melaporkan insiden keamanan siber. RUU ini harus memastikan bahwa setiap individu atau organisasi yang menjadi korban serangan siber memiliki akses yang jelas untuk melaporkan insiden, mendapatkan bantuan, serta mengetahui langkah apa yang akan diambil oleh pihak berwenang untuk menindaklanjuti laporan tersebut. Selain itu, masyarakat juga harus diberi kemudahan dalam memahami hak dan kewajiban mereka terkait dengan keamanan siber, seperti hak atas pelindungan data pribadi dan kewajiban untuk menjaga keamanan data mereka sendiri. Transparansi juga diperlukan dalam hal penyusunan kebijakan keamanan siber yang melibatkan partisipasi dari berbagai pihak, termasuk masyarakat, sektor swasta, dan ahli di bidang keamanan siber melalui konsultasi publik dan partisipasi aktif dari berbagai pihak, dengan demikian kebijakan yang dihasilkan akan lebih komprehensif dan berpotensi lebih efektif dalam melindungi keamanan siber nasional.

Prinsip akuntabilitas dan transparansi dalam penegakan hukum siber menjadi elemen penting dalam RUU ini. Setiap upaya penegakan hukum terhadap pelaku kejahatan siber, baik di tingkat nasional maupun internasional, harus dilakukan dengan prosedur yang transparan dan dapat dipertanggungjawabkan. Mekanisme penegakan hukum harus jelas, dengan adanya pembagian peran yang tegas antara lembaga yang bertanggung jawab atas keamanan siber, sehingga tindakan yang diambil tidak tumpang tindih dan efektif dalam menangani ancaman. Masyarakat juga harus mendapatkan informasi yang jelas tentang langkah yang diambil oleh pemerintah dalam menghadapi kasus-kasus kejahatan siber, terutama yang berdampak langsung pada kepentingan publik.

e. Prinsip-Prinsip Keamanan dan Ketahanan Siber Berbasis *Upstream dan Downstream Regulation Principles*

Dalam konteks Keamanan dan Ketahanan Siber, model *Upstream* dan *Downstream Regulation Principles* merupakan dua metode pendekatan penting dalam pengaturan dan pengelolaan Keamanan Siber. Prinsip Keamanan dan Ketahanan Siber berbasis *upstream* sendiri merupakan salah satu pendekatan hukum transformatif, dimana teori hukum transformatif sendiri merupakan teori yang dikembangkan oleh Ahmad M. Ramli.

Meningkatnya ancaman dan kejahatan siber saat ini menunjukkan urgensi model regulasi hulu atau *Upstream Regulation*. *Upstream Regulation* merupakan upaya pelindungan atau pengaturan hukum yang dimulai dari hulu. Hal ini diprioritaskan terutama pada negara dan perusahaan teknologi. Regulasi harus diprioritaskan terhadap sistem Kritikal yang digunakan oleh negara dan perusahaan yang berdampak pada kehidupan sehari-hari. *Upstream Regulation* menekankan pada berbagai unsur yang berada di posisi awal, atau sebelum suatu insiden keamanan siber terjadi. Hal ini termasuk ke dalam regulasi penyelenggaraan telekomunikasi bagi operator/ISP, pengembang dan produsen perangkat lunak, perangkat keras, dan penyedia infrastruktur lainnya. Terdapat beberapa prinsip dasar yang ada pada *upstream regulation*, yakni:

1) Regulasi model yang diproyeksikan mengatur persyaratan keandalan, ketangguhan, dan keamanan yang harus dipatuhi pengembang dan produsen perangkat lunak;
2) Memastikan standar keamanan produk perangkat keras, termasuk Pelindungan terhadap serangan fisik dan logis, serta pembaruan perangkat keras untuk memperbaiki kerentanan;

3) Menetapkan persyaratan keamanan bagi penyedia Infrastruktur Informasi Kritikal seperti pusat data, sistem kontrol industri, dan jaringan telekomunikasi untuk melindungi Infrastruktur Informasi Kritikal dari serangan; dan
4) Regulasi harus mampu menjangkau pengguna, terutama terkait transparansi dan instruksi penggunaan yang jelas.

Dalam implementasinya, model *Upstream Regulation* dapat dilihat pada regulasi *EU Cyber Resilience Act* (EU CRA). Regulasi ini mengatur kewajiban keandalan dan keamanan siber atas produk dan layanan teknologi informasi dan memastikannya sebelum dilepas dan tersedia di pasar. Tujuan dari EU CRA adalah untuk membuat perangkat lebih aman, dengan menerapkan persyaratan keamanan siber, dokumentasi, dan pelaporan kerentanan yang lebih ketat. Hal ini sesuai dengan implementasi model *Upstream Regulation* yang menekankan pada pengaturan yang dimulai dari hulu, yakni pada perusahaan yang menyediakan produk yang mengandung elemen digital. Selain EU CRA, model regulasi lainnya yang juga menekankan pada model *Upstream Regulation* adalah Perintah Eksekutif Presiden AS yang dikenal dengan *Executive Order* 14028 (EO 14028).

Model regulasi ini mewajibkan penyedia layanan untuk berbagi informasi insiden yang terkait ancaman siber, yang dapat mempengaruhi jaringan pemerintah. Selain itu, Pemerintah Federal juga didorong untuk mengamankan layanan *cloud*, arsitektur *zero-trust*, dan penerapan otentikasi multifaktor dan enkripsi. Selain itu, perintah eksekutif ini juga menekankan standar keamanan dasar untuk perangkat lunak maupun perangkat layanan digital yang dijual kepada pemerintah. Hal ini juga dinilai sesuai dengan model *upstream regulation*, dimana menekankan pada bagian hulu yakni lingkup pemerintah untuk mencegah ancaman terhadap

keamanan dan ketahanan siber.

Downstream Regulation dalam konteks keamanan dan ketahanan siber berfokus pada tahap hilir, yaitu setelah suatu insiden keamanan siber terjadi. Pendekatan ini mencakup serangkaian langkah dan kebijakan yang bertujuan untuk merespons, memitigasi dampak, serta mengelola konsekuensi dari insiden atau kejahatan siber yang sudah terjadi. Dengan prinsip ini, pengaturan dilakukan pada aspek penanganan yang memungkinkan pemulihan kondisi pasca insiden agar sistem atau layanan dapat kembali berfungsi normal. Contoh pengimplementasian *Downstream Regulation* dalam ketahanan dan ketahanan siber dapat ditemukan dalam berbagai kebijakan siber di negara lain seperti pada SACA 2022 di Amerika Serikat, yang menekankan pada berbagai mekanisme pelaporan insiden untuk menjaga transparansi dan meningkatkan respons instansi federal terhadap ancaman siber.

Bagian penting dari regulasi ini adalah wajib lapor insiden keamanan siber yang mengharuskan perusahaan kritikal melaporkan insiden ke lembaga pemerintah, seperti CISA dan FBI, dalam kurun waktu tertentu. Hal ini memastikan adanya langkah pemulihan yang terkoordinasi dan mempercepat proses mitigasi pasca-insiden. *Downstream regulation* ini menjadi pelengkap penting bagi *upstream regulation* dengan memastikan bahwa setiap insiden yang terjadi dikelola dengan efektif, baik dalam respons langsung maupun upaya pemulihan jangka panjang, sehingga ekosistem siber yang lebih aman dapat tercipta. Regulasi keamanan siber yang menyatukan pendekatan *upstream* dan *downstream* merupakan langkah baik yang harus diterapkan dalam

menghadapi ancaman siber modern.[58]

Dengan menggabungkan langkah preventif *(upstream)* yang meminimalkan risiko sejak awal, dan strategi penindakan *(downstream)* untuk merespons insiden yang telah terjadi memberikan Pelindungan yang lebih komprehensif. Hal ini tidak hanya meningkatkan ketahanan terhadap serangan siber, tetapi juga memastikan kelangsungan operasional di tengah potensi gangguan.

f. Prinsip Hukum Transformatif terkait dengan Norma, Lembaga, dan Proses Keamanan dan Ketahanan Siber

Prinsip Hukum Transformatif menekankan pentingnya hukum tidak hanya berfungsi untuk memelihara ketertiban, keadilan dan kepastian, tetapi juga berperan layaknya teknologi yang bisa mengubah, memberi arah bahkan memfiltrasi segala pengaruh buruh yang datang dari dalam maupun luar negeri. Hukum harus ditegakkan dan hukum sebagai infrastruktur transformasi harus menjadi pemberi arah sekaligus sarana untuk mengubah sesuai dengan yang menjadi leluhur negara. Prinsip ini menjadikan teknologi sebagai salah satu unsur nonyuridis dalam membentuk dan menegakkan hukum. Pada aspek normatif, hukum dan peraturan yang mengatur keamanan siber harus senantiasa dievaluasi dan disesuaikan untuk dapat menjawab tantangan dan ancaman baru yang muncul. Perubahan teknologi yang cepat dan munculnya metode serangan siber yang inovatif menuntut adanya pembaruan regulasi yang komprehensif dan adaptif.

Dari segi kelembagaan, kehadiran lembaga penegak hukum tidak cukup, tetapi juga diperlukan reformasi

[58] Ahmad M Ramli, (2024), "Pentingnya UU Keamanan dan Resiliensi Siber", https://teknokompas.com/read/2024/07/25/10363977/pentingnya-uu-keamanan-dan-ketahanan-siber?page=all [25/10/2024].

kelembagaan pembentuk hukum itu sendiri, setidaknya dalam hal menjaga kualitas substansi hukum dan efektivitas serta efisiensi pembentukan hukum itu sendiri.[59] Perlunya evaluasi terhadap lembaga pembentuk dan penegak hukum agar pembentukan hukum dapat dilakukan secara cepat dan efektif sehingga hukum tidak lagi tertinggal oleh perkembangan zaman dan penegakannya bisa dilakukan secara efektif. Dalam prosesnya, pemerintah sebagai regulator dituntut untuk terus mengantisipasi perkembangan teknologi yang semakin tiada batas agar dapat dituangkan ke dalam regulasi progresif yang dapat merespon tetapi juga memberi arah agar perkembangan teknologi terjadi secara produktif dalam menjamin keselamatan negara.

Lambatnya proses pembentukan hukum baru baik dari masalah birokrasi hingga proses legislasi, ini membuat hukum semakin tertinggal oleh perkembangan teknologi dan transformasi digital. Hal ini membuat dalam proses pembentukan regulasi tersebut harus ditata ulang mengingat transformasi digital memerlukan respons yang cepat dengan dibentuknya regulasi yang progresif dan pragmatis agar dapat bertransformasi bukannya terdistorsi.

C. Kajian terhadap Praktik Penyelenggaraan, Kondisi yang Ada, Permasalahan yang Dihadapi Masyarakat, dan Perbandingan dengan Negara Lain.

1. Kajian terhadap praktik

Praktik penyelenggaraan keamanan dan ketahanan siber di Indonesia telah mengalami perkembangan signifikan dalam beberapa tahun terakhir. Salah satu langkah penting yang diambil pemerintah adalah pembentukan BSSN melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (kini

[59] *Ibid.,* hlm. 29.

telah dicabut dengan Peraturan Presiden Nomor 28 Tahun 2021).[60] Berdasarkan ketentuan Pasal 2 Peraturan Presiden Nomor 28 Tahun 2021, BSSN mempunyai tugas untuk melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi negara. BSSN memiliki tugas dan fungsi melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber dan sandi negara.[61]

Dalam praktiknya, BSSN telah menjalankan beberapa inisiatif penting. Salah satunya adalah pengembangan dan implementasi Pusat Operasi Keamanan Siber Nasional *(National Security Operations Center* atau NSOC*)*. NSOC berfungsi sebagai pusat koordinasi untuk pemantauan, deteksi, dan respons terhadap ancaman siber di tingkat nasional. Melalui NSOC, Badan Siber dan Sandi Negara dapat melakukan analisis dan berbagi informasi mengenai ancaman siber secara *real-time* dengan berbagai pemangku kepentingan.

Selain itu, BSSN juga telah menginisiasi program peningkatan kapasitas dan kesadaran keamanan siber. Program ini mencakup pelatihan dan sertifikasi untuk profesional keamanan siber, serta kampanye edukasi publik untuk meningkatkan kesadaran masyarakat akan pentingnya keamanan siber. BSSN juga aktif menyelenggarakan latihan dan simulasi serangan siber untuk menguji kesiapan berbagai sektor dalam menghadapi ancaman siber.

Dari segi regulasi, praktik penyelenggaraan keamanan siber di Indonesia diatur oleh beberapa peraturan perundang-undangan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang

[60] Kominfo, (2020), "BSSN jadi lembaga utama keamanan siber ", <https://www.kominfo.go.id/berita/sorotan-media/detail/bssn-jadi-lembaga-utama-keamanan-siber> diakses pada 10 Oktober 2024.
[61] Pasal 3 Peraturan Presiden Nomor 28 Tahun 2021

Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menjadi landasan hukum utama dalam mengatur aktivitas di dunia maya. UU ini mencakup berbagai aspek, termasuk aturan mengenai tindak pidana siber dan pelindungan data pribadi.

Lebih lanjut, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) memberikan panduan lebih spesifik terkait keamanan sistem elektronik. PP PSTE mewajibkan penyelenggara sistem elektronik untuk menerapkan tata kelola, manajemen risiko, dan pelindungan terhadap data pribadi. Dalam praktiknya, pemerintah juga telah menerapkan kebijakan untuk melindungi Infrastruktur Informasi Kritikal nasional dengan menetapkan sektor-sektor prioritas yang harus dilindungi dari ancaman siber.

Kerja sama antara pemerintah dan sektor swasta juga menjadi bagian penting dalam praktik penyelenggaraan keamanan siber di Indonesia. Badan Siber dan Sandi Negara telah menjalin kemitraan dengan berbagai perusahaan teknologi dan keamanan siber untuk meningkatkan kapasitas nasional dalam menghadapi ancaman siber. Kerja sama ini mencakup pertukaran informasi, pengembangan teknologi, dan pelatihan SDM. Dalam konteks internasional, Indonesia juga aktif berpartisipasi dalam forum keamanan siber global. Negara ini telah menandatangani beberapa kesepakatan internasional terkait keamanan siber dan aktif dalam dialog bilateral, regional, dan multilateral untuk meningkatkan kerja sama dalam menangani ancaman siber lintas batas.

Meskipun demikian, praktik penyelenggaraan keamanan siber di Indonesia masih menghadapi tantangan dalam hal koordinasi antar lembaga. Badan Siber dan Sandi Negara menjadi *focal point* untuk keamanan siber nasional, masih terdapat irisan tugas dengan lembaga pemerintah lainnya. Upaya untuk meningkatkan koordinasi dan sinergi antar lembaga terus dilakukan untuk memastikan penyelenggaraan keamanan siber yang lebih efektif

dan efisien. Secara keseluruhan, praktik penyelenggaraan keamanan siber, ketahanan siber, dan persandian di Indonesia menunjukkan perkembangan positif, namun masih memerlukan penyempurnaan dan penguatan di berbagai aspek untuk menghadapi tantangan keamanan siber yang semakin kompleks di masa depan.

Untuk menghadapi tantangan di masa depan, Indonesia perlu terus melakukan evaluasi dan penyempurnaan terhadap strategi keamanan dan ketahanan siber yang ada. Badan Siber dan Sandi Negara telah mengambil langkah-langkah untuk memperkuat kerangka kerja nasional, termasuk penyusunan strategi nasional keamanan siber. Strategi tersebut diterapkan melalui penyelenggaraan keamanan dan ketahanan siber . Penyelenggaran keamanan siber dilakukan meliputi tata kelola, identifikasi, proteksi, deteksi, tanggap insiden siber, dan pemulihan. Dalam rangka meningkatkan efektivitas penyelenggaraan keamanan siber, dilaksanakan peningkatan kapasitas sumber daya manusia, pengembangan kapasitas teknologi yang lebih mutakhir, dan peningkatan kapasitas proses bisnis untuk mewujudkan ketahanan siber. Selanjutnya, perlu ada pengawasan dan evaluasi secara berkala terhadap yang dilakukan oleh penyelenggara infrastruktur informasi untuk memastikan bahwa kebijakan yang diambil dapat beradaptasi dengan cepat terhadap perkembangan ancaman siber yang dinamis.

Secara keseluruhan, praktik penyelenggaraan keamanan siber, ketahanan siber dan persandian di Indonesia telah mengalami perkembangan positif, terutama dengan adanya pembentukan Badan Siber dan Sandi Negara dan penyusunan beberapa regulasi kunci. Namun, tantangan besar masih menghambat efektivitas implementasi kebijakan ini, terutama dalam hal koordinasi antar lembaga, keterbatasan sumber daya manusia, dan belum adanya kerangka hukum yang menyeluruh. Untuk menghadapi ancaman siber yang semakin kompleks di masa

depan, Indonesia perlu memperkuat koordinasi nasional, meningkatkan kapasitas sumber daya manusia, mempercepat penyusunan regulasi terkait, dan memperluas kerja sama internasional di bidang keamanan siber.

Indonesia saat ini membutuhkan regulasi komprehensif yang mengatur mengenai keamanan dan ketahanan siber, mengingat hukum positif yang ada belum menjangkau hal ini. hukum positif *di bidang siber yang ada di* Indonesia saat ini lebih berfokus pada tindakan reaktif hukum pasca insiden. Perkembangan *international cyber law* menunjukan pendekatan yang mulai berubah, berupa pendekatan hulu (*upstream regulation*) yang diformulasikan untuk tindakan mitigasi risiko dan pencegahan sejak level hulu. Di samping itu, juga perlu dilakukan pendekatan proses berupa *middle-stream approach* dimana regulator secara aktif melakukan monitoring, evaluasi, dan/atau asesmen terhadap Infrastruktur Informasi Kritikal dan infrastruktur informasi yang memenuhi kriteria tertentu agar dapat mengatasi berbagai ancaman siber.

Selain itu, pendekatan hilir (*downstream regulation*) tetap digunakan. Formulasinya adalah menggunakan hukum positif yang ada dan juga membuat materi muatan terkait hal dimaksud dalam Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS).

2. Kondisi yang ada

Kondisi Perkembangan teknologi yang ada saat ini sangat berpengaruh terhadap berbagai sendi kehidupan masyarakat. Salah satu dampak dari hadirnya teknologi adalah kehadiran dunia siber. Saat ini, lembaga pemerintah yang bertanggung jawab atas keamanan, Pelindungan, dan kedaulatan siber nasional dipegang wewenangnya oleh BSSN. BSSN dibentuk berdasarkan penggabungan lembaga yang telah ada sebelumnya, yakni Lembaga Sandi Negara dan Direktorat Keamanan Informasi serta Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan

Digital.[62] Kondisi dunia siber yang semakin menjangkau manusia di dunia membuat meningkatnya ancaman terhadap dunia siber saat ini.

Berdasarkan hasil *Global Cybersecurity Index (GCI) 2024* yang dirilis oleh International Telecommunication Union (ITU), Indonesia menunjukkan kemajuan signifikan dalam pembangunan ekosistem keamanan siber nasional. Indonesia berhasil naik ke kategori *Tier* 1 (*role-modeling countries*), yang menempatkannya sejajar dengan negara-negara maju seperti Amerika Serikat, Jepang, dan Singapura dalam komitmen terhadap tata kelola keamanan siber. Peningkatan ini mencerminkan penguatan kerangka hukum, kelembagaan, serta strategi nasional yang dikembangkan melalui peran BSSN sebagai otoritas koordinatif di bidang keamanan siber. Keberhasilan tersebut tidak terlepas dari upaya pemerintah memperkuat aspek regulasi, kesiapsiagaan teknis, peningkatan kapasitas sumber daya manusia, dan kolaborasi internasional dalam menghadapi ancaman siber lintas batas.

Meskipun demikian, tantangan substantif masih dihadapi, antara lain dalam implementasi kebijakan di tingkat operasional, keterbatasan sumber daya manusia ahli di bidang keamanan siber, ketimpangan kesiapan antar sektor dan daerah, serta meningkatnya kompleksitas ancaman seperti *ransomware*, *phishing*, kebocoran data, dan disinformasi digital. Selain itu, kebutuhan akan penguatan Pelindungan data pribadi, keamanan infrastruktur informasi vital, serta penegakan hukum atas tindak kejahatan siber masih menjadi prioritas nasional. Kondisi ini menunjukkan urgensi pembentukan kerangka hukum yang lebih komprehensif melalui RUU KKS sebagai dasar hukum nasional yang mampu memperkuat tata kelola keamanan siber, meningkatkan resiliensi nasional terhadap ancaman digital, dan

[62] Issha Harumma, Kompas.com, "Badan Siber dan Sandi Negara: Sejarah, Tugas, dan Fungsinya", 2022, <https://nasional.kompas.com/read/2022/09/16/05050021/badan-siber-dan-sandi-negara--sejarah-tugas-dan-fungsinya> diakses pada 11 Oktober 2024.

memastikan kedaulatan siber Indonesia di tengah dinamika global yang semakin kompleks. [63]

Pada tahun 2024, permasalahan siber banyak terjadi dan menjadi isu hukum yang cukup besar di Indonesia. Kebocoran data dan serangan terhadap Pusat Data Nasional (PDN) pada bulan Juni 2024 silam, pencatutan NIK KTP untuk mendukung calon independen dalam pemilihan gubernur di sejumlah daerah, serta sejumlah kasus lainnya menandakan bahwa masih krisisnya keamanan dan pertahanan siber di Indonesia.

Menurut pendapat pengamat militer dan pertahanan dari *Institute for Security and Strategic Studies* (ISESS) Khairul Fahmi, bahwa peretasan serta serangan yang terjadi menunjukan bahwa terjadi kerentanan dalam sistem pertahanan siber. Dengan peretasan yang terjadi terus berulang, menandakan selain adanya kerentanan, juga terdapat banyak problem yang mendasari serangan siber di Indonesia. Selain aspek masyarakat yang belum menaruh perhatian serta kepedulian secara khusus untuk melindungi dirinya dari ancaman siber, Khairul Fahmi juga berpendapat kurangnya kepedulian, kesadaran, serta perhatian pemerintah dalam mencegah ancaman ini. Serangan siber seringkali diawali oleh kelalaian pemerintah yang memiliki akses masuk ke sistem data atau jaringan.[64]

Masalah lain dari rentannya keamanan dan ketahanan siber di Indonesia adalah masih lemahnya regulasi terkait tata kelola keamanan dan ketahanan siber.

Hal ini pada akhirnya mengakibatkan upaya mitigasi, pengawasan, pengelolaan, dan penanggulangan insiden siber menjadi tidak optimal dan memiliki banyak hambatan. Peran BSSN untuk menjamin keamanan siber menjadi tidak maksimal karena BSSN tidak memiliki kewenangan yang berkaitan dengan upaya investigasi insiden siber dan penanganan serangan siber. Oleh

[63]Global Cybersecurity Index Report 2024.
[64] CNN Indonesia, *Op.Cit*.

karena itu diperlukan peran bagi instansi Pemerintah yang melaksanakan tugas di bidang keamanan dan ketahanan siber untuk melakukan audit teknis terhadap insiden yang terjadi pada IIK. Ketentuan mengenai audit teknis dalam RUU KKS merupakan landasan hukum yang penting dalam upaya memperkuat penanganan insiden siber di Indonesia. Audit teknis didefinisikan sebagai proses pemeriksaan, penelusuran, dan pengumpulan fakta secara sistematis untuk mengungkap penyebab, modus, dampak, serta pihak yang bertanggung jawab atas terjadinya suatu insiden siber. Pendekatan ini menempatkan audit teknis bukan hanya sebagai kegiatan teknis, tetapi juga sebagai instrumen akuntabilitas publik dalam memastikan transparansi dan keandalan tata kelola keamanan siber nasional.

Pemberian kewenangan kepada instansi pemerintah yang melaksanakan tugas dan fungsi di bidang keamanan dan ketahanan siber untuk melakukan audit teknis merupakan langkah strategis dalam menjamin adanya otoritas tunggal yang kompeten dan independen. Kewenangan ini diperlukan untuk menghindari tumpang tindih fungsi antarinstansi serta memastikan proses penanganan insiden siber dilakukan secara profesional, terkoordinasi, dan berbasis bukti digital (digital evidence). Kewenangan tersebut juga sejalan dengan praktik internasional, di mana lembaga otoritas siber nasional seperti *Cybersecurity* and Infrastructure Security Agency (CISA) di Amerika Serikat atau National *Cyber* Security Centre (NCSC) di Inggris memiliki mandat serupa untuk melaksanakan investigasi teknis terhadap insiden yang berpotensi mengancam infrastruktur kritikal nasional.

Kewajiban bagi Penyelenggara IIK untuk memberikan data, informasi yang valid, serta akses terhadap sistem terdampak, merupakan bentuk tanggung jawab bersama dalam menjaga ketahanan siber nasional. Dalam konteks tata kelola risiko siber, kerja sama dan keterbukaan antara penyelenggara dan instansi

pemerintah menjadi elemen penting dalam proses pemulihan dan mitigasi dampak insiden. Prinsip ini sejalan dengan kerangka kerja NIST *Cybersecurity Framework* (NIST CSF 2.0) yang menekankan pentingnya proses respond dan recover berbasis kolaborasi lintas sektor.

Tumpang tindihnya pengaturan dalam tata kelola ini, tentu menjadi masalah sendiri dalam upaya pengaturan siber di Indonesia. Dengan begitu, diperlukan pembagian kewenangan yang jelas bagi pihak terkait dalam mengantisipasi, mengelola, menangani, dan menanggulangi insiden siber, agar mampu memberikan pelindungan yang maksimal terhadap dunia siber di Indonesia.

3. Permasalahan yang Dihadapi

Dengan semakin berkembangnya teknologi yang menimbulkan banyak dampak positif, seperti efisiensi dalam pekerjaan, kemudahan akses informasi, dan percepatan komunikasi, perkembangan ini tidak luput dari dampak negatif yang juga muncul. Peralihan dari zaman konvensional menjadi serba digital, meskipun menawarkan banyak kemudahan, juga menghadirkan risiko baru, terutama terkait dengan keamanan siber. Permasalahan ketahanan dan keamanan siber di Indonesia mencakup berbagai aspek yang saling terkait, mulai dari regulasi, teknologi, hingga kesadaran masyarakat.

Keamanan siber khususnya terhadap IIK merupakan hal yang tak dapat ditawar-tawar mengingat, gangguan sekecil apapun terhadap Infrastruktur Informasi, seperti infrastruktur listrik, air, telekomunikasi, keuangan dan perbankan, kesehatan, transportasi, akan mempengaruhi layanan umum terhadap masyarakat. Gangguan terkait hal ini berdampak sangat signifikan. Oleh karena itu, keberadaan undang-undang yang mengatur keamanan dan ketahanan siber merupakan sebuah keniscayaan.

Masyarakat juga perlu dibangun kesadarannya, khususnya terkait dengan pentingnya keamanan dan ketahanan siber. Budaya keamanan dan ketahanan siber tidak hanya penting untuk regulator dan pelaku usaha, tetapi juga perlu diamplifikasikan kepada seluruh masyarakat.

Salah satu kelemahan saat ini adalah belum optimalnya pengawasan terhadap penyelenggara infrastruktur informasi, khususnya IIK. Hal ini disebabkan karena belum adanya pengaturan yang komprehensif dan memiliki dasar hukum yang kuat. Oleh karena itu, RUU KKS perlu segera dibentuk dan diundangkan untuk menjawab tantangan dan persoalan yang sudah di depan mata bahkan insidennya sudah terjadi.

Selain kesadaran masyarakat yang masih rendah, permasalahan lain yang dihadapi adalah kurangnya infrastruktur keamanan siber yang memadai. Banyak organisasi belum memiliki sistem keamanan yang kuat untuk melindungi data pribadi dan aset digital mereka dari serangan siber. Meskipun telah ada regulasi yang mengatur keamanan siber seperti UU ITE, KUHP, dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik, implementasi di lapangan masih belum optimal. Organisasi seringkali hanya mengikuti peraturan secara formal tanpa benar-benar mengembangkan infrastruktur keamanan siber yang memadai.[65]

Banyaknya insiden kebocoran data, termasuk kasus peretasan data BPJS Kesehatan dan berbagai kementerian menimbulkan kerugian besar bagi masyarakat. Hal ini juga disebabkan masih rendahnya kesadaran masyarakat serta lemahnya regulasi dan penegakan hukum. Meskipun telah ada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, namun implementasinya masih terhambat dengan ketiadaan aturan yang

[65] Cindy Vania, (et.al), ″Tinjauan Yuridis terhadap Pelindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber ,″ Jurnal Multidisiplin Indonesia, Vol. 2, Nomor 3, Maret 2023.

spesifik mengenai keamanan dan ketahanan siber.

Indonesia juga menempati peringkat teratas dalam kasus pembobolan data se-ASEAN.[66] Dalam hal teknologi, perkembangan media sosial dan perangkat digital lainnya telah membuka peluang bagi peretasan dan serangan siber, terutama dengan adanya ketergantungan yang tinggi pada layanan digital dari perusahaan asing seperti Google dan Facebook. Sebagian besar pusat data dari perusahaan-perusahaan besar ini tidak berlokasi di Indonesia, yang menyebabkan kelemahan dalam kedaulatan data. Kedaulatan data sangat bergantung pada keberadaan pusat data di wilayah negara, yang memungkinkan negara memiliki kendali lebih kuat terhadap Pelindungan dan penggunaan data warganya.[67]

Melihat berbagai permasalahan di atas, solusi ~~yang~~ komprehensif untuk memperkuat ketahanan siber di Indonesia menjadi hal yang mendesak. Salah satu pendekatan yang bisa diambil dengan memperkuat kerangka regulasi yang mengatur Keamanan Siber secara menyeluruh. Pengesahan RUU KKS dapat menjadi langkah awal untuk menciptakan lingkungan siber yang aman dan terjaga bagi II dan IIK. RUU ini diharapkan tidak hanya mencakup aturan teknis mengenai pelindungan data dan penanggulangan serangan siber, tetapi juga memperkuat kolaborasi antara pemerintah, sektor swasta, dan masyarakat dalam hal pencegahan dan respons terhadap ancaman siber.

Di sisi lain, perlu ada peningkatan kesadaran dan literasi digital masyarakat untuk memperkuat ketahanan siber di tingkat individu. Pemerintah, institusi pendidikan, dan organisasi non-pemerintah perlu bekerja sama dalam melakukan edukasi mengenai pentingnya keamanan digital dan cara melindungi data pribadi. Kampanye kesadaran mengenai risiko kejahatan siber dan

---

[66] Arnold Hiras Simorangkir dan Arthur Josias Simon Runturambi, *"Budaya & Masyarakat Digital dalam Ketahanan Siber di Indonesia: Sebuah Adaptasi dari Pendekatan Capacity Maturity Model (CMM),"* Jurnal Multidisiplin Indonesia, Vol. 5, Nomor 4, Juni–Juli 2024.

[67] M. Prakoso Aji, *"Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Pelindungan Data Pribadi)*," Politica, Vol. 13, Nomor 2 (November 2022).

pelatihan keterampilan dasar dalam mengenali serta menghindari ancaman siber, seperti *phishing* dan *malware*, akan sangat membantu dalam meminimalisasi potensi serangan siber. Dengan pendekatan multidimensi yang melibatkan perbaikan regulasi, infrastruktur, dan peningkatan literasi digital, Indonesia dapat membangun ekosistem digital yang lebih aman dalam menghadapi tantangan siber di masa depan.

4. Perbandingan Regulasi dan Kelembagaan dengan Negara Lain

Pengaturan hukum internasional mengenai keamanan dan ketahanan siber saat ini diatur dalam regulasi yang dikenal sebagai "*UN Convention Against Cybercrime*". Dalam Article 1 mengenai *Statement of purpose* dijelaskan tujuan dari konvensi ini yaitu untuk:[68]

a. Mempromosikan dan memperkuat langkah-langkah untuk mencegah dan memerangi kejahatan siber secara lebih efisien dan efektif.
b. Mempromosikan, memfasilitasi, dan memperkuat kerja sama internasional dalam mencegah dan memerangi kejahatan siber.
c. Mempromosikan, memfasilitasi, dan mendukung bantuan teknis dan pengembangan kapasitas teknis dan pengembangan kapasitas untuk mencegah dan memerangi kejahatan siber, khususnya untuk negara berkembang.

Konvensi ini juga akan menjadi wadah untuk mencegah dan memberantas kejahatan siber termasuk eksploitasi seksual anak dan pencucian uang sekaligus meningkatkan kerja sama internasional, penegakan hukum, bantuan teknis dan pengembangan kapasitas yang berkaitan dengan kejahatan siber.[69] Isi dari konvensi ini mencakup beberapa aspek penting seperti:

[68] Article 1 UN Convention Against Cybercrime
[69] Ahmad M Ramli, (2024), ""UN Convention Against Cybercrime": Konvensi Pertama PBB Tentang Kejahatan Siber (Bagian I), <https://tekno.kompas.com/read/2024/08/19/09445517/un-convention-against-cybercrime-konvensi-pertama-pbb-tentang-kejahatan-siber?page=all#page2> diakses pada 29 September 2024.

a. Pengaturan hukum

   Setiap negara pihak harus mengadopsi Undang-Undang dan tindakan lainnya yang diperlukan untuk menetapkan pelanggaran hukum di bawah hukum domestiknya, seperti akses ilegal ke sistem teknologi informasi dan komunikasi (ICT) dan intersepsi ilegal.

b. Kerja sama internasional

   Konvensi ini bertujuan untuk meningkatkan koordinasi dan kerja sama antar negara dalam mencegah dan menghadapi kejahatan siber, termasuk pertukaran bukti digital dan kerja sama penegakan hukum di tingkat nasional, regional, dan internasional.

c. Bantuan teknis dan pembangunan kapasitas

   Konvensi ini menyediakan bantuan teknis dan pembangunan kapasitas bagi negara-negara, terutama negara-negara berkembang, untuk meningkatkan kemampuan mereka dalam menghadapi kejahatan siber. Ini termasuk transfer teknologi pada syarat yang disepakati bersama dan bantuan untuk meningkatkan Undang-Undang dan kerangka kerja nasional.

Selain *UN Convention Against Cybercrime*, terdapat juga Undang-Undang Ketahanan Siber (EU *Cyber* Resilience Act/CRA) yang telah disahkan oleh Uni Eropa sebagai upaya dalam menghadapi ancaman siber global.[70] Undang-undang ini bertujuan untuk memastikan ketangguhan produk dengan elemen digital dalam menghadapi ancaman siber global serta menjadi dasar dalam pembentukan *European Cybersecurity Agency* (ENISA) yang berperan dalam menghadapi peretasan dan kejahatan siber. Adapun materi muatan yang diatur dalam EU CRA yaitu:

a. Persyaratan keamanan siber sejak perencanaan, desain, pengembangan dan pemeliharaan produk.

[70] Ahmad M Ramli, (2024), "EU CRA: UU Baru Uni Eropa Menghadapi Peretasan Siber Global", <https://tekNomorkompas.com/read/2024/07/26/10441617/eu-cra-uu-baru-uni-eropa-menghadapi-peretasan-siber-global?page=all> [29/09/2024]

b. PDE perangkat lunak dan produk yang terhubung ke internet yang telah memenuhi persyaratan akan memiliki tanda “CE” sebagai bukti bahwa produk tersebut telah memenuhi standar baru.
c. Produsen dan pengecer wajib memprioritaskan keamanan siber sehingga pelanggan dan bisnis bisa membuat pilihan yang tepat.
d. Penerapan perlakuan khusus, contohnya pada perangkat lunak atau layanan *open source* yang sudah tercakup oleh regulasi yang ada.
e. EU CRA mengancam setiap pelanggaran atau ketidakpatuhan dengan sanksi denda dan pinalti yang berat, dimana setiap negara anggota EU dapat menentukan nilai dendanya sendiri dan melaporkannya ke ENISA.

Keamanan dan ketahanan siber merupakan dua aspek penting dalam menghadapi tantangan di dunia digital saat ini. Di tingkat regional, berbagai aturan dan kebijakan telah dikembangkan untuk memastikan Pelindungan terhadap IIK dan data sensitif. Sedangkan kebijakan keamanan siber di Indonesia, bertujuan untuk mengaitkan keamanan siber dengan ketahanan siber. Keduanya bertujuan untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Ini menunjukkan bahwa pendekatan yang komprehensif diperlukan untuk melindungi data dan sistem dari ancaman siber. Penerapan keamanan dan ketahanan siber yang dipraktikkan di Indonesia masih dalam skala nasional yang masih tersebar di berbagai lembaga atau instansi pemerintah seperti Kementerian Pertahanan dan Kepolisian Negara Republik Indonesia.

Hal ini disebabkan belum adanya peraturan perundang-undangan yang secara khusus mengatur keamanan dan ketahanan siber serta penerapan keamanan dan ketahanan siber belum terpadu dan terintegrasi. Di Indonesia, regulasi yang ada masih sangat terbatas dan memiliki kelemahan dalam melindungi

infrastruktur siber. Beberapa regulasi yang saat ini terkait dengan keamanan siber antara lain Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, dan Undang-Undang Nomor 43 Tahun 2008 tentang Wilayah Negara. Regulasi yang dijadikan payung hukum untuk masalah ini misalnya merujuk pada Undang-Undang ITE dan Peraturan Pemerintah PSTE.

Selain itu, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran, dan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, masih memiliki keterbatasan dalam konteks infrastruktur telekomunikasi, penyiaran, dan informatika untuk pelayanan publik. Peraturan pemerintah yang ada juga belum mengatur peran pemerintah dalam sistem keamanan dan ketahanan siber, sehingga pemanfaatannya untuk keamanan siber masih sangat terbatas. Salah satu upaya pemerintah dalam menangani ancaman dan serangan siber dapat dilihat dari adanya Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. namun pedoman tersebut disusun sebagai acuan tahapan penyiapan, pembinaan, pelaksanaan, dan pemantapan pertahanan siber hanya di lingkungan Kementerian Pertahanan dan TNI. Kemudian, dalam Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara juga memiliki keterbatasan untuk melakukan spionase siber maupun untuk melakukan penanggulangan serangan siber secara terbatas.[71]

Pada tahun 2017, BSSN resmi dibentuk oleh Pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden melalui menteri yang mengoordinasikan, menyinkronkan, dan mengendalikan penyelenggaraan pemerintahan di bidang politik, hukum, dan keamanan. Badan Siber dan Sandi Negara bertugas untuk menyelenggarakan keamanan siber secara efektif dan efisien

[71] *Ibid,* hlm. 33

dengan mendayagunakan, mengembangkan, meningkatkan, dan mengonsolidasikan seluruh unsur yang terkait dengan keamanan siber.

Kemudian badan ini bertujuan untuk melindungi kegiatan siber nasional tanpa melanggar hak individu atau perusahaan dalam pemanfaatan internet, sehingga jelas bahwa badan ini tidak akan mencampuri ranah pribadi pengguna internet. Namun, karena belum adanya regulasi yang jelas, koordinasi antar lembaga belum berjalan efektif dan masih berjalan sesuai dengan pedoman lembaga masing-masing. Praktik penyediaan keamanan dan ketahanan siber dapat dilihat pada lembaga Kementerian Pertahanan. Kementerian Pertahanan membentuk Pusat Pertahanan Siber (Pushansiber) yang bertugas melaksanakan tata kelola, kerja sama, operasi, dan jaminan pertahanan siber. Pushansiber berperan aktif dalam forum keamanan internasional tahunan yang berfokus pada kelompok kerja siber dan terlibat dalam berbagai diskusi kelompok fokus tentang kedaulatan siber dan data.[72]

Selanjutnya, TNI telah membentuk Satuan Siber (Satsiber) untuk melaksanakan kegiatan dan operasi pertahanan siber. Satsiber yang ada saat ini merupakan organisasi satuan tugas yang bertugas melaksanakan kegiatan dan operasi siber di lingkungan TNI dalam rangka mendukung tugas pokok TNI. Satsiber yang ada saat ini telah menjadi satuan kerja yang memiliki fungsi sebagai pengawasan dan pertahanan dalam menghadapi serangan siber dan kejahatan siber, memberikan respon cepat dan tanggap darurat, serta melapor kepada pimpinan TNI dalam rangka pengamanan institusi TNI dari ancaman kejahatan dan serangan siber.

Ada empat fungsi yang dimiliki Satsiber TNI, yaitu pendeteksian, pelindungan, pemulihan, dan memastikan sistem

[72] *ibid*

siber yang ada tidak terdapat celah atau kekurangan yang dapat dimasuki *malware* atau *backdoor*. Selain itu, di ~~tubuh~~ Kepolisian Negara Republik Indonesia terdapat Direktorat Tindak Pidana Siber (Dittipidsiber) yang berada di bawah Bareskrim Polri dengan fokus tugas melakukan penegakan hukum terhadap kejahatan siber yang secara umum terbagi menjadi kejahatan komputer dan kejahatan terkait komputer. Bentuk kejahatannya adalah peretasan sistem elektronik, penyadapan ilegal, perusakan web, gangguan sistem, dan manipulasi data. Kedua, kejahatan siber yang menggunakan komputer sebagai alat, seperti pornografi daring, perjudian daring, pencemaran nama baik daring, pemerasan daring, penipuan daring, ujaran kebencian, pengancaman daring, akses ilegal, dan pencurian data.[73]

Badan Intelijen Negara juga telah membentuk Deputi Siber yang bertugas mendukung kinerja BIN dalam tugas intelijen yang belum optimal apabila hanya mengandalkan kecerdasan manusia dan harus diperkuat dengan intelijen siber. Keberadaan Deputi tersebut menjalankan fungsi penyusunan rencana kegiatan dan/atau operasi intelijen siber, pelaksanaan kegiatan dan/atau operasi intelijen siber, koordinasi kegiatan dan/atau operasi intelijen siber, pengendalian kegiatan dan/atau operasi intelijen siber, dan penyusunan laporan intelijen siber. [74]

Menanggapi serangan siber tersebut, Kementerian Komunikasi dan Digital (dahulu Kementerian Komunikasi dan Informatika) telah membentuk tim yang bernama ID-SIRTII/CC *(Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center)* untuk memastikan keamanan internet di Indonesia. ID-SIRTII/CC dibentuk dengan tujuan untuk mendukung pelaksanaan proses penegakan hukum, menciptakan lingkungan dan pemanfaatan jaringan telekomunikasi berbasis protokol internet yang aman dari berbagai ancaman dan gangguan,

[73] *Ibid,* hlm. 33-34
[74] *Ibid,* hlm.34

serta mendukung pelaksanaan koordinasi dengan pihak terkait baik di dalam maupun di luar negeri dalam upaya pencegahan, deteksi, peringatan dini dan mitigasi insiden pada IIK. ID-SIRTII/CC telah berupaya melakukan pemantauan trafik anomali internet nasional sejak Januari sampai dengan Desember 2018, sebanyak 232.447.974 (dua ratus tiga puluh dua juta empat ratus empat puluh tujuh sembilan ratus tujuh puluh empat) serangan siber telah ditemukan pada jaringan Indonesia.[75]

Beberapa pengaturan di negara lain yaitu:

a. Pengaturan Keamanan dan Ketahanan Siber di Uni Eropa

1) *European Union Cyber Resilience Act (EU CRA)*

Kurangnya keamanan siber yang tepat pada produk dengan elemen digital di Uni Eropa disebabkan oleh kegagalan regulasi dan kemampuan pasar untuk mencegah hal tersebut. Hal ini dapat membahayakan keselamatan masyarakat dalam penggunaan produk yang mengandung elemen digital. Dari segi ekonomi, kegagalan pasar dalam memberikan keamanan siber dapat memberikan permasalahan dari segi konsumen dengan menurunnya permintaan terhadap produk, dan mengancam tingkat investasi yang dapat diberikan dari produk-produk tersebut.[76] Faktor-faktor tersebut yang mendasari Komisi Uni Eropa untuk menghadirkan Undang-Undang Ketahanan Siber yang baru. Pada 12 Maret 2024, Parlemen Eropa menyetujui Undang-Undang Ketahanan Siber Uni Eropa atau yang dikenal dengan nama *EU Cyber Resilience Act* (CRA).

Berbeda dengan EU *Cybersecurity* Act yang telah disahkan sebelumnya oleh Uni Eropa untuk mengatur kerangka kerja keamanan siber Uni Eropa, EU CRA merupakan regulasi yang bertujuan untuk meningkatkan

[75] *Ibid*

[76] Proposal untuk Peraturan Parlemen Eropa dan Dewan tentang produk mesin, COM (2021) 202 final.

ketahanan siber dari produk dan layanan yang dijual di pasar Uni Eropa.[77] Kehadiran EU CRA bertujuan untuk melengkapi EU *Cybersecurity* Act, guna memberikan pelindungan yang menyeluruh terhadap keamanan dan ketahanan siber. EU CRA merupakan instrumen hukum yang mengatur ketahanan dan desain keamanan produk, dimana produsen, penyedia layanan maupun distributor dari suatu produk yang dipasarkan, harus mampu memenuhi standar keamanan siber sesuai dengan klasifikasi risiko yang dimilikinya.[78]

Selain itu, produsen dan distributor juga dituntut mampu untuk bertanggung jawab terhadap persebaran produk dari ancaman siber di kemudian hari. EU CRA berupaya membangun ekosistem yang baik agar dapat menciptakan produk yang terpercaya dan mampu memacu pertumbuhan industri, yang diiringi dengan pelindungan yang optimal terhadap konsumen atau pengguna. EU CRA mengatur ketentuan terhadap produk yang mengandung elemen digital di dalamnya. Produk dengan elemen digital yang diatur dalam EU CRA mencakup perangkat lunak sebagai produk yang terpisah dari perangkat keras. Akan tetapi, terdapat pembatasan perangkat lunak yang diatur oleh CRA, bahwa CRA tidak mencakup perangkat lunak sebagai layanan, dan perangkat lunak yang bersifat gratis dan sumber terbuka tidak termasuk dalam cakupan Proposal, agar tidak menghambat inovasi penelitian.

Terdapat pengecualian lainnya, bahwa CRA tidak akan berlaku untuk produk dengan elemen digital yang sudah dalam ruang lingkup beberapa peraturan lain,

[77] Ahmad M Ramli, Kompas.com, "EU CRA: UU Baru Uni Eropa Menghadapi Peretasan Siber Global", 2024, https://tekNomorkompas.com/read/2024/07/26/10441617/eu-cra-uu-baru-uni-eropa-menghadapi-peretasan-siber-global?page=all diakses pada 28 September 2024.
[78] Article 5 EU CRA.

seperti peraturan EU tentang Perangkat Medis, Peraturan EU tentang persetujuan tipe otomotif, dan peraturan EU untuk penerbangan sipil.[79] Selain itu, CRA juga akan dikecualikan terhadap produk-produk digital yang secara eksklusif dikembangkan untuk keamanan nasional, tujuan militer, atau yang secara khusus dirancang untuk memproses informasi rahasia.[80] Dalam instrumen hukum ini juga diatur bahwa EU CRA menerapkan model "*Digital Upstream Regulation*" dengan pendekatan berbasis risiko. EU CRA mengkategorikan Produk Dengan Elemen Digital (PDED) menjadi kategori PDE default, dan PDE kategori Kritikal. Kategori Kritikal kemudian dibagi menjadi dua sub kategori, Kritikal kelas I dan Kritikal kelas II.[81]

Namun, untuk mengatasi kekhawatiran dunia industri, Uni Eropa menegaskan bahwa 90 persen produk PDE termasuk ke dalam Default yang hanya cukup menerapkan *self assessment*. Undang-Undang ini juga nantinya akan memiliki keterkaitan dengan regulasi sebelumnya yang telah mengatur terkait produk atau perangkat dengan elemen digital guna memberikan kesinambungan peraturan. Dalam EU CRA, diatur kewajiban untuk menyediakan layanan perawatan selama siklus penggunaan produk tersebut. Hal ini berarti EU CRA mengatur pelindungan terhadap produk dan layanan, mulai dari produk dan layanan tersebut dipasarkan hingga digunakan oleh konsumen.

PDE perangkat lunak dan produk yang terhubung ke internet, yang telah memenuhi persyaratan, nantinya akan diberikan tanda "CE", yang menandakan bahwa

[79] Article 2 (3) CRA
[80] Pier Giorgio Chiara, "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements", Int. Cybersecur. Law Rev. ,2022, hlm. 258-259.
[81] Ahmad M Ramli, "EU CRA: UU Baru Uni Eropa Menghadapi Peretasan Siber Global", Op.Cit.

produk telah mematuhi standar tersebut.[82] Selanjutnya, produsen dan distributor diwajibkan untuk memprioritaskan keamanan siber, guna memberikan pelindungan yang maksimal kepada penggunanya.[83] Selanjutnya, apabila terjadi insiden terhadap produk dengan elemen digital maka produsen, distributor, bahkan konsumen ataupun pihak lain dapat melaporkan kerentanan ataupun kerugian yang terjadi akibat ancaman siber kepada *Computer Security Incident Response Team* (CSIRT) yang ditunjuk sebagai koordinator ataupun Badan Keamanan Siber Uni Eropa (ENISA).[84]

Dari segi kelembagaan, EU CRA mengamanatkan ENISA sebagai komisi yang ~~dapat~~ mengatur kepatuhan dan segala hal yang berkaitan terhadap EU CRA. ENISA bertugas untuk mengembangkan kebijakan, kerangka kerja sertifikasi, koordinasi antar lembaga, mengawasi sertifikasi, menyiapkan panduan teknis maupun kebijakan lainnya guna memastikan produsen, penyedia layanan, maupun distributor mematuhi ketentuan regulasi EU CRA.[85] Dalam praktiknya, untuk mengawasi terkait pelanggaran, kepatuhan, dan menindaklanjuti insiden terkait kepatuhan terhadap EU CRA dilakukan oleh CSIRT.[86] Selanjutnya, untuk memastikan kepatuhan terhadap produsen, penyedia layanan, maupun distributor terhadap regulasi ini, EU CRA menetapkan ancaman denda yang cukup besar dan bervariasi antara satu negara dengan negara lainnya. Setiap negara dapat menentukan nilai dendanya sendiri dan melaporkannya

[82] Article 8 & 27 EU CRA
[83] Article 13 EU CRA.
[84] Article 15 EU CRA.
[85] Article 14 EU CRA.
[86] Article 14 EU CRA.

kepada ENISA. Namun, sebagai patokannya, denda dapat ditetapkan berkisar antara 5-15 juta lima sampai dengan lima belas) Euro, atau 1 (satu) hingga 2,5 (dua koma lima) persen dari omzet tahunan di seluruh dunia, tergantung pada keseriusan pelanggaran. Mana yang lebih tinggi, maka itulah yang akan dikenakan kepada pelanggar.[87] Akan tetapi, terdapat beberapa pengecualian terhadap pelanggaran tersebut, seperti misalnya pelanggar tergolong ke dalam kategori usaha kecil, mikro, dan menengah, dan ketentuan lainnya.[88]

2) *European Union Artificial Intelligence Act (EU AI Act)*

Kemajuan teknologi yang semakin berkembang pesat kian mempengaruhi penemuan-penemuan baru, dimana salah satu penemuan utamanya adalah kecerdasan buatan atau *Artificial Intelligence* (AI). Kehadiran AI yang dinilai semakin canggih, dengan kemampuannya untuk berpikir, memutuskan, dan bertindak atas kemauannya, membawa dampak yang disruptif terhadap berbagai struktur kehidupan sosial masyarakat.[89] Dalam menghadapi dan menyertai kemajuan teknologi AI, Uni Eropa menjadi inisiator dari Undang-Undang Kecerdasan Buatan yang dikenal dengan nama *European Artificial Intelligence Act ("EU AI Act"*) yang telah disahkan oleh parlemen Uni Eropa pada tanggal 13 Maret 2024 lalu. Disahkannya EU AI Act, menjadikannya kerangka hukum horizontal komprehensif pertama untuk regulasi sistem AI di seluruh Uni Eropa.[90] EU AI Act mulai berlaku di 27

[87] Article 64 EU CRA.
[88] Article 64 EU CRA.
[89] Eka Nanda dan Lintang Yudhantaka, "Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia", Notaire by Universitas Airlangga, Magister Kenotariatan, Vol. 5 Nomor 3, 2022, hlm. 352.
[90] White & Case, "Long awaited EU AI Act becomes law after publication in the EU's Official Journal", 2024, https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal, diakses pada 28 September 2024.

(dua puluh tujuh) Negara Anggota UE pada tanggal 1 Agustus 2024, dan penegakan sebagian besar ketentuannya akan dimulai pada tanggal 2 Agustus 2026.

Berlakunya EU AI Act mendorong regulasi AI yang memungkinkan terkendalinya lingkungan pengembangan, pengujian, dan validasi sistem AI inovatif, dan pengujian inovasi AI dalam dunia nyata.[91] Dalam EU AI Act, prinsip keamanan dan ketahanan siber pada sistem AI diatur dengan mengklasifikasikan AI berdasarkan tingkatan risikonya. Dalam arti lain, semakin tinggi risiko yang ditimbulkan oleh sistem AI, maka akan mengakibatkan timbulnya kerugian bagi masyarakat yang lebih besar dan semakin ketat juga peraturan yang diberlakukan.[92] Kategorisasi tingkat risiko AI yang diatur dalam EU AI Act, diantaranya adalah sistem AI yang dilarang (termasuk sistem AI manipulatif), AI berisiko tinggi dimana diatur pula kewajiban dari penyedia/pengembang atau pengendali AI, dan AI berisiko kecil.[93] Berkaitan dengan sanksi yang berlaku pun berbeda-beda tergantung pada kategorisasi risiko AI tersebut.

Sanksi maksimum untuk ketidakpatuhan terhadap aturan EU AI Act tentang penggunaan AI yang dilarang adalah denda administratif yang lebih tinggi hingga EUR 35 (tiga puluh) juta atau 7% (tujuh persen) dari omzet tahunan di seluruh dunia (Pasal 99 (3) EU AI Act).[94] Sanksi untuk pelanggaran ketentuan tertentu lainnya dikenakan denda maksimum EUR 15 juta atau 3 persen

[91] Ahmad M. Ramli, dalam Kompas.com, "UU AI Uni Eropa Disahkan: Inspirasi Model Regulasi Indonesia (Bagian I)", https://tekNomorkompas.com/read/2024/05/24/10183587/uu-ai-uni-eropa-disahkan-inspirasi-model-regulasi-indonesia-bagian-i, diakses pada 28 September 2024.
[92] *Ibid.*
[93] EU Artificial Intelligence Act, "High-level summary of the AI Act", 2024, https://artificialintelligenceact.eu/high-level-summary/, diakses pada 28 September 2024.
[94] Pasal 99 (3) European Artificial Intelligence Act.

dari omzet tahunan di seluruh dunia, mana yang lebih tinggi.[95] Sanksi maksimum untuk penyediaan informasi yang tidak benar, tidak lengkap, atau menyesatkan kepada badan yang diberitahukan atau otoritas nasional yang kompeten adalah EUR 7,5 juta atau 1% (satu persen) dari omzet tahunan di seluruh dunia, mana yang lebih tinggi (Pasal 99(5) EU AI Act).[96] Untuk UKM dan perusahaan rintisan, denda untuk semua hal di atas dikenakan persentase atau jumlah maksimum yang sama, tetapi mana yang lebih rendah (Pasal 99 ayat 6 EU AI Act).[97]

EU AI *Act* menekankan langkah untuk mengidentifikasi, menganalisis, mengevaluasi, dan menangani eksposur kerugian, serta memantau pengendalian risiko untuk memitigasi dampak buruk yang diakibatkan dari pengembangan dan penggunaan AI.[98] Dalam menunjang ketahanan dan keamanan siber yang dicita-citakan tersebut, EU AI Act kemudian mengatur ketentuan mengenai kewajiban dari penyedia model AI, dimana dijelaskan dalam Pasal 55 EU AI *Act*, bahwa salah satu poin utamanya adalah memastikan tingkat pelindungan keamanan siber yang memadai untuk model AI tujuan umum dengan risiko sistemik dan infrastruktur fisik model tersebut.[99]

3) *European Union General Data Protection Regulation* (GDPR)

Salah satu peraturan yang juga mencakup kaitannya dengan Keamanan Siber, yakni peraturan milik Uni Eropa yang dikenal dengan *European Union General Data*

[95] Pasal 99 (4) European Artificial Intelligence Act.
[96] Pasal 99 (5) European Artificial Intelligence Act.
[97] Pasal 99 (6) European Artificial Intelligence Act.
[98] Ahmad M. Ramli, *Op.Cit*. (Note 10).
[99] Pasal 55 European Artificial Intelligence Act.

Protection Regulation (GDPR). GDPR merupakan regulasi pelindungan data yang berlaku di Uni Eropa dengan tujuan untuk melindungi privasi dan data pribadi individu di wilayah tersebut. GDPR secara resmi berlaku di Uni Eropa pada 25 Mei 2018 di 27 (dua puluh tujuh) negara anggota dan negara yang masuk dalam Europe Economic Area (EEA).[100] Regulasi ini mengatur bahwa setiap individu berhak mendapatkan informasi dengan jelas tentang apa yang dilakukan terhadap data mereka. Semua pihak yang ingin memproses data pribadi juga wajib untuk memperoleh *consent* dari pemilik data. Hal ini dilakukan untuk mendorong penggunaan dan pemrosesan data pribadi yang lebih bertanggung jawab.[101] GDPR memberikan tuntutan bagi perusahaan agar lebih akuntabel, transparan, bertanggung jawab pada data pribadi pengguna dan meningkatkan keamanan sibernya. GDPR memiliki efek ekstrateritorial yang berarti regulasi ini berlaku bagi semua pihak di manapun berada, termasuk yang berada di luar UE, selama mereka melakukan kegiatan pemrosesan data individu yang tinggal di kawasan UE dan EEA.[102]

Pemrosesan data pribadi menurut GDPR adalah termasuk kegiatan pengumpulan, perekaman, pengorganisasian, penataan, penyimpanan, pengambilan, dan penggunaan data pribadi residen UE.[103] GDPR disebut sebagai hukum keamanan data pribadi paling ketat dan paling kuat di dunia karena keketatan, sanksi

[100] Kedutaan Besar Republik Indonesia Brussel, "A Policy Brief EU General Data Protection Regulation (GDPR), Research Series: Embassy of The Republic of Indonesia In Brussels", 2021, Nomor 6. https://kemlu.go.id/download/L1NoYXJlZCUyMERvY3VtZW50cy9icnVzc2VsL3Jlc2VhcmNoJTIwc2VyaWVzL0dEUFIlMjAtJTIwdXBkYXRlZC5wZGY=, diakses pada 28 September 2024.
[101] *Ibid.*
[102] Ben Wolford, "Does the GDPR apply to companies outside of the EU?", pada laman GDPR, https://gdpr.eu/companies-outside-of-europe/, diakses pada 28 September 2024.
[103] Pasal 4 European Union General Data Protection Regulation (GDPR).

dan skala penerapannya. GDPR berlaku tidak hanya bagi perusahaan, organisasi, atau entitas lain yang berbasis di UE yang memproses data pribadi orang di UE. Aturan ini juga berlaku bagi organisasi yang ada di luar UE yang melakukan kegiatan pemrosesan data dan menarget orang yang tinggal di wilayah UE. GDPR memberlakukan sanksi dan denda yang sangat keras kepada pihak yang melakukan pelanggaran. Denda dan hukuman bagi pihak pelanggar bisa mencapai puluhan juta euro.

Dalam ruang lingkupnya, GDPR hanya berlaku bagi data pribadi, dimana data pribadi adalah informasi apa saja yang berkaitan dengan seorang individu yang masih hidup baik secara langsung maupun tidak langsung dapat mengidentifikasi individu tersebut.[104] Dalam melakukan pemrosesan data tersebut diatur pula ketentuan bahwa wewenang pemrosesan data ~~tersebut~~ dapat dilakukan oleh pengontrol data, yakni pihak yang memutuskan mengapa dan bagaimana data pribadi akan diproses, dan pemroses data, yakni pihak ketiga yang memproses data pribadi atas nama *data controller*.[105] Pelaksanaan GDPR sendiri dikawal ketat oleh suatu badan yang disebut sebagai *European Data Protection Board* (EDPB). Sementara itu, pengawasan di masing-masing negara dikawal oleh *Data Protection Authorities* (DPA) atau *Supervisory Authorities* (SA). EDPB bekerja sama dengan DPA dalam mengawal penerapan GDPR.

Berkaitan dengan sanksi, GDPR menyatakan secara eksplisit bahwa sejumlah pelanggaran memiliki tingkat pelanggaran yang lebih parah dari lainnya dan hal itu membuat denda pun berbeda-beda. Ada dua tingkat denda atas pelanggaran GDPR yakni pelanggaran yang

[104] Kedutaan Besar Republik Indonesia Brussel, Op.Cit. (Note 28)
[105] *Ibid.*

tidak terlalu parah, dan pelanggaran yang serius. Pada pelanggaran yang tidak terlalu parah, dapat mengakibatkan denda hingga €10 juta atau sebesar 2% (dua persen) dari pendapatan global tahunan perusahaan dari tahun keuangan sebelumnya, berapapun jumlah yang lebih tinggi.[106]

Sedangkan pada Pelanggaran serius, Pelanggaran serius merupakan pelanggaran melawan prinsip pelindungan data pribadi dan hak subyek. Ini dapat berdampak pada denda hingga €20 juta atau 4% (empat persen) dari pendapatan global perusahaan tahunan dari tahun keuangan sebelumnya, berapapun jumlah yang lebih tinggi.[107]

b. Pengaturan Keamanan dan Ketahanan Siber di Jepang (*The Basic Act on Cyber Security)*

Seiring kemajuan perkembangan teknologi, ancaman dari risiko kejahatan siber global pun semakin meningkat dan menjadi perhatian penting bagi banyak negara, salah satunya Jepang. Dalam rangka memenuhi kebutuhan untuk melindungi Infrastruktur Informasi Kritikal demi menjaga ketahanan serta keamanan siber, Jepang akhirnya mengesahkan undang-undang mengenai keamanan siber yang dikenal dengan nama *The Basic Act on Security* pada tanggal 5 November 2014. Undang-Undang ini dibuat dengan tujuan sebagai penetapan kebijakan dasar untuk inisiatif keamanan siber Jepang dengan memperjelas hal-hal yang mencakup tanggung jawab pemerintah pusat dan daerah, dan mengatur perumusan strategi keamanan siber dan hal-hal lain yang akan menjadi pondasi inisiatif keamanan

[106] Article 83 Paragraph (4) European Union General Data Protection Regulation (GDPR).
[107] Article 83 paragraph (4) European Union General Data Protection Regulation.

siber.[108] Selain itu, Undang-Undang tersebut dibentuk untuk menginisiasi keamanan siber secara komprehensif dan efektif. Jika dikaitkan dengan undang-undang di Jepang lainnya yaitu *Basic Act on the Formation of an Advanced Information and telecommunications Network Society* (Act Nomor 144 of 2000) dengan cara membentuk Markas Besar Strategis Keamanan Siber (*Cyber Security Strategic Headquarters*).[109]

Istilah Keamanan Siber atau "*cyber security*" yang digunakan dalam Undang-Undang tersebut mendefinisikan bahwa langkah-langkah yang diperlukan diambil untuk mencegah kebocoran, kehilangan, atau kerusakan informasi yang direkam, dikirim, ditransmisikan, atau diterima dalam bentuk elektronik, bentuk magnetik, atau bentuk lain yang tidak dapat dirasakan oleh indera manusia *(unintangible).*[110] Melalui *The Basic Act on Cyber Security,* Jepang ingin memastikan bahwa arus informasi yang bebas melalui pengembangan internet dan jaringan informasi dan telekomunikasi canggih lainnya serta melalui penggunaan teknologi informasi dan komunikasi menjadi perhatian yang penting.[111] Selain itu, kebijakan keamanan siber harus dikembangkan dengan prinsip untuk meningkatkan kesadaran masyarakat mengenai keamanan siber dan mendorong untuk mengambil tindakan sukarela untuk membangun sistem yang tangguh yang dapat mencegah kerusakan yang disebabkan oleh ancaman terhadap keamanan siber dan dengan cepat pulih dari kerusakan atau kegagalan.[112]

[108] Article 1 *The Basic Act on Cybersecurity*
[109] *Ibid.*
[110] Article 2 *The Basic Act on Cybersecurity*
[111] Article 3 (1) *The Basic Act on Cybersecurity*
[112] Article 3 (2) *The Basic Act on Cybersecurity*

Kebijakan Keamanan Siber harus dikembangkan dengan prinsip untuk mengembangkan Internet dan jaringan informasi dan telekomunikasi canggih lainnya, dan secara positif mempromosikan tindakan untuk membangun ekonomi dan masyarakat yang kritikal melalui pemanfaatan teknologi informasi dan komunikasi.[113]

Selanjutnya, Jepang melalui Undang-Undangnya juga menegaskan bahwa kebijakan siber harus dimajukan melalui kerja sama internasional dengan prinsip mengambil peran utama dalam perumusan dan pengembangan kerangka kerja keamanan siber internasional dengan mempertimbangkan fakta bahwa menanggapi ancaman keamanan siber adalah masalah umum di seluruh komunitas internasional, dan bahwa ekonomi dan masyarakat Jepang beroperasi dalam konteks hubungan yang erat dan saling bergantung secara internasional.[114] Namun, kebijakan tersebut tetap harus mempertimbangkan kembali prinsip-prinsip dasar dari Undang-Undang Dasar tentang Pembentukan Masyarakat Jaringan Informasi dan Telekomunikasi yang Maju[115], dan pengembangannya dengan tidak melanggar hak-hak masyarakat.[116]

Dalam ketentuannya, Undang-Undang ini mengatur beberapa kewajiban dan tanggung jawab diantaranya tanggung jawab pemerintah nasional untuk merumuskan dan melaksanakan kebijakan keamanan siber secara menyeluruh sesuai dengan asas-asas dasar[117], tanggung jawab pemerintah daerah untuk merumuskan dan

[113] Article 3 (3) *The Basic Act on Cybersecurity*.
[114] Article 3 (4) *The Basic Act on Cybersecurity*
[115] Article 3 (5) *The Basic Act on Cybersecurity*
[116] Article 3 (6) *The Basic Act on Cybersecurity*
[117] Article 4 *The Basic Act on Cybersecurity*

menerapkan kebijakan keamanan siber secara mandiri dengan mempertimbangkan peran yang tepat dengan pemerintah nasional[118], tanggung jawab penyedia infrastruktur sosial untuk memperdalam minat dan pemahamannya terhadap pentingnya keamanan siber[119], tanggung jawab badan usaha terkait dunia maya dan badan usaha lainnya yang bergerak di bidang siber untuk menyelenggarakan keamanan siber secara aktif[120], tanggung jawab organisasi pendidikan dan penelitian untuk wajib secara mandiri dan aktif berupaya menjamin keamanan siber dan membina sumber daya manusia terkait dengan keamanan siber, serta melakukan penelitian di bidang keamanan siber[121], dan tanggung jawab dan upaya masyarakat untuk memperdalam minat dan pemahaman terhadap pentingnya keamanan siber.[122]

Pada kebijakan dasar Undang-Undang ini, pemerintah pusat memiliki kewajiban yang utama dalam keamanan siber. Seperti dijelaskan bahwa pemerintah pusat berkewajiban menyediakan langkah-langkah seperti merumuskan standar, latihan dan praktik, penyebarluasan informasi, serta mendorong kegiatan sukarela lainnya dan langkah-langkah lain yang diperlukan terkait keamanan siber.[123] Selain itu pemerintah pusat berkewajiban meningkatkan koordinasi antar kementerian terkait langkah-langkah yang diperlukan untuk memungkinkan pemangku kepentingan seperti pemerintah pusat, pemerintah daerah, penyedia Infrastruktur Informasi Kritikal, dan

[118] Article 5 *The Basic Act on Cybersecurity*
[119] Article 6 *The Basic Act on Cybersecurity*
[120] Article 7 *The Basic Act on Cybersecurity*
[121] Article 8 *The Basic Act on Cybersecurity*
[122] Article 9 *The Basic Act on Cybersecurity*
[123] Article 14 *The Basic Act on Cybersecurity*

badan usaha yang terkait dengan dunia maya, untuk bekerja sama menyusun kebijakan keamanan siber secara terpadu.[124]

Selanjutnya, Pasal 17 Undang-Undang ini mengatur ketentuan mengenai Dewan Keamanan Siber, dimana bertugas untuk menyelenggarakan konsultasi yang diperlukan terkait dengan pengembangan kebijakan keamanan siber.[125] Dalam Pasal 17 ayat (4) diatur ketentuan bahwa setiap orang yang melaksanakan atau pernah melaksanakan tugas Dewan, dilarang membocorkan atau menyalahgunakan rahasia yang diketahuinya sehubungan dengan rincian tersebut tanpa alasan yang dapat dibenarkan.[126] Sejalan dengan hal itu, diatur pula ketentuan mengenai Markas Besar dari Dewan Keamanan Siber yang dapat mendelegasikan sebagian tugasnya kepada pihak-pihak yang diatur dalam Undang-Undang tersebut. Pasal 31 ayat (2) juga mengatur ketentuan bahwa Pegawai suatu perseroan yang telah diberi tugas atau orang yang pernah menduduki jabatan dewan tersebut dilarang membocorkan atau menyalahgunakan informasi rahasia yang diperoleh sehubungan dengan tugas, tanpa alasan yang dapat dibenarkan.[127] Untuk menjamin hal tersebut, Undang-Undang ini mengatur mengenai ketentuan pidana yakni pada BAB V, Pasal 38 yang menjelaskan bahwa Barang Siapa melanggar ketentuan Pasal 17 ayat (4) atau Pasal 31 ayat (2) dipidana dengan pidana penjara paling lama 1 (satu) tahun atau denda paling banyak 500,000 yen.[128]

[124] Article 16 *The Basic Act on Cybersecurity*
[125] Article 17 *The Basic Act on Cybersecurity*
[126] Article 17 (4) *The Basic Act on Cybersecurity*
[127] Article 31 (2) *The Basic Act on Cybersecurity*
[128] Article 38 The Basic Act on Cybersecurity

c. Pengaturan Keamanan dan Ketahanan Siber di Singapura

1) *Personal Data Protection Act* (PDPA)

Dengan berkembangnya teknologi sebagai penopang kehidupan masyarakat dunia, saat ini ancaman dan tantangan dari kejahatan siber pun semakin meningkat. Terlebih, di era digital saat ini, pelindungan mengenai data menjadi hal yang sangat penting, karena data di era digital ini merupakan hal yang sangat penting bagi setiap orang. Di Singapura, pengaturan mengenai pelindungan data diatur dalam *Personal Data Protection Act Nomor 26 of 2012 Singapore* (PDPA 2012 Singapura). Instrumen hukum ini memuat beberapa prinsip pelindungan data pribadi, diantaranya:

a) *Consent*, suatu organisasi dapat memperoleh, menggunakan atau membuka data pribadi seseorang apabila mendapat kesepakatan dari subjek data.

b) *Purpose,* suatu organisasi dapat memperoleh atau mengumpulkan, menggunakan dan membuka data pribadi seseorang dalam keadaan apapun, dan apabila mereka menginformasikan kepada subyek data tujuan dari diminta atau dikumpulkannya, digunakan dan diumumkannya data pribadi seseorang kepada yang bersangkutan.

c) *Reasonableness*, suatu organisasi dapat mengumpulkan, menggunakan atau mengumumkan data pribadi seseorang apabila ia melakukannya dengan tujuan yang pantas dan beralasan.

Guna mengimplementasikan prinsip yang termuat dalam PDPA 2012 Singapura, dalam

instrumen hukum tersebut diatur mengenai Komisi Pelindungan Data Pribadi Singapura atau dikenal dengan istilah *Personal Data Protection Commission and Administration*. Lembaga tersebut terdiri dari paling sedikit 3 (tiga) anggota dan paling banyak 17 (tujuh belas) anggota. Tujuan dari adanya komisi ini adalah untuk mendorong kepatuhan terhadap PDPA 2012 Singapura, mendorong perhatian masyarakat mengenai pelindungan data di Singapura, menerima pelaporan dan konsultasi terkait pelindungan data, memberikan masukan kepada pemerintah terkait masalah pelindungan data yang terjadi, mewakili pemerintah Singapura di dunia internasional dalam hal pelindungan data, melaksanakan penelitian dan riset serta edukasi terkait pelindungan data pribadi, dan serangkaian kewajiban lainnya sebagaimana diatur dalam PDPA 2012 Singapura.

Selain Komisi Pelindungan Data Pribadi Singapura, terdapat juga *Advisory Committees* yang berfungsi memberikan masukan kepada komisi terkait dengan tugasnya dalam Undang-Undang. Komisi Pelindungan Data Pribadi Singapura dapat berkonsultasi kepada *Advisory Committees* terkait dengan pelaksanaan tugas pokok dan fungsinya sebagaimana yang diatur dalam PDPA 2012 Singapura.

Dalam PDPA 2012, diatur juga mengenai Komisi Banding yang terdiri dari 3 (tiga) atau lebih anggota dari panel banding.[129] Komisi ini menerima banding dari setiap orang atau organisasi yang hendak mengajukan banding terhadap putusan yang

[129] Section 33 Singapore Personal Data Protection Act 2012

dikeluarkan oleh Komisi Pelindungan Data Pribadi Singapura dalam jangka waktu 28 (dua puluh delapan) hari. Guna memastikan kepatuhan terhadap Undang-Undang ini, PDPA 2012 Singapura juga mengatur ketentuan sanksi bagi pelanggarnya. PDPA 2012 Singapura mengatur sanksi pidana bagi pelanggaran ketentuan yang telah diatur di dalamnya, berupa denda paling besar $790.000 (tujuh ratus sembilan puluh ribu dollar) dan ancaman pidana penjara hingga 3 (tiga) tahun.

2) Cybersecurity Act

Di era transformasi digital saat ini, keamanan siber merupakan suatu hal yang sangat penting bagi setiap orang. Saat ini, keamanan siber bahkan sangat berdampak dan berpengaruh terhadap perdagangan global dan kegiatan politik dunia. Oleh karena itu, diperlukannya pelindungan hukum terhadap keamanan dan ketahanan siber, guna memastikan pelindungan siber bagi setiap orang. Singapura merupakan salah satu dari sekian banyak negara di dunia yang menaruh perhatian cukup besar terhadap keamanan siber. Pada tanggal 2 Maret 2018, Singapura telah mengesahkan Undang-Undang Keamanan Siber (*Cybersecurity Act*). Undang-Undang tersebut memprioritaskan empat tujuan kunci, yakni:[130]

a) Memperkuat Pelindungan Infrastruktur Informasi Kritikal nasional Singapura terhadap serangan siber;
b) Memberikan otorisasi terhadap the *Cyber Security Agency of Singapore* (CSA) atau Badan

[130] Singapore Cybersecurity Act.

Keamanan Siber Singapura untuk mencegah dan merespons ancaman serta insiden keamanan siber ;

c) Membangun *framework* untuk berbagi informasi siber; dan
d) Membangun *framework* untuk melakukan lisensi terhadap penyedia jasa keamanan siber.

Di Singapura, terdapat beberapa sektor Infrastruktur Informasi Kritikal yang diidentifikasikan oleh CSA bersama dengan pimpinan dari tiap sektor yakni energi, air, perbankan dan finansial, kesehatan, transportasi, pemerintahan, informasi dan komunikasi media, keamanan dan layanan darurat.[131] *Cybersecurity Act* mengatur pemberian lisensi terhadap penyedia jasa pengamanan siber. Hal ini dilakukan untuk menciptakan jaminan terhadap keamanan dan kenyamanan penggunanya, serta meningkatkan kualitas dan standar penyedia jasa tersebut di samping mengevaluasi kinerja pemberi jasa tersebut dari waktu ke waktu.[132] *Cybersecurity Act* juga mengatur insiden keamanan siber sebagai "sebuah tindakan atau kegiatan yang dilakukan tanpa otoritas yang sah atau melalui komputer atau sistem komputer yang membahayakan atau mempengaruhi keamanan siber dari komputer atau sistem komputer lain.[133]

Secara garis besar, Undang-Undang ini menitikberatkan pentingnya pengaturan standar mengenai keamanan siber, pertukaran informasi,

[131] First Schedule Essential Services Singapore Cybersecurity Act.
[132] Kevin Iskandar Putra, "Belajar Dari Tata Kelola Keamanan Siber Singapura", Center For Digital Society, Case Study Series 44, Januari 2019, hlm 3.
[133] Singapore Cybersecurity Act.

dan tata kelola insiden keamanan siber.[134] Akan tetapi, dalam instrumen hukum ini tidak mengatur ketentuan dari pihak yang dapat bergerak ketika berada dalam kondisi darurat. Dalam *Cybersecurity Act*, terdapat CSA yang memiliki fungsi untuk mengawasi, mengelola, dan melaksanakan keamanan siber di Singapura. Pada Pasal 3 sampai dengan Pasal 9 CSA mengatur mengenai wewenang *Commissioner of Cybersecurity* yang merupakan otoritas utama dibawah CSA untuk dapat menetapkan standar keamanan untuk sektor Infrastruktur Informasi Kritikal, serta kewajiban untuk mematuhi instruksi keamanan dari CSA.[135] Selanjutnya, CSA juga dapat memerintahkan audit kepatuhan keamanan siber kepada sektor Infrastruktur Informasi Kritikal. CSA juga dapat memerintahkan sektor Infrastruktur Informasi Kritikal tersebut untuk memberikan informasi yang relevan tentang keamanan siber mereka.[136]

CSA juga memiliki kewenangan untuk memberikan arahan kepada penyelenggara dari sektor Infrastruktur Informasi Kritikal tersebut untuk mengoordinasikan respon nasional apabila terdapat insiden siber. Apabila terdapat insiden siber, CSA memiliki wewenang untuk melakukan investigasi terhadap insiden siber, termasuk hak untuk mengakses informasi dan sistem yang terlibat.[137] Apabila terdapat kasus di luar negeri yang menyebabkan atau memberikan risiko tinggi terhadap ancaman siber Singapura, maka Kepolisian

[134] Kevin Iskandar Putra, Op.Cit., hlm. 4.
[135] Article 3 - 9 Singapore Cybersecurity Act.
[136] Article 22 Singapore Cybersecurity Act.
[137] Article 27 Singapore Cybersecurity Act.

Singapura dapat mengadakan investigasi bersama mitra di luar negeri, dan berdasarkan *Cybersecurity Act* memperbolehkan adanya pemberian informasi dan investigasi. Dalam hal upaya pencegahan serangan siber, CSA akan membentuk *the Singapore Computer Emergency Response Team* (SingCERT) untuk membantu proses deteksi, resolusi, dan pencegahan insiden serangan siber.

Langkah-langkah yang dikeluarkan oleh SingCERT untuk mencegah kejahatan siber diantaranya adalah menyiarkan peringatan, masukan dan *security patches*, meningkatkan kesadaran keamanan siber melalui seminar dan lokakarya, dan berkolaborasi dengan badan CERT lainnya untuk menanggapi insiden keamanan siber.[138] Untuk memaksimalkan tata kelola keamanan siber di Singapura, Singapura bekerja sama dengan berbagai instansi dan lembaga, seperti Federasi Informasi dan Komunikasi Singapura (SITF). Kerja sama tersebut menghasilkan beberapa kebijakan, seperti keanggotaan yang berasal dari masyarakat umum, pihak swasta dan asosiasi perdagangan, untuk memberikan edukasi terkait bidang keamanan siber dan membagikan hasil riset melalui rekomendasi kebijakan keamanan siber ke sekolah serta ruang lingkup yang lain.[139]

Selain itu, Singapura juga bekerja sama bersama Komisi Pelindungan Data Pribadi (PDPC) di Singapura serta Menteri Pendidikan. Kerja sama tersebut berupaya untuk mengedukasi informasi serta literasi keamanan siber dan digital di

[138] Cybersecurity Act.
[139] Kevin Iskandar Putra, Op.CIt, hlm. 6.

lingkungan pendidikan. Sebagai upaya untuk kepatuhan terhadap regulasi *Cybersecurity Act*, dalam Undang-Undang ini diatur mengenai besaran denda yang dapat dikenakan bagi pelanggaran terhadap Undang-Undang ini, mulai dari sanksi pidana denda maksimal Singapura $100.000 (seratus ribu dollar Singapura) pidana penjara maksimal 10 (sepuluh) tahun, hingga sanksi administratif.[140]

d. Pengaturan Keamanan dan Ketahanan Siber di Amerika Serikat *(Executive Order on Improving the Nation's Cybersecurity United States)*

Keamanan Siber merupakan suatu isu yang sangat penting dan menjadi isu yang sering dibicarakan saat ini. Terlebih, dengan meningkatnya perkembangan teknologi dan dampak yang dihasilkannya. Di masa ketika teknologi berkembang dengan cepat, keamanan siber semakin penting untuk melawan serangan jahat yang semakin canggih. Pada bulan Mei 2021 lalu, Presiden Amerika Serikat, Joe Biden, mengeluarkan perintah eksekutif untuk meningkatkan keamanan siber negara. Hal tersebut tertuang dalam *Executive Order on Improving the Nation's Cybersecurity United States* (EO US 14028). Pengesahan EO US 14028 dilatarbelakangi oleh peretasan Colonial Pipeline pada tahun 2021. Colonial Pipeline adalah sebuah peristiwa serangan *ransomware* yang menyerang peralatan terkomputerisasi yang mengelola jaringan pipa.[141] Hal ini menyebabkan kekurangan bahan bakar dan membutuhkan pembayaran tebusan sebesar

[140] *Article 51, Personal Data Protection Act* 2012

[141] CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years",https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years, diakses pada 13 Oktober 2024.

$5 juta (lima juta dolar Amerika Serikat) dari peretas sistemnya.

Hal ini yang membuat pemerintah Amerika Serikat berupaya menanggulangi kejahatan serupa dikemudian hari dan berupaya memperkuat keamanan siber dan rantai pasokan dari perangkat lunak. Dalam EO US 14028, ditekankan sebagai upaya menanggulangi tindak kejahatan siber, pemerintah federal dan pihak swasta harus bersama-sama bekerja sama meningkatkan upayanya untuk mengupayakan keamanan dan ketahanan siber. Sektor swasta harus mampu beradaptasi dan memastikan produknya dibuat dan dioperasikan dengan aman, dan bermitra dengan Pemerintah Federal untuk membangun dunia siber yang aman.[142] Untuk menghilangkan hambatan dan mengatasi ancaman, Pemerintah Federal dapat membuat kontrak untuk bekerja sama dengan Penyedia Layanan Teknologi Informasi (TI) dan Teknologi Operasional (OT) untuk menjalankan sistem informasi Pemerintah Federal.[143]

Nantinya, penyedia layanan dapat memiliki akses terhadap informasi ancaman dan insiden siber pada sistem informasi Pemerintah Federal. Akan tetapi, terdapat batasan dalam mengakses informasi tersebut, karena informasi yang lebih sensitif dikelola oleh Badan Keamanan Siber dan Keamanan Infrastruktur (CISA), Biro Investigasi Federal (FBI) maupun *Intelligence Community* (IC). Dalam EO US 14028 juga mengatur kewenangan dari Direksi *Office of Management and Budget* (OMB) untuk meninjau *Federal Acquisition Regulation* (FAR) dan persyaratan kontrak dengan penyedia layanan TI dan OT untuk merekomendasikan

[142] Bagian 1 Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[143] *Article 2 (a) Executive Order on Improving the Nation's Cybersecurity United States 14028*

pembaruan untuk persyaratan dan bahasa tersebut kepada Dewan FAR dan lembaga terkait lainnya.[144] Kontrak antara penyedia layanan dan pemerintah federal harus dipastikan bahwa penyedia layanan mengumpulkan data terkait keamanan siber yang dikendalikan, membagikan data dengan lembaga yang relevan sesuai arahan Direktur OMB, berkolaborasi dengan badan keamanan siber atau Investigasi Federal dalam menginvestigasi insiden siber, dan berbagi informasi ancaman dan insiden siber dengan badan-badan yang diperlukan.[145]

Dalam praktiknya, penyedia layanan dituntut untuk mampu bekerja sama dengan lembaga terkait, seperti CISA, FBI, dan lainnya guna mencegah, menginvestigasi, dan menanggulangi tindakan kejahatan siber.[146] Selanjutnya, EO US 14028 mengamanahkan untuk melakukan modernisasi keamanan siber di lingkup pemerintah federal guna mencegah kejahatan siber dan melindungi privasi serta kebebasan sipil. EO US 14028 mengamanahkan untuk mengedepankan penggunaan teknologi *cloud computing* sesuai panduan OMB, mengimplementasikan *Zero Trust Architecture* sebagaimana yang telah dikembangkan oleh *National Institute of Standards and Technology* (NIST) dalam standar dan panduannya, dan memberikan laporan terkait modernisasi keamanan siber di lingkup Pemerintah Federal kepada Direktur OMB dan Asisten Presiden dan Penasihat Keamanan Nasional (APNSA).[147] Dengan penggunaan teknologi tersebut, diharapkan dapat memungkinkan Pemerintah Federal untuk

[144] *Article 2 (b) Executive Order on Improving the Nation's Cybersecurity United States 14028*
[145] *Article 2(c) Executive Order on Improving the Nation's Cybersecurity United States 14028*
[146] *Article 2 Executive Order on Improving the Nation's Cybersecurity United States 14028*
[147] *Article 3* Executive Order *on Improving the Nation's Cybersecurity United States 14028*

mencegah, mendeteksi, menilai, dan memulihkan insiden siber. Selain itu, CISA juga harus dapat memodernisasi program, layanan, dan kemampuan keamanan siber agar dapat berfungsi dengan penuh dalam sistem *Zero Trust Architecture*.[148]

Dalam upaya meningkatkan keamanan rantai pasokan perangkat lunak dengan tujuan meningkatkan kemampuan perangkat lunak untuk ketahanan dan keamanan siber, EO US 14028 mengatur kewajiban Pemerintah Federal untuk meningkatkan keamanan rantai pasokan perangkat lunak, dengan meminta masukan dari Pemerintah Federal, sektor swasta, akademisi, dan pihak lainnya agar perangkat lunak yang digunakan di lingkup pemerintah federal telah sesuai standar dan prosedur yang diatur dalam instrumen hukum ini.[149] Nantinya, NIST akan mengeluarkan pedoman yang merekomendasikan standar minimum untuk pengujian vendor atas kode sumber perangkat lunak mereka, untuk memastikan kualitas dan standar dari vendor perangkat lunak yang akan digunakan dalam lingkup pemerintah federal.

Pada bagian ini, diatur pula ketentuan untuk memilih vendor perangkat lunak yang akan digunakan di lingkup pemerintahan federal, seperti kriterianya, mekanisme pengecekannya, persyaratan, dan ketentuan lainnya guna memastikan bahwa vendor tersebut telah tepat dan memenuhi kriteria untuk dapat digunakan dalam lingkup pemerintah federal.[150] Setiap tahunnya, menteri perdagangan harus berkonsultasi dengan pimpinan lembaga lain yang relevan dan harus

[148] *Article 3 Executive Order on Improving the Nation's Cybersecurity United States 14028*
[149] Bagian 4 Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[150] Bagian 4 Executive Order *on Improving the Nation's Cybersecurity United States 14028*

melaporkan kepada Presiden melalui APNSA terkait laporan dari implementasi kebijakan instrumen hukum ini. Selanjutnya, EO US 14028 ini sebagaimana yang juga diatur ketentuannya pada Pasal 871 Undang-Undang Keamanan Dalam Negeri Tahun 2002, juga mengamanatkan pembentukan Badan Peninjauan keamanan siber yang dilakukan oleh Menteri Keamanan Dalam Negeri setelah berkonsultasi dengan Jaksa Agung. Nantinya, badan tersebut akan meninjau dan menilai, berkenaan dengan insiden siber yang signifikan. EO US 14028 juga mengatur ketentuan terkait kewenangan, tanggung jawab, struktural, dan tugas serta fungsi badan, yang mana ditentukan oleh Menteri Keamanan Dalam Negeri.[151]

Dalam EO US 14028 diatur pula ketentuan terkait standardisasi pedoman yang digunakan oleh pemerintah federal untuk menanggapi kerentanan dan insiden keamanan siber. Pedoman tersebut dibentuk oleh Menteri Keamanan Dalam Negeri yang berkoordinasi kepada lembaga lain yang relevan seperti Direktur CISA, Kepala Keamanan Informasi Federal, dan pihak lainnya. Pedoman tersebut harus digunakan dalam sistem informasi badan federal dan harus sesuai dengan standar yang ditetapkan oleh NIST. Ketentuan pedoman tersebut juga diatur di dalam EO US 14028 ini agar substansi dan pengawasan serta perkembangannya dapat berlaku efektif.[152] Guna meningkatkan deteksi kerentanan dan keamanan siber pada jaringan pemerintah federal, dalam instrumen hukum ini juga diatur kewajiban deteksi dini kerentanan pada sumber daya pemerintah federal.

[151] Article 5 Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[152] Pasal 6 Executive Order *on Improving the Nation's Cybersecurity United States 14028*

Lembaga dalam pemerintahan federal harus menerapkan inisiatif *Endpoint Detection and Response* (EDR) agar mendukung deteksi proaktif insiden keamanan siber dalam infrastruktur Pemerintah Federal, respon insiden, serta menjaga keamanan dan ketahanan siber. Guna memaksimalkan sistem EDR, maka setiap lembaga federal harus memiliki sumber daya yang mumpuni untuk memastikan hal tersebut.[153] Selanjutnya, agar proses investigasi dan remediasi pemerintah federal berjalan maksimal untuk merespons insiden siber, EO US 14028 mewajibkan penyedia layanan TI maupun OT di sistem informasi federal untuk memelihara data yang berkaitan dengan insiden siber, dan diwajibkan mencatat peristiwa dan menyimpan data relevan dalam sistem data jaringan lembaga. Pencatatan, penyimpanan, manajemen, dan pengelolaan data diatur ketentuannya dalam EO US ini, agar dapat dilindungi secara maksimal dan mampu untuk menangani risiko maupun insiden siber.[154]

5. Perbandingan Regulasi Pelindungan Infrastruktur Informasi Kritikal dengan Negara Lain

Infrastruktur informasi kritikal nasional merupakan sekumpulan sumber daya teknologi informasi yang penting bagi keberlangsungan operasi suatu negara. Kegagalan atau kerusakan pada infrastruktur informasi kritikal nasional dapat mengakibatkan kerugian besar bagi negara yang bersangkutan, baik secara finansial maupun secara reputasi. Oleh karena itu, diperlukan tindakan pencegahan dan tindakan mitigasi yang ketat untuk melindungi IIK nasional. Berikut ini adalah beberapa regulasi terkait pelindungan IIK Nasional yang ada di negara lain,

[153] Pasal 7 Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[154] Pasal 8 Executive Order *on Improving the Nation's Cybersecurity United States 14028*

misalnya:

a. Jepang

Pelindungan IIK di negara Jepang dilakukan melalui sejumlah tindakan preventif yang dilakukan oleh pemerintah dan sektor swasta. Tindakan preventif ini meliputi pengembangan kerangka kerja keamanan informasi dan standar industri yang kuat, serta pengembangan sistem keamanan jaringan komputer yang handal. Salah satu kerangka kerja keamanan informasi yang dikembangkan oleh pemerintah Jepang adalah *Basic Act on Cybersecurity* yang mengatur tentang keamanan jaringan komputer di Jepang dan memberikan arahan kepada pemerintah dan sektor swasta untuk mengelola keamanan jaringan komputer yang dimilikinya. Selain itu, pemerintah Jepang juga telah mengeluarkan beberapa standar industri yang terkait dengan keamanan informasi, seperti standar keamanan jaringan komputer yang dikembangkan oleh *National Institute of Information and Communications Technology* (NICT). Standar ini mengatur tentang persyaratan keamanan jaringan komputer yang harus dipenuhi oleh organisasi dan sistem yang bergantung pada jaringan komputer di Jepang. Untuk menjamin keamanan jaringan komputer yang dimiliki oleh organisasi dan sistem di Jepang, pemerintah Jepang juga telah mengembangkan sistem keamanan jaringan komputer yang handal. Salah satu contohnya adalah *Cybersecurity Early Warning Partnership* (CEWP), yang merupakan sebuah sistem yang digunakan untuk mendeteksi dan mencegah serangan jaringan komputer yang dilakukan oleh pihak yang tidak bertanggung jawab.

Selain tindakan preventif, pelindungan infrastruktur informasi vital di Jepang juga dilakukan melalui tindakan kuratif yang dilakukan ketika terjadi kegagalan atau kerusakan pada infrastruktur informasi vital. Tindakan kuratif

ini meliputi pemulihan sistem keamanan jaringan komputer yang terganggu, serta penanganan dan pemulihan data yang terhapus atau rusak. Untuk memastikan bahwa pelindungan infrastruktur informasi vital di Jepang dapat dilakukan secara efektif, pemerintah Jepang juga telah mengembangkan sistem pelatihan dan sertifikasi yang terkait dengan keamanan informasi.

Di Negara Jepang, pelindungan infrastruktur informasi vital (*vital information infrastructure protection* atau VIPS) merupakan suatu sistem yang dirancang untuk melindungi infrastruktur informasi yang penting bagi kelangsungan kegiatan ekonomi, sosial, dan keamanan negara. Pelindungan ini meliputi sistem informasi yang digunakan di sektor publik seperti keuangan, transportasi, komunikasi, energi, dan lainnya. Untuk melindungi infrastruktur informasi vital ini, pemerintah Jepang telah menetapkan sejumlah kebijakan dan regulasi yang bertujuan untuk mencegah terjadinya kegagalan sistem informasi, kejahatan *cyber*, dan gangguan lainnya yang dapat merugikan kelangsungan operasi infrastruktur informasi vital. Salah satu kebijakan yang diterapkan adalah pembentukan sebuah badan yang bertanggung jawab untuk mengelola dan melindungi infrastruktur informasi vital, yaitu Badan Pelindungan Infrastruktur Informasi Vital (*Information Security Policy Council* atau ISPC).

Badan ini bertanggung jawab untuk mengkoordinasikan dan mengembangkan kebijakan pelindungan infrastruktur informasi vital di Jepang, serta memantau dan mengevaluasi implementasi kebijakan tersebut. Selain itu, ISPC juga bertanggung jawab untuk memberikan saran dan bantuan teknis kepada sektor publik dan swasta yang memiliki infrastruktur informasi vital dalam mengelola dan melindungi sistem informasi mereka.

Selain ISPC, pemerintah Jepang juga telah mengeluarkan sejumlah peraturan yang bertujuan untuk melindungi infrastruktur informasi vital, di antaranya adalah:

1) Peraturan tentang Keamanan Sistem Informasi (*Information Security Basic Act*) yang mengatur tentang keamanan sistem informasi yang digunakan di sektor publik.
2) Peraturan tentang Keamanan Sistem Informasi di Sektor Swasta (*Private Information Security Act*) yang mengatur tentang keamanan sistem informasi yang digunakan di sektor swasta.
3) Peraturan tentang Keamanan Sistem Informasi di Sektor Keuangan (Financial Information Security Act) yang mengatur tentang keamanan sistem informasi yang digunakan di sektor keuangan.

Pelindungan infrastruktur informasi vital di Jepang juga meliputi upaya pencegahan dan pemulihan terhadap kegagalan sistem informasi, serta penanganan terhadap kejahatan *cyber* dan gangguan lainnya. Pemerintah Jepang juga telah mengeluarkan peraturan yang bertujuan untuk mencegah terjadinya kegagalan sistem informasi, di antaranya adalah:

1) Peraturan tentang Penyusunan dan Pemeliharaan Rencana Penanganan Kegagalan Sistem Informasi (*Information System Failure Countermeasure Planning and Maintenance Act*) yang mengatur tentang cara menyusun dan memelihara rencana penanganan kegagalan sistem informasi di sektor publik dan swasta.
2) Peraturan tentang Penyusunan dan Pemeliharaan Rencana Penanganan Kegagalan Sistem Informasi di Sektor Keuangan (*Financial Information System Failure Countermeasure Planning and Maintenance Act*) yang mengatur tentang cara menyusun dan memelihara

rencana penanganan kegagalan sistem informasi di sektor keuangan.

b. Korea Selatan

Di Korea Selatan, pelindungan IIK merupakan prioritas penting bagi pemerintah dan sektor swasta. IIK terdiri dari sistem dan jaringan teknologi informasi yang penting untuk kelangsungan hidup dan keamanan negara, seperti sistem keuangan, sistem transportasi, sistem komunikasi, dan sistem keamanan nasional.

Untuk melindungi IIK di Korea Selatan, pemerintah telah menetapkan beberapa peraturan dan kebijakan yang bertujuan untuk mencegah, mengurangi, dan menanggulangi ancaman terhadap IIK. Salah satu kebijakan tersebut adalah "*Act on the Protection of Critical Information Infrastructure (CII Act)*", yang merupakan undang-undang yang mengatur tentang pelindungan IIK di Korea Selatan.

Act on the Protection of Critical Information Infrastructure (CII Act) memuat beberapa ketentuan mengenai pengelolaan dan pelindungan infrastruktur informasi kritikal, termasuk:

1) Penunjukan instansi pemerintah sebagai pengelola IIK.
2) Penyusunan rencana pelindungan IIK oleh pengelola IIK.
3) Penyediaan dukungan teknis dan keuangan bagi pengelola IIK.
4) Penyelenggaraan audit keamanan IIK.
5) Penyelenggaraan sistem pemantauan dan pelaporan kegiatan yang terkait dengan IIK.

Selain itu, pemerintah Korea Selatan juga telah menetapkan sejumlah kebijakan dan peraturan lainnya yang bertujuan untuk melindungi IIK, seperti "*Act on the Management of Electronic Financial Transactions*", yang mengatur tentang keamanan transaksi keuangan elektronik, dan "*Act on the Promotion of Information and Communications*

Network Utilization and Information Protection", yang mengatur tentang keamanan jaringan informasi dan komunikasi.

Pemerintah Korea Selatan juga telah menciptakan sejumlah lembaga yang bertugas untuk melindungi IIK, seperti *National Cybersecurity Center*, yang bertugas mengelola dan melindungi IIK di Korea Selatan. Selain itu, pemerintah juga telah menyediakan dukungan teknis dan keuangan bagi perusahaan swasta yang mengelola IIK agar dapat meningkatkan keamanan sistem mereka. Selain itu, pemerintah Korea Selatan juga telah mengeluarkan undang-undang yang mengatur tindakan penanganan *cyber threats*, seperti *Cybersecurity Act*, yang bertujuan untuk meningkatkan keamanan siber di Korea Selatan.

Untuk meningkatkan keamanan siber di Korea Selatan, pemerintah juga telah menciptakan lembaga penanganan *cyber threats*, seperti *Korean Internet Security Agency* (KISA), yang bertugas melakukan investigasi dan memberikan dukungan teknis kepada perusahaan yang mengalami serangan *cyber*. Selain itu, pemerintah Korea Selatan juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan kapasitas keamanan siber di sektor swasta, termasuk memberikan dukungan keuangan bagi perusahaan yang ingin meningkatkan keamanan sibernya.

Di samping itu, pemerintah Korea Selatan juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan edukasi dan kesadaran masyarakat tentang pentingnya keamanan siber. Ini termasuk program edukasi keamanan siber yang diselenggarakan oleh lembaga seperti KISA, serta kampanye yang bertujuan untuk meningkatkan kesadaran masyarakat tentang pentingnya menjaga keamanan siber.

Dengan demikian, pemerintah Korea Selatan telah melakukan berbagai upaya untuk meningkatkan keamanan

siber di negara tersebut, termasuk dengan menciptakan lembaga yang bertugas mengelola dan melindungi IIK, mengeluarkan undang-undang yang mengatur tindakan penanganan *cyber threats*, serta memfokuskan pada peningkatan kapasitas keamanan siber di sektor swasta dan edukasi masyarakat tentang keamanan siber.

c. Singapura

Singapura telah melakukan berbagai upaya untuk melindungi IIK di negara tersebut, termasuk dengan mengeluarkan kebijakan-kebijakan yang bertujuan untuk meningkatkan keamanan siber di negara tersebut.

Salah satu kebijakan yang telah dikeluarkan oleh pemerintah Singapura adalah *Cyber Security Act*, yang bertujuan untuk meningkatkan keamanan siber di negara tersebut dengan mengatur tindakan penanganan *cyber threats*, serta mengelola dan melindungi IIK di Singapura. Selain itu, pemerintah juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan kapasitas keamanan siber di sektor swasta, termasuk memberikan dukungan keuangan bagi perusahaan yang ingin meningkatkan keamanan sibernya.

Untuk mengelola dan melindungi IIK di Singapura, pemerintah telah menciptakan sejumlah lembaga yang bertugas untuk menangani *cyber* threats, seperti *Cyber Security Agency of Singapore* (CSA). Lembaga ini bertugas melakukan investigasi dan memberikan dukungan teknis kepada perusahaan yang mengalami serangan *cyber*. Selain itu, CSA juga bertugas mengelola dan melindungi IIK di Singapura, serta memberikan edukasi dan saran kepada masyarakat tentang keamanan siber.

Di samping itu, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada

peningkatan edukasi dan kesadaran masyarakat tentang pentingnya keamanan siber. Ini termasuk program edukasi tentang keamanan siber yang diselenggarakan oleh lembaga-lembaga seperti CSA, serta kampanye yang bertujuan untuk meningkatkan kesadaran masyarakat tentang pentingnya menjaga keamanan siber.

Selain itu, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan keamanan siber di sektor publik, termasuk dengan menciptakan sejumlah lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor publik, serta memberikan dukungan teknis dan keuangan bagi perusahaan yang mengelola IIK di sektor publik.

Di samping itu, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan keamanan siber di sektor kritikal, seperti sektor keuangan, kesehatan, dan energi. Hal ini termasuk menciptakan lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor tersebut, serta memberikan dukungan teknis dan keuangan bagi perusahaan yang mengelola IIK di sektor tersebut.

Pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan keamanan siber di sektor industri, termasuk dengan menciptakan lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor industri, serta memberikan dukungan teknis dan keuangan bagi perusahaan yang mengelola IIK di sektor industri.

Untuk meningkatkan keamanan siber di sektor-sektor tersebut, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan kapasitas keamanan siber, termasuk dengan memberikan dukungan keuangan bagi perusahaan yang ingin meningkatkan

keamanan sibernya, serta menyelenggarakan program edukasi mengenai keamanan siber untuk masyarakat. Selain itu, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan koordinasi antarlembaga dalam penanganan *cyber* threats, termasuk dengan menciptakan sejumlah lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor tersebut, serta menyelenggarakan program edukasi mengenai keamanan siber untuk masyarakat. Untuk meningkatkan keamanan siber di sektor-sektor tersebut, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan koordinasi antarlembaga dalam penanganan *cyber* threats, termasuk dengan menciptakan sejumlah lembaga yang bertugas untuk mengelola dan melindungi infrastruktur informasi kritikal di sektor tersebut, serta menyelenggarakan program edukasi tentang keamanan siber untuk masyarakat.

Untuk meningkatkan keamanan siber di sektor tersebut, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan koordinasi antar lembaga dalam penanganan *cyber* threats, termasuk dengan menciptakan sejumlah lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor tersebut, serta menyelenggarakan program edukasi tentang keamanan siber untuk masyarakat.

Pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan keamanan siber di sektor transportasi, termasuk dengan menciptakan lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor transportasi, serta memberikan dukungan teknis dan keuangan bagi perusahaan yang mengelola IIK di sektor transportasi.

Selain itu, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan keamanan siber di sektor pertahanan, termasuk dengan menciptakan lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor pertahanan, serta memberikan dukungan teknis dan keuangan bagi perusahaan yang mengelola IIK di sektor pertahanan. Untuk meningkatkan keamanan siber di sektor tersebut, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan kapasitas keamanan siber, termasuk dengan memberikan dukungan keuangan bagi perusahaan yang ingin meningkatkan keamanan sibernya, serta menyelenggarakan program edukasi mengenai keamanan siber untuk masyarakat. Di samping itu, pemerintah Singapura juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan koordinasi antarlembaga dalam penanganan *cyber* threats, termasuk dengan menciptakan sejumlah lembaga yang bertugas untuk mengelola dan melindungi IIK di sektor tersebut, serta menyelenggarakan program edukasi mengenai keamanan siber untuk masyarakat.

Dengan demikian, pemerintah Singapura telah melakukan berbagai upaya untuk melindungi IIK di negara tersebut, termasuk dengan mengeluarkan kebijakan yang bertujuan untuk meningkatkan keamanan siber di negara tersebut, menciptakan lembaga yang bertugas untuk mengelola dan melindungi IIK, serta memfokuskan pada peningkatan kapasitas keamanan siber di sektor swasta dan publik, serta peningkatan edukasi dan kesadaran masyarakat tentang keamanan siber. Pemerintah juga telah mengeluarkan kebijakan yang memfokuskan pada peningkatan koordinasi antar lembaga dalam penanganan *cyber* threats, serta memfokuskan pada peningkatan keamanan siber di sektor-sektor kritikal seperti sektor keuangan, kesehatan, dan

pertahanan.

c. Amerika

Di Amerika Serikat, pelindungan infrastruktur informasi kritikal merupakan prioritas utama bagi pemerintah federal, negara bagian, dan pemerintah lokal. IIK (*Critical Information Infrastructure*, CII) merujuk pada sistem, jaringan, dan teknologi yang mendukung kegiatan penting bagi keamanan nasional, ekonomi, dan kelangsungan hidup masyarakat.

Untuk melindungi CII, pemerintah AS menggunakan berbagai strategi, termasuk:

1) Pendirian lembaga khusus untuk mengelola masalah keamanan infrastruktur informasi. Misalnya, National *Cybersecurity* and *Communications Integration Center* (NCCIC) adalah lembaga yang berfokus pada keamanan jaringan siber dan komunikasi di AS.
2) Pemberian bantuan keuangan kepada pemilik infrastruktur untuk meningkatkan keamanannya. Misalnya, Departemen Keamanan Dalam Negeri AS menyediakan dana tahunan untuk membantu pemilik CII memperbaiki keamanan sistem mereka.
3) Pembentukan standar dan regulasi yang harus dipenuhi oleh pemilik CII. Misalnya, NCCIC telah menetapkan standar keamanan yang harus dipenuhi oleh pemilik CII di sektor energi, telekomunikasi, dan transportasi.
4) Pendirian lembaga penelitian dan pengembangan untuk mempelajari masalah keamanan infrastruktur informasi misalnya, Departemen Energi AS memiliki lembaga penelitian yang bertanggung jawab untuk mengembangkan teknologi dan solusi keamanan yang sesuai untuk infrastruktur energi.
5) Penyediaan latihan dan sosialisasi keamanan infrastruktur informasi kepada pemilik CII. Misalnya,

NCCIC menyelenggarakan pelatihan dan sosialisasi secara berkala untuk membantu pemilik CII meningkatkan keamanan sistem mereka.

6) Penyediaan layanan bantuan keamanan infrastruktur informasi kepada pemilik CII. Misalnya, NCCIC menyediakan layanan bantuan keamanan infrastruktur informasi yang bisa diakses oleh pemilik CII melalui situs web mereka.
7) Penyelidikan dan penuntutan terhadap pelaku kejahatan siber yang menyerang infrastruktur informasi kritikal. Misalnya, *Federal Bureau of Investigation* (FBI) dan Departemen Kehakiman AS memiliki tim khusus yang bertanggung jawab untuk menyelidiki dan menuntut pelaku kejahatan *cyber* yang menyerang CII.
8) Penyediaan sistem deteksi dan mitigasi ancaman *cyber* untuk mengamankan CII. Misalnya, NCCIC telah mengembangkan sistem deteksi dan mitigasi ancaman siber yang digunakan oleh pemilik CII untuk mengamankan jaringan mereka.
9) Penggunaan teknologi enkripsi untuk mengamankan data yang tersimpan di IIK. Enkripsi merupakan teknik yang digunakan untuk menyandikan data sehingga tidak dapat dibaca oleh orang yang tidak memiliki kunci enkripsi.
10) Penyediaan sistem otomatisasi untuk mengelola dan mengamankan IIK. Misalnya, pemilik CII dapat menggunakan sistem otomatisasi untuk mengelola dan mengamankan sistem mereka dengan lebih efisien.
11) Penggunaan teknologi pemantauan dan deteksi ancaman untuk mengidentifikasi ancaman yang mungkin terjadi terhadap IIK misalnya, pemilik CII dapat menggunakan sistem pemantauan dan deteksi ancaman untuk mengamati aktivitas jaringan mereka dan mengidentifikasi ancaman yang mungkin terjadi.

12) Penyediaan sistem keamanan fisik untuk melindungi IIK dari ancaman fisik misalnya, pemilik CII dapat menggunakan sistem keamanan fisik seperti pagar, kamera pengintai, dan sistem deteksi kebakaran untuk melindungi sistem mereka dari ancaman fisik.
13) Penyediaan sistem keamanan logis untuk melindungi IIK dari ancaman logis, misalnya, pemilik CII dapat menggunakan sistem keamanan logis seperti sistem autentikasi, enkripsi, dan sistem deteksi ancaman untuk melindungi sistem mereka dari ancaman logis.
14) Penyediaan solusi keamanan yang disesuaikan dengan kebutuhan masing-masing pemilik IIK. Misalnya, pemilik CII dapat bekerja sama dengan penyedia layanan keamanan untuk mengembangkan solusi keamanan yang sesuai dengan kebutuhan mereka.
15) Penyediaan layanan bantuan keamanan infrastruktur informasi kepada masyarakat umum. Misalnya, pemerintah AS menyediakan layanan bantuan keamanan infrastruktur informasi kepada masyarakat umum melalui situs web seperti www.staysafeonline.org yang menyediakan informasi dan panduan keamanan siber untuk masyarakat umum.
16) Dalam mengelola pelindungan IIK, pemerintah AS juga bekerja sama dengan sektor swasta dan organisasi nirlaba. Kerja sama ini dianggap penting karena sebagian besar CII di AS dimiliki oleh sektor swasta.
17) Selain itu, pemerintah AS juga terlibat dalam kerja sama internasional untuk melindungi IIK. Misalnya, AS sering bekerja sama dengan negara lain dalam menangani ancaman siber yang bersifat internasional.

Di samping strategi dan kerja sama yang telah disebutkan di atas, pemerintah AS juga memiliki beberapa program spesifik yang bertujuan untuk melindungi infrastruktur

informasi kritikal di berbagai sektor. Beberapa di antaranya adalah:

1) Program *Cybersecurity* and *Infrastructure Security Agency* (CISA) yang berfokus pada peningkatan keamanan infrastruktur informasi di sektor publik dan swasta. Program ini membantu pemilik CII untuk meningkatkan keamanan sistem mereka melalui penyediaan layanan bantuan keamanan, sosialisasi keamanan, dan penyelenggaraan latihan keamanan.
2) Program Energy Sector *Cybersecurity* Program yang bertujuan untuk meningkatkan keamanan infrastruktur informasi di sektor energi. Program ini melibatkan Departemen Energi AS, sektor energi, dan lembaga penelitian untuk mengembangkan solusi keamanan yang sesuai untuk infrastruktur energi.
3) *Program Transportation Security Administration* (TSA) yang bertujuan untuk meningkatkan keamanan infrastruktur informasi di sektor transportasi. Program ini melibatkan Departemen Transportasi AS, sektor transportasi, dan lembaga penelitian untuk mengembangkan solusi keamanan yang sesuai untuk infrastruktur transportasi.
4) Program *Health and Human Services* (HHS) yang bertujuan untuk meningkatkan keamanan infrastruktur informasi di sektor kesehatan. Program ini melibatkan Departemen Kesehatan dan Layanan Sosial AS, sektor kesehatan, dan lembaga penelitian untuk mengembangkan solusi keamanan yang sesuai untuk infrastruktur kesehatan.

Pelindungan IIK di AS merupakan prioritas utama karena CII merupakan salah satu fondasi keamanan nasional dan ekonomi AS. Oleh karena itu, pemerintah AS terus berupaya untuk meningkatkan keamanan CII dengan menggunakan berbagai strategi dan kerja sama yang tepat.

d. Perancis

Di Perancis, pelindungan IIK merupakan salah satu prioritas utama bagi pemerintah. IIK merujuk pada sistem, jaringan, dan layanan informasi yang penting bagi kelangsungan hidup dan keamanan negara, ekonomi, dan masyarakat.

Untuk melindungi IIK, Perancis telah menetapkan beberapa tindakan yang dapat diambil oleh pemerintah, perusahaan, dan individu. Pertama, pemerintah Perancis telah mengeluarkan beberapa peraturan dan regulasi yang mengatur pelindungan IIK. Misalnya, Peraturan Menteri Dalam Negeri No. 2005-1524 tentang Pelindungan Infrastruktur Informasi kritikal menetapkan standar dan prosedur yang harus diikuti oleh perusahaan yang mengelola IIK. Kedua, pemerintah Perancis juga telah menciptakan sebuah lembaga yang bertugas mengelola dan melindungi IIK. Lembaga ini disebut "ANSSI" atau *Agence nationale de la sécurité des systèmes d'information*. ANSSI bertanggung jawab untuk menetapkan standar dan prosedur keamanan informasi, serta memberikan saran dan dukungan teknis kepada perusahaan yang mengelola IIK. Ketiga, Perancis juga telah menciptakan sebuah sistem yang disebut "CERT-FR" atau *Computer Emergency Response Team - France*. CERT-FR merupakan sebuah lembaga yang bertugas menangani dan mengatasi kejadian keamanan informasi, seperti serangan *cyber*, di Perancis. CERT-FR juga bertugas memberikan saran dan bantuan kepada perusahaan yang mengalami kejadian keamanan informasi. Keempat, Perancis juga telah menciptakan sebuah sistem yang disebut "INFIRM" atau *Infrastructures de Résilience et de Mutualisation*. INFIRM merupakan sebuah sistem yang dikelola oleh ANSSI yang bertujuan untuk menjamin kelangsungan operasional IIK di Perancis. INFIRM menyediakan fasilitas dan layanan yang

dibutuhkan untuk menjamin kelangsungan operasional IIK, seperti layanan komunikasi dan jaringan yang handal. Kelima, Perancis juga telah menetapkan beberapa tindakan yang harus diambil oleh perusahaan yang mengelola IIK. Misalnya, perusahaan yang mengelola IIK harus memiliki sistem keamanan informasi yang handal, serta harus mengikuti standar dan prosedur yang ditetapkan oleh ANSSI. Selain itu, perusahaan yang mengelola IIK juga harus memiliki tim keamanan informasi yang terlatih dan handal, serta harus melakukan tes keamanan secara berkala untuk memastikan bahwa sistem keamanan mereka masih efektif. Keenam, Perancis juga telah menciptakan sebuah sistem yang disebut "*DIRECCTE*" atau Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi. *DIRECCTE* merupakan sebuah lembaga yang bertugas mengelola dan melindungi IIK di tingkat regional. *DIRECCTE* bertanggung jawab untuk mengelola dan melindungi IIK di wilayahnya masing-masing, serta memberikan saran dan dukungan teknis kepada perusahaan yang mengelola IIK di wilayahnya. Ketujuh, Perancis juga telah menetapkan beberapa tindakan yang harus diambil oleh individu untuk melindungi IIK. Misalnya, individu harus memastikan bahwa komputer mereka terinstall dengan antivirus yang handal, serta harus menjaga keamanan informasi yang mereka miliki, seperti *password*, dengan baik. Selain itu, individu juga harus selalu waspada terhadap serangan *cyber* dan segera melaporkannya kepada lembaga yang tepat jika terjadi kejadian keamanan informasi. Kedelapan, Perancis juga telah menciptakan sebuah sistem yang disebut "CNIL" atau *Commission nationale de l'informatique et des libertés*. CNIL merupakan sebuah lembaga yang bertugas mengelola dan melindungi hak privasi individu di Perancis. CNIL bertanggung jawab untuk mengelola dan melindungi hak privasi individu di

Perancis, serta memberikan saran dan dukungan teknis kepada individu yang membutuhkannya. Kesembilan, Perancis juga telah menciptakan sebuah sistem yang disebut "HADOPI" atau *Haute Autorité pour la diffusion des œuvres et la protection des droits sur* internet. HADOPI merupakan sebuah lembaga yang bertugas mengelola dan melindungi hak cipta di Perancis. HADOPI bertanggung jawab untuk mengelola dan melindungi hak cipta di Perancis, serta memberikan saran dan dukungan teknis kepada individu yang membutuhkannya. Kesepuluh, Perancis juga telah menciptakan sebuah sistem yang disebut "CNAMTS" atau *Caisse nationale d'assurance maladie des travailleurs salariés*. CNAMTS merupakan sebuah lembaga yang bertugas mengelola dan melindungi sistem kesehatan di Perancis. CNAMTS bertanggung jawab untuk mengelola dan melindungi sistem kesehatan di Perancis, serta memberikan saran dan dukungan teknis kepada individu yang membutuhkannya.

Perancis juga telah menciptakan sebuah sistem yang disebut "*Conseil national du numérique*" atau *National Digital Council*. *Conseil national du numérique* merupakan sebuah lembaga yang bertugas mengelola dan melindungi sistem teknologi informasi di Perancis. *Conseil national du numérique* bertanggung jawab untuk mengelola dan melindungi sistem teknologi informasi di Perancis, serta memberikan saran dan dukungan teknis kepada individu yang membutuhkan.

e. Australia

IIK di Australia terdiri dari sistem, jaringan, dan layanan yang penting bagi kelangsungan hidup, keamanan, dan kesejahteraan masyarakat, ekonomi, dan keamanan nasional. Untuk melindungi infrastruktur ini, Australia telah menetapkan sejumlah regulasi dan kebijakan yang mengatur pengelolaan, pemeliharaan, dan pengembangan IIK. Berikut

adalah deskripsi lebih detail tentang pelindungan IIK di Australia:

1) Kebijakan IIK: Pemerintah Australia telah menetapkan kebijakan IIK yang mengatur pengelolaan, pemeliharaan, dan pengembangan IIK di negara ini. Kebijakan ini juga mencakup langkah-langkah preventif yang harus diambil untuk mencegah serangan terhadap IIK, seperti peningkatan keamanan jaringan dan sistem, serta tindakan pemulihan cepat setelah terjadi serangan.
2) Agen pelindung IIK: Pemerintah Australia telah menunjuk agen khusus yang bertanggung jawab untuk melindungi IIK di negara ini. Agen ini bernama Australian *Cyber Security Centre* (ACSC) dan merupakan bagian dari *Australian Signals Directorate* (ASD). ACSC bertanggung jawab untuk mengatur dan mengelola kebijakan IIK, serta memberikan saran dan bantuan teknis kepada pemegang IIK dalam mengelola dan memelihara keamanan sistem mereka.
3) Regulasi IIK: Pemerintah Australia juga telah menetapkan regulasi yang mengatur pengelolaan, pemeliharaan, dan pengembangan IIK. Regulasi ini bertujuan untuk menjamin bahwa IIK di Australia terlindungi dengan baik dari serangan atau kegagalan yang dapat merugikan kelangsungan hidup, keamanan, dan kesejahteraan masyarakat, ekonomi, dan keamanan nasional.
4) Standar keamanan IIK: Pemerintah Australia juga telah menetapkan standar keamanan IIK yang harus dipenuhi oleh pemegang IIK. Standar ini mencakup sejumlah persyaratan keamanan yang harus dipenuhi, seperti peningkatan keamanan jaringan dan sistem, pengelolaan risiko keamanan, serta tindakan pemulihan cepat setelah terjadi serangan. Standar keamanan ini harus dipenuhi oleh semua pemegang IIK untuk memastikan bahwa IIK

di Australia terlindungi dengan baik.

5) Pengawasan IIK: Pemerintah Australia juga mengelola sistem pengawasan IIK yang memantau dan mengevaluasi keamanan IIK di negara ini. Sistem ini menggunakan teknologi canggih untuk memantau aktivitas di jaringan dan sistem IIK, serta memberikan laporan kepada pemerintah tentang keamanan infrastruktur tersebut.
6) Pelatihan dan sosialisasi keamanan IIK: Pemerintah Australia juga menyelenggarakan pelatihan dan sosialisasi keamanan IIK bagi pemegang IIK. Pelatihan ini bertujuan untuk meningkatkan kesadaran dan kemampuan pemegang infrastruktur dalam mengelola dan memelihara keamanan sistem mereka.
7) Kerja sama dengan sektor swasta: Pemerintah Australia juga bekerja sama dengan sektor swasta dalam upaya pelindungan IIK. Kerjasama ini meliputi pertukaran informasi keamanan, serta bantuan teknis dan pelatihan keamanan bagi pemegang IIK di sektor swasta.
8) Kerja sama internasional: Selain itu, pemerintah Australia juga bekerja sama dengan pemerintah dan lembaga internasional dalam upaya pelindungan IIK. Kerja sama ini meliputi pertukaran informasi keamanan, serta bantuan teknis dan pelatihan keamanan bagi pemegang IIK di negara-negara lain.
9) Penanganan serangan terhadap IIK: Pemerintah Australia juga memiliki mekanisme penanganan serangan terhadap IIK. Mekanisme ini meliputi langkah-langkah preventif seperti peningkatan keamanan jaringan dan sistem, serta tindakan pemulihan cepat setelah terjadi serangan.
10) Penanganan kegagalan IIK: Selain itu, pemerintah Australia juga memiliki mekanisme penanganan kegagalan IIK. Mekanisme ini meliputi tindakan

pemulihan cepat untuk memastikan bahwa IIK kembali berfungsi secepat mungkin setelah terjadi kegagalan. Pemerintah juga menyediakan saran dan bantuan teknis bagi pemegang IIK dalam mengelola dan memelihara keamanan sistem mereka agar terhindar dari kegagalan di masa yang akan datang.

Secara keseluruhan, pelindungan IIK di Australia merupakan upaya komprehensif yang meliputi kebijakan, regulasi, standar keamanan, pengawasan, pelatihan dan sosialisasi, kerjasama dengan sektor swasta dan internasional, serta penanganan serangan dan kegagalan. Upaya ini dilakukan untuk memastikan bahwa IIK di Australia terlindungi dengan baik dan dapat terus berfungsi dengan baik untuk kelangsungan hidup, keamanan, dan kesejahteraan masyarakat, ekonomi, dan keamanan nasional.

f. Malaysia

Pelindungan IIK di Malaysia diatur dalam Undang-Undang tentang *Cybersecurity Act of* 2024 [25]. Undang-Undang ini bertujuan untuk meningkatkan keamanan siber nasional dengan mengatur pembentukan Komite Keamanan Siber Nasional, perkuatan tugas dan wewenang Kepala Badan Keamanan Siber Nasional, perkuatan fungsi dan tugas pimpinan sektor infrastruktur informasi kritikal nasional, kewajiban terhadap entitas IIK nasional, serta pengelolaan ancaman keamanan siber dan insiden keamanan siber pada IIK nasional, mengatur penyedia layanan keamanan siber melalui perizinan, dan lain-lain. Pemerintah Malaysia menerapkan berbagai strategi yang diamanatkan dalam undang- undang, meliputi:.

1) Pembentukan Komite Keamanan Siber Nasional (*National Cyber Security Committee/*NCSC) (Part II section 5)

a) Undang-Undang tersebut membentuk komite untuk mengawasi kebijakan keamanan siber, yang diketuai oleh Perdana Menteri. Komite terdiri atas Perdana Menteri, Menteri keuangan, Menteri Luar Negari, Menteri Pertahanan, Menteri Dalam Negeri, Menteri Komunikasi, Menteri Digital, Menteri Sekretariat Negara, Kepala Angkatan Bersenjata, Kepala Kepolisian, DIrektur Jenderal Keamanan Nasional.

b) Fungsi dari komite adalah menyusun dan menetapkan kebijakan nasional keamanan siber, menetapkan strategi keamanan siber nasional, memonitor implementasi dari kebijakan dan strategi keamanan siber nasional, memberikan arahan kebijakan terkait keamanan siber kepada CEO NACSA dan pimpinan sektor IIKN, dan fungsi lain yang tidak bertentang dengan Undang-undang.

c) Komite dapat menetapkan Sub-Komite yang diperlukan untuk memperkuat fungsi Komite.

2) Perkuatan tugas dan wewenang Badan Keamanan Siber Nasional *(National Cyber Security Agency/NACSA)*

a) Tugas *Chief Executive* (CEO NACSA) adalah memberikan saran dan rekomendasi kepada komite terkait kebijakan, strategi dan langkah startegis yang diperlukan dalam Keamanan Siber Nasional.

b) Melaksanakan kebijakan, strategi, dan Langkah-langkah strategis yang telah ditetapkan dan diarahkan oleh Komite.

c) Mengoordinasikan dan memonitor implementasi kebijakan, strategi, dan langkah strategis yang ditetapkan oleh komite.

d) Mengumpulkan, mengolah, dan mendistribusikan informasi atau data kepada pembina sektor IIV dan komite.

3) Perkuatan Fungsi Pimpinan Sektor Infrastruktur Informasi kritikal Nasional (*sector lead-spesific governance*)
   a) Pemrakarsa merupakan kementerian yang mengatur dan mengoordinasikan sektort strategis
   b) Tugasnya adalah menetapkan penyelenggara IIV di sektornya, menjalankan strategi, kebijakan, dan langkah strategis yang ditetapkan oleh komite dan NACSA, melakukan monitoring terhadap implementasi, serta menyampaikan laporan situasional kepada Chief Executive NACSA
4) Kewajiban Terhadap Pengelola IIK Nasional
   a) Menyampaikan informasi yang relevan terkait IIK yang dikelolanya kepada *sector lead*.
   b) Menerapkan pedoman code of practices yang disusun oleh NACSA dalam rangka implementasi kontrol keamanan pada penyelenggara IIK.
   c) Menerapkan penilaian risiko dan audit secara periodik.
   d) Menyampaikan laporan insiden siber kepada *Chief Executive* NACSA dan *sector lead*.
5) Pelanggaran Terhadap IIK yang Berasal dari Ekstra teritorial (Part I section 3)

   Undang-Undang ini menyatakan bahwa segala bentuk pelanggaran yang mempengaruhi IIK Malaysia, bahkan jika dilakukan oleh entitas asing di luar Malaysia, maka akan diproses secara hukum oleh Pemerintah Malaysia. Persyaratan Lisensi untuk Penyedia Layanan Keamanan Siber Siapa pun yang menawarkan, mengiklankan, atau mewakili diri mereka sendiri sebagai penyedia layanan keamanan siber harus memiliki lisensi kecuali yang melibatkan sistem di luar Malaysia atau perusahaan terkait (*Holding*, anak perusahaan, anak perusahaan

holding). Jenis layanan yang harus memiliki lisensi meliputi:

a) Layanan pemantauan pusat operasi keamanan terkelola: memantau sistem komputer orang lain untuk ancaman siber dan menentukan respons yang diperlukan.
b) Pengujian penetrasi: Menilai kerentanan keamanan siber mensimulasikan serangan dan merekomendasikan tindakan mitigasi.

D. Kajian terhadap Implikasi Penerapan Regulasi

Pada era digital saat ini, keamanan dan ketahanan siber menjadi salah satu permasalahan yang sangat krusial. Meningkatnya ancaman siber, menuntut setiap negara untuk dapat memperkuat keamanan serta ketahanan siber untuk dapat menyesuaikan kebutuhan. Untuk itu, Indonesia memerlukan kerangka hukum yang solid untuk melindungi IIK dan data penting milik negara. Oleh karenanya, RUU KKS menjadi langkah strategis dalam hal memperkuat kewenangan BSSN. BSSN sebagai lembaga yang bertanggung jawab dalam pengelolaan keamanan siber di Indonesia perlu dilengkapi dengan kewenangan yang lebih luas melalui RUU ini.

Pembentukan RUU KKS akan menjadi langkah yang baik dalam penguatan kebijakan nasional. Hal ini dikarenakan RUU KKS bertujuan untuk menciptakan kerangka hukum yang jelas dalam menangani isu-isu keamanan siber. Selain itu, RUU KKS akan memberikan dampak pelindungan IIK dalam memastikan bahwa IIK negara terlindungi dari serangan siber. Oleh karenanya, RUU KKS dibutuhkan juga sebagai langkah peningkatan kewenangan Badan Siber dan Sandi Negara dalam melakukan penanggulangan terhadap ancaman siber.

Melalui RUU KKS, BSSN dapat memperkuat kewenangannya dengan diberikannya otoritas untuk melakukan pemantauan dan deteksi dini terhadap ancaman siber. RUU KKS juga dapat memperluas kewenangan BSSN dalam memfasilitasi koordinasi antar berbagai

lembaga pemerintah dalam penanganan insiden siber. Hal ini tentunya tidak hanya berdampak pada kewenangan represif BSSN melainkan juga menjadi langkah bagi kewenangan preventif BSSN dalam mengembangkan program edukasi untuk meningkatkan kesadaran masyarakat tentang keamanan siber.

Pembentukan RUU KKS tentunya akan berdampak pada meningkatnya keamanan nasional yang lebih baik. Dengan diperkuatnya kewenangan BSSN, maka peran BSSN juga akan lebih efektif dalam melindungi data serta infrastruktur negara. Selain itu keamanan siber yang baik dapat meningkatkan kepercayaan masyarakat dan investor terhadap ekosistem digital Indonesia. RUU KKS diharapkan juga dapat membantu BSSN dalam membuka peluang bagi kerja sama dengan negara lain dalam bidang keamanan siber .

Dalam regulasi yang berlaku saat ini, pengembangan peran BSSN sangat tergantung pada penerbitan regulasi baru yang dapat memperluas kewenangan dan tanggung jawabnya. Perluasan peran ini harus tetap konsisten dengan tugas dan fungsi yang telah ditentukan oleh peraturan presiden. Dengan kata lain, meskipun BSSN memiliki potensi untuk berperan lebih strategis dalam keamanan siber nasional, kemampuan lembaga ini untuk berkembang dan beradaptasi dengan tantangan baru seperti ancaman siber yang semakin kompleks sangat dipengaruhi oleh sejauh mana peraturan tambahan memungkinkan BSSN untuk menjalankan tugas baru yang sesuai dengan pengembangan perannya.

Oleh karenanya, RUU KKS sangat penting untuk memperkuat kewenangan BSSN dan meningkatkan kemampuan Indonesia dalam menghadapi ancaman siber. Dengan landasan hukum yang kuat, BSSN dapat lebih efektif dalam melindungi keamanan nasional, mendorong pertumbuhan ekonomi digital, dan meningkatkan kerja sama internasional. Upaya untuk segera merealisasikan RUU ini perlu didorong agar Indonesia dapat menjadi negara yang lebih aman dan siap menghadapi tantangan siber di masa depan. RUU KKS diharapkan dapat menjadi langkah yang baik dalam kaitannya dengan perluasan

kewenangan BSSN sebagai badan yang berwenang dalam menghadapi ancaman siber di Indonesia.

Dengan adanya RUU KKS, langkah-langkah preventif dan pencegahan terhadap serangan siber akan menjadi lebih komprehensif dan terstruktur. Pengesahan Undang-Undang ini memberikan landasan hukum yang kuat dalam menanggulangi ancaman siber secara lebih sistematis, mulai dari peningkatan pengawasan terhadap IIK hingga pelindungan terhadap data pribadi masyarakat. Di bawah payung hukum ini, pemerintah dapat mengimplementasikan standar keamanan yang lebih tinggi untuk berbagai sektor, termasuk sektor publik dan swasta, yang selama ini rentan terhadap serangan siber.

Dengan RUU ini, pemerintah dapat mengoordinasikan berbagai lembaga terkait, BSSN, TNI, Polri, dan lembaga pemerintah lainnya, untuk bekerja sama dalam deteksi dini dan penanggulangan insiden siber. Langkah-langkah kolaboratif ini diharapkan dapat mencegah kerugian besar yang ditimbulkan oleh serangan siber, seperti pencurian data atau kerusakan sistem infrastruktur yang dapat melumpuhkan aktivitas ekonomi dan layanan publik.

Selain itu, RUU ini akan memperkuat mekanisme pemulihan dan penanggulangan setelah terjadi serangan siber. Setiap insiden dapat ditangani lebih cepat karena adanya prosedur standar yang diatur dalam Undang-Undang, termasuk pelibatan tim tanggap darurat keamanan siber (CERT) dan badan penegak hukum. Hal ini memungkinkan pemerintah untuk merespon ancaman secara proaktif dan melibatkan masyarakat dalam mengidentifikasi dan melaporkan aktivitas mencurigakan. Hal ini akan memperkuat ketahanan siber nasional secara keseluruhan, mengingat ancaman siber semakin kompleks dan sering kali melibatkan aktor non-negara yang memiliki kemampuan teknologi canggih.

RUU KKS berpotensi menimbulkan irisan tugas antar lembaga negara. Hal ini disebabkan oleh kompleksitas pengaturan yang ada serta banyaknya lembaga yang terlibat dalam pengelolaan dan penegakan hukum di bidang siber. Dalam konteks ini, penting untuk memahami

bagaimana RUU KKS dapat mempengaruhi struktur kelembagaan yang ada dan potensi konflik yang mungkin muncul.

Salah satu alasan utama mengapa RUU ini berpotensi menciptakan irisan tugas adalah karena adanya pengaturan yang bersifat *overlapping* dengan Undang-Undang yang sudah ada, seperti UU ITE. RUU KKS memberikan wewenang besar kepada BSSN untuk melakukan penapisan konten dan aplikasi elektronik, yang sebelumnya telah diatur dalam UU ITE. Dengan demikian, terdapat risiko bahwa dua lembaga atau lebih dapat mengklaim kewenangan yang sama dalam hal penegakan hukum dan pengawasan keamanan siber.

Hal ini dapat menyebabkan kebingungan dalam implementasi kebijakan serta memperlambat respon terhadap insiden siber, karena masing-masing lembaga mungkin memiliki prosedur dan standar yang berbeda. Selain itu, RUU ini juga mengatur tentang sertifikasi perangkat siber, yang sebelumnya telah diatur dalam ketentuan UU ITE. Potensi irisan tugas ini menimbulkan pertanyaan mengenai siapa yang berhak melakukan sertifikasi serta bagaimana mekanisme pengawasan akan dilaksanakan. Tanpa adanya kejelasan mengenai pembagian tugas dan tanggung jawab antar lembaga, akan sulit untuk mencapai efektivitas dalam pengelolaan keamanan siber nasional.

Lebih jauh lagi, RUU ini tampaknya tidak memberikan kerangka pengawasan yang memadai bagi pelaksanaan kewenangan besar yang diberikan kepada BSSN. Ketiadaan mekanisme pengawasan dapat membuka peluang bagi penyalahgunaan kewenangan oleh lembaga tertentu, terutama dalam hal penapisan konten. Misalnya, definisi mengenai apa yang dianggap "berbahaya" dalam konteks konten yang akan disensor tidak jelas, sehingga dapat menimbulkan ambiguitas dan potensi pelanggaran hak asasi manusia.

Dalam hal ini, penting untuk menyeimbangkan antara kebutuhan untuk melindungi keamanan siber dengan penghormatan terhadap kebebasan sipil. Dari perspektif kebijakan publik, sinergi antara berbagai pemangku kepentingan sangat diperlukan untuk menciptakan kerangka kerja yang komprehensif dalam menangani isu keamanan

siber. RUU ini seharusnya melibatkan kolaborasi antara pemerintah pusat, pemerintah daerah, sektor swasta, serta masyarakat sipil.

Jika pengelolaan keamanan siber hanya menjadi domain lembaga negara tanpa melibatkan partisipasi publik dan sektor swasta maka kebijakan tersebut berisiko tidak efektif. Hal ini juga berpotensi mengabaikan inovasi dan solusi kreatif dari pihak swasta serta masyarakat yang sering kali lebih cepat beradaptasi dengan perkembangan teknologi. Keberadaan dua Peraturan Presiden terkait keamanan siber yakni Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Kritikal juga menunjukkan bahwa pemerintah sudah memiliki kerangka kerja untuk menangani isu keamanan siber. Namun, jika RUU KKS tidak dirumuskan dengan hati-hati, bisa jadi justru akan menambah lapisan regulasi yang membingungkan alih-alih menyederhanakan proses pengelolaan.

Dalam konteks global, banyak negara telah menghadapi tantangan serupa ketika merumuskan Undang-Undang terkait keamanan siber. Pengalaman mereka menunjukkan bahwa penting untuk membangun kerangka hukum yang fleksibel dan adaptif agar dapat mengatasi dinamika ancaman siber yang terus berkembang. Oleh karena itu, Indonesia perlu belajar dari praktik terbaik internasional sambil tetap mempertimbangkan konteks lokalnya.

Secara keseluruhan, perancangan RUU KKS di Indonesia memiliki potensi untuk menciptakan irisan tugas antar lembaga negara jika tidak dikelola dengan baik. Ketiadaan kejelasan mengenai pembagian tugas antar lembaga serta kurangnya mekanisme pengawasan dapat memperburuk situasi ini. Oleh karena itu, penting bagi para pembuat kebijakan untuk memastikan bahwa RUU tersebut dirumuskan dengan melibatkan semua pemangku kepentingan dan mempertimbangkan aspek hukum serta hak asasi manusia agar dapat menciptakan kerangka kerja keamanan siber yang efektif dan inklusif di Indonesia.

Pembentukan RUU KKS diharapkan dapat memberikan dampak signifikan terhadap aspek beban keuangan negara. Dengan adanya Undang-Undang ini, Badan Siber dan Sandi Negara akan memperoleh kewenangan yang lebih besar dalam mengelola dan mengawasi keamanan siber di Indonesia, yang sebelumnya sangat terbatas. Hal ini penting mengingat Indonesia merupakan salah satu negara dengan jumlah pengguna internet yang tinggi, sehingga rentan terhadap serangan siber. Dengan memperkuat posisi BSSN, negara dapat lebih efisien dalam mengalokasikan anggaran untuk pertahanan siber, yang pada gilirannya dapat mengurangi potensi kerugian finansial akibat serangan siber yang diperkirakan mencapai triliunan rupiah setiap tahun.

RUU KKS juga berpotensi untuk meningkatkan transparansi dan akuntabilitas dalam pengelolaan anggaran terkait keamanan siber. Dengan adanya regulasi yang jelas, BSSN dapat menetapkan prioritas dalam pengeluaran dan memastikan bahwa dana yang dialokasikan digunakan secara efektif untuk mitigasi risiko dan penanggulangan serangan siber. Ini akan membantu pemerintah dalam merencanakan anggaran dengan lebih baik, serta memberikan jaminan kepada masyarakat bahwa dana publik digunakan untuk melindungi kepentingan nasional. Penetapan standar dan prosedur operasional yang diatur dalam RUU ini juga dapat membantu BSSN dalam melakukan evaluasi kinerja dan pengawasan terhadap penggunaan anggaran.

Pembentukan RUU KKS tidak hanya akan memperkuat lembaga BSSN dalam menjalankan kewenangannya, tetapi juga memberikan dampak positif terhadap pengelolaan keuangan negara. Melalui peningkatan kapasitas dan kewenangan BSSN, diharapkan Indonesia dapat lebih siap menghadapi ancaman siber yang terus berkembang. Hal ini akan menciptakan lingkungan digital yang lebih aman dan stabil, serta mendukung pertumbuhan ekonomi digital yang berkelanjutan tanpa harus terbebani oleh kerugian akibat serangan siber.

Namun, jika dilihat dari sisi anggaran dan keuangan negara, penerapan RUU KKS potensial menambah beban keuangan negara. Hal terjadi karena beberapa faktor, yakni:

1. Pembentukan dan Penguatan Infrastruktur Siber

   RUU KKS akan mengharuskan pembentukan dan penguatan infrastruktur keamanan siber nasional, yang mencakup teknologi, perangkat lunak, jaringan, dan sumber daya manusia. Biaya yang mungkin timbul antara lain:

   a. Pengadaan teknologi canggih untuk mencegah, mendeteksi, dan merespons ancaman siber;
   b. Pembangunan pusat data yang aman dan terlindungi dari serangan siber; dan
   c. Peningkatan kapasitas sumber daya manusia di sektor siber, termasuk pelatihan dan sertifikasi bagi profesional keamanan siber.

2. Peningkatan Kapasitas BSSN dan Lembaga Terkait

   Dengan berlakunya RUU KKS, BSSN dan lembaga terkait lainnya seperti Kementerian Komunikasi dan Digital akan memerlukan anggaran lebih besar untuk menjalankan fungsinya, termasuk:

   a. Pengembangan sistem dan perangkat pemantauan serta investigasi insiden siber;
   b. Perekrutan tenaga ahli siber yang kompeten untuk melakukan pengawasan dan audit keamanan siber; dan
   c. Kerja sama internasional untuk menghadapi ancaman siber lintas negara, yang melibatkan alokasi anggaran untuk kerjasama, konferensi, dan pelatihan internasional.

3. Penyusunan dan Implementasi Regulasi Baru

   RUU KKS akan menciptakan regulasi baru yang harus diimplementasikan di berbagai sektor, termasuk sektor publik dan swasta. Hal ini bisa menciptakan beban tambahan dalam hal:

   a. Biaya penerapan regulasi dan standar baru terkait keamanan siber, yang memerlukan investasi dalam teknologi dan audit

berkala; dan

b. Pengawasan kepatuhan oleh pemerintah, termasuk pemberian sanksi bagi entitas yang tidak mematuhi aturan keamanan siber.

4. Dukungan untuk Sektor Swasta dan Publik

Pemerintah mungkin perlu memberikan dukungan kepada sektor swasta dan publik untuk menerapkan standar keamanan siber yang lebih ketat, terutama bagi perusahaan kecil dan menengah yang mungkin tidak memiliki kemampuan keuangan untuk berinvestasi dalam teknologi keamanan siber tingkat tinggi.

5. Potensi Pengurangan Beban Jangka Panjang

Meski akan ada biaya tambahan yang dikeluarkan dalam implementasi awal, RUU KKS juga memiliki potensi untuk mengurangi beban keuangan jangka panjang dengan:

a. Mengurangi risiko serangan siber yang merugikan, yang dapat menyebabkan kerugian ekonomi besar bagi pemerintah dan sektor swasta;

b. Menghindari kebocoran data yang bisa menimbulkan biaya kompensasi dan pemulihan besar, serta merusak reputasi pemerintah; dan

c. Meningkatkan ketahanan ekonomi nasional dari ancaman digital yang semakin kompleks.

RUU KKS berfokus pada penguatan infrastruktur dan strategi untuk menghadapi ancaman siber di tingkat nasional. Dalam implementasinya, beban keuangan negara tentu akan meningkat, namun hal tersebut perlu dilihat dari perspektif jangka panjang, di mana manfaat yang diterima negara dan masyarakat bisa sebanding, bahkan melebihi beban tersebut. Di balik beban finansial yang besar, manfaat yang diterima dapat mencakup banyak aspek yang esensial bagi ketahanan dan stabilitas negara di masa depan. Salah satu manfaat yang paling utama adalah Pelindungan IIK nasional. Infrastruktur seperti jaringan listrik, telekomunikasi, air, serta layanan keuangan sangat rentan

terhadap serangan siber, yang jika tidak dilindungi dengan baik, dapat mengakibatkan gangguan masif pada ekonomi nasional dan kesejahteraan publik. Serangan terhadap infrastruktur ini, seperti yang terjadi dalam beberapa serangan siber skala besar di dunia, dapat mengakibatkan kerugian ekonomi yang jauh lebih besar dibandingkan dengan investasi dalam sistem pertahanan siber.

Keuntungan lainnya adalah meningkatnya kepercayaan investor dan pelaku ekonomi. Dalam era ekonomi digital, keamanan siber menjadi salah satu faktor utama dalam keputusan investasi. Negara dengan sistem keamanan siber yang kuat lebih mungkin menarik investor asing, yang merasa yakin bahwa aset dan data mereka terlindungi. Selanjutnya, pelindungan data pribadi akan semakin kuat dengan adanya regulasi yang lebih tegas. Dimana era pelanggaran data dan pencurian identitas menjadi masalah serius di seluruh dunia, regulasi keamanan siber tidak hanya melindungi entitas bisnis besar, tetapi juga individu. *General Data Protection Regulation* (GDPR) di Eropa, misalnya, telah menunjukkan bagaimana regulasi yang baik dapat memberikan dampak positif dalam melindungi hak privasi dan keamanan data masyarakat.

Secara jangka panjang, investasi dalam keamanan siber akan membantu negara mengurangi biaya yang diakibatkan oleh serangan siber, baik yang berbentuk kerugian finansial maupun gangguan pada infrastruktur publik. Studi oleh *Center for Strategic and International Studies* (CSIS) memperkirakan bahwa serangan siber mengakibatkan kerugian ekonomi global sekitar USD 600 miliar per tahun[155]. Tanpa Pelindungan yang memadai, potensi kerugian di masa depan bisa lebih besar seiring dengan perkembangan teknologi dan meningkatnya jumlah data digital yang diproses setiap harinya. Selain itu, penguatan ketahanan siber nasional berfungsi sebagai penangkal ancaman geopolitik yang semakin kompleks. Serangan siber yang dilancarkan oleh

[155] The Economic Impacts of Cyber Crime: How it Costs Us All, www.citationcyber.com, diakses pada 11 Oktober 2024

negara atau aktor non-negara dapat digunakan sebagai alat perang asimetris. Dengan demikian, ketahanan siber yang kuat menjadi bagian integral dari strategi pertahanan nasional .

E. Kajian terhadap Praktik dan Koordinasi Penyelenggaraan Negara.

Ketahanan siber di Indonesia semakin penting seiring meningkatnya jumlah pengguna internet dan kemajuan teknologi yang pesat. Masyarakat kini mengandalkan sistem digital dalam berbagai aspek kehidupan, seperti perbankan, pendidikan, kesehatan, hingga urusan administrasi publik. Namun, ketergantungan ini juga diiringi oleh peningkatan risiko kejahatan siber yang dapat merugikan secara finansial dan sosial. Serangan seperti pencurian data pribadi, penyebaran *malware*, dan penipuan berbasis digital menjadi ancaman yang kian nyata. Meskipun Indonesia telah memiliki BSSN serta regulasi terkait, seperti UU ITE, sistem ketahanan siber di Indonesia masih dinilai belum cukup untuk menghadapi kejahatan siber yang semakin canggih. Hal ini menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan, terutama terhadap pengguna yang tidak terlindungi secara optimal, seperti pelaku usaha kecil dan individu.

Permasalahan utama yang dihadapi masyarakat terkait ketahanan siber adalah lemahnya pelindungan data pribadi dan kurangnya kesadaran tentang praktik keamanan digital yang baik. Kebocoran data yang melibatkan informasi sensitif sering kali terjadi akibat serangan siber atau lemahnya sistem keamanan pada *platform* yang digunakan masyarakat. Misalnya, kasus pencurian data pada sektor perbankan dan *e-commerce* sering kali mengekspos informasi pribadi pengguna yang kemudian disalahgunakan untuk kegiatan kriminal seperti pencurian identitas dan penipuan. Bagi masyarakat, hal ini dapat menimbulkan dampak jangka panjang, seperti kerugian finansial, hilangnya rasa aman, serta rusaknya reputasi digital. Tanpa ketahanan siber yang memadai, pengguna platform digital tetap rentan terhadap berbagai serangan siber yang bisa merugikan mereka secara serius. Oleh karena itu, ketahanan siber perlu diperkuat tidak hanya melalui regulasi

yang jelas, tetapi juga melalui edukasi publik untuk meningkatkan pemahaman dan kewaspadaan masyarakat terhadap ancaman siber.

Dalam menghadapi permasalahan ini, diperlukan penguatan kerangka ketahanan siber yang tidak hanya berfokus pada pencegahan serangan tetapi juga mampu merespons dan memulihkan kerugian yang dialami masyarakat akibat serangan siber. Pemerintah dapat mempertimbangkan pengesahan RUU KKS yang dapat memberikan landasan hukum yang lebih kuat bagi BSSN dan lembaga terkait lainnya untuk berkoordinasi dalam menghadapi ancaman siber secara efektif. RUU KKS diharapkan mampu mengatur ketahanan siber secara komprehensif, termasuk pemantauan risiko, pemberian standar keamanan minimum bagi penyelenggara sistem elektronik, serta pelindungan hak pengguna digital. Dengan adanya regulasi yang lebih tegas, diharapkan masyarakat tidak hanya terlindungi dari risiko serangan siber tetapi juga lebih percaya diri dalam memanfaatkan teknologi digital secara aman

BAB III
EVALUASI DAN ANALISIS PERATURAN PERUNDANG-UNDANGAN

A. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik

Dalam konteks pengaturan keamanan siber di Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) memuat beberapa pasal yang relevan untuk mendukung fungsi BSSN dalam menjaga keamanan sistem elektronik. Namun, tinjauan terhadap beberapa pasal tersebut menunjukkan adanya kebutuhan regulasi tambahan yang lebih komprehensif melalui RUU KKS. Pasal 13 UU ITE, misalnya, menetapkan tanggung jawab penyelenggara sistem elektronik dalam menjaga keamanan sistem, sementara BSSN bertindak sebagai pengawas sertifikasi elektronik untuk memastikan kepatuhan terhadap regulasi dan standar keamanan. Namun, cakupan pasal ini masih terbatas, terutama dalam aspek pemantauan berkelanjutan dan penegakan keamanan yang lebih terstruktur, sehingga diperlukan UU KKS untuk memperkuat pengawasan dan penegakan hukum pada sektor ini.

Selanjutnya, Pasal 19 UU ITE mengatur penggunaan sistem elektronik dalam transaksi elektronik, dengan BSSN berperan dalam memastikan keandalan dan integritas sistem yang digunakan. Meskipun demikian, UU ITE belum sepenuhnya menangani isu keandalan sistem secara menyeluruh, seperti pengembangan standar keamanan yang dapat mengakomodasi ancaman siber yang terus berkembang. UU KKS diharapkan dapat menghadirkan kebijakan yang lebih kuat dalam menetapkan dan mengawasi standar keamanan bagi sistem transaksi elektronik, baik untuk penyelenggara lokal maupun asing, demi menjaga kepercayaan publik terhadap keamanan transaksi digital. Selain itu, aspek mitigasi risiko dan pemulihan dalam menghadapi insiden siber yang kompleks juga perlu dipertegas dalam UU KKS, mengingat saat ini UU ITE tidak memberikan panduan yang cukup rinci untuk menangani serangan yang lebih serius, seperti *ransomware* dan *hacking*.

Pasal 27 sampai dengan Pasal 29 UU ITE yang berfokus pada pelarangan tindakan ilegal, pemulihan data, dan pelindungan dari ancaman kekerasan di ruang siber juga memiliki keterbatasan. UU ITE memang mengatur sanksi terhadap penggunaan sistem elektronik yang menyimpang, namun Undang-Undang ini kurang memberikan pendekatan holistik terkait keamanan siber nasional. UU KKS dapat memperkuat aspek ini dengan memberikan mandat kepada BSSN dan instansi terkait untuk secara proaktif mengidentifikasi, mencegah, dan memitigasi potensi serangan siber yang meluas. Selain itu, UU KKS diharapkan mencakup kerangka kerja untuk kolaborasi antara BSSN, penyelenggara sistem elektronik, dan penegak hukum, sehingga penanganan terhadap insiden siber bisa lebih efektif.

B. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara

Pada tahun 2017 merupakan titik penting dalam transformasi keamanan informasi dan siber di Indonesia yang ditandai dengan didirikannya BSSN berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara. Mengacu pada hal tersebut, berdasarkan Pasal 1 ayat (1) Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, BSSN kemudian didefinisikan sebagai “Lembaga Pemerintah Non-Kementerian”. Berdasarkan Pasal 2 Peraturan Presiden ini, tugas BSSN adalah melaksanakan keamanan siber, sementara persandian menjadi salah satu fungsi dalam lingkup kerja BSSN.

Beberapa bulan setelah pendirian BSSN, Peraturan Presiden Nomor 133 Tahun 2017 diterbitkan untuk mengubah Peraturan Presiden Nomor 53 Tahun 2017. Salah satu perubahan penting dalam peraturan ini adalah penghapusan istilah "Lembaga Pemerintah Non-Kementerian" dari definisi BSSN. Perubahan ini menandai adanya evolusi peran BSSN dari sekedar lembaga teknis ke lembaga dengan tugas dan fungsi yang lebih strategis dalam keamanan siber nasional. Penghapusan istilah ini juga memberikan fleksibilitas lebih kepada BSSN dalam

mengembangkan struktur kelembagaan dan fungsinya, seiring dengan meningkatnya kebutuhan keamanan siber di tingkat nasional maupun internasional.

Evolusi peran BSSN semakin terlihat jelas dengan diterbitkannya Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara yang memperluas tugas dan fungsi BSSN. Berdasarkan Pasal 2 Peraturan Presiden ini, tugas BSSN tidak hanya melaksanakan keamanan siber, tetapi terdapat penambahan persandian dan/atau melaksanakan keamanan sandi. Perihal persandian, pada Peraturan Presiden Nomor 53 Tahun 2017 tentang tentang Badan Siber dan Sandi Negara jo. Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, hanya termasuk ke dalam fungsi dari BSSN. Dengan diundangkannya Peraturan Presiden terbaru yaitu Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Sandi dan Siber Negara, persandian menjadi tugas utama dari BSSN.

Perluasan tugas ini memberikan perluasan terhadap fungsi yang dimiliki oleh BSSN, yaitu perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi, pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi negara, penyusunan norma, standar, prosedur, dan kriteria di bidang persandian, pelaksanaan bimbingan teknis dan supervisi di bidang persandian, koordinasi pelaksanaan tugas, pembinaan, dan dukungan administrasi kepada seluruh unsur organisasi di lingkungan BSSN, pengelolaan barang milik negara yang menjadi tanggung jawab BSSN, pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN, dan pengawasan atas pelaksanaan tugas di lingkungan Badan Siber dan Sandi Negara. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara menunjukkan bahwa BSSN kini memiliki peran strategis yang lebih luas dalam kebijakan dan tata kelola siber Indonesia.

Untuk memastikan efektivitas BSSN dalam menjalankan fungsinya, diperlukan harmonisasi antara berbagai peraturan yang mengatur

BSSN, baik dalam lingkup keamanan siber maupun persandian. Transformasi Lembaga Sandi Negara menjadi BSSN mencerminkan adaptasi pemerintah Indonesia terhadap tantangan era digital. Dalam kerangka regulasi yang ada saat ini, pengembangan peran BSSN sangat bergantung pada penerbitan regulasi baru yang akan memperluas kewenangan dan tanggung jawabnya. Setiap perluasan peran tersebut harus tetap sejalan dengan tugas dan fungsi yang telah ditetapkan melalui peraturan presiden. Artinya, meskipun BSSN memiliki potensi untuk memainkan peran yang lebih strategis dalam keamanan siber nasional, kemampuan lembaga ini untuk berkembang dan beradaptasi dengan tantangan baru, seperti ancaman siber yang semakin kompleks, sangat dipengaruhi oleh sejauh mana peraturan tambahan memungkinkan BSSN untuk melaksanakan tugas tambahan yang sejalan dengan pengembangan peran baru dari BSSN.

C. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber berfokus pada pelindungan ruang siber dan penanganan krisis yang terkait dengan serangan siber. Beberapa poin penting yang berhubungan langsung dengan keamanan dan keamanan siber antara lain penguatan tata kelola, manajemen risiko, kesiapsiagaan dan ketahanan terhadap insiden siber, serta pelindungan IIK. Peraturan ini juga menekankan pentingnya kolaborasi antara instansi negara dan pemangku kepentingan lainnya, baik dalam menangani insiden maupun dalam membangun kapabilitas dan kapasitas keamanan siber. Selain itu, Peraturan Presiden ini mengatur tentang kebijakan kriptografi nasional dan kerja sama internasional untuk memastikan ruang siber yang aman, terbuka, dan stabil.

Dalam rangka RUU KKS, evaluasi yang bisa dilakukan meliputi efektivitas implementasi strategi keamanan siber nasional ini, terutama pada aspek pelindungan IIK dan kesiapsiagaan dalam menghadapi

krisis. Evaluasi bisa dilakukan terhadap kualitas manajemen risiko yang diterapkan, mengingat semakin meningkatnya ancaman siber yang bisa berdampak luas terhadap ekonomi dan kedaulatan negara. Di samping itu, penguatan kapabilitas teknologi serta peningkatan keterampilan SDM dalam keamanan siber, termasuk pendidikan yang dimulai sejak usia dini, menjadi poin penting yang perlu terus dipantau dan dievaluasi. Evaluasi lainnya bisa diarahkan pada tingkat sinergi antar lembaga dan seberapa baik implementasi kebijakan kriptografi nasional untuk mendukung ketahanan siber negara.

Peraturan Presiden ini juga masih menunjukkan beberapa kekurangan yang perlu diperbaiki dalam RUU KKS. Salah satu kekurangannya adalah perlunya peningkatan sistem pemantauan secara *real-time* yang lebih kuat dan menyeluruh, terutama dalam deteksi dini terhadap potensi ancaman siber yang dapat berkembang menjadi krisis nasional. Selain itu, regulasi yang lebih jelas terkait dengan pemulihan sistem setelah krisis dan upaya mitigasi yang cepat dan tepat sasaran perlu dimasukkan dalam RUU. Koordinasi yang lebih intensif antara sektor pemerintah dan sektor swasta dalam penanganan insiden siber juga perlu diperkuat.

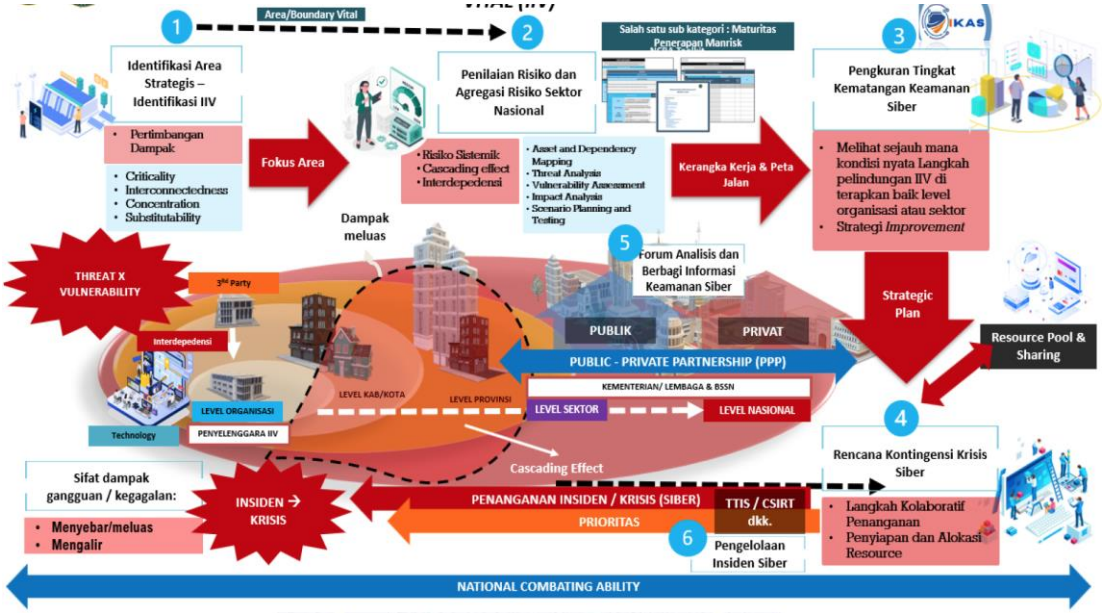
Berdasarkan uraian di atas, bahwa hukum positif atau regulasi eksisting saat ini belum mengakomodasi kebutuhan hukum dan kerangka kebijakan terkait dengan keamanan dan ketahanan siber yang membutuhkan pendekatan regulasi baik di level hulu, level menengah, dan level hilir. Dengan demikian, dibutuhkan pembentukan Undang-Undang tersendiri yang mengatur materi muatan didasari prinsip dan *best practices* internasional di bidang keamanan dan ketahanan siber.

D. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital

Pemerintah telah menetapkan Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) yang bertujuan untuk melindungi keberlangsungan penyelenggaraan IIV secara aman, andal, dan terpercaya; mencegah terjadinya gangguan,

kerusakan, dan/atau kehancuran pada IIV akibat serangan siber, serta meningkatkan kesiapan dalam menghadapi insiden siber dan mempercepat pemulihan dari dampak insiden siber. IIV sendiri didefinisikan sebagai Sistem Elektronik yang memanfaatkan teknologi informasi dan/ atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan sistem elektronik lainnya dalam menunjang sektor strategis, yang jika terjadi gangguan, kerusakan, dan/ atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.

Secara umum konsepsi pelindungan IIV diterapkan dengan mengedepankan pertimbangan risiko terhadap aset-aset informasi yang bersifat kritikal bagi layanan vital, seperti ditunjukkan pada Gambar 1.



Gambar 1. Konsepsi Pelindungan IIV Nasional

Pada tahap awal implementasi kebijakan, negara perlu mengidentifikasi infrastruktur informasi yang memiliki potensi dampak serius bagi masyarakat. Potensi dampak tersebut dapat dilihat dari seberapa penting sistem tersebut menunjang layanan (*criticality*), seberapa banyak layanan lain yang bergantung terhadap sistem tersebut (*interdependencies, concentration*), ketersediaan sistem lain yang dapat

menggantikan ketika terjadi gangguan (*substitution*) dan tingkat interkoneksi sistem dengan sistem lainnya (*interconnectedness*). Dalam melakukan proses identifikasi IIV perlu dipertimbangkan dampak yang mungkin timbul akibat insiden mulai dari level organisasi atau Penyelenggara Sistem Elektronik sampai dengan level nasional atau yang dikenal sebagai dampak berjenjang (*cascading effect*) baik dalam satu sektor ataupun sektor lainnya. Secara keseluruhan proses identifikasi sistem elektronik strategis tersebut telah diatur dalam kebijakan teknis, yaitu Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital.

Tahap berikutnya adalah penerapan kerangka kerja pelindungan terhadap sistem IIV sesuai dengan hasil manajemen risiko yang ada di masing-masing organisasi penyelenggara IIV. Kerangka kerja yang diterapkan berupa pemenuhan kontrol keamanan yang dapat berupa pemenuhan kebijakan keamanan, penerapan teknologi pelindungan, atau peningkatan kapasitas SDM terkait keamanan siber yang dapat mengacu kepada Peraturan BSSN Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan IIV dan Peraturan BSSN Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas SDM Keamanan Siber dan Sandi. Selanjutnya untuk mengukur pencapaian dan efektivitas dari penerapan kontrol keamanan yang telah dilaksanakan oleh penyelenggara IIV maka perlu dinilai penerapannya dalam sebuah penilaian tingkat kematangan yang mengacu kepada Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber. Hasil dari pengukuran tersebut dapat dijadikan sebagai dasar dalam penyusunan rencana strategis untuk mempersiapkan sumber daya dalam menghadapi setiap ancaman dan insiden siber. Selain itu, hasil dari pengukuran tingkat kematangan dapat digunakan oleh pemerintah dalam menyusun rencana kontingensi nasional untuk menghadapi potensi terjadinya krisis siber yang dapat mengacu kepada Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber.

Untuk mengantisipasi terjadinya krisis siber perlu adanya pihak yang diberikan kewenangan untuk mengelola setiap insiden siber yang

terjadi pada sistem elektronik IIV. Penanganan dan pemulihan insiden siber pada sistem elektronik IIV perlu dilakukan dengan tepat dan cepat. Karena, potensi dampaknya yang dapat meluas dan mengakibatkan berhentinya layanan publik. Oleh karena itu, perlu dibentuk Tim Tanggap Insiden Siber yang bertugas mengelola setiap insiden siber yang terdeteksi pada sektor IIV. Nantinya, eskalasi penanganan dan pemulihan terhadap insiden siber di sektor IIV dapat dilakukan secara bertahap mulai dari Tim Tanggap Insiden Siber Organisasi, Sektoral, hingga Nasional. Secara umum tata kelola pengelolaan insiden siber diatur lebih lanjut dalam Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.

Peningkatan kapasitas proses bisnis untuk memastikan penyelenggaraan keamanan dan ketahanan siber dapat berjalan efektif dan efisien, salah satunya adalah dengan melakukan peningkatan kapasitas proses bisnis selain peningkatan kapasitas SDM dan teknologi.

Peningkatan kapasitas proses bisnis dilakukan salah satunya adalah melalui penerapan manajemen risiko keamanan siber secara berkelanjutan sebagai bagian dari tata kelola keamanan siber untuk memastikan setiap potensi ancaman dapat teridentifikasi sejak awal sehingga dapat dilakukan mitigasi risiko secara optimal. Untuk mendukung upaya mitigasi risiko dan penanganan insiden secara efektif maka pembelajaran dari setiap penanganan insiden sebelumnya menjadi sangat penting bagi setiap penyelenggara infrastruktur informasi. Oleh karena itu sangat penting bagi setiap penyelenggara infrastruktur informasi khususnya penyelenggara infrastruktur informasi kritikal untuk saling berbagi informasi insiden siber. Informasi hasil pembelajaran ini selanjutnya dapat dikelola menjadi suatu ensiklopedi atau pustaka penanganan insiden siber yang dapat diakses secara nasional.

Dalam upaya pelindungan atau proteksi infrastruktur informasi khususnya untuk menjamin terselenggaranya layanan keamanan informasi yang meliputi kerahasiaan dan keutuhan data/informasi dari

pihak yang tidak berwenang serta jaminan keotentikan sumber data/informasi agar dapat divalidasi secara tepat maka penerapan persandian menjadi kunci utama yang tidak dapat ditawar lagi. Dengan menerapkan persandian, pihak yang tidak berwenang tidak dapat mengakses informasi yang bukan haknya, dan jika terjadi upaya modifikasi oleh pihak yang tidak berhak dapat diidentifikasi. Selain itu melalui jaminan keotentikan sumber data/informasi maka pihak yang terlibat komunikasi tidak dapat menyangkal karena dapat dibuktikan secara teoritis menggunakan teknik persandian.

Guna memastikan penyelenggaraan keamanan siber dapat memenuhi standar keamanan yang telah ditentukan oleh pemerintah melalui BSSN, maka setiap penyelenggara infrastruktur informasi harus melakukan pengukuran tingkat kematangan keamanan siber. Pengukuran dilakukan secara berkala dan berkelanjutan untuk mengantisipasi perkembangan teknologi dan lingkungan internal maupun eksternal. Disisi lain, untuk menjamin kepatuhan terhadap pemenuhan standar keamanan dapat terjaga secara berkelanjutan, maka secara periodik juga perlu dilakukan audit dan asesmen keamanan siber.

BAB IV
LANDASAN FILOSOFIS, SOSIOLOGIS, YURIDIS

A. Landasan Filosofis

Secara filosofis, pengaturan terkait keamanan siber menggunakan berbagai pendekatan yang saat ini digunakan oleh dunia internasional dan berbagai negara dalam bentuk pendekatan *Cybersecurity.* Hal ini pun mencerminkan pengakuan serta pelindungan kepentingan umum serta pelindungan terhadap hak dasar manusia untuk memperoleh kehidupan yang aman dan dilindungi oleh negara. Dengan demikian, penyusunan RUU KKS memiliki dasar filosofis yang kokoh dan dapat dipertanggungjawabkan. Pancasila dalam hal ini menjadi landasan filosofi utama dalam kaitannya dengan jaminan keamanan dan ketahanan siber. Pancasila sebagai *rechtsidee* (cita hukum) yang merupakan konstruksi berpikir dalam mengarahkan hukum kepada apa yang menjadi cita-cita bangsa.

Menurut Attamimi, Pancasila sebagai *rechtsidee* akan melakukan fungsinya yang bersifat konstitutif sekaligus regulatif terhadap sistem norma hukum Indonesia secara konsisten dan berlaku terus menerus.[156] Sebagai cita bangsa tersebut, Pancasila memiliki 3 (tiga) nilai, yang pertama adalah nilai dasar dimana asas-asas yang diterima sebagai dalil yang sedikit banyak mutlak yang terdiri dari ketuhanan, kemanusiaan, persatuan, nilai kerakyatan dan nilai keadilan. Kedua, nilai instrumental, dimana merupakan pelaksanaan umum dari nilai-nilai dasar, terutama berbentuk norma hukum yang selanjutnya dikristalisasi dalam peraturan perundang-undangan. Ketiga, nilai praktis yakni nilai yang sesungguhnya dilaksanakan dalam kenyataan yang berasal dari nilai dasar.[157]

Cita hukum bersifat normatif dan konstitutif. Dalam konteks normatif, cita hukum berfungsi sebagai prasyarat *transcendental* yang

[156] Teguh Prasetyo, "Membangun Hukum Nasional Berdasarkan Pancasila", Jurnal Hukum dan peradilan, Vol. 3 Nomor 3, 2014, hlm. 216.
[157] Teguh Prasetyo, *Hukum dan Sistem Hukum Berdasarkan Pancasila*, Media Perkasa, Yogyakarta, 2013, hlm. 2

mendasari setiap hukum positif yang memiliki nilai, serta menjadi landasan moral hukum dan tolok ukur sistem hukum positif itu sendiri. Sementara itu, dalam arti konstitutif, cita hukum berfungsi untuk mengarahkan hukum ke arah tujuan yang ingin dicapai. Gustaf Radbruch mengemukakan bahwa "*rechtsidee*" berfungsi sebagai dasar konstitutif bagi hukum positif, memberikan makna kepada hukum tersebut. Rechtsidee juga berperan sebagai tolok ukur regulatif untuk menilai keadilan hukum positif.[158] Cita hukum memiliki pengaruh yang signifikan dan berfungsi sebagai asas umum yang memberikan pedoman (*guiding principle*), norma untuk evaluasi (kaidah evaluasi), serta faktor pendorong dalam pelaksanaan hukum, termasuk dalam pembentukan, penemuan, penerapan hukum, dan perilaku hukum itu sendiri.

Mengacu pada sila ketiga Pancasila, yaitu “Persatuan Indonesia” menjadi dasar dari landasan filosofis dari keamanan dan ketahanan siber. Dalam konteks ini, negara bertanggung jawab untuk menjamin pelindungan dari adanya ancaman siber dengan memperkuat keamanan dan ketahanan siber sebagai bentuk upaya pertahanan negara dan meningkatkan integritas bangsa. Persatuan mencerminkan kebutuhan untuk mengintegrasikan berbagai elemen masyarakat, pemerintah, dan sektor swasta dalam menghadapi ancaman siber. Persatuan juga berarti menjaga identitas nasional ditengah arus globalisasi dan kemajuan teknologi. Regulasi keamanan dan ketahanan siber yang berlandaskan pada sila ini, akan mengupayakan pelindungan data dan informasi yang berhubungan erat dengan identitas bangsa sehingga dapat mencegah ancaman yang dapat merusak integritas nasional, serta menjaga nilai-nilai bangsa. Pancasila dalam hal ini juga mendasari adanya persatuan dari lembaga terkait untuk berkolaborasi demi mencapai tujuan keamanan dan ketahanan siber. Regulasi keamanan dan ketahanan siber harus dapat menciptakan kerangka kerja yang memfasilitasi kolaborasi antara BSSN, kementerian terkait lembaga penegak hukum, hingga sektor swasta agar tercapai tujuan Indonesia yang lebih cepat

[158] Sahat Maruli Tua S., “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber”, SASI, Vol. 27 Nomor 1, 2021.

tanggap dan efektif dalam menangani ancaman siber.

Pada dasarnya kelima sila dari Pancasila telah membentuk satu kesatuan yang menjadi dasar dari filsafat bangsa Indonesia. Sila pertama, Ketuhanan Yang Maha Esa, mencerminkan keyakinan bangsa terhadap keberadaan Tuhan dan kesadaran akan keterbatasan makhluk-Nya. Sila kedua, kemanusiaan yang adil dan beradab, menyoroti upaya negara untuk mencapai kesejahteraan umat manusia. Sila ketiga, persatuan Indonesia, menekankan pentingnya persatuan sebagai kekuatan untuk mencapai tujuan bersama. Sila keempat, kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam permusyawaratan/perwakilan, menunjukkan bahwa Indonesia menganut prinsip demokrasi dalam semua aspek kehidupan. Sila kelima, keadilan sosial bagi seluruh rakyat Indonesia, menegaskan keinginan untuk memberikan keadilan dan kesejahteraan kepada seluruh rakyat.[159]

Perkembangan dunia teknologi saat ini memberikan ancaman yang semakin nyata dan mengkhawatirkan. Pesatnya perkembangan teknologi memberikan manfaat sekaligus ancaman yang besar terhadap dunia siber.[160] Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menjelaskan bahwa tujuan pembentukan Negara Republik Indonesia adalah untuk membentuk pemerintahan Negara Indonesia yang mampu melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum. Hal ini menegaskan bahwa salah satu tugas dari negara yakni memberikan pelindungan bagi setiap bangsa Indonesia. Salah satu pelindungan yang menjadi kewajiban negara kepada segenap bangsa Indonesia adalah pelindungan dalam mengakses dunia siber.

Sebagaimana yang tercantum dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa “Negara Indonesia adalah negara hukum”, maka

[159] Candra Irawan, *Politik Hukum Hak Kekayaan Intelektual Indonesia,* Bandung: Mandar Maju, 2011, hlm. 22
[160] Dinda Aprilita Herera & Muhamad Hasan Sebyar, “Pelindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru”, Jurnal Hukum dan Kewargunaan Vol. 1 Nomor 5 Tahun 2023.

pada dasarnya sudah menjadi kewajiban bagi negara ini dalam memperkuat hukum yang dapat menjamin pelindungan bagi masyarakat dari segala bentuk ancaman siber.[161] Hal ini sejalan dengan yang ditetapkan dalam konstitusi negara yang dimuat pada Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menentukan bahwa "Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.[162] Konstitusi tersebutlah yang mendasari bahwa sudah semestinya negara dapat menjamin hak masyarakat atas pelindungan diri dari segala bentuk ancaman, salah satunya ancaman siber demi menjunjung hak asasi manusia.

Landasan filosofis ketahanan siber berasaskan kedaulatan negara, pelindungan dan kepastian hukum, ekstrateritorialitas, transparansi, inovasi teknologi yang bertanggung jawab, pengembangan ekonomi digital, serta penghargaan dan pelindungan hak asasi manusia. Secara yuridis, pengaturan ketahanan siber menjadi sangat penting mengingat kerangka hukum Indonesia sebelumnya cenderung berfokus pada aspek keamanan siber tanpa sepenuhnya mempertimbangkan aspek pemulihan pasca insiden. Dengan ancaman siber yang semakin canggih dan berpotensi mengganggu pelayanan publik, stabilitas ekonomi, dan kedaulatan negara, ketahanan siber menjadi fondasi penting bagi terwujudnya Indonesia yang berdaulat, mandiri, dan berkepribadian dalam tataran ruang siber, sekaligus mendukung pertumbuhan ekonomi digital dengan memberikan kepastian hukum dan rasa aman bagi pengguna teknologi informasi.

B. Landasan Sosiologis

Landasan sosiologis dalam RUU KKS bahwa di Indonesia mencakup pemahaman tentang interaksi masyarakat dengan teknologi informasi

[161] Pasal 1 Ayat (3) Undang-Undang Dasar Negara Republik Indonesia 1945.
[162] Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik indonesia 1945.

serta dampaknya terhadap kehidupan sosial. Terdapat beberapa pertimbangan sosiologis yang perlu diuraikan dalam melihat urgensi RUU KKS di Indonesia

Pertama, berkaitan dengan iklim perkembangan teknologi informasi dan komunikasi yang pesat, dimana kehidupan masyarakat Indonesia tidak dapat dipisahkan dari fenomena sosiologi siber. Hal ini dikarenakan dengan semakin terintegrasinya kehidupan masyarakat di ruang siber meningkatkan ancaman kejahatan siber. Aspek penting dari sosiologi siber di Indonesia adalah maraknya kasus kejahatan siber yang terjadi di Indonesia, dimana pada tahun 2023 saja telah tercatat lebih dari 279,84 (dua ratus tujuh puluh sembilan koma delapan puluh empat) juta serangan siber telah terjadi di Indonesia.[163] Peningkatan akses dan penggunaan teknologi informasi berdampak pada munculnya berbagai bentuk perilaku menyimpang, seperti pembobolan akun, pencurian data pribadi, penyebaran konten berbahaya, dan penipuan daring[164].

Salah satu contoh nyatanya adalah serangan *ransomware* Lock Bit 3.0 pada Pusat Data Nasional (PDN) milik Kementerian Komunikasi dan Digital (dahulu Kementerian Komunikasi dan Informatika) yang terjadi pada bulan Juni 2024 kemarin.[165] Serangan ini menyebabkan gangguan pada layanan publik penting seperti pendaftaran peserta didik baru dan layanan imigrasi, menunjukkan betapa rentannya IIK tanpa pelindungan hukum yang kuat. Hal ini menunjukkan bahwa masih terdapat isu yang perlu diperhatikan dalam konteks keamanan siber di Indonesia.

Pada 20 Juni 2024, PDNS 2 Surabaya terkena serangan siber yang mengganggu layanan penting dan berdampak pada instansi pemerintah,

---

[163] OJK Indonesia, (2024), "Strategi Mencegah Serangan Siber", <https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/4021/strategi-mencegah-serangan-siber> diakses pada 10 Oktober 2024 pukul 15.27 WIB.

[164] Chintia, Ervina, et al. "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya." *Journal Information Engineering and Educational Technology)* Volume 02, Nomor 02, 2019, hlm.66

[165] Novalia Panji Nugroho, (2024), "BSSN Dorong Penyusunan RUU KKS", <https://nasional.tempo.co/read/1884272/bssn-dorong-penyusunan-ruu-keamanan-dan-ketahanan-siber> diakses pada 10 Oktober 2024 pukul 15.05 WIB

termasuk layanan imigrasi. Gangguan ini diakibatkan oleh *ransomware Brain Chipper*, dengan tuntutan tebusan sebesar USD 8 (delapan) juta. Pemulihan layanan berlangsung selama beberapa hari, dan serangan ini menggarisbawahi kebutuhan akan sistem backup dan *Disaster Recovery Plan* (DRP) yang kuat untuk ketahanan siber di masa depan.[166]

Kedua, keamanan siber berkaitan erat dengan kepercayaan publik terhadap Infrastruktur Informasi.[167] Tanpa adanya regulasi yang jelas, masyarakat cenderung merasa khawatir saat menggunakan layanan digital sehingga dengan adanya Undang-Undang ini dapat membangun kepercayaan publik dengan memberikan jaminan hukum atas pellindungan data pribadi dan keamanan informasi, sehingga masyarakat merasa aman dalam berinteraksi di ruang siber. Adapun dasar regulasi yang menjadi acuan dalam berperilaku di ruang siber adalah Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Kedua, Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Kritikal.

Ketiga, media sosial dan komunikasi daring telah mengubah pola interaksi dan komunikasi masyarakat. Ruang digital telah menjadi lahan subur bagi penyebaran informasi, baik yang faktual maupun yang bersifat hoaks atau misinformasi. Dilansir dari Katadata.com, jumlah pengguna media sosial di Indonesia pada tahun 2024 mencapai 191 (seratus sembilan puluh satu) juta pengguna atau 73,7% (tujuh puluh tiga koma tujuh persen) dari jumlah penduduk di Indonesia sehingga fenomena ini menjadi tantangan tersendiri bagi masyarakat yang harus dapat memfilter informasi dengan baik dan bijak.[168] Selain itu, peningkatan penggunaan media sosial dan internet di Indonesia tidak dibarengi dengan peningkatan literasi digital/teknologi di masyarakat

---

[166] *Ibid,* hlm.208

[167] Mochamad Januar Rizki, (2021), "Keamanan dan Ketahanan Siber Perlu Payung Hukum Komprehensif", <https://www.hukumonline.com/berita/a/keamanan-dan-ketahanan-siber-perlu-payung-hukum-komprehensif-lt607fcfb349c85/> diakses pada 10 Oktober 2024, pukul 15.20 WIB

[168] Andreas Daniel Panggabean, (2024), "Ini Data Statistik Penggunaan Media Sosial Masyarakat Indonesia Tahun 2024", <https://www.rri.co.id/iptek/721570/ini-data-statistik-penggunaan-media-sosial-masyarakat-indonesia-tahun-2024> diakses pada 10 Oktober 2024 pukul 15.46 WIB.

sehingga akan semakin memperbesar peluang pihak tidak bertanggungjawab dalam melakukan ancaman kejahatan siber.

Dengan memperhatikan beberapa pertimbangan sosiologis tersebut, maka kebutuhan akan eksistensi UU KKS sangat diperlukan. Dengan adanya regulasi yang komprehensif, diharapkan dapat meningkatkan pelindungan terhadap masyarakat, menjaga stabilitas nasional, dan mendukung perkembangan ekonomi digital di Indonesia, khususnya pelindungan terhadap Infrastruktur Informasi dan Infrastruktur Informasi Kritikal.

C. Landasan Yuridis

Landasan yuridis pembentukan RUU KKS dapat diidentifikasi dari kebutuhan regulasi yang komprehensif guna menghadapi ancaman siber yang semakin kompleks di tengah kemajuan teknologi. Meskipun Indonesia telah memiliki Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, keberadaannya belum cukup efektif dalam menangani kejahatan siber yang kian berkembang pesat. Hal ini terlihat dari keterbatasan wewenang BSSN yang belum mampu menjangkau seluruh aspek keamanan siber, baik dalam ranah publik maupun privat. Selain itu, BSSN juga masih fokus pada kegiatan pengawasan dan koordinasi, tanpa memiliki instrumen hukum yang kuat untuk menangani kejahatan siber secara langsung.

Saat ini, hukum terkait keamanan siber di Indonesia masih tergolong fragmentaris dan belum menyeluruh. Terdapat Peraturan Perundang-undangan yang berkaitan dengan keamanan siber. Secara hierarkis, Undang-Undang Nomor 8 Tahun 2016 tentang Informasi dan Transaksi Elektronik sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik berfokus pada pelindungan data pribadi dan kriminalisasi tindakan yang berkaitan dengan dunia maya, tetapi tidak mencakup secara rinci kebijakan penguatan ketahanan siber nasional. Peraturan perundang-undangan lain yang berkaitan dengan keamanan

siber, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU PDP tidak mengatur secara spesifik tentang keamanan dan ketahanan siber. Hal ini juga sama seperti di dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Pelaksanaan Sistem dan Transaksi Elektronik, yang merupakan peraturan pelaksana dari UU ITE.

KUHP Nasional yang terbaru sudah mengakomodir kejahatan dunia digital/siber yang marak belakangan terakhir. Bahkan perkembangan kejahatan digital/siber di masa mendatang. Dengan begitu, KUHP Nasional sejatinya melengkapi berbagai kekurangan yang terdapat dalam UU No.19 Tahun 2016 tentang Perubahan atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta UU tindak pidana lainnya.

Peraturan perundang-undangan yang telah disebutkan di atas dinilai oleh banyak pihak masih terfragmentasi dan tidak memberikan kerangka hukum yang komprehensif untuk menangani ancaman kejahatan siber yang kompleks, seperti serangan *ransomware* dan pencurian identitas. Kasus seperti kebocoran data Tokopedia pada 2020, yang mempengaruhi lebih dari 90 (sembilan puluh) juta pengguna, menunjukkan kurangnya pelindungan hukum yang kuat dalam menindak pelanggaran data pribadi pada skala besar.[169] Selain itu, kasus seperti serangan *ransomware*, *hacking*, dan pencurian data yang kini makin meningkat. Oleh karena itu, keadaan sebagaimana telah diuraikan di atas menghadirkan urgensi bahwa diperlukan sebuah regulasi yang khusus mengatur keamanan dan ketahanan siber secara komprehensif, terutama untuk mengharmonisasikan regulasi nasional dengan standar keamanan siber internasional juga untuk mengisi kekosongan hukum dan memberikan kepastian hukum.

[169] Fadhila Rahman Najwa, *"Analisis Hukum Terhadap Tantangan Keamanan Siber : Studi Kasus Penegakan Hukum Siber di Indonesia,"* AL-BAHST: Jurnal Ilmu Sosial, Politik, dan Hukum, Vol. 2, Nomor 1, April 2024.

BAB V
JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP MATERI MUATAN

A. Sasaran

Indonesia memerlukan pengaturan yang komprehensif di bidang keamanan dan ketahanan siber. Regulasi ini diharapkan mampu melindungi IIK dan Infrastruktur Informasi pada umumnya, dan mencegah insiden siber yang semakin meningkat di sektor publik dan privat. Dengan adanya regulasi ini, Indonesia akan memiliki landasan hukum yang lebih kuat untuk menanggapi serangan siber dan meningkatkan ketahanan nasional di era digital. Oleh karena itu, pemerintah sudah seharusnya mempunyai suatu regulasi atau pengaturan terkait dengan keamanan dan ketahanan siber, mengingat semakin meningkatnya ancaman dan serangan siber di era digital saat ini.

Sebagai upaya memperkuat ekosistem keamanan siber nasional, BSSN perlu berperan sebagai kolaborator utama yang mendorong sinergi antar-pemangku kepentingan pemerintah, sektor swasta, dan masyarakat. Fokus utama harus diarahkan pada peningkatan kapasitas operasional BSSN untuk memastikan respons terhadap ancaman siber dilakukan secara terpadu dan efisien, dengan meminimalkan irisan tugas antar pemangku kepentingan.

Untuk mendukung peran ini, BSSN harus memiliki sumber daya manusia yang kompeten, infrastruktur teknologi mutakhir, dan alokasi anggaran yang memadai guna memastikan kemampuannya dalam mendeteksi, mencegah, melindungi, serta menangani ancaman siber secara cepat mulai dari serangan *malware* hingga pencurian data sensitif.

B. Arah dan Jangkauan Pengaturan

1. Arah Pengaturan

Arah pengaturan RUU KKS menekankan perlunya sinergi, kolaborasi dan koordinasi antar lembaga dalam menangani insiden siber, baik di tingkat nasional maupun internasional. Dalam hal ini, RUU mengintegrasikan peran pemerintah, pelaku usaha, dan masyarakat untuk mendukung ketahanan siber yang berkelanjutan. RUU ini memperkuat dan memperhatikan peraturan yang relevan, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, sehingga mampu menyelaraskan kebijakan yang ada dengan kebutuhan pengamanan siber nasional.

2. Jangkauan Pengaturan

Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber memiliki jangkauan pengaturan yang mencakup aspek strategis dan teknis dalam pengelolaan keamanan siber di Indonesia mulai dari aspek tata kelola, identifikasi, deteksi, proteksi dan respons. Jangkauan ini meliputi pelindungan terhadap IIK, pengamanan data dan informasi, serta pengelolaan risiko siber yang dapat mempengaruhi stabilitas nasional. Selain itu, RUU ini mengatur tanggung jawab Penyelenggara Infrastruktur Informasi dan Penyelenggara IIK sebagai bagian dari PSE dalam memastikan keamanan data dan efektivitas pengelolaan sistem yang digunakan. Dengan perkembangan ancaman dan serangan siber yang dinamis, pengaturan ini juga diarahkan untuk menciptakan mekanisme adaptif, seperti penilaian risiko berkala dan pembaruan kebijakan keamanan berbasis teknologi terkini. Hal ini bertujuan memastikan pelindungan yang komprehensif terhadap berbagai sektor, termasuk administrasi pemerintahan, ekonomi, pertahanan, dan sosial.

C. Ruang Lingkup dan Materi Muatan

Adapun ruang lingkup materi muatan RUU KKS adalah sebagai berikut:

1. Pengaturan Keamanan Siber

Keamanan siber dalam konteks pelindungan infrastruktur informasi memerlukan pendekatan yang holistik dan sistematis, mengingat karakteristik ancaman siber yang dinamis, transnasional, dan berpotensi mengganggu stabilitas nasional. Perkembangan tantangan keamanan siber modern menunjukkan bahwa pertahanan teknis semata tidak cukup efektif tanpa didukung oleh kerangka tata kelola yang kuat, kesadaran manusia, dan proses yang terintegrasi. Dalam ekosistem digital yang saling terkoneksi, kerentanan pada satu titik dapat berdampak sistemik yang meluas, sehingga memerlukan paradigma keamanan yang tidak hanya berfokus pada pencegahan tetapi juga pada ketahanan (resiliensi) untuk memastikan kelangsungan fungsi kritikal. Kerangka keamanan siber mencakup enam pilar utama: tata kelola yang komprehensif, identifikasi risiko yang berkelanjutan, proteksi multi-lapis, deteksi dini yang proaktif, respons insiden yang terstruktur, serta pemulihan yang terencana. Pendekatan siklus berkelanjutan ini merefleksikan pemahaman bahwa keamanan siber bukanlah tujuan akhir melainkan proses dinamis yang memerlukan penyesuaian terus-menerus sesuai dengan evolusi ancaman.

Pembedaan perlakuan terhadap infrastruktur informasi kritikal dibangun atas dasar analisis risiko yang proporsional, yang mengakui bahwa tidak semua infrastruktur informasi memiliki dampak yang sama terhadap keamanan nasional dan pelayanan publik. Dari perspektif akademis, klasifikasi infrastruktur berdasarkan tingkat kritikalitasnya merupakan prinsip manajemen risiko yang rasional, di mana sumber daya keamanan dialokasikan sesuai dengan potensi dampak gangguan. Infrastruktur informasi kritikal, yang jika terganggu akan berdampak serius pada

kepentingan umum, pelayanan publik, pertahanan keamanan, atau perekonomian nasional, memerlukan standar keamanan yang lebih ketat dengan mekanisme pengawasan eksternal. Pendekatan ini didasarkan pada konsep "*defense in depth"* yang diakui secara internasional, yang mengharuskan lapisan pertahanan berjenjang dengan sistem pemantauan terpusat, penggunaan produk dengan elemen digital yang telah melalui asesmen ketat, serta integrasi dengan pusat koordinasi keamanan nasional. Argumentasi akademis di balik pengaturan ini adalah bahwa infrastruktur kritikal merupakan bagian dari "*national critical functions*" yang harus dipertahankan fungsinya bahkan dalam situasi ancaman siber yang serius, sehingga memerlukan persyaratan keamanan yang lebih ketat dibandingkan infrastruktur informasi umum.

Pengaturan manajemen krisis siber merupakan perwujudan dari pemahaman bahwa ancaman siber dapat berkembang menjadi krisis nasional yang memerlukan respons terkoordinasi di tingkat strategis. Krisis siber merupakan situasi kedaruratan yang melampaui kapasitas respons individu atau organisasi, sehingga memerlukan koordinasi antar pemangku kepentingan dengan prinsip "*shared responsibility*". Kerangka manajemen krisis yang dibangun berdasarkan tiga fase utama sebelum krisis (peringatan dini dan persiapan), selama krisis (penanggulangan dan pemulihan darurat), serta pasca krisis (evaluasi dan pembelajaran) mencerminkan siklus manajemen krisis. Pendekatan berfase ini didasarkan pada analisis bahwa krisis siber memiliki dinamika unik yang memerlukan respons yang disesuaikan dengan tahapan evolusi krisis, di mana kesiapsiagaan sebelum krisis seringkali menentukan efektivitas respons selama krisis. Argumentasi yang mendasari pengaturan ini adalah bahwa keamanan siber merupakan komponen integral dari ketahanan nasional modern, yang memerlukan integrasi antara aspek teknis, operasional, dan kebijakan dalam satu kerangka respons yang terkoordinasi, sehingga mampu menjaga kelangsungan fungsi-fungsi kritikal

negara dalam menghadapi ancaman siber yang semakin kompleks dan terkoordinasi.

Dalam manajemen krisis siber diperlukan adanya penetapan status krisis siber sebagai langkah strategis awal dalam penanganan krisis siber. Dari perspektif yuridis, penetapan status Krisis Siber memberikan dasar hukum eksplisit bagi mobilisasi sumber daya negara secara terpadu ketika insiden siber telah mencapai tingkat eskalasi yang mengancam keamanan nasional, keselamatan rakyat, keutuhan wilayah, dan kedaulatan negara, sekaligus memperjelas kewenangan dan tanggung jawab institusional dalam situasi darurat yang memerlukan respons cepat dan terkoordinasi. Dari sudut pandang politik hukum, penetapan status ini mencerminkan komitmen negara dalam melaksanakan fungsi pelindungan konstitusional secara proaktif melalui respons preventif yang terstruktur sebelum dampak merusak mencapai tingkat kritikal, sekaligus memperkuat legitimasi pemerintahan dalam menjaga stabilitas sistem pemerintahan dan pelayanan publik di tengah ancaman siber yang semakin kompleks dan transnasional, sehingga memastikan keberlanjutan tata kelola negara yang efektif dalam menghadapi tantangan keamanan digital.

Penetapan status Krisis Siber perlu diemban oleh Presiden Republik Indonesia dalam kapasitasnya sebagai kepala negara dan kepala pemerintahan. Sebagai kepala negara, Presiden memiliki legitimasi konstitusional untuk menetapkan status krisis yang berimplikasi pada stabilitas sistem pemerintahan dan keberlanjutan negara, sementara sebagai kepala pemerintahan, Presiden berwenang mengaktifkan seluruh kapasitas negara secara terkoordinasi lintas kementerian/lembaga, pemerintah daerah, serta pemangku kepentingan terkait dalam respons krisis.

Proses penetapan status krisis siber tersebut dilakukan Presiden berdasarkan pertimbangan, masukan, dan rekomendasi strategis dari berbagai pihak termasuk BSSN yang memiliki kapasitas teknis dari aspek keamanan dan ketahanan siber,

sehingga keputusan yang diambil tidak hanya didasarkan pada analisis risiko objektif melalui sistem deteksi dini yang andal, tetapi juga mencerminkan pertimbangan politik kenegaraan yang komprehensif, sehingga status Krisis Siber hanya ditetapkan ketika benar-benar diperlukan sebagai langkah preventif strategis yang mempertimbangkan dimensi keamanan nasional, stabilitas ekonomi, dan Pelindungan terhadap pelayanan publik yang menjadi tulang punggung kehidupan berbangsa dan bernegara.

Penyelenggaraan Manajemen Krisis Siber yang diatur pada RUU KKS meliputi sebelum krisis siber, saat terjadi krisis siber dan setelah terjadi krisis siber.

a. Sebelum krisis siber

Penyelenggaraan sebelum krisis siber terjadi dilakukan paling sedikit melalui:

1) tanggap Insiden Siber;
2) peringatan dini Krisis Siber;
3) penetapan status Krisis Siber oleh Presiden

Berkaitan dengan pelaksanaan tanggap insiden siber, hal ini dilakukan secara bertahap oleh Tim Tanggap Insiden Siber organisasi, Tim Tanggap Insiden Siber sektor, dan Tim Tanggap Insiden Siber nasional.

Terkait dengan penyusunan rencana kontinjensi yang dilakukan tidak dalam situasi krisis siber, maka dibutuhkan beberapa patokan untuk dapat menjadi acuan dalam proses penyusunannya. Rencana kontingensi disusun dengan memperhatikan situasi nasional yang sedang menjadi fokus perhatian, risiko nasional yang timbul, dan juga ancaman serangan siber yang sedang terjadi pada saat rencana kontingensi tersebut disusun.

Pertimbangan dalam menentukan situasi nasional didasarkan pada lingkungan strategis dan perkembangan situasi nasional yang saat itu sedang dihadapi, sebagai contoh dalam hal kegiatan yang merupakan bagian prioritas dari

RPJMN (Rencana Pembangunan Jangka Menengah Nasional), Pemilu, presidensial di forum internasional (semacam Keketuaan ASEAN, presidensial G20, dan sebagainya). Hal ini dilakukan sebagai langkah antisipasi agar proses pelaksanaan kegiatan tersebut terselenggara dengan aman di ruang siber. Penekanan ini menjadi prioritas untuk menghadirkan pemerintah, dalam hal ini BSSN, dalam mengamankan ruang siber di

Indonesia. Terkait dengan situasi nasional maka hal ini dapat didasarkan pada penetapan presiden atau pemerintah mengenai situasi nasional yang perlu menjadi fokus perhatian.

Dalam hal pertimbangan penyusunan rencana kontinjensi krisis siber didasarkan pada risiko nasional yang timbul, hal ini didasarkan pada pelaksanaan pengamanan siber didasarkan pada risiko nasional yang dinilai dapat timbul sesuai dengan perkembangan teknologi atau hal lain yang dapat mempengaruhi layanan sistem elektronik maupun sistem pengamanan yang ada di ruang siber. Terkait hal ini, risiko nasional keamanan siber dapat disusun dari penggabungan risiko PIIK yang kemudian dapat dilakukan penilaian dan penyusunan risiko yang sedang dihadapi saat ini. Penyusunan risiko nasional keamanan siber perlu disusun oleh BSSN.

Rencana kontinjensi krisis siber juga disusun dengan mempertimbangkan ancaman serangan siber yang terjadi. Jenis ancaman serangan siber ini ditentukan berdasarkan lanskap keamanan siber yang disusun oleh BSSN. Lanskap keamanan siber selama ini telah disusun oleh Tim TIS Nasional sehingga hal ini dapat dilanjutkan ke depannya.

Rencana kontinjensi krisis siber merupakan panduan bagi seluruh pihak yang terkait, dalam melakukan penanganan ketika krisis siber terjadi. Oleh karena itu, rencana kontinjensi krisis siber menjadi penting untuk

ditetapkan oleh pihak yang berwenang. Terkait dengan hal tersebut, Kepala BSSN selaku pimpinan dari instansi pemerintah yang bertugas di bidang keamanan dan ketahanan siber, mempunyai kewenangan dan kewajiban untuk menetapkan rencana kontinjensi krisis siber.

Tentunya dalam penyusunan rencana kontinjensi krisis siber ini BSSN wajib mengikutsertakan instansi penyelenggara negara, sedangkan keikutsertaan dari pemangku kepentingan yang terdiri dari quad helix selain instansi penyelenggara negara (akademisi, pelaku usaha, dan komunitas/masyarakat) dapat menjadi opsi.

Setelah penyusunan rencana kontinjensi krisis siber dilakukan maka perlu dilakukan pengujian guna memastikan aktualitas, validitas, dan kualitas rencana kontinjensi krisis siber yang telah disusun. Oleh karena itu, perlu dilakukan simulasi terhadap rencana kontinjensi krisis siber ini. Terkait dengan hal tersebut, BSSN selaku instansi pemerintah yang membidangi keamanan dan ketahanan siber menjadi penjuru dalam melakukan simulasi ini. Tentunya simulasi tidak dapat dilakukan sendiri oleh BSSN namun wajib melibatkan instansi penyelenggara negara maupun seluruh pemangku kepentingan. Hal ini sejalan dengan praktik terbaik pelaksanaan simulasi keamanan siber nasional yang dilakukan oleh Belanda. Di Belanda simulasi keamanan siber nasional dilakukan setiap 2 tahun sekali dengan melibatkan lebih dari 1500 entitas.

Tahapan ini meliputi angka 1, 2, dan 3. Angka 1 menunjukkan adanya tahapan sebelum masuk tahap sebelum krisis siber maka didahului dengan adanya insiden siber. Insiden siber ini mengacu pada peraturan perundang-undangan lainnya yang sudah ada, dengan mengkategorikan insiden organisasi, insiden sektor, dan insiden nasional. Setelah menjadi insiden siber nasional kemudian masih terjadi

eskalasi maka hal itu dapat masuk menjadi tahapan sebelum krisis siber.

Pada tahapan ini didahului dengan adanya peringatan dini oleh Tim TIS Nasional kepada PSE yang berpotensi akan terdampak krisis siber. Selain itu, pada angka 1 menggambarkan adanya laporan yang disampaikan Tim TIS Nasional kepada Kepala BSSN mengenai situasi ini. Pada angka 2 Kepala BSSN melakukan penilaian ulang kemudian dalam hal mendekati krisis siber maka Kepala BSSN mengajukan penetapan status krisis siber kepada presiden. Dalam hal melakukan penilaian ulang ini Kepala BSSN dapat mengikutsertakan kepala instansi yang terkait sesuai dengan kebutuhan. Pada angka 3 setelah mendapatkan usulan penetapan status krisis siber dari Kepala BSSN maka presiden dapat mempertimbangkan usulan tersebut dan menetapkan status krisis siber. Dalam menetapkan status tersebut, presiden menindaklanjuti dengan pembentukan gugus tugas. Pihak yang terlibat di dalam gugus tugas tersebut merupakan prerogatif presiden dalam menentukan pemimpin gugus tugas beserta anggotanya. Namun demikian, BSSN selaku instansi pemerintah yang mempunyai tugas di bidang keamanan dan ketahanan siber merupakan instansi utama yang perlu terlibat di dalam gugus tugas tersebut.

Tahap sebelum krisis siber diawali dengan adanya peringatan dini yang dilakukan oleh Tim TIS Nasional kepada PSE yang terdampak. Peringatan dini yang dikeluarkan oleh Tim TIS Nasional perlu ada dasar yang tepat yang telah disepakati bersama. Peringatan dini krisis siber perlu dikeluarkan tepat sebelum mencapai ambang batas krisis siber terjadi, sehingga peringatan dini ini dikeluarkan sebelum ambang batas krisis siber terpenuhi namun tidak terlalu jauh dari ambang batas krisis siber tersebut. Oleh karena itu, peringatan dini krisis siber dikeluarkan dengan mendasarkan

pada insiden siber maupun peristiwa siber yang terjadi pada saat tersebut. Terkait dengan itu maka insiden siber maupun peristiwa siber tersebut juga perlu mengacu pada ambang batas yang telah dibahas sebelumnya, yaitu dengan memperhatikan:

1) korban jiwa, hilang, dan terluka.
2) kerugian finansial.
3) kondisi keamanan dan ketertiban umum.
4) kerusakan pada IIK.

b. Saat terjadi krisis siber

Dalam hal terjadi eskalasi Insiden Siber yang terus meningkat dan berpotensi menjadi Krisis Siber, tim tanggap insiden siber nasional melalui Kepala Badan Siber dan Sandi Negara mengusulkan status Krisis Siber kepada Presiden. Berdasarkan usulan ini, Presiden dapat menetapkan status Krisis Siber dan membentuk Gugus Tugas Krisis Siber.

Dalam penanganan saat terjadi krisis siber yang terjadi, dilaksanakan paling sedikit melalui:

1) penanggulangan Krisis Siber untuk memitigasi Krisis Siber;
2) pemulihan Krisis Siber dilakukan untuk memastikan Infrastruktur Informasi berfungsi kembali;
3) pelaporan dilakukan untuk menyampaikan status penanganan Krisis Siber kepada Presiden; dan
4) pengakhiran status Krisis Siber melalui penetapan oleh Presiden.

Tahapan ini menunjukkan bahwa gugus tugas memberikan laporan secara berkala kepada presiden. Laporan tersebut berisi progres kegiatan penanggulangan dan pemulihan yang telah dilakukan selama masa krisis siber ini berlangsung. Dalam hal situasi sudah mulai terkendali, maka gugus tugas menyusun laporan akhir yang juga mengusulkan kepada presiden tentang pengakhiran status krisis siber.

Dalam hal presiden telah mempertimbangkan situasi krisis siber telah dapat dikendalikan, maka presiden menetapkan penghentian status krisis siber. Hal ini akan ditindaklanjuti oleh BSSN mengenai tindak lanjut setelah krisis siber ini dapat dikendalikan.

Ketika tahapan saat krisis siber terjadi, pihak yang mempunyai peran utama adalah gugus tugas yang dibentuk oleh presiden. Gugus tugas berperan pada saat pelaksanaan kegiatan penanggulangan, pemulihan, dan pelaporan penanganan. Terkait dengan hal ini, gugus tugas tidak melaksanakan sendiri kegiatan penanggulangan maupun pemulihan krisis siber secara teknis. Gugus tugas hanya menentukan kebijakan dalam penanganan pada tahap saat krisis siber. Hal ini dapat diilustrasikan bahwa gugus tugas melaksanakan kegiatan kebijakan sedangkan pelaksana kegiatan penanggulangan dan pemulihan krisis siber secara teknis adalah PSE terdampak maupun Tim TIS Organisasi, Tim TIS Sektor yang terdampak, serta Tim TIS Nasional. Oleh karena itu, peranan gugus tugas berada pada lingkup strategis, bukan taktis maupun teknis.

Dengan demikian gugus tugas melaksanakan tugasnya dengan melakukan koordinasi dan supervisi kepada PSE yang terdampak. Untuk memperjelas pelaksanaan yang akan dilaksanakan oleh gugus tugas, maka gugus tugas wajib merujuk pada rencana kontingensi yang telah disusun sebelum memasuki tahapan krisis siber dan ditetapkan oleh Kepala BSSN.

Namun demikian perlu diberikan kelonggaran bagi gugus tugas untuk mengeluarkan kebijakan di luar rencana kontinjensi krisis siber yang telah disusun, sepanjang situasi tersebut sangat berbeda dengan skenario ancaman siber yang terdapat pada rencana kontinjensi krisis siber.

c. Setelah krisis siber

Dalam hal Krisis siber telah selesai, Presiden menetapkan pengakhiran Krisis Siber. Penyelenggaraan Setelah Krisis Siber dilaksanakan paling sedikit melalui:

1) penghitungan perkiraan nilai kerusakan dan kerugian akibat Krisis Siber;
2) penghitungan perkiraan biaya pemulihan akibat Krisis Siber; dan
3) evaluasi atas penanganan Krisis Siber.

Tahapan setelah krisis siber dilakukan oleh BSSN dengan PSE yang terdampak. Kegiatan yang dilakukan pada tahapan ini adalah menghitung nilai kerugian, biaya pemulihan, dan melakukan evaluasi terhadap kebijakan yang telah disusun sebelumnya terkait dengan penanganan krisis siber.

Pada tahap ini secara umum akan menghitung dampak krisis siber secara kuantitatif. Penghitungan dampak krisis siber secara kuantitatif ini sangat besar manfaatnya mengingat beberapa hal:

1) Pada saat krisis siber terjadi maka pengerahan sumber daya dilakukan secara bersama-sama. Pemerintah, selaku pihak yang memberikan panduan dan kebijakan, bersama dengan PSE yang terdampak, akademisi, komunitas, masyarakat, bahkan dapat juga melibatkan pelaku usaha lainnya, menghadapi dan menangani krisis siber dengan tujuan krisis siber tidak meluas dan dapat ditangani dengan cepat dan tepat. Oleh karena itu, penghitungan dampak krisis siber ini menjadi bagian pertanggungjawaban setelah pengerahan sumber daya dilakukan dengan sangat masif.
2) Penghitungan dampak krisis siber ini tidak bertujuan agar pemerintah memberikan ganti rugi atau memberikan bantuan dalam rangka pemulihan data/sistem/layanan yang diberikan oleh sistem elektronik. Hal ini didasarkan

bahwa krisis siber ini tentunya telah menyerang masif ke sebagian besar atau dapat mengarah ke hampir seluruh sistem elektronik pada IIK. Tentunya ini berdampak kepada sebagian besar layanan kepada publik atau berkaitan dengan hajat hidup orang banyak. Oleh karena itu, dengan pertimbangan tersebut maka pemerintah berfokus pada pengembalian atau pemulihan kembali data/sistem/layanan yang terdampak.

3) Penghitungan ini dapat menjadikan gambaran mengenai besarnya kerugian yang akan dialami jika terkena serangan siber. Tentunya hal ini dapat menjadi referensi bagi BSSN dan pemangku kepentingan lainnya dalam merumuskan kebijakan berkaitan dengan keamanan siber

4) Penghitungan ini juga dapat memberikan gambaran mengenai besarnya dan luasnya dampak yang ditimbulkan. Hal ini dapat menjadi referensi dalam meningkatkan kewaspadaan terhadap keamanan siber bagi seluruh lapisan masyarakat. Terlebih lagi bahwa ancaman dan serangan siber ini nyata terjadi dalam kehidupan sehari-hari yang terkadang tidak dihiraukan oleh setiap orang mengingat serangan siber ini lebih sering tidak menimbulkan efek yang terlihat secara jelas dan nyata terhadap data/sistem/layanan yang nantinya akan diperoleh setiap orang.

Terkait dengan penghitungan dampak krisis siber, maka objek penghitungan dampak dapat diperluas menjadi sebagai berikut:

1) Penghitungan perkiraan nilai kerusakan dan kerugian;

Penghitungan ini didasarkan pada perkiraan nilai dari akibat langsung yang dialami dari krisis siber tersebut. Penghitungan perkiraan nilai kerusakan dan kerugian ini dapat dihitung terhadap:

a) Nilai aset yang rusak; penghitungan nilai aset yang rusak dapat dilakukan dengan berbagai macam cara. Namun demikian, untuk pengaturan di dalam rancangan undang-undang ini akan lebih tepat dengan mendasarkan pada ketentuan manajemen aset yang berlaku atau dengan membandingkan nilai aset yang rusak dengan nilai aset sebelum terjadinya krisis siber.

b) Kerugian ekonomi yang timbul akibat adanya aset yang rusak. Penghitungan ini dapat dilakukan dengan menghitung dari keuntungan ekonomi yang dapat diperoleh apabila sistem elektronik tersebut berfungsi dengan baik.

c) Penurunan tingkat reputasi. Hal ini tentu dilakukan terhadap persepsi publik melalui survei dengan sampel yang telah ditentukan.

2) Penghitungan perkiraan biaya pemulihan.

3) Penghitungan korban jiwa, hilang, dan terluka.

Penyelenggara Infrastruktur Informasi (PII) wajib melaksanakan kegiatan tata Kelola, identifikasi, proteksi, deteksi, tanggap insiden siber, dan pemulihan NIST CSF. PII memiliki tanggung jawab fundamental untuk melindungi infrastruktur informasi yang dimiliki atau dikelolanya. Kewajiban ini merupakan bagian integral dari tata kelola keamanan informasi yang didasarkan pada ketentuan peraturan perundang-undangan, prinsip Pelindungan data, serta tanggung jawab etis terhadap masyarakat pengguna.

PII juga memiliki dimensi publik yang luas. Dimana infrastruktur informasi saat ini tidak hanya menampilkan dan mengolah informasi, namun juga menyediakan layanan pengelolaan data pribadi, data transaksi keuangan, dan layanan publik lainnya bagi masyarakat. Kegagalan dalam melindungi sistem dapat menimbulkan dampak signifikan, seperti kerugian

ekonomi, gangguan layanan publik, dan menurunnya kepercayaan masyarakat terhadap badan usaha ataupun institusi penyelenggara. Oleh karena itu, upaya pelindungan sistem elektronik tidak hanya menjadi kewajiban administratif, tetapi juga bentuk tanggung jawab sosial untuk menjaga kepentingan publik.

Dari perspektif operasional, infrastruktur informasi yang aman akan mendukung keberlangsungan layanan, menjaga integritas dan kerahasiaan data, serta memastikan ketersediaan layanan digital secara berkesinambungan. Hal ini sangat penting terutama bagi Penyelenggara Infrastruktur Informasi yang berperan dalam penyelenggaraan infrastruktur dan layanan penting yang termasuk dalam kategori Infrastruktur Informasi Kritikal (IIK), di mana gangguan terhadap sistem tersebut dapat berdampak langsung pada keamanan nasional, stabilitas ekonomi, dan keselamatan masyarakat.

Selain itu, penerapan langkah-langkah pelindungan sistem elektronik yang memadai juga mencerminkan komitmen PII terhadap profesionalisme dan tata kelola yang baik. Keamanan yang terjamin akan meningkatkan kepercayaan publik, memperkuat reputasi lembaga, serta mendukung terciptanya ekosistem digital yang aman dan andal.

Dalam menjalankan kewajiban pelindungan tersebut, PII perlu menerapkan kerangka kerja pelindungan yang komprehensif untuk membantu mereka dalam mengidentifikasi, melindungi, mendeteksi, merespon, dan menangani insiden siber. Kerangka kerja pelindungan tersebut terdiri atas fungsi Tata Kelola, Identifikasi, Proteksi, Deteksi, Tanggap, dan Pemulihan Insiden Siber.

Fungsi Tata Kelola merupakan kumpulan kegiatan yang harus dilakukan oleh PII untuk mengidentifikasi, merencanakan, memonitor, dan mengevaluasi hasil kegiatan pada fungsi-fungsi lainnya sesuai kebutuhan dan kondisi organisasi. Kegiatan pada fungsi Tata Kelola meliputi pemahaman terhadap:

a. penetapan strategi dan kebijakan keamanan siber.
b. pengelolaan risiko siber.
c. pengaturan struktur organisasi dan tanggung jawab keamanan siber.
d. kepatuhan terhadap standar, pedoman, dan peraturan perundang-undangan.
e. pelatihan dan peningkatan kapasitas sumber daya manusia.

Fungsi identifikasi merupakan kumpulan kegiatan yang harus dilakukan oleh PII untuk mengidentifikasi asset organisasi (misalnya, data, perangkat keras, perangkat lunak, sistem, fasilitas, layanan, sumber daya manusia), identifikasi siapa saja pemasok di organisasi, serta identifikasi ancaman siber yang memungkinkan organisasi untuk memprioritaskan upaya pelindungan yang sesuai dengan strategi manajemen risiko dan kebutuhan organisasi yang telah ditetapkan dalam aspek tata kelola. Hasil dari kegiatan identifikasi nantinya akan menjadi rekomendasi bagi PII dalam melaksanakan kegiatan proteksi. Kegiatan pada fungsi identifikasi meliputi:

a. Identifikasi asset infrastruktur informasi yang dimiliki atau dikelola.
b. Identifikasi ancaman terhadap asset infrastruktur informasi.
c. Identifikasi risiko sisber jika terjadi serangan siber pada asset infrastruktur informasi.

Fungsi proteksi merupakan Kumpulan kegiatan yang harus dilakukan oleh PII untuk membatu dalam mengamankan aset informasi guna mencegah atau mengurangi kemungkinan dan dampak insiden keamanan siber yang merugikan, serta meningkatkan kemungkinan dan dampak pemanfaatan peluang. Fungsi proteksi harus dilaksanakan secara berkelanjutan, berkala, dan konsisten. Kegiatan pada fungsi Proteksi meliputi:

a. Penggunaan kontrol akses dan manajemen identitas.
b. Proteksi data, jaringan, dan aplikasi.
c. Penguatan sistem dan perangkat lunak terhadap kerentanan.

d. Pelatihan kesadaran keamanan siber bagi pengguna.
e. Pengendalian teknologi dan prosedur keamanan fisik dan lingkungan.
f. Penerapan standar keamanan siber dalam perencanaan, pembangunan, pengoperasian, pemeliharaan, dan pengawasan infrastruktur informasi.
g. Pelaksanaan pelindungan data/informasi berkualifikasi termasuk data pribadi.
h. Membuat dokumen elektronik dan rekam cadannya.
i. Menerapkan persandian yang aman, andal, dan tepercaya.

Fungsi proteksi merupakan kumpulan kegiatan yang harus dilakukan oleh PII untuk mendeteksi potensi serangan dan penyusupan keamanan siber yang berhasil ditemukan dan dianalisis. Fungsi deteksi memungkinkan PII dalam mengidentifikasi adanya anomali, analisis ancaman, evaluasi indikator penyusupan, dan potensi kejadian buruk lainnya yang mengindikasikan terjadinya serangan dan insiden keamanan siber secara tepat waktu. Fungsi ini mendukung respons insiden dan aktivitas pemulihan yang sukses. Oleh karena itu fungsi deteksi harus dilaksanakan secara berkelanjutan, berkala, dan konsisten. Kegiatan pada fungsi deteksi meliputi:

a. Pemantauan sistem untuk deteksi terhadap ancaman siber melalui *system security operation center*.
b. Penerapan *system log* untuk melihat apakah ada potensi ancaman siber yang mungkin menyerang organisasi.
c. Pelaksanaan audit sebagai bagian dari meningkatkan kepatuhan.

Fungsi Tanggap Insiden Siber merupakan kumpulan kegiatan yang harus dilakukan oleh PII untuk menerapkan Langkah-langkah yang diperlukan organisasi dalam mengatasi dampak dari insiden keamanan siber yang terdeteksi. Tanggap insiden siber diperlukan untuk memberikan seluruh pihak di organisasi mengenai gambaran apa yang harus dilakukan dalam menangani

insiden siber, mencegah meluasnya insiden siber, dan meminimalisir dampak insiden siber. Dalam konteks tanggap insiden siber, organisasi perlu memperhatikan kegiatan yang meliputi:

a. manajemen inisiden siber.
b. analisis insiden siber.
c. pelaporan dan komunikasi insiden siber.
d. mitigasi insiden siber.

Fungsi pemulihan merupakan kumpulan kegiatan yang harus dilakukan oleh PII untuk menerapkan Langkah-langkah yang diperlukan dalam memastikan layanan dan operasional bisnis dapat kembali aktif atau berjalan sebagaimana mestinya setelah terkena dampak dari insiden siber. Kegiatan pada fungsi pemulihan meliputi:

a. kegiatan pemulihan yang terencana, terverifikasi, dan terdokumentasi, dimana organisasi dapat melaksanakan proses pemulihan sesuai dengan rencana yang telah ditetapkan.
b. komunikasi pemulihan yang dikoordinasikan dengan pemangku kepentingan baik internal maupun eksternal. Masing-masing penyelenggara Infrastruktur Informasi melaksanakan komunikasi pemulihan yang dikoordinasikan dengan pemangku kepentingan baik internal maupun eksternal sehingga mempercepat pemulihan sistem terdampak.

Ketersediaan infrastruktur yang memadai dengan didukung oleh teknologi yang mumpuni dalam penyelenggaraannya telah menjadi elemen yang penting dalam mendukung peningkatan perekonomian nasional, mensejahterakan masyarakat, dan meningkatkan daya saing suatu negara dalam persaingan global. Infrastruktur juga berpengaruh penting bagi peningkatan kualitas hidup dan kesejahteraan masyarakat, antara lain dalam peningkatan nilai konsumsi, peningkatan produktivitas kerja, dan

akses kepada lapangan kerja.

Pelindungan infrastruktur informasi kritikal adalah komponen penting dalam paradigma keamanan nasional yang bertujuan untuk menjaga keberlangsungan layanan strategis bagi masyarakat dan Negara dari ancaman keamanan siber. Ketersediaan infrastruktur kritikal yang memadai sangat penting dalam mendukung pembangunan nasional, serta upaya Pemerintah untuk meningkatkan kualitas hidup dan kesejahteraan masyarakat. Sehingga, apabila terjadi gangguan terhadap infrastruktur vital tersebut, maka berpotensi memiliki dampak serius bagi masyarakat luas

Pelindungan terhadap infrastruktur kritikal seperti jaringan kereta api, pembangkit listrik, bandara, jaringan telekomunikasi, sistem keuangan, sistem kendali proses, jaringan pipa gas, sistem pasokan air, dan lainnya tidak bisa hanya dilakukan melalui pendekatan pelindungan fisik saja. Namun dengan adanya penggunaan teknologi informasi dan komunikasi pada operasional infrastruktur kritikal, maka jenis ancaman terhadapnya menjadi lebih kompleks, yakni dengan munculnya ancaman siber. Hal ini disebabkan penggunaan teknologi informasi dan komunikasi terbukti telah memberikan efisiensi dan mengubah cara penyelenggara infrastruktur informasi kritikal dalam mengendalikan operasional layanan kritikalnya. Contoh penggunaan teknologi seperti *cloud computing*, *next generation mobile computing*, interkoneksi jaringan, serta *industrial control system* telah banyak digunakan oleh penyelenggara infrastruktur informasi kritikal untuk menggerakan mesin, memberikan informasi jumlah muatan pada tanki, memberikan informasi ketersediaan ruang perawatan, otomatisasi *conveyor*, pertukaran informasi dan data, dan lain sebagainya.

Oleh karena itu, pemerintah perlu untuk menetapkan infrastruktur informasi apa saja yang berpotensi memiliki dampak serius kepada masyarakat jika terjadi gangguan terhadapnya.

Potensi dampak yang dimaksud meliputi kerugian terhadap perekonomian nasional, terganggunya kepentingan umum, serta pertahanan dan keamanan. Infrastruktur informasi tersebut perlu untuk diidentifikasi dan invetarisir untuk memberikan prioritasi Pelindungan terhadap setiap asset informasi yang terhubung kepada infrastruktur informasi tersebut. Hal ini disebabkan oleh adanya keterhubungan antar layanan vital melalui ruang siber yang membuka potensi ancaman melalui upaya-upaya pengrusakan yang dapat dilakukan oleh *hacker* ataupun pihak yang tidak berkepentingan melalui serangan siber.

PII yang ditetapkan sebagai Penyelenggara Infrastruktur Informasi Kritikal (PIIK) juga menerapkan pelindungan sebagaimana kerangka kerja pelindungan yang terdiri atas fungsi tata Kelola, identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan atas insiden siber. Karena sifat kritikalitas dari layanan yang diberikan kepada Masyarakat, maka perlu ditambahkan kegiatan-kegiatan lain yang ditunjukan untuk memberikan jaminan keamanan pada PIIK meliputi:

a. Menggunakan PDED yang telah lulus asessmen dan memenuhi syarat kriteria keamanan berdasarkan peraturan perundang-undangan.
b. Membuat dokumen elektronik dan rekam cadangnya serta menghubungkannya ke pusat data tertentu.
c. Mengintegrasikan sistem pemantauan Keamanan Siber IIK dengan pusat pemantauan keamanan nasional (*National Security Operation Center*).
d. Menyampaikan temuan hasil deteksi yang telah di analisis dan diklasifikasikan sesuai dengan tingkat risiko kepada pengatur dan pengawas sektor.
e. Melaksanakan audit keamanan siber secara berkala dan menyeluruh.
f. Melaporkan hasil pelaksanaan audit keamanan siber kepada pengatur dan pengawas sektor dan instansi pemerintah yang

melaksanakan tugas di bidang keamanan dan ketahanan siber; dan

g. Melaporkan Insiden siber kepada pengatur dan pengawas sektor dan instansi pemerintah yang melaksanakan tugas di bidang keamanan dan ketahanan siber.

Dalam penyelenggaraan pelindungan Infrastruktur Informasi Kritikal diperlukan kerja sama dan kolaborasi antar PIIK di masing-masing sektor. Oleh karena itu, diperlukan koordinator yang bertugas memberikan pembinaan dan pengawasan terhadap penyelenggaraan pelindungan IIK di masing-masing sektor. Peran Kementerian atau Lembaga di masing-masing sektor menjadi suatu hal yang penting untuk memberikan pengaturan dan pengawasan kepada PIIK di sektornya. Informasi hasil penyelenggaraan pelindungan IIK di masing-masing sektor perlu untuk dianalisis dan disampaikan kepada Presiden. Oleh karena itu, perlu adanya Instansi Pemerintah yang bertugas sebagai coordinator nasional yang membantu Pengatur dan Pengawas sektor untuk saling berkoordinasi dan berkolaborasi.

2. Pengaturan Ketahanan Siber

Ketahanan siber merupakan konsep kritikal yang melampaui batasan keamanan siber tradisional dengan menekankan kemampuan sistem untuk bertahan, pulih, dan beradaptasi pasca serangan. Dalam konteks nasional, ketahanan siber tidak sekadar melindungi infrastruktur informasi dari gangguan, melainkan memastikan kelangsungan fungsi inti negara dalam menghadapi ancaman yang semakin kompleks. Berbeda dengan keamanan siber yang berfokus pada pencegahan serangan, ketahanan siber mengakui ketidakmungkinan mencegah 100% (seratus persen) serangan dan lebih menekankan pada kemampuan sistem untuk tetap beroperasi atau segera pulih pasca insiden, menjadikannya prasyarat bagi kedaulatan negara di ruang siber.

Pendekatan ketahanan siber yang efektif harus dibangun atas tiga pilar utama yang saling terkait yaitu: kapasitas sumber daya manusia, kapasitas teknologi, dan kapasitas proses bisnis. Pengembangan kapasitas sumber daya manusia mencakup penyediaan tenaga ahli, peningkatan kompetensi melalui pelatihan dan sertifikasi, serta pembentukan budaya kesadaran keamanan informasi. Pada aspek teknologi, diperlukan pengaturan ketat terhadap Produk dengan Elemen Digital berdasarkan tingkat risiko, pengembangan teknologi keamanan siber, dan penerapan keamanan rantai pasokan. Sementara itu, peningkatan kapasitas proses bisnis menjamin tata kelola yang efektif melalui manajemen risiko, berbagi informasi ancaman, penerapan persandian, dan audit berkala. Ketiga pilar ini harus diterapkan secara holistik dengan pendekatan hulu-tengah-hilir untuk menciptakan ekosistem digital yang tangguh.

3. Peningkatan Kapasitas SDM

Urgensi pengaturan mengenai peningkatan kapasitas sumber daya manusia dalam RUU KKS didasarkan pada kenyataan bahwa manusia merupakan unsur paling menentukan dalam menjaga, mengelola, dan mempertahankan keamanan siber nasional. Teknologi siber secanggih apa pun tidak akan mampu memberikan Pelindungan yang efektif tanpa didukung oleh sumber daya manusia yang kompeten, beretika, dan memiliki kesadaran tinggi terhadap keamanan informasi. Saat ini, Indonesia menghadapi kesenjangan signifikan antara kebutuhan dan ketersediaan tenaga ahli di bidang keamanan siber. Berdasarkan laporan *Global Cybersecurity Index (GCI)* tahun 2024, salah satu tantangan utama yang menghambat peningkatan peringkat Indonesia dalam keamanan siber global adalah keterbatasan kualitas dan kuantitas sumber daya manusia yang memahami keamanan siber secara mendalam, termasuk dalam aspek teknis, kebijakan, maupun kesadaran publik.

Ketersediaan sumber daya manusia yang kompeten di bidang keamanan siber tidak hanya diperlukan dalam jumlah yang memadai, namun juga harus memiliki kualifikasi yang sesuai dengan standar kompetensi yang yang diperlukan. Peningkatan kapasitas sumber daya manusia harus dilakukan secara komprehensif melalui penyediaan tenaga ahli yang memadai, peningkatan kompetensi melalui sertifikasi formal, alih teknologi dan keahlian dari pihak yang lebih berpengalaman, serta pembentukan budaya kesadaran keamanan informasi yang kuat di seluruh tingkatan organisasi. Proses ini memerlukan koordinasi yang baik antara berbagai pemangku kepentingan, dimana setiap penyelenggara infrastruktur informasi memiliki tanggung jawab utama dalam mengembangkan kapasitas sumber daya manusianya, sementara lembaga pemerintah bertugas mengoordinasikan upaya peningkatan kapasitas dalam lingkup sektornya, dan BSSN memiliki tanggung jawab strategis dalam mengoordinasikan secara nasional untuk memastikan konsistensi dan keselarasan dengan kebijakan keamanan dan ketahanan siber nasional. Pelaporan berkala tentang perkembangan kapasitas sumber daya manusia diperlukan untuk memantau efektivitas program pengembangan serta mengidentifikasi kebutuhan penyesuaian yang diperlukan, sehingga tercipta ekosistem sumber daya manusia yang mampu menjaga ketahanan siber Indonesia dalam menghadapi ancaman yang terus berevolusi.

Kesenjangan ini menimbulkan risiko strategis bagi negara. Rendahnya kapasitas SDM menyebabkan lemahnya deteksi dini terhadap insiden siber, lambatnya penanganan, serta tingginya potensi kebocoran data dan serangan terhadap infrastruktur informasi kritikal. Di sektor pemerintahan, minimnya tenaga profesional bersertifikasi keamanan siber menyebabkan banyak sistem informasi belum dikelola sesuai dengan standar keamanan internasional. Di sektor swasta, terutama industri keuangan, energi, dan kesehatan, keterbatasan SDM siber berpotensi

menimbulkan gangguan operasional yang berdampak luas terhadap stabilitas ekonomi dan layanan publik, sehingga peningkatan kapasitas sumber daya manusia bukan sekadar kebutuhan teknis, tetapi merupakan strategi nasional untuk melindungi kepentingan nasional dari Ancaman Siber dan Serangan Siber.

RUU KKS mengatur peningkatan kapasitas sumber daya manusia untuk menjawab kebutuhan mendesak tersebut secara sistematis dan terukur. Peningkatan kapasitas harus dilaksanakan secara terpadu oleh Penyelenggara Infrastruktur Informasi dan Penyelenggara Infrastruktur Informasi kritikal (IIK), baik dari kalangan pemerintah maupun swasta. Hal ini didasari oleh kesadaran bahwa ancaman siber bersifat lintas sektor dan tidak mengenal batas institusional, sehingga seluruh penyelenggara sistem elektronik yang berperan penting bagi kehidupan masyarakat harus memiliki kemampuan dan kesadaran keamanan informasi yang memadai. Tujuan peningkatan kapasitas SDM tidak hanya untuk memenuhi kebutuhan tenaga ahli secara kualitas dan kuantitas, tetapi juga untuk menanamkan budaya sadar keamanan informasi di seluruh lapisan organisasi dan masyarakat.

Pengalaman selama ini menunjukkan bahwa program pelatihan dan sertifikasi SDM siber di berbagai instansi sering kali berjalan terpisah, tidak sinkron, dan tanpa standar kompetensi nasional yang seragam. Akibatnya, terjadi ketimpangan kemampuan antara sektor yang satu dengan yang lain. Melalui pengaturan ini, RUU KKS mendorong lahirnya tata kelola peningkatan kapasitas SDM yang terintegrasi dimulai dari pelaporan di tingkat penyelenggara, koordinasi sektoral oleh Pengatur dan Pengawas Sektor, hingga koordinasi nasional oleh instansi yang berwenang di bidang keamanan dan ketahanan siber. Pendekatan berlapis ini diharapkan dapat menciptakan harmonisasi kebijakan, efisiensi sumber daya, dan peningkatan kualitas SDM secara merata di seluruh sektor.

Dengan demikian, urgensi pengaturan bagian ini terletak pada kebutuhan mendesak untuk membangun ekosistem sumber daya manusia keamanan siber yang kuat, berkelanjutan, dan terkoordinasi secara nasional. Tanpa adanya kerangka hukum yang tegas, program pengembangan kapasitas akan tetap bersifat sektoral dan sporadis, sehingga Indonesia berisiko tertinggal dalam menghadapi eskalasi ancaman siber global. Melalui pengaturan ini, RUU KKS berupaya memastikan bahwa setiap individu, institusi, dan sektor memiliki kemampuan, kesadaran, dan tanggung jawab yang sama dalam menjaga keamanan dan ketahanan siber nasional. Langkah ini menjadi investasi strategis bagi keberlanjutan pembangunan digital Indonesia serta Pelindungan terhadap kedaulatan dan kepentingan nasional di ruang siber.

4. Peningkatan Kapasitas Teknologi

Transformasi digital nasional telah mengubah hampir seluruh aspek kehidupan di Indonesia, mulai dari tata kelola pemerintahan, sistem ekonomi, hingga layanan publik. Infrastruktur digital kini menjadi tulang punggung bagi aktivitas negara dan masyarakat, namun pada saat yang sama memperluas permukaan serangan (*attack surface*) yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Di tengah percepatan digitalisasi nasional, ancaman siber meningkat secara signifikan baik dari sisi volume, kompleksitas, maupun dampak yang ditimbulkan. Berdasarkan laporan *Fortinet Global Threat Landscape Report 2024*, sebanyak 82% (delapan puluh dua persen) organisasi di kawasan Asia Tenggara, termasuk Indonesia, mengalami insiden siber signifikan sepanjang tahun 2024. Serangan terhadap Pusat Data Nasional (PDN) pada tahun 2024 menjadi bukti nyata betapa rentannya infrastruktur teknologi Indonesia, baik karena lemahnya sistem keamanan maupun ketergantungan terhadap perangkat dan aplikasi yang belum tersertifikasi.

Kondisi tersebut memperlihatkan bahwa Indonesia belum memiliki kapasitas teknologi keamanan siber yang memadai untuk mengantisipasi ancaman yang terus berkembang. Ketergantungan terhadap produk dan layanan digital asing yang tidak selalu transparan dari sisi keamanan menimbulkan risiko serius bagi kedaulatan data dan keamanan nasional. Kesenjangan riset dan inovasi dalam bidang keamanan siber juga memperburuk situasi, karena hingga kini sebagian besar teknologi enkripsi, deteksi ancaman, dan sistem pertahanan siber masih mengandalkan teknologi impor. Oleh sebab itu, peningkatan kapasitas teknologi menjadi kebutuhan mendesak dalam membangun ketahanan siber yang tangguh, mandiri, dan berkelanjutan.

Pengaturan mengenai peningkatan kapasitas teknologi dalam RUU Keamanan dan Ketahanan Siber (RUU KKS) menjadi landasan strategis untuk menjawab tantangan tersebut. Pengaturan mengenai kewajiban penggunaan Perangkat dan Elemen Digital *Dengan Elemen Digital (PDED*) yang memenuhi standar keamanan, mekanisme sertifikasi risiko, kewajiban penyedia layanan dan perangkat untuk melaksanakan audit serta pembaruan keamanan, riset dan pengembangan teknologi keamanan siber, pemanfaatan kecerdasan artifisial (AI) yang beretika, serta penguatan keamanan rantai pasokan teknologi nasional. Pengaturan ini sejalan dengan standar global seperti *NIST SP 800-161 Rev1 (2022)* mengenai keamanan rantai pasokan, *Cyber Resilience Act (CRA)* Uni Eropa tahun 2023 yang mewajibkan seluruh produk digital aman sepanjang siklus hidupnya, serta *OECD AI Principles* dan *UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)* yang menjadi pedoman etika internasional dalam pengembangan dan penerapan kecerdasan artifisial.

Urgensi pengaturan ini didasarkan pada lima hal utama. Pertama, meningkatnya ancaman terhadap infrastruktur digital nasional yang kini bersifat sistemik dan lintas batas negara, sehingga memerlukan standar keamanan teknologi yang kuat agar

stabilitas nasional dan pelayanan publik tidak terganggu. Kedua, adanya ketergantungan besar terhadap teknologi asing tanpa mekanisme verifikasi keamanan yang memadai, yang dapat membuka celah penyusupan atau kebocoran data. RUU KKS berupaya menjawab hal ini melalui pengaturan sertifikasi risiko dan kewajiban penggunaan PDED yang telah lulus asesmen oleh instansi berwenang. Ketiga, lemahnya riset dan inovasi dalam bidang keamanan siber nasional, yang mengharuskan adanya kebijakan untuk memperkuat kolaborasi antara pemerintah, perguruan tinggi, dan industri dalam pengembangan teknologi keamanan seperti *post-quantum cryptography (PQC)*, sistem deteksi ancaman berbasis AI, dan sistem pertahanan siber mandiri. Keempat, perlunya pengaturan etika dalam pemanfaatan kecerdasan artifisial untuk memastikan teknologi tersebut tetap berorientasi pada nilai kemanusiaan, transparansi, keamanan, dan pelindungan data pribadi. Kelima, meningkatnya risiko keamanan rantai pasokan akibat kompleksitas hubungan antara penyedia teknologi, pemasok, dan operator, yang membutuhkan mekanisme audit, penilaian risiko, serta kontrak keamanan yang ketat.

Melalui pengaturan yang komprehensif ini, RUU KKS mendorong terwujudnya sistem keamanan teknologi nasional yang berdaulat dan terpercaya. Penyelenggara infrastruktur informasi diwajibkan menggunakan PDED yang telah disertifikasi sesuai dengan klasifikasi risiko rendah, menengah, atau tinggi serta melaksanakan asesmen mandiri atau eksternal sesuai dengan tingkat risiko yang dihadapi. Penyedia perangkat wajib mendaftar di instansi yang berwenang, mendokumentasikan kerentanan, menyediakan pembaruan keamanan, serta melaksanakan audit berkala terhadap keamanan produknya. Penyelenggara layanan diwajibkan menggunakan tenaga kerja yang tersertifikasi, baik berdasarkan standar nasional maupun internasional yang diakui pemerintah. Pengaturan ini juga membuka ruang bagi setiap orang untuk melakukan riset dan pengembangan teknologi keamanan

siber guna meningkatkan kemandirian, kolaborasi, dan daya saing nasional, serta memastikan Pelindungan terhadap hak kekayaan intelektual hasil inovasi di bidang keamanan dan ketahanan siber.

Selain itu, RUU KKS menegaskan bahwa pemanfaatan kecerdasan artifisial harus dilakukan dengan memperhatikan nilai etika yang mencakup aspek inklusivitas, kemanusiaan, keamanan, transparansi, dan akuntabilitas. Pemerintah berperan dalam mengatur, mengoordinasikan, dan mengawasi pengembangan serta penerapan AI agar tetap aman, tepercaya, dan sesuai dengan kepentingan nasional. Dalam hal keamanan rantai pasokan, setiap penyelenggara infrastruktur informasi, penyelenggara IIK, maupun penyedia perangkat diwajibkan menerapkan standar keamanan untuk mencegah dan menanggulangi ancaman siber yang mungkin timbul sepanjang proses perancangan, pengadaan, distribusi, hingga pemeliharaan.

Dengan pengaturan ini, RUU KKS tidak hanya berfungsi sebagai perangkat hukum, tetapi juga sebagai kerangka kebijakan untuk mengarahkan pembangunan kapasitas teknologi keamanan siber nasional secara sistematis. Tujuannya adalah memastikan bahwa Indonesia mampu melindungi infrastruktur digital strategisnya, mengembangkan teknologi keamanan yang mandiri, memperkuat daya saing global, serta menjaga kedaulatan digital di tengah dinamika geopolitik siber dunia. Dengan demikian, pengaturan peningkatan kapasitas teknologi menjadi salah satu pilar utama dalam mewujudkan sistem keamanan dan ketahanan siber nasional yang tangguh, berkelanjutan, dan berorientasi pada kepentingan nasional.

5. Peningkatan Kapasitas Proses Bisnis

Peningkatan Kapasitas Proses Bisnis dalam RUU KKS memegang peran strategis sebagai pilar tata kelola keamanan siber nasional yang berorientasi pada efektivitas, efisiensi, dan keberlanjutan. Pengaturan ini muncul dari kebutuhan nyata untuk

memperkuat fondasi kelembagaan dan teknis dalam penyelenggaraan keamanan siber, terutama dalam menghadapi peningkatan frekuensi dan kompleksitas ancaman siber global. Di tengah meningkatnya ketergantungan terhadap sistem digital di seluruh sektor publik dan privat, diperlukan mekanisme yang sistematis untuk memastikan bahwa proses bisnis dalam pengelolaan keamanan siber berjalan secara terukur, transparan, dan adaptif terhadap dinamika ancaman yang terus berkembang.

Peningkatan kapasitas proses bisnis dimaksudkan untuk mewujudkan tata kelola keamanan siber yang efektif dan efisien. Substansi ini merefleksikan prinsip *Cybersecurity governance* sebagaimana diatur dalam standar internasional seperti ISO/IEC 27001 dan NIST *Cybersecurity Framework* (CSF), yang menekankan pentingnya penerapan proses manajemen risiko, berbagi informasi, enkripsi (persandian), pengukuran kematangan, serta audit dan asesmen secara berkala. Kelima komponen ini saling terintegrasi dalam menciptakan siklus peningkatan berkelanjutan (*continuous improvement*) terhadap kesiapan dan ketahanan siber nasional. Tanpa tata kelola proses bisnis yang kuat, keamanan siber berisiko hanya menjadi pendekatan reaktif yang tidak mampu memberikan pelindungan menyeluruh terhadap Infrastruktur Informasi dan infrastruktur informasi kritikal.

Manajemen risiko keamanan siber sebagai fondasi tata kelola yang harus diterapkan oleh setiap penyelenggara infrastruktur informasi. Urgensi pengaturan ini didorong oleh fakta bahwa insiden siber kerap terjadi akibat lemahnya identifikasi risiko dan minimnya mekanisme pengendalian internal. Data dari World Economic Forum Global Risk Report 2024 menunjukkan bahwa risiko siber menempati posisi ketiga terbesar dari seluruh risiko global dalam lima tahun ke depan. Oleh karena itu, penerapan manajemen risiko yang sesuai standar dan peraturan menjadi instrumen wajib agar setiap penyelenggara dapat mendeteksi, menilai, dan merespons risiko dengan tepat. Kewajiban pelaporan

kepada pengatur dan pengawas sektor menciptakan sistem pertanggungjawaban berlapis yang memperkuat koordinasi lintas lembaga dan sektor, sejalan dengan prinsip *multi-stakeholder approach* yang diadopsi dalam tata kelola siber modern.

Berbagi informasi keamanan siber, yang merupakan salah satu praktik terbaik internasional dalam memperkuat *situational awareness* dan respons cepat terhadap insiden siber. Pengaturan ini penting karena ancaman siber bersifat lintas batas dan tidak dapat ditangani secara parsial oleh satu entitas saja. Menurut laporan ENISA Threat Landscape 2024, lebih dari 70% mitigasi insiden berhasil karena adanya kolaborasi berbagi informasi antar lembaga dan negara. Dengan adanya pasal ini, Indonesia memperkuat posisi dalam membangun ekosistem keamanan siber nasional berbasis kepercayaan (*trusted information sharing ecosystem*) dengan memperhatikan prinsip validitas, keandalan, dan Pelindungan data. Kewajiban partisipasi penyelenggara infrastruktur informasi kritikal (IIK) dan koordinasi oleh instansi pemerintah yang berwenang menunjukkan upaya untuk menciptakan sistem terpadu berbasis *national cyber fusion center*, di mana informasi ancaman, kerentanan, dan respons dapat dikelola secara terintegrasi.

Penyelenggaraan Persandian, yang menjadi aspek fundamental dalam Pelindungan data dan komunikasi. Urgensi pengaturan ini didorong oleh meningkatnya serangan terhadap kerahasiaan dan integritas data, termasuk kebocoran data pribadi, manipulasi komunikasi, dan eksploitasi enkripsi lemah. Penerapan standar kriptografi nasional, seperti yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN), bertujuan untuk menjamin keamanan dan keandalan sistem persandian di seluruh lapisan infrastruktur informasi. Pengaturan ini juga sejalan dengan praktik global seperti US Federal Information Processing Standards (FIPS 140-3) dan EU *Cybersecurity* Act, yang menegaskan pentingnya penggunaan kriptografi bersertifikat untuk menjaga keutuhan

sistem nasional. Selain itu, kewajiban penggunaan persandian oleh penyelenggara IIK dan sertifikasi terhadap penyedia teknologi enkripsi memperkuat kedaulatan digital nasional dan mengurangi ketergantungan terhadap algoritma kriptografi asing yang berpotensi menimbulkan risiko keamanan.

Pengukuran tingkat kematangan keamanan siber (*Cybersecurity maturity level*) sebagai mekanisme evaluasi periodik terhadap penerapan kebijakan dan kontrol keamanan. Pengaturan ini berkaitan erat dengan kebutuhan untuk menilai efektivitas sistem keamanan secara objektif dan berbasis data. Pendekatan ini sejalan dengan konsep Capability Maturity Model Integration (CMMI) dan kerangka NIST CSF 2.0, yang menekankan pentingnya evaluasi rutin untuk memastikan kesiapan organisasi menghadapi ancaman. Dengan kewajiban pelaporan hasil pengukuran kepada instansi pengatur dan pengawas sektor, pemerintah dapat memperoleh gambaran nasional tentang kesiapan siber, mengidentifikasi sektor yang rentan, dan merancang intervensi kebijakan berbasis bukti (*evidence-based policy*).

Audit dan asesmen keamanan siber mempertegas pentingnya pengawasan dan akuntabilitas dalam tata kelola keamanan siber. Audit dan asesmen menjadi instrumen untuk memastikan kesesuaian penerapan kebijakan dengan standar yang berlaku, sekaligus mendeteksi kelemahan sistem secara dini. Urgensinya semakin tinggi mengingat serangan siber sering kali terjadi akibat lemahnya *compliance monitoring*. Pengaturan mengenai pelaksanaan audit internal dan eksternal, serta penetapan daftar pelaksana independen oleh instansi berwenang, memastikan bahwa proses verifikasi dilakukan secara obyektif dan profesional. Selain itu, mekanisme audit eksternal memperkuat *checks and balances* terhadap pelaksanaan keamanan siber di sektor publik maupun privat, sehingga keandalan sistem nasional dapat terjaga.

Perlunya desain tata kelola keamanan siber yang menyeluruh dan berlapis, mulai dari perencanaan risiko, pertukaran informasi,

pelindungan teknis melalui persandian, hingga evaluasi kinerja melalui pengukuran kematangan dan audit. Pengaturan ini muncul sebagai respons atas meningkatnya kompleksitas ancaman siber, kebutuhan koordinasi antar sektor, serta tuntutan untuk membangun ekosistem keamanan siber nasional yang tangguh, adaptif, dan berdaulat. Dengan kerangka ini, RUU KKS tidak hanya berfungsi sebagai instrumen hukum, tetapi juga sebagai *blueprint* kebijakan yang memperkuat ketahanan nasional di ruang siber, sejalan dengan arah transformasi digital Indonesia menuju 2045.

6. Kerja Sama Internasional

Kerja sama internasional di bidang keamanan dan ketahanan siber merupakan upaya kolaboratif antara Pemerintah Indonesia dan komunitas global untuk memperkuat kemampuan nasional dalam menghadapi ancaman siber yang bersifat lintas batas dan transnasional. Dalam praktiknya, kerja sama ini mencakup pertukaran informasi ancaman siber dan serangan siber, peningkatan kapasitas sumber daya manusia melalui pelatihan dan transfer teknologi, penyusunan standar serta norma internasional yang sejalan dengan kepentingan nasional, serta kolaborasi dalam penelitian dan pengembangan teknologi keamanan siber. Ketentuan ini menjadi dasar hukum bagi Indonesia untuk berperan aktif dalam tata kelola keamanan siber global dan memastikan ruang siber nasional tetap aman, tangguh, dan berdaulat.

Urgensi pengaturan kerja sama internasional didasari oleh karakter ruang siber yang tidak mengenal batas geografis sehingga ancamannya bersifat global. Tidak ada satu negara pun yang mampu melindungi dirinya secara mandiri dari serangan siber. Oleh karena itu, penting untuk menegaskan bahwa keamanan dan ketahanan siber tidak dapat dilakukan oleh Indonesia sendiri, melainkan memerlukan kerja sama internasional dalam menangani ancaman dan serangan siber yang bersifat transnasional dan *borderless*. Melalui kerja sama internasional, Indonesia dapat

memperkuat deteksi dini dan mitigasi ancaman, menyesuaikan kebijakan nasional dengan standar dan protokol global, meningkatkan kapasitas kelembagaan dan sumber daya manusia, serta memperkuat posisi diplomasi siber nasional di berbagai forum regional dan multilateral.

Saat ini Indonesia telah menjalin berbagai bentuk kerja sama internasional di bidang keamanan dan ketahanan siber. Secara bilateral, Indonesia telah menjalin kemitraan dengan sepuluh negara sahabat yang memiliki kepentingan dan kapasitas dalam bidang keamanan siber. Pada tingkat regional, Indonesia aktif dalam kerja sama ASEAN melalui ASEAN *Cybersecurity* Cooperation Strategy dan forum ASEAN Ministerial Conference on *Cybersecurity* (AMCC), serta di kawasan Asia Pasifik dan negara-negara anggota Organisasi Kerja Sama Islam (OKI). Sementara pada tingkat global, Indonesia berpartisipasi dalam kerja sama multilateral di bawah naungan Perserikatan Bangsa-Bangsa, antara lain melalui *United Nations Office on Drugs and Crime* (UNODC) dan *United Nations Institute for Disarmament Research* (UNIDIR). Kerja sama yang dilakukan sesuai perjanjian dan kesepakatan internasional tersebut secara umum mencakup penegakan hukum bersama terhadap kejahatan siber, peningkatan kapasitas kelembagaan, serta pertukaran informasi mengenai ancaman dan serangan siber.

Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang berwenang memiliki mandat untuk menjalin kerja sama internasional dalam rangka memperkuat keamanan dan ketahanan siber nasional. Kerja sama ini mencakup pertukaran informasi, penelitian dan pengembangan kebijakan, serta penanganan ancaman siber transnasional yang dapat mempengaruhi lebih dari satu negara. Pelaksanaan kerja sama tersebut didasarkan pada perjanjian internasional, kesepakatan regional atau bilateral, serta konvensi internasional yang telah diratifikasi atau diaksesi oleh Indonesia. Selain itu, BSSN bekerja sama dengan badan publik

penyelenggara atau pemilik infrastruktur informasi internasional, baik dari kalangan pemerintah, non-pemerintah, maupun perusahaan multinasional, dengan tetap mengutamakan kepentingan nasional, arah politik luar negeri, ketentuan perundang-undangan, serta prinsip hukum internasional.

Untuk memajukan kepentingan siber Indonesia di tingkat global, BSSN berpartisipasi aktif dalam berbagai program dan forum internasional, termasuk perumusan konsep, norma, dan panduan keamanan siber secara bilateral, regional, dan multilateral. Pemerintah juga berperan aktif dalam forum internasional untuk memecahkan persoalan keamanan siber, membangun kemitraan dengan berbagai negara dan penyelenggara sistem elektronik atau pemilik infrastruktur informasi strategis, serta meningkatkan kapasitas keamanan siber di kawasan. Dalam pelaksanaan diplomasi siber, BSSN bekerja sama dengan kementerian dan lembaga terkait, terutama Kementerian Luar Negeri yang memiliki mandat utama dalam urusan hubungan luar negeri. Untuk memperkuat diplomasi siber, pemerintah dapat menugaskan atau menunjuk atase keamanan dan ketahanan siber di perwakilan luar negeri sebagai perpanjangan tangan diplomasi teknis di bidang siber.

Kerja sama internasional ini bersifat berkelanjutan, adaptif, dan berbasis kepentingan nasional. Dalam situasi tertentu, seperti ketika terjadi insiden siber berskala besar, kerja sama internasional dapat diaktifkan untuk memperkuat koordinasi, penanganan darurat, dan pemulihan sistem. Selain itu, kerja sama ini juga dilakukan dalam tahap-tahap perumusan kebijakan dan implementasi strategi keamanan siber nasional agar selalu selaras dengan norma dan praktik terbaik internasional. Pelaksanaannya dilakukan secara transparan, akuntabel, dan terkoordinasi lintas lembaga guna mencegah tumpang tindih kewenangan. Bentuk pelaksanaannya dapat berupa perjanjian formal, *memorandum of understanding* (MoU), pertukaran nota diplomatik, atau mekanisme

kerja sama teknis antar lembaga yang relevan.

Dengan demikian, pengaturan mengenai kerja sama internasional dalam RUU KKS memiliki nilai strategis sebagai dasar hukum bagi Indonesia untuk memperkuat posisi dan peran dalam tata kelola keamanan siber global. Ketentuan ini memastikan bahwa upaya menjaga keamanan dan ketahanan siber nasional dilakukan secara kolaboratif, sesuai hukum nasional, serta sejalan dengan prinsip tanggung jawab bersama (*shared responsibility*) dalam mewujudkan ruang siber yang aman, stabil, dan terpercaya bagi seluruh pemangku kepentingan, sekaligus memperkuat kedaulatan digital dan diplomasi siber Indonesia di tataran internasional.

7. Peran Pemerintah

Perkembangan teknologi informasi dan komunikasi menjadikan ruang siber sebagai domain strategis yang memiliki pengaruh signifikan terhadap keamanan nasional, stabilitas ekonomi, kesejahteraan sosial, dan kedaulatan negara. Dalam konteks ini, kehadiran pemerintah dalam penyelenggaraan keamanan dan ketahanan siber menjadi faktor penentu dalam menjaga keutuhan negara dari berbagai ancaman yang semakin kompleks dan canggih. Pemerintah perlu memainkan peran sentral dalam membangun kerangka kebijakan yang komprehensif, mengoordinasikan berbagai pemangku kepentingan, serta memastikan kesiapsiagaan nasional dalam menghadapi insiden siber yang berpotensi mengganggu pelayanan publik dan kepentingan strategis negara. Tanpa kepemimpinan yang kuat dari pemerintah, fragmentasi kebijakan dan penanganan ancaman siber akan mengurangi efektivitas sistem pertahanan nasional, sehingga diperlukan sinergi antarlembaga yang terkoordinasi dengan baik sebagai wujud negara hadir dalam melindungi seluruh elemen bangsa dari risiko serangan siber.

Dalam penyelenggaraannya, pemerintah harus mengambil inisiatif strategis melalui penyusunan standar dan kebijakan nasional yang menjadi pedoman bagi seluruh pemangku kepentingan, sekaligus mendorong peningkatan kesadaran dan pembentukan budaya keamanan siber di masyarakat. Upaya ini perlu didukung dengan pengembangan kapasitas sumber daya manusia melalui pendidikan, pelatihan, dan peningkatan kompetensi di bidang keamanan siber, yang merupakan fondasi krusial bagi ketahanan nasional dalam menghadapi ancaman yang terus berevolusi. Selain itu, pemerintah wajib memfasilitasi pengembangan ilmu pengetahuan, teknologi, riset, dan inovasi untuk memperkuat ekosistem industri teknologi keamanan siber nasional, sekaligus melakukan pengawasan kepatuhan terhadap ketentuan yang berlaku. Tidak kalah pentingnya adalah kemampuan pemerintah dalam menyusun rencana kontingensi krisis siber, melakukan penindakan terhadap pelanggaran dan kejahatan siber, pemberian penghargaan kepada Penyelenggara IIK yang telah memenuhi standar Keamanan Siber dan memiliki kinerja Keamanan Siber yang baik, serta memantau anomali trafik internet secara proaktif sebagai langkah pencegahan dini. Dengan pendekatan holistik yang mengintegrasikan aspek kebijakan, teknis, hukum, dan edukasi, peran pemerintah menjadi kunci dalam membangun ruang siber yang aman, resilien, dan mendukung pertumbuhan ekonomi digital yang berkelanjutan.

8. Audit Teknis

Audit teknis IIK merupakan proses pemeriksaan, penelusuran, dan pengumpulan fakta secara sistematis terhadap suatu Insiden Siber dengan tujuan untuk menemukan penyebab, modus, dampak, serta pihak yang bertanggung jawab atas terjadinya insiden yang dilakukan berdasarkan permintaan dari Penyelenggara IIK.

Instansi pemerintah yang melaksanakan tugas dan fungsi di bidang Keamanan dan Ketahanan Siber berwenang melakukan audit teknis IIK terhadap Insiden Siber yang terjadi pada IIK.

Selama pelaksanaan audit teknis IIK, Penyelenggara IIK wajib:

a. menyampaikan data dan/atau informasi yang valid; dan
b. memberikan akses terhadap IIK yang terdampak.

Hasil audit teknis IIK disampaikan kepada lembaga yang melakukan permintaan audit.

9. Partisipasi Masyarakat

Keterlibatan masyarakat dapat memberikan legitimasi yang kuat dalam suatu peraturan perundangan, ketika masyarakat dilibatkan dan dipertimbangkan “suaranya" dalam ekosistem pengaturan keamanan dan ketahanan siber maka dukungan publik terhadap suatu kebijakan yang diusulkan juga akan meningkat. Peran dari publik juga menjadi salah satu bentuk akuntabilitas masyarakat sebagai *peer reviewer non-formal* yang menguji kelaikan, kepraktisan, dan dampak sosial dari konsep pengaturan undang-undang keamanan dan ketahanan siber. Pelibatan masyarakat dapat menjadi salah satu investasi pemerintah untuk menciptakan kedaulatan digital yang kuat bukan hanya secara teknis namun juga demokratis dan berkeadilan. Untuk itu dalam mewujudkan keterlibatan masyarakat dan lintas sektor pada ekosistem keamanan dan ketahanan siber maka perlu pengaturan yang lebih terperinci mengenai partisipasi masyarakat.

Keamanan dan ketahanan siber tidak dapat dicapai semata-mata melalui upaya pemerintah dan penyelenggara infrastruktur informasi, melainkan memerlukan keterlibatan aktif seluruh elemen masyarakat sebagai bagian integral dari ekosistem digital nasional. Dalam konteks ruang siber yang bersifat terbuka dan saling terhubung, setiap individu dan organisasi menjadi bagian dari rantai keamanan yang saling memengaruhi, sehingga kesadaran dan kemampuan masyarakat dalam mengenali ancaman

siber, melaporkan insiden, serta menerapkan praktik keamanan yang baik menjadi faktor penentu dalam membangun ketahanan nasional. Partisipasi masyarakat tidak hanya berperan sebagai lapis pertahanan awal dalam mendeteksi dan mencegah serangan siber, tetapi juga sebagai mitra strategis dalam membangun budaya keamanan informasi yang menjadi fondasi ketahanan siber jangka panjang, sejalan dengan prinsip penghargaan dan pelindungan hak asasi manusia yang menjadi salah satu asas penyelenggaraan keamanan dan ketahanan siber.

Bentuk partisipasi masyarakat dalam keamanan dan ketahanan siber dapat diwujudkan melalui berbagai mekanisme, mulai dari pelaporan ancaman dan insiden siber, peningkatan kapasitas melalui pelatihan keamanan siber, hingga keterlibatan dalam komunitas keamanan siber yang saling berbagi informasi. Keterlibatan masyarakat sipil, akademisi, komunitas teknologi, dan kelompok relawan keamanan siber memiliki peran strategis dalam memperkuat deteksi dini ancaman, mempercepat respons insiden, serta memperkaya pengetahuan kolektif dalam menghadapi perkembangan ancaman yang semakin kompleks. Dengan demikian, pengembangan kerangka kebijakan yang mendorong partisipasi masyarakat bukan hanya merupakan kebutuhan operasional, tetapi juga refleksi dari pendekatan keamanan siber yang holistik dan berkelanjutan, yang mengakui bahwa keamanan siber yang efektif harus dibangun dari bawah (*bottom-up*) sekaligus diarahkan dari atas (*top-down*), sehingga tercipta ekosistem yang kolaboratif, responsif, dan resilien terhadap berbagai ancaman yang muncul di ruang siber.

10. Pendanaan

Pendanaan yang memadai dan berkelanjutan merupakan faktor kritikal dalam mewujudkan penyelenggaraan keamanan dan ketahanan siber yang efektif. Tanpa komitmen anggaran yang jelas dan terstruktur, berbagai upaya strategis seperti pengembangan

kapasitas sumber daya manusia, peningkatan infrastruktur teknologi, pelaksanaan manajemen krisis siber, serta penguatan sistem deteksi dan respons insiden tidak dapat berjalan optimal. Dalam konteks negara Indonesia dengan karakteristik geografis yang luas dan kompleks, pendanaan menjadi poros utama dalam mengintegrasikan berbagai inisiatif keamanan siber dari tingkat pusat hingga daerah. Pemerintah perlu memastikan alokasi anggaran yang proporsional. Tanpa pendanaan yang memadai, upaya melindungi infrastruktur informasi dan infrastruktur informasi kritikal dari ancaman siber akan menjadi rentan dan tidak berkelanjutan, sehingga membahayakan keamanan nasional, stabilitas ekonomi, dan pelayanan publik.

Diversifikasi sumber pendanaan menjadi prinsip penting untuk memastikan fleksibilitas dan ketahanan dalam implementasi kebijakan keamanan dan ketahanan siber. Ketergantungan hanya pada satu sumber pendanaan dapat menimbulkan risiko ketika terjadi fluktuasi ekonomi atau perubahan prioritas anggaran. Oleh karena itu, selain mengandalkan Anggaran Pendapatan dan Belanja Negara sebagai tulang punggung utama, diperlukan pemanfaatan Anggaran Pendapatan dan Belanja Daerah yang disesuaikan dengan kebutuhan dan risiko siber di masing-masing wilayah.

Selain itu, sumber pendanaan lain yang sah dan tidak mengikat perlu dipertimbangkan untuk memperkuat ekosistem keamanan siber nasional, selama tetap memenuhi prinsip transparansi, akuntabilitas, dan tidak bertentangan dengan kedaulatan negara. Dana ini dirancang guna mendukung dalam Pengembangan sumber Daya Manusia, Penelitian dan pengembangan serta pemberian penghargaan sebagai salah satu sumber pendanaan alternatif.

Penting untuk memastikan bahwa sumber pendanaan tambahan tidak membawa ketergantungan yang dapat mengurangi otonomi kebijakan atau membahayakan keamanan informasi

strategis. Dengan pendekatan pendanaan yang komprehensif dan beragam ini, penyelenggaraan keamanan dan ketahanan siber dapat berjalan secara efektif, responsif terhadap perkembangan ancaman, sekaligus tetap menjaga prinsip transparansi.

11. Penyidikan

Perkembangan ancaman kejahatan siber sebagai dampak dari teknologi informasi dan komunikasi yang berkembang pesat telah mengubah lanskap tindak pidana menjadi bentuk yang lebih kompleks dalam ruang siber. Karakteristik unik tindak pidana siber yang bersifat transnasional, jejak digital yang rentan dimanipulasi, memerlukan pemahaman teknis yang mendalam mengenai sistem elektronik dan infrastruktur informasi serta menuntut pendekatan penyidikan yang berbeda. Keberadaan bukti elektronik yang menjadi inti dalam penanganan kasus siber memerlukan penanganan khusus untuk menjaga integritas, autentisitas, *chain of custody* dan memastikan *admissibility*-nya dalam proses peradilan. Oleh karena itu, diperlukan kerangka hukum yang mengakomodir kekhususan teknis penyidikan kasus siber, sekaligus memastikan pelindungan hak-hak dasar warga negara sesuai dengan prinsip negara hukum.

Dalam konteks pelindungan infrastruktur informasi dan infrastruktur informasi kritikal yang berdampak bagi keamanan nasional, stabilitas ekonomi, dan pelayanan publik, mekanisme penyidikan tindak pidana siber dilakukan sesuai dengan ketentuan peraturan perundang-undangan. Dengan demikian, kerangka hukum penyidikan tindak pidana siber harus mampu menggabungkan prinsip-prinsip hukum acara pidana untuk menghadapi tantangan ~~unik~~ kejahatan di ruang siber.

12. Sanksi Adminstratif

Dalam kerangka hukum keamanan dan ketahanan siber, sanksi administratif memiliki peran strategis sebagai instrumen

pencegahan (preventif) dan pemulihan *(corrective)* sebelum suatu pelanggaran tereskalasi menjadi tindak pidana. Berbeda dengan sanksi pidana yang bersifat represif dan ultimum remedium, sanksi administratif dirancang untuk mendorong kepatuhan normatif melalui mekanisme pengawasan berkelanjutan, koreksi prosedural, dan penguatan akuntabilitas institusional. Sanksi administratif dalam RUU ini dapat digunakan oleh pemerintah sebagai reaksi atas pelanggaran administrasi/ ketidakpatuhan terhadap kewajiban yang terdapat dalam norma hukum/ ketentuan undang-undang yang bersifat administratif.

Dalam RUU ini terdapat sanksi administratif dan sanksi pidana yang satu sama lain tidak saling meniadakan. Pengenaan sanksi administratif dalam RUU ini berbeda dengan pengenaan sanksi administratif pada peraturan perundang-undangan lain, karena ketentuan kewajiban yang dilanggar tentu berbeda dan tidak akan sama. Dengan kata lain bahwa sanksi administratif dalam RUU ini bersifat *complimentary* dan tidak bersifat untuk duplikasi.

Dalam konteks RUU Keamanan dan Ketahanan Siber, sanksi administratif tidak hanya berfungsi sebagai alat penegakan hukum, tetapi juga sebagai mekanisme insentif negatif yang mendorong pelaku usaha, penyelenggara infrastruktur, dan subjek hukum lainnya untuk mematuhi pengaturan keamanan dan ketahanan siber secara proaktif. Hal ini sejalan dengan prinsip *risk-based regulation* yang dianut dalam kerangka regulasi siber global yang menempatkan sanksi administratif sebagai bagian integral dari sistem tata kelola keamanan siber nasional.

Pendekatan sanksi administratif dalam regulasi teknologi didasarkan pada teori responsive regulation, yang menekankan bahwa efektivitas regulasi tidak hanya bergantung pada ancaman hukuman, tetapi pada gradasi respons terhadap tingkat kepatuhan. Dalam konteks ini, sanksi administratif seperti peringatan tertulis, denda, atau penarikan produk merupakan

langkah awal dalam *"enforcement pyramid"* sebelum tindakan pidana diambil.

Pada Bab ini secara eksplisit menyebutkan norma-norma substantif yang apabila dilanggar akan dikenai sanksi administratif, antara lain:

a. Kewajiban Penyelenggara Infrastruktur Informasi melaksanakan enam pilar keamanan siber (tata kelola, identifikasi, proteksi, deteksi, tanggap insiden, pemulihan).
b. Kewajiban khusus Penyelenggara IIK, termasuk integrasi dengan *National Security Operations Center* (NSOC) dan pelaporan insiden.
c. Kewajiban Penyedia PDED memenuhi standar keamanan, transparansi kerentanan, dan mekanisme pembaruan.
d. Kewajiban penggunaan persandian sesuai dengan standar nasional.

Pelanggaran terhadap ketentuan tersebut bersifat administratif-teknis, bukan kriminal, karena umumnya berkaitan dengan kelalaian prosedural, ketidaksesuaian standar, atau keterlambatan pelaporan, bukan niat jahat *(mens rea)*. Oleh karena itu, sanksi administratif memberikan ruang bagi pelaku untuk memperbaiki sistem dan menghindari kerugian lebih luas.

Pengenaan sanksi administratif dapat mendorong perilaku agar kembali kepada sikap yang sesuai hukum. Pengenaan sanksi administratif dapat dikategorikan dalam beberapa konteks tindakan, yakni:

a. Penyelenggara Infrastruktur Informasi, Penyelenggara IIK dan Penyedia PDED yang tidak melaksanakan kewajibannya.
b. Sanksi administratif diberikan oleh BSSN atau pengawas dan pengatur sektor terkait sesuai dengan ketentuan peraturan perundang-undangan.
c. Pengenaan sanksi administratif tidak menghapuskan tanggung jawab pidana dan perdata.

Dalam pemberian sanksi administratif disesuaikan dengan

besaran pelanggaran yang dilakukan. Selain itu, ketentuan sanksi administratif juga dapat ditentukan berdasarkan klasifikasi jenis pelanggaran yang dilakukan.

Dalam RUU ini terdapat 2 (dua) bentuk sanksi administratif, yaitu:

a. peringatan tertulis; dan
b. denda administratif.

Sanksi administratif dapat diterapkan secara berjenjang, mulai dari yang berbobot ringan seperti teguran, hingga yang berbobot lebih berat seperti denda. Hal ini berarti bahwa penerapan sanksi administratif yang lebih berat harus didahului dengan pemberian sanksi administratif yang paling ringan. Jika pihak yang dikenai sanksi tidak menanggapi sanksi administratif yang paling ringan maka sanksi administratif yang lebih berat dapat diberikan.

Peringatan tertulis merupakan tahap awal sebelum pemberian sanksi administratif yang lebih berat. Sebagai bentuk *early warning* yang bertujuan edukatif dan korektif, peringatan tertulis memberikan kesempatan kepada pelanggar untuk memperbaiki ketidaksesuaian dalam jangka waktu tertentu sebelum sanksi lebih berat dijatuhkan. Pendekatan ini sejalan dengan prinsip *good governance* dan *due process* dalam administrasi negara modern. Pemberian sanksi ini juga dapat dilakukan lebih dari 1 (satu) kali.

Pengenaan denda administratif merupakan reaksi terhadap pelanggaran norma yang ditujukan untuk menambah hukuman yang pasti. Pemerintah berwenang untuk menjatuhkan hukuman berupa denda (*geldboete*) terhadap subjek hukum yang telah melakukan pelanggaran administrasi berdasarkan UU KKS. Denda administratif telah ditentukan mengenai jumlah yang dikenakan kepada pihak yang melanggar ketentuan yang bersifat administratif dalam undang-undang ini. Denda administratif hanya dapat diterapkan atas dasar kekuatan wewenang yang diatur dalam undang-undang dalam arti formal, sehingga perlu disebutkan lembaga yang dapat menjatuhkan sanksi administratif.

Penerapan sanksi administratif harus diimbangi dengan jaminan keadilan prosedural (*procedural fairness*) untuk mencegah penyalahgunaan wewenang.

Sanksi administratif dalam RUU ini juga perlu dipahami dalam kerangka hukum administrasi negara Indonesia. Sebagaimana diatur dalam Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan bahwa sanksi administratif merupakan bagian dari tindakan administratif yang dapat diuji melalui Peradilan Tata Usaha Negara maka setiap keputusan sanksi harus memenuhi syarat keabsahan formal dan materiil, termasuk dasar hukum yang jelas, alasan yang logis, dan tidak bertentangan dengan asas-asas umum pemerintahan yang baik.

13. Ketentuan Pidana

Terhadap materi yang telah diatur dalam UU KKS, terhadap pelanggaran akan ditetapkan sanksi yang proporsional dengan perbuatan/pelanggaran yang dilakukan. Penerapan sanksi diharapkan selain sebagai upaya memberikan efek jera, juga untuk dapat memberikan pemahaman kepada masyarakat agar dapat menaruh perhatian dan memahami pentingnya terkait pelindungan, keamanan, dan juga ketahanan siber.

Dalam UU KKS, diatur sanksi pidana mengingat banyaknya kasus serangan dan kejahatan siber di era digital ini serta menimbulkan kerugian yang sangat besar bagi korban kejahatan siber. Besaran sanksi pidana yang dijatuhkan dapat dirumuskan sesuai dengan ketentuan peraturan-perundang-undangan.

Setiap Orang yang melakukan tindak pidana yang mengakibatkan terganggunya atau tidak berfungsinya IIK, dipidana dengan pidana penjara paling lama seumur hidup atau 20 (dua puluh) tahun atau pidana denda paling banyak kategori VIII dan Setiap Orang secara tanpa hak mengakses IIK mengakibatkan informasi elektronik dan/atau Dokumen Elektronik pada IIK tidak dapat diakses oleh pihak yang berhak disertai dengan permintaan

tebusan, dipidana dengan pidana penjara paling lama seumur hidup atau 20 (dua puluh) tahun atau pidana denda paling banyak kategori VIII.

Adapun tindak pidana yang dikenakan pidana dalam UU KKS yaitu:

a. perbuatan yang ditujukan terhadap komputer dan/atau sistem elektronik serta informasi elektronik dan/atau dokumen elektronik milik pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan.
b. dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun seperti melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
c. dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik tertentu milik Orang lain yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
d. dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
e. dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi

Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

f. dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

g. dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   1) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan;
   2) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses,

   dengan tujuan memfasilitasi perbuatan kejahatan siber, namun bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik.

h. dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

i. dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam huruf a sampai dengan huruf h mengakibatkan kerugian bagi Orang lain.

j. dengan sengaja melakukan perbuatan sebagaimana dimaksud dalam huruf a sampai dengan huruf h di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

14. Ketentuan Penutup

Dalam sistem hukum positif Indonesia, ketentuan penutup dalam suatu undang-undang bukan sekadar formalitas teknis, melainkan bagian integral dari mekanisme transisi hukum *(legal transition mechanism)* yang menjamin kepastian hukum, kelangsungan administrasi negara, dan efektivitas implementasi norma baru. Ketentuan penutup berfungsi sebagai "jembatan normatif" antara rezim hukum lama dan rezim hukum baru, sehingga tidak terjadi *legal vacuum* atau *regulatory shock* yang dapat mengganggu stabilitas tata kelola sektor terkait.

Dalam konteks RUU tentang Keamanan dan Ketahanan Siber, ketentuan penutup memiliki peran strategis karena Regulasi ini bersifat transformasional, mengubah paradigma pengaturan siber dari pendekatan reaktif-pidana (seperti dalam UU ITE) menjadi pendekatan proaktif-resilien berbasis risiko dan tanggung jawab institusional. Selain itu, subjek hukum yang diatur sangat luas meliputi instansi pemerintah, pelaku usaha, hingga masyarakat sehingga memerlukan masa transisi untuk adaptasi teknis, organisasi, dan budaya. Di satu sisi, implementasi norma teknis (antara lain audit, asesmen PDED, integrasi NSOC) memerlukan infrastruktur pendukung, kapasitas kelembagaan, dan peraturan pelaksana yang tidak dapat dibangun secara instan. Oleh karena itu, ketentuan penutup ini dirancang sebagai mekanisme legal yang responsif terhadap realitas implementasi, sekaligus menjaga prinsip non-retroaktivitas dan Pelindungan kepercayaan yang sah *(rechtsvertrouwen)* sebagaimana dijamin dalam UUDNRI Tahun 1945 dan prinsip umum hukum administrasi negara.

Pengaturan mengenai “Penyelenggara Infrastruktur Informasi, Penyelenggara IIK, dan Pemerintah wajib menyesuaikan dengan Undang-Undang ini paling lama 2 (dua) tahun sejak Undang-Undang ini diundangkan” mengadopsi prinsip *grace period* yang lazim dalam regulasi teknologi global. Masa 2 tahun dalam ketentuan ini merupakan jangka waktu proporsional yang mempertimbangkan kompleksitas teknis dalam membangun sistem deteksi, proteksi, dan pelaporan siber, kebutuhan pelatihan SDM dan restrukturisasi organisasi, proses sertifikasi produk digital dan audit eksternal yang memerlukan waktu.

Tanpa masa transisi, pelaku usaha (khususnya UMKM) dan sektor publik berpotensi langsung dikenai sanksi administratif atau pidana meskipun belum memiliki kapasitas memadai, yang bertentangan dengan prinsip keadilan substantif dan proporsionalitas.

Pengaturan mengenai “Pada saat Undang-Undang ini mulai berlaku, semua peraturan perundang-undangan yang mengatur mengenai Keamanan dan Ketahanan Siber dinyatakan tetap berlaku selama tidak bertentangan dengan ketentuan dalam Undang-Undang ini” mewujudkan prinsip *lex posterior derogat legi priori* (hukum yang lebih baru mengesampingkan hukum yang lebih lama) secara selektif, bukan secara otomatis mencabut seluruh peraturan lama. Pendekatan ini mencegah kekosongan hukum pada masa transisi, menghormati prinsip hierarki peraturan perundang-undangan (UU No. 12 Tahun 2011), memungkinkan penggunaan peraturan teknis yang masih relevan selama tidak bertentangan dengan prinsip dasar RUU ini. Hal ini sejalan dengan praktik global, di mana regulasi kontemporer terkait keamanan siber tidak serta merta mencabut regulasi sektoral nasional, tetapi mensyaratkan kesesuaian prinsip *(consistency check)*.

Pengaturan mengenai “Peraturan pelaksanaan Undang-Undang ini harus telah ditetapkan paling lama 2 (dua) tahun terhitung sejak Undang-Undang ini diundangkan” mencerminkan

komitmen negara terhadap efektivitas hukum *(effectiveness of law).* Tanpa peraturan pelaksana seperti Peraturan Pemerintah tentang peraturan pelaksana UU ini maka norma dalam UU ini akan bersifat deklaratif dan tidak operasional. Ketentuan ini mencegah praktik *legislative delay* yang sering menghambat implementasi UU sektoral di Indonesia.

Pengaturan mengenai "Undang-Undang ini mulai berlaku pada tanggal diundangkan" mengikuti asas publisitas hukum yang berarti suatu peraturan hanya mengikat setelah diundangkan dalam Lembaran Negara (UU No. 12 Tahun 2011 sebagaimana telah diubah terakhir kali dengan UU No. 13 Tahun 2022). Hal ini menjamin transparansi dan aksesibilitas hukum bagi seluruh warga negara dan pelaku usaha, sebagaimana dijamin dalam UUD 1945.

Badan Publik Penyelenggara atau Pemilik Infrastruktur Informasi, serta badan yang telah berfungsi sebagai unsur penyelenggaraan Keamanan dan Ketahanan Siber, tetap beroperasi sebagaimana mestinya hingga diubah atau diganti berdasarkan ketentuan dalam Undang-Undang ini.

Selain itu, Badan Siber dan Sandi Negara diwajibkan untuk menyesuaikan penyelenggaraan tugas dan fungsinya sesuai dengan ketentuan dalam Undang-Undang ini dalam jangka waktu paling lama 2 (dua) tahun sejak Undang-Undang ini diberlakukan.

BAB VI
PENUTUP

A. Simpulan

Berdasarkan uraian dalam bab sebelumnya, dapat ditarik simpulan sebagai berikut :

1. Ruang Siber dan ekosistem digital telah menjadi bagian tak terpisahkan dari kehidupan masyarakat dan penyelenggaraan negara serta memiliki pengaruh signifikan terhadap keamanan nasional, stabilitas ekonomi, kesejahteraan sosial, reputasi negara, dan pelayanan publik. Transformasi digital selain memberikan manfaat besar bagi kehidupan manusia juga telah menimbulkan ancaman baru dalam bentuk kejahatan siber, yang kini menjadi ancaman global serius bagi banyak negara, termasuk Indonesia. Dunia siber yang terus berkembang telah menciptakan tantangan baru dalam menjaga keamanan dan kedaulatan nasional, serta memelihara stabilitas ekonomi, pelayanan publik, dan kesejahteraan sosial. Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber bertujuan untuk memperkuat pengaturan dan Pelindungan siber di Indonesia dalam menghadapi tantangan ancaman siber global dan domestik. Prinsip utama dalam Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber meliputi kedaulatan siber, pelindungan data pribadi, keamanan nasional, serta akuntabilitas yang saling terintegrasi. RUU ini mendorong sinergi antara pemerintah dan masyarakat dalam menciptakan lingkungan siber yang aman. RUU ini juga mengadopsi prinsip-prinsip internasional dalam ketahanan siber, termasuk komitmen untuk mengadaptasi standar global demi memperkuat regulasi nasional yang sesuai dengan konteks sosial-politik Indonesia. Perbandingan dengan regulasi siber negara lain, seperti Uni Eropa, Jepang, Singapura, dan Amerika Serikat, memberikan acuan untuk memperbaiki strategi dan kebijakan keamanan siber nasional.

2. Hukum positif atau regulasi eksisting saat ini belum mengakomodasi kebutuhan hukum dan kerangka kebijakan terkait dengan keamanan dan ketahanan siber yang membutuhkan pendekatan regulasi baik di level hulu, level menengah, dan level hilir. Dengan demikian, dibutuhkan pembentukan Undang-Undang tersendiri yang mengatur materi muatan didasari prinsip-prinsip dan *best practices* internasional di bidang keamanan dan ketahanan siber. Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber diproyeksikan untuk diterapkan dalam kerangka keamanan dan ketahanan siber sejak level hulu (*upstream digital legal approach*), dalam arti Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber memberikan persyaratan terpenuhinya kriteria keamanan dan ketahanan produk dengan elemen digital sebelum dipasarkan dan digunakan oleh pengguna Infrastruktur Digital atau Infrastruktur Informasi. Pendekatan ini dikombinasikan dengan *Middle Stream Digital Legal Approach* dan *Downstream Digital Legal Approach*.
3. Secara filosofis, pengaturan terkait keamanan siber menggunakan berbagai pendekatan yang saat ini digunakan oleh dunia internasional dan berbagai negara dalam bentuk pendekatan *Cybersecurity*. Hal ini pun mencerminkan pengakuan serta pelindungan kepentingan umum serta pelindungan terhadap hak-hak dasar manusia untuk memperoleh kehidupan yang aman dan dilindungi oleh negara. Dengan demikian, penyusunan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber memiliki dasar filosofis yang kokoh dan dapat dipertanggungjawabkan. Pancasila dalam hal ini menjadi landasan filosofi utama dalam kaitannya dengan jaminan keamanan dan ketahanan siber. Pancasila sebagai *rechtsidee* (cita hukum) yang merupakan konstruksi berpikir dalam mengarahkan hukum kepada apa yang menjadi cita-cita bangsa.
4. Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber mengatur hal-hal sebagai berikut: Ketentuan Umum, Asas

dan Tujuan, Keamanan Siber, Ketahanan Siber, Kerja Sama Internasional, Peran Pemerintah, Audit Teknis, Partisipasi Masyarakat, Pendanaan, Penyidikan, Sanksi Administratif, Ketentuan Pidana, dan Ketentuan Penutup.

B. Saran

1. Indonesia memerlukan pengaturan yang komprehensif di bidang keamanan dan ketahanan siber. Regulasi ini diharapkan mampu melindungi Infrastruktur Informasi dan Infrastruktur Informasi Kritikal serta mencegah insiden siber yang semakin meningkat di sektor publik dan privat. Dengan adanya regulasi ini, Indonesia akan memiliki landasan hukum yang lebih kuat untuk menanggapi serangan siber dan meningkatkan ketahanan nasional di era digital. Oleh karena itu, Pemerintah sudah seharusnya mempunyai suatu regulasi atau pengaturan terkait dengan Keamanan dan Ketahanan Siber, mengingat semakin meningkatnya ancaman siber di era digital saat ini.
2. Badan Siber dan Sandi Negara harus didukung oleh SDM dan ahli yang kompeten serta infrastruktur teknologi yang memadai sehingga dapat berfungsi secara optimal dalam melakukan deteksi dini, pencegahan, serta penanganan cepat terhadap berbagai bentuk ancaman dan serangan siber, mulai dari serangan *malware, ransomware*, hingga pencurian data sensitif. Diperlukan juga koordinasi yang erat antarlembaga untuk optimalisasi fungsi penanganan keamanan dan ketahanan siber yang tangguh dan berkelanjutan.

DAFTAR PUSTAKA

Peraturan perundang-undangan

United Nations Convention Against *Cyber*crime

European Union *Cyber* Resilience Act (EU CRA)

European Union Artificial Intelligence Act (EU AI Act)

European Union General Data Protection Regulation (GDPR).

Executive Order on Improving the Nation's *Cybersecurity* United States

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Peraturan Pemerintah Nomor 71 Tahun 2019

Keputusan Presiden Nomor 103 Tahun 2001

Peraturan Menteri Kominfo Nomor 17 Tahun 2010

Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber

Peraturan Presiden Nomor 53 Tahun 2017

Peraturan Presiden Nomor 133 Tahun 2017

Peraturan Presiden Nomor 28 Tahun 2021

Peraturan Presiden Nomor 47 Tahun 2023

Personal Data Protection Act (PDPA)

Peraturan Badan Siber dan Sandi Negara 2014

Global Cybersecurity Index Report 2024

National Cyber Security Index Report 2023.

The Basic Act on *Cyber* Security

Singapore *Cybersecurity* Act

Singapore Personal Data Protection Act 2012

Literatur

Ahmad M. Ramli & Tasya Safiranita, Hukum Sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital, Bandung:

Refika Aditama, 2022.

Anggika Rahmadiani (et.al), “Strategi Keamanan Siber Indonesia: Rekomendasi Rencana Aksi Dan Implementasi”, dipublikasikan oleh Center for Digital Society, Faculty of Social and Political Sciences Universitas Gadjah Mada, 2019.

Anak Agung Banyu Perwita, "Hakikat Prinsip dan Tujuan Pertahanan-Keamanan Negara.” Dalam Tim Propatria Institute, Mencari Format Komprehensif Sistem Pertahanan dan Keamanan Negara, Jakarta: Propatria, 2006.

Dewan Ketahanan Nasional. "Sebuah Konsep dan Sistem Keamanan Bagi Bangsa Indonesia." Sekretariat Jenderal Dewan Ketahanan Nasional, 2010.

Dwiono, Sugeng, et al. "Hukum Tata Negara: Deskripsi dan Tinjauan Kritikal." CV. Edupedia *Publisher,* 2024

Kevin Iskandar Putra, “Belajar Dari Tata Kelola Keamanan Siber Singapura”, Center For Digital Society, Case Study Series 44, Januari 2019

M. Smith (2015). Research Handbook on International Law and Cyberspace. Massachusetts: Elgar Publishing Limited.

Mokhamad, Johan. Manajemen Keamanan Sistem Informasi, UIN Maliki Press: Malang, 2023.

Pandji Santoso, “Administrasi Publik: Teori dan Aplikasi Good Governance”, Bandung: Refika Aditama, 2008.

Pier Giorgio Chiara, “The *Cyber* Resilience Act: the EU Commission’s proposal for a horizontal regulation on *Cybersecurity* for products with digital elements”, Int. *Cyber*secur. Law Rev., 2022

Proposal untuk Peraturan Parlemen Eropa dan Dewan tentang produk mesin, COM (2021) 202 final.

Rachmat Agung, Keamanan Jaringan, Penerbit KBM : Jogjakarta, 2024

Teguh Prasetyo, Hukum dan Sistem Hukum Berdasarkan Pancasila, Media Perkasa, Yogyakarta, 2013

Candra Irawan, Politik Hukum Hak Kekayaan Intelektual Indonesia, Bandung: Mandar Maju, 2011

Jurnal

Adristi, Fikri Irfan, and Erika Ramadhani. "Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede." *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, Vol. 2, Nomor 6 2024.Aulianisa, Sarah Safira, dan Indirwan Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of *Cyber* Security and Resilience in Indonesia." *Lex Scientia Law Review* 4.1, 2020.

Arnold Hiras Simorangkir dan Arthur Josias Simon Runturambi, "Budaya & Masyarakat Digital dalam Ketahanan Siber di Indonesia: Sebuah Adaptasi dari Pendekatan Capacity Maturity Model (CMM)," Jurnal Multidisiplin Indonesia, Vol. 5, Nomor 4, Juni–Juli 2024.

Anthony J., "What Is Extraterritorial Jurisdiction", Cornell Law Review, Volume 99, Issue 6 September 2014 - Symposium on Extraterritoriality.

Bhavna Arora, "Exploring and Analyzing Internet Crimes and Their Behaviours", Perspectives in Science Vol. 8, 2016

Chiara Vincha, Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber Indonesia, Jurnal Ketahanan Nasional, Vol.30 Nomor2, 2024.

Chintia, Ervina, et al. "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya." *Journal Information Engineering and Educational Technology)* Volume 02, Nomor 02, 2019.

Cynthia Rahmawati, "Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0", Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU), Vol. 1, Nomor 1, 2019

Cindy Vania, (et.al), "Tinjauan Yuridis terhadap Pelindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," Jurnal Multidisiplin Indonesia, Vol. 2, Nomor 3, Maret 2023.

Damar Apri Sudarmadi dan Arthur Josias Simon Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia", Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2,

Nomor2, 2019

Dinda Aprilita Herera & Muhamad Hasan Sebyar, “Pelindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru”, Jurnal Hukum dan Kewargunaan Vol. 1 Nomor 5 Tahun 2023.

Eka Nanda dan Lintang Yudhantaka, “Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia”, Notaire by Universitas Airlangga, Magister Kenotariatan, Vol. 5 Nomor 3, 2022.

Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," AL-BAHST: Jurnal Ilmu Sosial, Politik, dan Hukum, Vol. 2, Nomor 1, April 2024.

Febyola Indah (et.al), “Peran *Cyber* Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka), Jurnal Bidang Penelitian Informatika Vol. 1 Nomor 1, 2022.

Haikal, Muhammad Fikri, and Deasy Mauliana. "Akuntabilitas dan Transparansi dalam Pelayanan Publik (Studi Kasus Pelayanan E-KTP di Kantor Kecamatan Tallo Kota Makassar)." Jurnal Administrasi Negara Volume 28 Nomor 1, 2022

Makbul Rizki, Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi

Tantangan Perkembangan Teknologi dan Informasi, Vol. 14 Nomor 1, Politeia: Jurnal Ilmu Politik, 2022.

Misael Sousa de Araujo (et.al), “Resilience in the Context of *Cyber* Security: A Review of the Fundamental Concepts and Relevance”, Applied Sciences, 2024.

Neltje, Jeane, and Indrawieny Panjiyoga. "Nilai-Nilai Yang Tercakup Di Dalam Asas Kepastian

Hukum. *Innovative: Journal of Social Science Research* 3.5 (2023)

Prakoso Aji, *“Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Pelindungan Data Pribadi)”,* Jurnal Politica, Vol. 13 Nomor 2, 2022.

Putri, B. E. "Penerapan Prinsip-Prinsip Good Corporate Governance pada PT Purnama Semesta Alamiah." Agora Vol. 2 Nomor 2, 2014.

Rosy, Afifah Fidina. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of *Cyber* Security." *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan* 1.2 (2020)

Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Analisis, dan Perkembangannya", Technology and Economics Law Journal Vol. 2 Nomor 2, 2023.

Ratno Dwi Putra (et.al), "Ancaman Siber Dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)", Jurnal Peperangan Asimetris Universitas Pertahanan, Vol. 4 Nomor2, 2018

Sinta Dewi, "Prinsip-Prinsip Pelindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya", Jurnal Sosiohumaniora, Vol. 19 Nomor 3, 2017

Suriaatmadja, Steffi Rifasa Tohir, and Ira Dewi Rachmadiani. "Pelindungan Hukum Terhadap Dokter Umum dalam Melakukan Pelayanan Kesehatan di Masa Pandemi Covid 19 Ditinjau dari UU Wabah Tahun 1984." Innovative: Journal Of Social Science Research 4.3 (2024)

Sahat Maruli Tua S., "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber", SASI, Vol. 27 Nomor 1, 2021

Sitanggang, Andri Sahata, Fernanda Darmawan, and Dony Saputra. "Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber." Jurnal Pendidikan dan Teknologi Indonesia 4.3 (2024)

Vania, Cindy, (et,al). "Tinjauan Yuridis terhadap Pelindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber ," Jurnal Multidisiplin Indonesia, Vol. 2, Nomor 3, Maret 2023.

Teguh Prasetyo, "Membangun Hukum Nasional Berdasarkan Pancasila", Jurnal Hukum dan peradilan, Vol. 3 Nomor 3, 2014

Yusup Ginanjar, “Strategi Indonesia Membentuk *Cyber* Security Dalam Menghadapi Ancaman *Cyber* Crime Melalui Badan Siber dan Sandi Negara”, Jurnal Dinamika Global Vol. 7 Nomor 2, 2022

Artikel/internet

Ahmad M Ramli, Kompas.com, “EU CRA: UU Baru Uni Eropa Menghadapi Peretasan Siber Global”, 2024, <https://tekNomorkompas.com/read/2024/07/26/10441617/eu-cra-uu-baru-uni-eropa-menghadapi-peretasan-siber-global?page=all>, diakses pada 28 September 2024.

Ahmad M. Ramli, Kompas.com, “UU AI Uni Eropa Disahkan: Inspirasi Model Regulasi Indonesia (Bagian I)”, <https://tekNomorkompas.com/read/2024/05/24/10183587/uu-ai-uni-eropa-disahkan-inspirasi-model-regulasi-indonesia-bagian-i>, diakses pada 28 September 2024.

Ahmad M Ramli, “UU Pelindungan Data Pribadi, Big Data, dan Ekonomi Digital”, Kompas.com, <https://nasional.kompas.com/read/2022/10/10/09570741/uu-pelindungan-data-pribadi-big-data-dan-ekonomi-digital?page=3)>, diakses pada 13 Oktober 2024.

Ahmad M Ramli, (2024), ““UN Convention Against *Cyber*crime”: Konvensi Pertama PBB Tentang Kejahatan Siber (Bagian I), <https://tekNomorkompas.com/read/2024/08/19/09445517/un-convention-against-*cyber*crime-konvensi-pertama-pbb-tentang-kejahatan-siber?page=all#page2> diakses 29 September 2024.

Aptika, “Pentingnya Pelindungan Data Pribadi Di Era Digital”, Aptika Kominfo, Dalam <Https://Aptika.Kominfo.Go.Id/2021/10/Pentingnya-Pelindungan-Data-Pribadi-Di-Era-Digital/>,Diakses pada 24 September 2024.

Arundati Swastika Waranggani, “NCSI : Keamanan Siber Indonesia Peringkat 83 dari 160 Negara“, dalam <https://www.cloudcomputing.id/berita/ncsi-Cybersecurity-indonesia-peringkat-83>, diakses 5 November 2024.

AntaraNews, (2023), “BSSN ungkap serangan Keamanan Siber di 2022 turun dibanding 2021”, <https://www.antaranews.com/berita/3356178/bssn-ungkap-serangan-keamanan-siber-di-2022-turun-dibanding-2021> diakses pada 26 September 2024.

Andreas Daniel Panggabean, (2024), "Ini Data Statistik Penggunaan Media Sosial Masyarakat Indonesia Tahun 2024", <https://www.rri.co.id/iptek/721570/ini-data-statistik-penggunaan-media-sosial-masyarakat-indonesia-tahun-2024> diakses pada 10 Oktober 2024

AntaraNews, "Cyber Resiliency" Dinilai Kunci Hadapi Ancaman Siber Yang Kian Intens, 2023, <https://www.antaranews.com/berita/3737610/cyber-resiliency-dinilai-kunci-hadapi-ancaman-siber-yang-kian-intens>, [diakses pada 11/10/2024].

Admin Aptika, “Kebijakan Keamanan dan Pertahanan Siber, Aptika Kominfo, dalam <https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/>, diakses pada 23 September 2024.

Ben Wolford, “Does the GDPR apply to companies outside of the EU?”, pada laman GDPR, https://gdpr.eu/companies-outside-of-europe/, diakses pada 28 September 2024.

BPPTIK, “Jenis-Jenis Serangan Siber di Era Digital”, 2023. <https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital>, diakses pada 10 Oktober 2024.

CSIRT, (2024), “Sertifikasi Keamanan Siber Terbaik Untuk Meningkatkan Karier Anda di 2024”, <https://csirt.teknokrat.ac.id/sertifikasi-keamanan-siber-terbaik-untuk-meningkatkan-karier-anda-di-2024/> diakses pada 30 September 2024.

CNN Indonesia, “Buruk Keamanan Siber di Indonesia Akibat Ego Sektoral”, 2024, <https://www.cnnindonesia.com/nasional/20240627100303-20-1114729/buruk-keamanan-siber-di-indonesia-akibat-egosektoral>diakses pada 11 Oktober 2024.

CISA, “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years”,https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years, diakses pada 13 Oktober 2024.

Direktorat Jenderal Aplikasi Informatika (Kominfo), “Kebijakan Keamanan dan Pertahanan Siber”, <https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/>, diakses pada 30 September 2024.

EU Artificial Intelligence Act, “High-level summary of the AI Act”, 2024, <https://artificialintelligenceact.eu/high-level-summary/>, diakses pada 28 September 2024.

IBM, “Apa yang dimaksud dengan serangan siber?”, <https://www.ibm.com/id-id/topics/cyber-attack>, diakses pada 10 Oktober 2024.

Issha Harumma, Kompas.com, “Badan Siber dan Sandi Negara: Sejarah, Tugas, dan Fungsinya”, 2022, <https://nasional.kompas.com/read/2022/09/16/05050021/badan-siber-dan-sandi-negara--sejarah-tugas-dan-fungsinya> diakses pada 11 Oktober 2024.

Kebijakan Keamanan dan Pertahanan Siber, www.aptika.kominfo.go.id, Diakses pada 30 September 2024

Kedutaan Besar Republik Indonesia Brussel, A Policy Brief EU General Data Protection Regulation (GDPR), Research Series: Embassy of The Republic of Indonesia In Brussels, 2021, Nomor 6. <https://kemlu.go.id/download/L1NoYXJlZCUyMERvY3VtZW50cy9icnVzc2VsL3Jlc2VhcmNoJTIwc2VyaWVzL0dEUFIlMjAtJTIwdXBkYXRlZC5wZGY=>, diakses pada 28 September 2024.

Kominfo, (2020), “BSSN jadi lembaga utama Keamanan Siber ”, <https://www.kominfo.go.id/berita/sorotan-media/detail/bssn-jadi-lembaga-utama-keamanan-siber> diakses pada 10 Oktober 2024.

Mochamad Januar Rizki, hukumonline.com, “Perlu Memperjelas Kewenangan Penyidik BSSN Dalam Revisi UU ITE”, 2024, <https://www.hukumonline.com/berita/a/perlu-memperjelas-

kewenangan-penyidik-bssn-dalam-revisi-uu-ite-lt64e60d510425b/?page=1> diakses pada 11 Oktober 2024.

Mochamad Januar Rizki, (2021), "Keamanan dan Ketahanan Siber Perlu Payung Hukum Komprehensif", <https://www.hukumonline.com/berita/a/keamanan-dan-ketahanan-siber-perlu-payung-hukum-komprehensif-lt607fcfb349c85/> diakses pada 10 Oktober 2024

NIST, "Glossary: Cybersecurity", Computer Security Resource Center CSRC, diakses dari <https://csrc.nist.gov/glossary/term/Cybersecurity>, diakses pada 13 Oktober 2024.

NIST, "Glossary: Cyber Threat", Computer Security Resource Center CSRC, diakses dari <https://csrc.nist.gov/glossary/term/cyber_threat>, diakses pada 13 Oktober 2024.

OJK Indonesia, (2024), "Strategi Mencegah Serangan Siber", <https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/4021/strategi-mencegah-serangan-siber> diakses pada 10 Oktober 2024

Rachel Holmes, (2024), "What is a Cybersecurity Audit? vs. Cybersecurity Assessment", <https://www.bitsight.com/blog/Cybersecurity-audit-assessment-which-do-you-need>, diakses pada 30 September 2024

Tentang BSSN, <https://www.bssn.go.id/> , Diakses pada 26 September 2024

The Economic Impacts of Cyber Crime: How it Costs Us All, <www.citationcyber.com>, diakses pada 11 Oktober 2024.

The White House Office of the Press Secretary, (2013), "Presidential Policy Directive - Critical Infrastructure Security and Resilience", <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructuresecurity-and-resil> diakses pada 10 Oktober 2024.

Universitas Islam Indonsia, "Transformasi Digital dan Resiliensi Siber", dalam Seminar dan Workshop "Yogyakarta Cyber Resilience 2023" yang diselenggarakan di Universitas Islam Indonesia pada 19 Juni 2023, <https://www.uii.ac.id/transformasi-digital-dan-ketahanan-

siber/> diakses pada 10 oktober 2024.

The White House Office of the Press Secretary, (2013), "Presidential Policy Directive - Critical Infrastructure Security and Resilience", <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructuresecurity-and-resil> diakses pada 10 Oktober 2024.

Vangie Beal and Natalie Medleva, "Cyberspace", Techopedia, diakses dari <https://www.techopedia.com/definition/2493/cyberspace#:~:text=Cyberspace%20refers%20to%20the%20virtual,for%20communication%20and%20data%20exchange>., diakses pada 13 Oktober 2024.

White & Case, "Long awaited EU AI Act becomes law after publication in the EU's Official Journal", 2024, <https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal>, diakses pada 28 September 2024.

Willa Wahyuni, "8 Prinsip Hak Privasi dalam Aturan Pelindungan Data Pribadi",

Hukum Online.com, dalam <https://www.hukumonline.com/berita/a/8-prinsip-hak-privasi-dalam-aturan-pelindungan-data-pribadi-lt64a2dcec71359/>, diakses 24 September 2024.

Willa Wahyuni, "Melihat Prinsip dan Dasar Pemrosesan Data Pribadi", HukumOnline.com, dalam <https://www.hukumonline.com/berita/a/melihat-prinsip-dan-dasar-pemrosesan-data-pribadi-lt64a2df2ad70ce/>, diakses pada 24 September 2024 .

Wanda Ayu A., ui.ac.id, "Pentingnya Keamanan Siber Bagi Pertahanan dan Keamanan Nasional", 2017, <https://www.ui.ac.id/pentingnya-keamanan-siber-bagi-pertahanan-dan-keamanan-nasional/?> diakses pada 11 Oktober 2024.

https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html diakses terkahir pada 24 Februari 2025