Lampiran V
Nomor :
Tanggal:

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

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)*, misal-nya 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 Joko Widodo pada tanggal 13 April 2021 menandatangani Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Penerbitan Peraturan Presiden tersebut didasari oleh perlu dilakukannya penataan organisasi Badan Siber dan Sandi Negara dalam rangka mewujudkan keamanan, perlindungan, 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 Badan Siber dan Sandi Negara sehingga dapat dilakukan dengan lebih efektif dan efisien. Badan Siber dan Sandi Negara merupakan lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden. Organisasi dan Tata Kerja Badan Siber dan Sandi Negara 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

[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.

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. 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.

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

Pemanfaatan Ruang Siber sebagai pola baru bagi masyarakat dalam beraktivitas merupakan hak asasi yang wajib dilindungi negara. Hal tersebut tercantum dalam konstitusi, tepatnya pada 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 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 perlindungan masyarakat di Ruang Siber, khususnya terkait keamanan dan ketahanan siber dalam Undang-Undang masih belum komprehensif dan terintegrasi dengan baik.

Perangkat hukum yang tidak memadai dalam menindak lanjuti amar konstitusi membuat persoalan keamanan dan ketahanan siber tidak terselesaikan. Permasalahan utamanya adalah tindak kejahatan yang memanfaatkan Ruang Siber pun kian masif, sepanjang tahun 2020 telah tercatat 2.255 kasus dengan berbagai modus kejahatan bahkan pencurian data juga terus terjadi. 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 layanan 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.

Laporan dari Badan Siber dan Sandi Negara mencatat adanya peningkatan serangan siber pada sektor pemerintahan, keuangan, dan infrastruktur publik setiap tahunnya. Menurut data Badan Siber dan Sandi Negara pada tahun 2022, terdapat lebih dari 1,6 miliar anomali trafik atau serangan siber yang terdeteksi, yang menunjukkan adanya peningkatan ancaman siber yang signifikan dari tahun-tahun sebelumnya.[4] 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*, faktor utama yang harus dibenahi ialah pranata hukum (*Legal*) di tanah air untuk mengatasi permasalahan tersebut.

Oleh karena itu, 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 perlindungan 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

[4] 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

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. Badan Siber dan Sandi Negara telah mengajukan RUU KKS dalam Prolegnas Jangka Menengah Tahun 2025-2029 kepada Kemenkumham. Melalui kajian akademik substansi RUU KKS ini, Badan Siber dan Sandi Negara Bersama dengan UNPAD akan merumuskan konsep dan mengkaji substansi RUU KKS. Kajian ini diarahkan untuk dapat 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).

Jika dalam proses kajian ditemukan berbagai pengaturan terkait keamanan dan ketahanan siber dalam peraturan perundang-undangan lain maka konsep RUU KKS perlu menerapkan metode *omnibus law* (sesuai ketentuan dalam UU Nomor 13 Tahun 2022 tentang Perubahan

Kedua atas UU Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan) untuk dalam perancangannya. Sehingga RUU tersebut akan didesain untuk mengubah sekaligus norma hukum yang bersifat general dalam beberapa Undang-Undang yang mencantumkan pengaturan terkait keamanan dan ketahanan siber untuk mengintegrasikannya satu sama lain. Dengan demikian, Undang-Undang dapat tersusun lebih sistematis dengan materi muatan yang komprehensif terkait keamanan dan ketahanan siber untuk melindungi hak-hak masyarakat saat memanfaatkan ruang siber serta menjaga keamanan dan ketahanan siber Indonesia.

B. Identifikasi Masalah

1. Permasalahan apa yang dihadapi terkait pembentukan/penyusunan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber dan bagaimana permasalahan tersebut dapat diatasi?
2. Mengapa perlu adanya Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber sebagai dasar pemecahan masalah tersebut?
3. Apa yang menjadi pertimbangan landasan filosofis, sosiologis, dan yuridis pembentukan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber?
4. Bagaimana sasaran, arah dan jangkauan pengaturan serta ruang lingkup materi muatan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber?

C. Tujuan dan Kegunaan Kegiatan Penyusunan Naskah Akademik

Sesuai dengan ruang lingkup identifikasi masalah yang dikemukakan, tujuan penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber adalah sebagai berikut :

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

Adapun kegunaan penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber sebagai acuan atau referensi penyusunan dan pembahasan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber.

D. Metode

Penyusunan Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber 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 akan 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 adalah lingkungan nonfisik yang memungkinkan aktivitas interaksi digital antar manusia dan

[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.

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 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:

1. Kecerdasan Buatan *(Artificial Intelligence/AI)*: Digunakan untuk menciptakan pengalaman pengguna yang dipersonalisasi, seperti rekomendasi konten di platform digital atau *chatbot* otomatis.
2. Komputasi Awan *(Cloud Computing)*: Penyimpanan data yang terdesentralisasi dan diakses melalui internet, memungkinkan kolaborasi dan akses jarak jauh.
3. Keamanan Siber *(Cybersecurity)*: Sistem yang melindungi jaringan dan data dari ancaman siber, seperti serangan malware, peretasan, dan pencurian identitas.

4. *Internet of Things* (IoT): Koneksi antara perangkat fisik dengan internet yang memungkinkan pertukaran data secara *real-time*.

Infrastruktur Informasi Kritikal yang bergantung pada ruang siber meliputi sektor-sektor penting yang esensial bagi berjalannya kehidupan sehari-hari, seperti komunikasi, energi, layanan finansial, pemerintah, kesehatan, dan transportasi. Gangguan pada Infrastruktur Informasi Kritikal 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, 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 Infrastruktur Informasi Kritikal seperti jaringan listrik atau layanan kesehatan, 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 perlindungan 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, perlindungan, dan pemulihan sistem komunikasi elektronik serta komputer, yang mencakup perlindungan 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 perlindungan 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]

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

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

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 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

---

[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.

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 siber atau *cyber defense* merupakan suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara.[13] Selain itu, 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.[14] 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, 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.[15] 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*

---

[13] Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber

[14] 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.

[15] 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.

to adverse conditions, stresses, attacks, or compromises in systems that use or are enabled by cyber resources."[16]

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. 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.[17]

Ketahanan siber melihat keamanan siber sebagai mekanisme perlindungan suatu kerahasiaan, integritas, dan ketersediaan informasi dari serangan di dunia maya. Ini melibatkan fungsi-fungsi seperti menemukan, memperbaiki, dan mengurangi tingkat risiko terhadap ancaman siber dan serangan siber. Urgensi pertahanan siber ditujukan untuk mengantisipasi datangnya ancaman dan serangan siber yang terjadi dan menjelaskan posisi ketahanan saat ini, sehingga diperlukan kesiapan dan ketanggapan dalam menghadapi ancaman serta memiliki kemampuan untuk memulihkan akibat dampak serangan yang terjadi di ranah siber.

Oleh karena itu, prinsip-prinsip pertahanan siber yang efektif menjadi sangat penting dalam menjaga keamanan informasi dan sistem digital. Prinsip-prinsip ini mencakup beberapa elemen kunci, seperti model pengamanan informasi yang terstruktur dan terintegrasi sesuai dengan standar institusi berwenang, serta penjaminan kerahasiaan, integritas, dan ketersediaan informasi

---

[16] *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.

[17] 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].

sejak tahap perancangan. Selain itu, pertahanan siber membutuhkan kebijakan, kelembagaan, teknologi, infrastruktur pendukung, dan sumber daya manusia (SDM) berkompeten dengan integritas tinggi. Implementasi teknologi keamanan, seperti *firewall*, antivirus, dan enkripsi, kerja sama internasional, serta pengembangan hukum siber juga berperan penting.

Proses implementasi ini perlu dilakukan secara fisik dan logis yang terintegrasi, dengan memaksimalkan teknologi lokal untuk mewujudkan kemandirian, serta penetapan zona pengamanan berdasarkan klasifikasi SDM guna mencapai keamanan siber yang efektif dan komprehensif. Dalam memahami konsep ketahanan siber, penting juga untuk memahami berbagai aspek yang terlibat, diantaranya adalah pencegahan serangan siber melalui penerapan kebijakan keamanan yang kuat, pelatihan SDM bersertifikasi tentang praktik keamanan siber, dan pengujian kelemahan sistem. Selain itu juga, penting untuk memantau keamanan secara proaktif dalam mendeteksi serangan yang terjadi. Pada konteks hukum transformatif, ketahanan siber juga dapat dipahami sebagai bagian dari upaya untuk menciptakan sistem hukum yang adaptif terhadap perubahan teknologi.

Hukum transformatif berfokus pada bagaimana hukum dapat berperan dalam mengubah perilaku sosial dan menciptakan keadilan dalam konteks yang lebih luas.[18] 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

[18] 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.[19] 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".[20] 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

[19] 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.

[20] NIST, "Glossary: Cyber Threat", *Computer Security Resource Center CSRC,* diakses dari https://csrc.nist.gov/glossary/term/cyber_threat, diakses pada 13 Oktober 2024.

internal maupun eksternal yang mana mencakup aspek ideologi, politik, ekonomi, dan teknologi.[21]

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.[22] 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

[21] *Ibid*.
[22] Pasal 1 ayat (4) Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.

informasi.[23] 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*), 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.[24]

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.[25] 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 ini, seperti

---

[23] IBM, "Apa yang dimaksud dengan serangan siber?", https://www.ibm.com/id-id/topics/cyber-attack, diakses pada 10 Oktober 2024.

[24] 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.

[25] Ahmad M. Ramli dan Tasya Safiranita Ramli, *Hukum sebagai Infrastruktur Transformasi Indonesia*: *Regulasi dan Kebijakan Digital*, Op.Cit.

pencurian identitas, penipuan *online*, dan serangan terhadap Infrastruktur Informasi Kritikal. 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 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;

(1) *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;

(2) *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;

(3) *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;

(4) *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;

(5) *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;

(6) *Offense against Intellectual Property,* yakni kejahatan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet;

(7) *Carding,* yakni aksi mencuri nomor kartu-kartu penting milik orang lain dan dipergunakan untuk transaksi perdagangan di internet;

(8) *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.[26]

Beberapa insiden kejahatan siber di Indonesia menunjukkan pola yang berulang serta tantangan signifikan yang dihadapi oleh penegak hukum dalam menanganinya. Berikut adalah pola-polanya :[27]

[26] 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

[27] 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

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

Kasus C : Serangan Ransomware

Teknologi yang Digunakan	:	*Ransomware*
Tantangan	:	Koordinasi antarlembaga 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 berkelanjutan bagi penegak hukum 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.[28]

6. Relevansi dengan KKS

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 perlindungan 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*

[28] *Ibid,* hlm.82

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 perlindungan 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 konteks hukum dan regulasi, teori hukum transformatif yang diperkenalkan oleh Ahmad M. Ramli menekankan pentingnya peran hukum sebagai infrastruktur yang mendukung transformasi digital.[29] Hukum tidak lagi hanya berfungsi untuk menegakkan ketertiban, tetapi juga sebagai alat untuk menghadapi realitas digital yang dinamis. Dalam hal

[29] Ahmad M. Ramli dan Tasya Safiranita Ramli, *Hukum sebagai Infrastruktur Transformasi Indonesia*: *Regulasi dan Kebijakan Digital*, Op.Cit.

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. 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.[30] Secara keseluruhan, asas

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

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 kontrol penuh atas ruang siber atau Infrastruktur Informasi Kritikal digitalnya berisiko kehilangan kedaulatan terhadap ancaman yang datang dari dunia maya, yang kini menjadi salah satu bidang ancaman terbesar di era digital ini.

2. Pelindungan dan Kepastian Hukum

Asas perlindungan hukum adalah nilai dasar dari aturan hukum yang sifatnya memberikan perlindungan bagi objek hukum.[31] Asas perlindungan hukum merupakan nilai dasar yang menjadi pondasi dalam penyusunan aturan hukum. Asas ini berfungsi untuk memberikan jaminan perlindungan 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 perlindungan 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

[31] Suriaatmadja, Steffi Rifasa Tohir, and Ira Dewi Rachmadiani. "Perlindungan 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

beroperasi secara efektif dan aman, bahkan di tengah gangguan dan utamanya memberikan pelindungan. Hal ini menyebabkan pentingnya asas pelindungan dalam hal 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 perlindungan hukum juga berfungsi untuk mengatur hak dan kewajiban antara penyelenggara sistem siber dengan pengguna, serta memberikan perlindungan hukum terhadap pihak-pihak yang dirugikan akibat pelanggaran terhadap ketentuan keamanan siber. Dalam hal terjadi insiden atau pelanggaran, asas perlindungan hukum mengharuskan adanya mekanisme pemulihan yang cepat dan adil, agar para pihak yang terdampak dapat memperoleh ganti rugi atau perlindungan yang layak sesuai dengan hukum yang berlaku.

Secara keseluruhan, asas perlindungan hukum dalam Undang-Undang Keamanan dan Ketahanan Siber bertujuan untuk menciptakan keseimbangan antara kemajuan teknologi dan perlindungan hak-hak individu dan masyarakat. Dengan prinsip perlindungan 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 perlindungan hukum dan perlakuan yang adil di bawah hukum.[32] 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, maka 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

[32] 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

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 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.

3. Yurisdiksi Ekstrateritorial

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.[33] Dengan cara ini, pembuat

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

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.[34]

4. 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 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.

5. 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,

[34] *Ibid*

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.

6. 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-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.

Adapun prinsip keamanan dan ketahanan siber yaitu:

1. **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.[35] Keamanan siber juga mencakup perlindungan 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

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

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 penting bagi negara, serta melindungi sistem elektronik yang strategis atau kritikal bagi kelangsungan pelayanan publik atau kelangsungan negara sendiri.[36] 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,

[36] 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.

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 bertanggung jawab.[37] Sedangkan, PP PSTE memberikan pedoman tentang lima komponen sistem elektronik yang harus dipertahankan, yaitu perangkat keras, perangkat lunak, tenaga ahli, tata kelola, dan pengamanan.[38] Prinsip kedaulatan siber juga telah tercantum dalam Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber (selanjutnya

[37] Pasal 15 Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.
[38] Pasal 4 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

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.[39] 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.[40]

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 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

[39] BAB III angka 3.2, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.
[40] BAB II angka 2.4, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber

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.

2. 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.[41] Setiap penggunaan data pribadi harus sejalan dengan

[41] 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.

persetujuan pemilik data, serta tidak boleh digunakan untuk kepentingan lain tanpa izin lebih lanjut.[42]

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.*[43] 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.[44] 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 perlindungan 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 Framework*. *APEC Privacy Framework* menegaskan bahwa data pribadi harus diperoleh, disimpan, diproses, atau digunakan secara adil ("*fairly*") dan sah ("*lawfully*").[45] Untuk menilai apakah data pribadi tersebut diperoleh secara adil, biasanya dilihat dari metode yang digunakan dalam

---

[42] *Ibid*.

[43] 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.

[44] 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.

[45] BAB iii Bagian III Angka 18, *APEC Privacy Framework*.

pengumpulan, penyimpanan, pemrosesan, atau penggunaannya.[46] 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.[47] 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 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

[46] Sinta Dewi, "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya", *Jurnal Sosiohumaniora*, 19(3), Nov. 2017, hlm 209.

[47] 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 .

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.[48] 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.[49] 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.

3. Keamanan Nasional

Sebagai sebuah konsep/prinsip, keamanan telah mengalami evolusi pemaknaan yang luas dan berkembang mengikuti perkembangan dinamika perubahan zaman. Secara etimologis,

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

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."[50]

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.[51] 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 terhadap makna dan substansi yang terkandung didalamnya akan bervariasi tergantung kepada tata nilai, persepsi, dan kepentingan.[52] Kamnas dalam konteks Indonesia diartikan sebagai kondisi di mana sebuah

[50] 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)
[51] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
[52] Dewan Ketahanan Nasional, Sebuah Konsep dan Sistem Keamanan Bagi Bangsa Indonesia, Sekretariat Jenderal Dewan Ketahanan Nasional, 2010, hlm. 44.

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.[53]

Seiring dengan berkembangnya teknologi dan digitalisasi, ancaman terhadap keamanan nasional kini mencakup ancaman siber yang bisa mempengaruhi kestabilan politik, ekonomi, serta keamanan publik. 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 peretasan terhadap Infrastruktur Informasi Kritikal negara, sabotase siber, atau bahkan spionase, berpotensi untuk 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 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

[53] *Ibid.*

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:[54]

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 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

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

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:[55]

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 Badan Siber dan Sandi Negara yang tercantum dalam Pasal 2 dan 3 Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara dalam hal ini juga memiliki keterkaitan dengan prinsip keamanan nasional.

[55] *Ibid.*

Badan Siber dan Sandi Negara sebagai lembaga pemerintah yang bertanggung jawab dalam keamanan siber dan persandian memiliki tugas untuk melindungi ruang siber Indonesia. Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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*,[56] di mana *state-centered security* menitikberatkan pada perlindungan 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 perlindungan 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 Kamnas 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 perlindungan terhadap warga negara, melalui pengelolaan ancaman siber yang

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

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 kerjasama 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.

4. 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.[57] Akuntabilitas *(accountability)* yaitu berfungsinya seluruh komponen penggerak jalannya kegiatan perusahaan, sesuai dengan tugas dan kewenangannya masing-masing. Arti dari akuntabel itu sendiri

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

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.[58] 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 baik adalah sistem

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

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.*[59] 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

[59] 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.

siber, baik itu pemerintah, lembaga negara, maupun pihak swasta yang diberikan kewenangan, harus mampu mempertanggungjawabkan segala tindakannya, terutama yang berkaitan dengan penanganan ancaman siber, perlindungan data, dan pemulihan insiden siber. Setiap pihak yang terlibat ini wajib menjelaskan secara terbuka alasan di balik setiap kebijakan yang diambil, termasuk dalam aspek teknis, seperti kebijakan perlindungan Infrastruktur Informasi Kritikal, 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 perlindungan data yang diterapkan oleh pemerintah dan pihak swasta. Dalam RUU KKS, prinsip ini harus tercermin melalui kewajiban lembaga terkait untuk memberikan laporan publik mengenai insiden siber, 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, 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-langkah yang diambil oleh pemerintah dalam menghadapi kasus-kasus kejahatan siber, terutama yang berdampak langsung pada kepentingan publik.

5. 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. Teori hukum transformatif menunjukkan bahwa hukum tidak hanya sekedar memberikan kepastian dan ketertiban, tetapi juga berfungsi sebagai pendorong dan penuntun dalam transformasi Indonesia menuju era industri 5.0.[60] Teori transformatif menekankan pentingnya pendekatan dan analisis risiko dalam pembentukan hukum yang dalam hal ini mencakup perubahan kelembagaan, penguatan keadilan, pengembangan pola pikir dan perilaku masyarakat, serta pengaturan perilaku industri demi keberlanjutan manusia dan ekosistemnya.

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

[60] Ahmad M. Ramli dan Tasya Safiranita Ramli, *Hukum sebagai Infrastruktur Transformasi Indonesia*: *Regulasi dan Kebijakan Digital*, Op.Cit.

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 perlindungan 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.[61]

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

6. 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.

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

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 kelembagaan pembentuk hukum itu sendiri, setidaknya dalam hal menjaga kualitas substansi hukum dan efektivitas serta efisiensi pembentukan hukum itu sendiri.[62] 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

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

memerlukan respons yang cepat dengan dibentuknya regulasi yang progresif dan pragmatis agar dapat bertransformasi bukannya terdistorsi. Penerapan prinsip ini dalam Keamanan dan Ketahanan siber dapat memprioritaskan proses pembentukan hukum dan model hukum terintegrasi dalam bentuk *Omnibus Law*.

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 Badan Siber dan Sandi Negara melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (kini telah dicabut dengan Peraturan Presiden Nomor 28 Tahun 2021).[63] Berdasarkan ketentuan Pasal 2 Peraturan Presiden Nomor 28 Tahun 2021, Badan Siber dan Sandi Negara mempunyai tugas untuk melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi negara. Badan Siber dan Sandi Negara 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.[64]

Dalam praktiknya, Badan Siber dan Sandi Negara telah menjalankan beberapa inisiatif penting. Salah satunya adalah pengembangan dan implementasi Pusat Operasi Keamanan Siber

[63] 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.
[64] Pasal 3 Peraturan Presiden Nomor 28 Tahun 2021

Nasional *(National Cyber Security Operations Center* atau CSOC*)*. CSOC berfungsi sebagai pusat koordinasi untuk pemantauan, deteksi, dan respons terhadap ancaman siber di tingkat nasional. Melalui CSOC, Badan Siber dan Sandi Negara dapat melakukan analisis dan berbagi informasi mengenai ancaman siber secara *real-time* dengan berbagai pemangku kepentingan.

Selain itu, Badan Siber dan Sandi Negara 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. Badan Siber dan Sandi Negara 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 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, PP PSTE memberikan panduan lebih spesifik terkait keamanan sistem elektronik. Peraturan ini mewajibkan penyelenggara sistem elektronik untuk menerapkan tata kelola, manajemen risiko, dan perlindungan 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, seperti sektor energi, transportasi, keuangan, dan telekomunikasi.

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 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 antarlembaga. Meskipun Badan Siber dan Sandi Negara menjadi *focal point* untuk keamanan siber nasional, masih ada tumpang tindih kewenangan dengan lembaga lain seperti Kementerian Komunikasi dan Digital, Kepolisian, dan Badan Intelijen Negara. 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. Namun, strategi tersebut harus diiringi dengan peningkatan kapasitas sumber daya manusia, peningkatan anggaran untuk keamanan siber, serta pengembangan teknologi yang lebih mutakhir. Selanjutnya, perlu ada pengawasan dan evaluasi secara berkala terhadap pelaksanaan strategi ini 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 tentang keamanan dan ketahanan siber, mengingat hukum positif yang ada belum menjangkau hal ini. Hukum positif dalam arti *cyberlaw* Indonesia yang telah dibahas lebih berfokus pada tindakan reaktif hukum pasca insiden. Perkembangan internasional 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 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, perlindungan, dan kedaulatan siber nasional dipegang wewenangnya oleh Badan Siber dan Sandi Negara. Badan Siber dan Sandi Negara 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.[65] Kondisi dunia siber yang semakin menjangkau manusia di dunia membuat meningkatnya ancaman terhadap dunia siber saat ini. Indonesia, sebagai negara berdaulat tergolong kedalam negara dengan insiden siber terbanyak di dunia.

[65] 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.

Pada tahun 2023, Indonesia menduduki peringkat ke-8 (delapan) di dunia dengan jumlah kasus kebocoran data tertinggi dan negara dengan pembobolan data terbanyak di Asia Tenggara.[66] Berdasarkan data dari index, pertahanan siber Indonesia juga tergolong lemah karena berada di kisaran 3,46 (tiga koma empat puluh enam) poin, jauh dari indeks rata-rata global di angka 6,19 (enam koma sembilan belas) poin.[67] Berdasarkan data dari *National Cyber Security Index* (NCSI) pada tahun 2023 silam, Indonesia berada pada peringkat ke-49 (empat puluh sembilan) keamanan cyber dari 176 (seratus tujuh puluh enam) negara.[68] Pada tahun 2024 ini pun, 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

---

[66] 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.

[67] *Ibid*.

[68] National Cyber Security Index Report 2023.

pemerintah dalam mencegah ancaman ini. Serangan siber seringkali diawali oleh kelalaian pemerintah yang memiliki akses masuk ke sistem data atau jaringan.[69]

Selain dari masalah kelalaian dan perhatian pemerintah, masalah lain dari rentannya keamanan dan ketahanan siber di Indonesia adalah masih belum baiknya kelemahan dalam regulasi terkait tata kelola sistem siber oleh pemerintah. Badan Siber dan Sandi Negara selaku badan pemerintah di bawah Presiden yang salah satu tugasnya adalah menjaga keamanan siber masih memiliki tumpang tindih kewenangan dalam hal tata kelola keamanan siber dengan lembaga lain. Dalam UU ITE, Undang-Undang Pelindungan Data Pribadi (UU PDP), dan Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Kritikal menyebut bahwa keamanan informasi juga berada dalam lingkup kewenangan Kementerian Komunikasi dan Digital. Hal ini menandakan bahwa terjadinya tumpang tindih kewenangan antara Badan Siber dan Sandi Negara dengan Kementerian Komunikasi dan Digital untuk mengelola keamanan siber.

Hal ini pada akhirnya mengakibatkan upaya mitigasi, pengawasan, pengelolaan, dan penanggulangan insiden siber menjadi tidak optimal dan memiliki banyak hambatan. Peran Badan Siber dan Sandi Negara untuk menjamin keamanan siber tidak bisa menjadi maksimal karena Badan Siber dan Sandi Negara tidak memiliki kewenangan dalam hal penindakan, termasuk yang berkaitan dengan upaya penyelidikan dan penanganan serangan siber. Kewenangan yang tidak jelas antar lembaga menyebabkan menjadi sulitnya dilakukan melakukan manajemen kelola siber. Dalam rapat antara Badan Siber dan Sandi Negara dengan Komisi

[69] CNN Indonesia, *Op.Cit*.

I DPR pada 22 Agustus 2023, Badan Siber dan Sandi Negara mengatakan bahwa seringkali mampu mendeteksi kasus kebocoran data, dan memberikan notifikasi kepada PSE terkait untuk menindaklanjutinya.[70]

Akan tetapi, karena tidak ada kewenangan Badan Siber dan Sandi Negara dalam penyidikan dan penindakan terhadap bidang teknologi informasi dan transaksi elektronik yang mengakibatkan adanya serangan siber, maka membuat upaya pencegahan ancaman siber dari notifikasi yang dikirimkan tidak bisa berkelanjutan dan berjalan maksimal. Kewenangan untuk melakukan penyidikan dan penindakan yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang disahkan pada awal 2024 hanya memberikan kewenangan penyidikan kepada Kepolisian dan Pejabat Pegawai Negeri Sipil (PPNS) di lingkup kementerian.[71] Hal ini menyebabkan Badan Siber dan Sandi Negara tidak memiliki kewenangan untuk melakukan penyidikan tersebut.

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.

[70] 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.

[71] Pasal 43 ayat (1) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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 Infrastruktur Informasi Kritikal adalah 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, termasuk Infrastruktur Informasi Kritikal. Hal ini disebabkan karena belum adanya dasar regulasi yang memberi wewenang kepada Badan Siber dan Sandi Negara untuk melaksanakan tugas

dan fungsi tersebut dengan dasar hukum yang detail. Membiarkan keadaan ini berlarut-larut akan berdampak pada kerentanan sistem keamanan dan ketahanan siber nasional. Oleh karena itu, RUU KKS perlu segera dibentuk dan diundangkan untuk menjawab tantangan dan persoalan dimaksud 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.[72]

Hal ini terlihat dari banyaknya insiden kebocoran data, termasuk kasus peretasan data BPJS Kesehatan dan berbagai kementerian, yang menimbulkan kerugian besar bagi masyarakat. Rendahnya kesadaran masyarakat juga diperparah oleh lemahnya regulasi dan penegakan hukum yang ada. Meskipun telah ada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, namun implementasinya masih terhambat dengan ketiadaan aturan yang spesifik mengenai keamanan dan ketahanan siber.

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

Selain itu, Indonesia juga menghadapi tantangan dari sisi infrastruktur dan kapabilitas sumber daya manusia. Berdasarkan data dari *National Cyber Security Index* (NCSI) pada tahun 2023 silam, Indonesia berada pada peringkat ke-49 keamanan cyber dari 176 negara.[73] Indonesia juga menempati peringkat teratas dalam kasus pembobolan data se-ASEAN.[74] 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 perlindungan dan penggunaan data warganya.[75]

Melihat berbagai permasalahan di masyarakat yang telah diuraikan, solusi yang komprehensif untuk memperkuat ketahanan siber di Indonesia menjadi hal yang mendesak. Salah satu pendekatan yang bisa diambil adalah 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. RUU ini diharapkan tidak hanya mencakup aturan teknis tentang perlindungan data dan penanggulangan serangan siber, tetapi juga memperkuat kolaborasi antara pemerintah, sektor swasta, dan

[73] National Cyber Security Index Report 2023.
[74] 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.
[75] M. Prakoso Aji, *"Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)*," Politica, Vol. 13, Nomor 2 (November 2022).

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 pelatihan keterampilan dasar dalam mengenali serta menghindari ancaman siber, seperti *phishing* dan *malware*, akan sangat membantu dalam meminimalisasi potensi serangan siber. Dengan pendekatan multi-dimensi 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:[76]

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

[76] Article 1 UN Convention Against Cybercrime

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.[77] Isi dari konvensi ini mencakup beberapa aspek penting seperti

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. Ini 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

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

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.[78] 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 :

- Persyaratan keamanan siber sejak perencanaan, desain, pengembangan dan pemeliharaan produk.
- 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.
- Produsen dan pengecer wajib memprioritaskan keamanan siber sehingga pelanggan dan bisnis bisa membuat pilihan yang tepat.
- Penerapan perlakuan khusus, contohnya pada perangkat lunak atau layanan *open source* yang sudah tercakup oleh regulasi yang ada.
- EU CRA mengancam setiap pelanggaran atau ketidakpatuhan dengan sanksi denda dan pinalti yang berat, dimana setiap

[78] 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]

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 perlindungan terhadap Infrastruktur Informasi Kritikal dan data sensitif. Kebijakan keamanan siber di Indonesia, misalnya, mengaitkan keamanan siber dengan pertahanan 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 positif yang secara khusus mengatur fenomena 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 PTSE. Namun demikian, RUU KKS ini belum mampu

mencakup penanganan praktik penyadapan (intersepsi) dalam tata kelola dunia maya atau perdagangan elektronik *(e-commerce)* serta belum mampu menjangkau seluruh aspek keamanan siber yang begitu luas.[79]

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 Permenhan 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.[80]

Pada tahun 2017, Badan Siber dan Sandi Negara 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

[79] Aulianisa, Sarah Safira, and 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), hlm. 32-33
[80] *Ibid,* hlm. 33

keamanan siber secara efektif dan efisien dengan mendayagunakan, mengembangkan, meningkatkan, dan mengkonsolidasikan 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.[81]

Selanjutnya, TNI di bawah Kementerian Pertahanan 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 AD dalam rangka mendukung tugas pokok TNI AD. Satsiber yang ada saat ini telah menjadi satuan kerja yang memiliki fungsi sebagai pengawasan dan pertahanan dalam menghadapi serangan siber dan kejahatan serta memberikan respon cepat dan tanggap darurat. melapor kepada

[81] *ibid*

pimpinan TNI AD dalam rangka pengamanan institusi TNI AD dari ancaman kejahatan dan serangan siber.

Ada empat fungsi yang dimiliki Satsiber TNI, yaitu pendeteksian, perlindungan, pemulihan dan memastikan sistem 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.[82]

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. [83]

Menanggapi serangan siber tersebut, Kementerian Komunikasi dan Digital (dahulu Kementerian Komunikasi dan

[82] *Ibid,* hlm. 33-34
[83] *Ibid,* hlm.34

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, serta mendukung pelaksanaan koordinasi dengan pihak terkait baik di dalam maupun di luar negeri dalam upaya pencegahan, deteksi, peringatan dini dan mitigasi insiden pada Infrastruktur Informasi Kritikal. ID-SIRTII/CC telah berupaya melakukan pemantauan trafik anomali internet nasional sejak Januari sampai dengan Desember 2018, sebanyak 232.447.974 serangan siber telah ditemukan pada jaringan Indonesia.[84]

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.[85] Faktor-faktor tersebut yang

[84] *Ibid*

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

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 ketahanan siber dari produk dan layanan yang dijual di pasar Uni Eropa.[86] 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.[87]

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

[86] 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.
[87] Article 5 EU CRA.

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 lunak yang bersifat gratis dan sumber terbuka tidak termasuk dalam cakupan Proposal, agar tidak menghambat inovasi penelitian.

Selain itu, terdapat pengecualian lainnya, bahwa CRA tidak akan berlaku untuk produk dengan elemen digital yang sudah dalam ruang lingkup beberapa peraturan lain, seperti peraturan EU tentang Perangkat Medis, Peraturan EU tentang persetujuan tipe otomotif, dan peraturan EU untuk penerbangan sipil.[88] 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.[89] 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 (PDE) menjadi kategori PDE default, dan PDE kategori

[88] Article 2 (3) CRA

[89] 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.

Kritikal. Kategori Kritikal kemudian dibagi menjadi dua sub kategori, Kritikal kelas I dan Kritikal kelas II.[90]

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 produk telah mematuhi standar tersebut.[91] Selanjutnya, produsen dan distributor diwajibkan untuk memprioritaskan keamanan siber, guna memberikan pelindungan yang maksimal kepada penggunanya.[92] Selanjutnya, apabila terjadi insiden terhadap produk dengan elemen digital, maka produsen, distributor, maupun konsumen ataupun pihak lain dapat melaporkan kerentanan ataupun kerugian yang terjadi akibat ancaman siber kepada Tim Respons Insiden Keamanan Komputer (CSIRT) yang

[90] Ahmad M Ramli, "EU CRA: UU Baru Uni Eropa Menghadapi Peretasan Siber Global", Op.Cit.
[91] Article 8 & 27 EU CRA
[92] Article 13 EU CRA.

ditunjuk sebagai koordinator ataupun Badan Keamanan Siber Uni Eropa (ENISA).[93]

Dari segi kelembagaan, EU CRA mengamanahkan komisi yang dapat mengatur kepatuhan dan segala hal yang berkaitan terhadap EU CRA. Komisi tersebut merupakan ENISA. 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.[94] Dalam praktiknya, untuk mengawasi terkait pelanggaran, kepatuhan, dan menindaklanjuti insiden terkait kepatuhan terhadap EU CRA dilakukan oleh CSIRT.[95] 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 kepada ENISA. Namun, sebagai patokannya, denda dapat ditetapkan berkisar antara 5-15 juta Euro, atau 1 hingga 2,5 persen dari omzet tahunan di seluruh dunia, tergantung pada keseriusan pelanggaran. Mana yang lebih tinggi, maka itulah yang akan dikenakan kepada pelanggar.[96] Akan tetapi, terdapat beberapa

[93] Article 15 EU CRA.
[94] Article 14 EU CRA.
[95] Article 14 EU CRA.
[96] Article 64 EU CRA.

pengecualian terhadap pelanggaran tersebut, seperti misalnya pelanggar tergolong ke dalam kategori Usaha Kecil, Mikro, dan Menengah, dan ketentuan lainnya.[97]

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.[98] Dalam menghadapi dan menyertai kemajuan teknologi AI, Uni Eropa menjadi inisiator dari Undang-Undang Kecerdasan Buatan yang dikenal dengan nama *European Artificial Intelligence Ac*t (**"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.[99] EU AI Act mulai berlaku di seluruh 27 Negara Anggota UE pada tanggal 1 Agustus 2024, dan penegakan sebagian besar ketentuannya akan dimulai pada tanggal 2 Agustus 2026.

---

[97] Article 64 EU CRA.

[98] 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.

[99] 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.

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.[100] 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.[101] 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.[102] 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 juta atau 7% (tujuh persen) dari omzet tahunan di seluruh dunia (Pasal 99 (3) EU AI Act).[103] Sanksi untuk pelanggaran ketentuan tertentu lainnya dikenakan denda maksimum EUR 15 juta atau 3 persen dari omzet tahunan di seluruh dunia, mana

[100] 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.
[101] *Ibid.*
[102] EU Artificial Intelligence Act, "High-level summary of the AI Act", 2024, https://artificialintelligenceact.eu/high-level-summary/, diakses pada 28 September 2024.
[103] Pasal 99 (3) European Artificial Intelligence Act.

yang lebih tinggi.[104] 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 persen dari omzet tahunan di seluruh dunia, mana yang lebih tinggi (Pasal 99(5) EU AI Act).[105] 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).[106]

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.[107] 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.[108]

Tidak hanya itu, peran dari dewan penasihat juga diperlukan dalam mencapai keamanan siber pada sistem AI. Pasal 66 EU AI Act menjelaskan tanggung jawab dari Dewan penasihat, dimana salah satunya

[104] Pasal 99 (4) European Artificial Intelligence Act.
[105] Pasal 99 (5) European Artificial Intelligence Act.
[106] Pasal 99 (6) European Artificial Intelligence Act.
[107] Ahmad M. Ramli, *Op.Cit*. (Note 10).
[108] Pasal 55 European Artificial Intelligence Act.

adalah bekerja sama dengan lembaga-lembaga, badan-badan, kantor dan agen persatuan, kelompok ahli dan jaringan serikat yang relevan khususnya dibidang keamanan produk dan keamanan siber untuk memberikan pelindungan data dan hak-hak dasar konsumen. Forum ini wajib dibentuk untuk memberikan keahlian teknis dan memberikan nasihat kepada Dewan dan Komisi, dan untuk berkontribusi terhadap tugas-tugas mereka berdasarkan Peraturan ini. Dalam pasal ini juga dijelaskan bahwa Badan Hak Asasi Manusia, Badan Keamanan Siber Uni Eropa (ENISA)**,** Komite Standardisasi Eropa (CEN), Komite Standarisasi Elektronik Eropa (CENELEC), dan Institut Standar Telekomunikasi Eropa (ETSI) akan menjadi anggota tetap forum penasehat. Forum penasehat ini harus menyusun peraturan prosedur dan menyiapkan pendapat, rekomendasi dan masukan tertulis atas permintaan Dewan atau Komisi.

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 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

negara anggota dan negara yang masuk dalam Europe Economic Area (EEA).[109] 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.[110] GDPR memberikan tuntutan bagi perusahaan agar lebih akuntabel, transparan, bertanggung jawab pada data pribadi pengguna dan meningkatkan cybersecurity-nya. GDPR memiliki efek ekstra teritorial 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.[111]

Pemrosesan data pribadi menurut GDPR adalah termasuk kegiatan pengumpulan, perekaman, pengorganisasian, penataan, penyimpanan, pengambilan, dan penggunaan data pribadi residen UE.[112] GDPR disebut sebagai hukum keamanan data pribadi paling ketat dan paling kuat di dunia karena keketatan, sanksi dan skala penerapannya. GDPR berlaku tidak hanya bagi perusahaan, organisasi, atau

---

[109] 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.

[110] *Ibid.*

[111] 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.

[112] Pasal 4 European Union General Data Protection Regulation (GDPR).

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 hidup yang dapat secara langsung atau tidak langsung mengidentifikasi individu tersebut.[113] 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*.[114] Pelaksanaan GDPR sendiri dikawal ketat oleh suatu badan yang disebut sebagai European Data Protection Board (EDPB), yang sengaja dibentuk khusus untuk pengawal pelaksanaan GDPR di tingkat Uni Eropa. Sementara itu, pengawasan di masing-masing negara dikawal oleh *Data Protection Authorities* atau *Supervisory Authorities*. EDPB bekerja sama dengan DPA dalam mengawal penerapan GDPR. DPA di

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

masing-masing negara memiliki peran dan tugasnya masing-masing yang antara lain:

a) untuk melakukan monitoring terhadap penerapan GDPR;
b) menginformasikan dan meningkatkan kesadaran publik tentang hak dan resiko dalam kaitannya dengan pelindungan data pribadi di bawah GDPR;
c) Meningkatkan kesadaran *data controller* dan *data processor* tentang kewajiban mereka dalam menangani data pribadi milik orang di bawah GDPR;
d) Bekerja sama dengan sesama badan otoritas pengawas GDPR di masing-masing negara UE dan *European Data Protection Board*;
e) Menangani pengaduan terhadap laporan pelanggaran GDPR dan melakukan investigasi atas pengaduan tersebut;
f) Memiliki kewenangan untuk melakukan investigasi, tindakan korektif dan kepenasehatan (Pasal 58);[115]
g) Memiliki kewenangan untuk menjatuhkan denda pada Pengendali dan Prosesor Data Pribadi (Pasal 83).[116]

Berkaitan dengan sanksi, GDPR menyatakan secara eksplisit bahwa sejumlah pelanggaran memiliki tingkat pelanggaran yang lebih parah dari lainnya dan

[115] Article 58 European Union General Data Protection Regulation (GDPR).
[116] Article 83 European Union General Data Protection Regulation (GDPR).

hal itu membuat denda pun berbeda-beda. Ada dua tingkat denda atas pelanggaran GDPR yakni pelanggaran yang 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.[117] Termasuk pelanggaran pada pasal-pasal yang mengatur hal-hal di bawah ini:[118]

a) Mengatur tentang Pengendali dan Prosesor Data Pribadi, Pengendali dan Prosesor Data Pribadi harus patuh terhadap aturan yang mengatur pelindungan data pribadi dalam melakukan pemrosesan data pribadi. Sebagai sebuah organisasi yang melakukan pengumpulan data pribadi pengguna dan mengolahnya, mereka harus memahami Pasal 8, Pasal 11, Pasal 25 sampai dengan Pasal 39, Pasal 42, dan Pasal 43.
b) Mengatur tentang *certification bodies*, Badan terakreditasi yang bertanggung jawab atas sertifikasi terhadap organisasi harus melakukan tindakan evaluasi dan penilaian kerja tanpa bias melalui proses yang transparan. Lihat Pasal 42 dan Pasal 43.
c) Mengatur tentang *monitoring bodies*, Badan yang dibuat untuk memiliki level keahlian

[117] Article 83 Paragraph (4) European Union General Data Protection Regulation (GDPR).
[118] Kedutaan Besar Republik Indonesia Brussel, *Op.Cit*. (Note 28)

yang sesuai harus mendemonstrasikan independensi dan mengikuti prosedur yang ada dalam menangani komplain atau pelanggaran yang dilaporkan secara transparan dan netral.

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.[119] Denda serius diberikan untuk pelanggaran hal-hal di bawah ini:[120]

a) Prinsip dasar pemrosesan data pribadi (Pasal 5, Pasal 6 dan Pasal 9). Sesuai dengan aturan GDPR, pemrosesan data pribadi harus dilakukan sesuai hukum, adil dan transparan. Data Pribadi dikumpulkan untuk tujuan yang jelas, dijaga akurasinya dan diproses sesuai dengan tata cara yang diatur dalam GDPR untuk memastikan keamanannya. Organisasi atau perusahaan hanya boleh memproses data pribadi jika mereka memenuhi 6 dasar hukum dalam pemprosesan data seperti tertua pada GDPR Pasal 6.

[119] Article 83 paragraph (4) European Union General Data Protection Regulation.
[120] Kedutaan Besar Republik Indonesia Brussel, *Op.Cit*. (Note 28)

b) Status persetujuan atau *the conditions for consent* (Pasal 7) saat organisasi atau perusahaan melakukan pemrosesan data dengan dasar telah mendapat persetujuan atau *consent* dari pemilik data, maka organisasi tersebut perlu memiliki dokumentasi untuk membuktikannya.

c) Hak Subjek Data (Pasal 12 sampai dengan Pasal 22) Individu pemilik data pribadi memiliki hak untuk tahu data apa dari dirinya yang dikumpulkan oleh organisasi atau perusahaan dan apa yang mereka lakukan terhadap datanya. Setiap individu juga memiliki hak untuk mendapatkan *copy* dari data yang telah dikumpulkan, untuk mengoreksi datanya, dan di beberapa kasus juga berhak agar datanya bisa dihapus.

d) Transfer Data kepada Organisasi Internasional atau Penerima di negara Ketiga (Pasal 44 sampai dengan Pasal 49) Sebelum organisasi atau pihak *data controller* mentransfer data pribadi siapapun ke negara ketiga atau organisasi internasional lainnya, *European Commission* harus menentukan bahwa negara ketiga atau organisasi internasional yang menjadi pihak ketiga itu memiliki tingkat pelindungan data pribadi yang memadai. Proses transfer sendiri harus dilindungi hukum.

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 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 siber.[121] Selain itu, Undang-Undang ini dilahirkan untuk mencapai tujuan memajukan inisiatif keamanan siber secara komprehensif dan efektif, dalam hubungannya dengan *Basic Act on the Formation of an Advanced Information and telecommunications Network Society* (Act Nomor 144 of 2000) dengan cara seperti membentuk Markas Besar Strategis Keamanan Siber (*Cybersecurity Strategic Headquarters*).[122]

Istilah Keamanan Siber atau "*cyber security*" yang digunakan dalam Undang-Undang ini

[121] Article 1 *The Basic Act on Cybersecurity*
[122] *Ibid.*

mendefinisikan bahwa langkah-langkah yang diperlukan telah 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.[123] 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.[124] 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.[125]

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.[126]

[123] Article 2 *The Basic Act on Cybersecurity*
[124] Article 3 (1) *The Basic Act on Cybersecurity*
[125] Article 3 (2) *The Basic Act on Cybersecurity*
[126] Article 3 (3) *The Basic Act on Cybersecurity*.

Selanjutnya, Jepang melalui Undang-Undang ini juga menegaskan bahwa kebijakan siber harus dimajukan melalui kerja sama internasional dengan prinsip bagi Jepang untuk 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.[127] Namun, kebijakan tersebut tetap harus kembali untuk mempertimbangkan prinsip-prinsip dasar dari Undang-Undang Dasar tentang Pembentukan Masyarakat Jaringan Informasi dan Telekomunikasi yang Maju[128], dan pengembangannya tidak dengan melanggar hak-hak masyarakat.[129]

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[130], tanggung jawab pemerintah daerah untuk merumuskan dan menerapkan kebijakan keamanan siber secara mandiri dengan mempertimbangkan peran yang tepat dengan pemerintah nasional[131], tanggung jawab penyedia

[127] Article 3 (4) *The Basic Act on Cybersecurity*
[128] Article 3 (5) *The Basic Act on Cybersecurity*
[129] Article 3 (6) *The Basic Act on Cybersecurity*
[130] Article 4 *The Basic Act on Cybersecurity*
[131] Article 5 *The Basic Act on Cybersecurity*

infrastruktur sosial untuk memperdalam minat dan pemahamannya terhadap pentingnya keamanan siber[132], tanggung jawab badan usaha terkait dunia maya dan badan usaha lainnya yang bergerak di bidang siber untuk menyelenggarakan keamanan siber secara aktif[133], 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[134], dan tanggung jawab dan upaya masyarakat untuk memperdalam minat dan pemahaman terhadap pentingnya keamanan siber.[135]

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.[136] Selain itu juga, 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 badan usaha yang terkait dengan dunia maya, untuk

[132] Article 6 *The Basic Act on Cybersecurity*
[133] Article 7 *The Basic Act on Cybersecurity*
[134] Article 8 *The Basic Act on Cybersecurity*
[135] Article 9 *The Basic Act on Cybersecurity*
[136] Article 14 *The Basic Act on Cybersecurity*

bekerja sama menyusun kebijakan keamanan siber secara terpadu.[137]

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.[138] 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.[139] 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 ini. Pasal 31 ayat (2) ini juga mengatur ketentuan bahwasannya, Pegawai atau pegawai suatu perseroan yang telah diserahi tugas sesuai dengan ayat sebelumnya atau orang yang pernah menduduki jabatan tersebut dilarang membocorkan atau menyalahgunakan informasi rahasia yang diperoleh sehubungan dengan tugas berdasarkan pengabaian tersebut, tanpa alasan yang dapat dibenarkan.[140] Untuk menjamin hal tersebut, Undang-Undang ini mengatur mengenai ketentuan pidana yakni pada BAB V, Pasal 38 yang menjelaskan bahwa Barang Siapa melanggar

[137] Article 16 *The Basic Act on Cybersecurity*
[138] Article 17 *The Basic Act on Cybersecurity*
[139] Article 17 (4) *The Basic Act on Cybersecurity*
[140] Article 31 (2) *The Basic Act on Cybersecurity*

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.[141]

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

[141] Article 38 The Basic Act on Cybersecurity

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.[142] Komisi ini menerima banding dari setiap orang atau organisasi yang hendak mengajukan banding terhadap putusan yang 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

[142] Section 33 Singapore Personal Data Protection Act 2012

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 :[143]

1. Memperkuat perlindungan Infrastruktur Informasi Kritikal nasional Singapura terhadap serangan siber;
2. Memberikan otorisasi terhadap the *Cyber Security Agency of Singapore* (CSA) atau Badan Keamanan Siber Singapura untuk mencegah dan merespons ancaman serta insiden keamanan siber ;
3. Membangun *framework* untuk berbagi informasi siber; dan
4. 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.[144] *Cybersecurity Act* mengatur pemberian lisensi terhadap penyedia jasa pengamanan siber. Hal ini dilakukan untuk menciptakan jaminan terhadap keamanan dan

[143] Singapore Cybersecurity Act.
[144] First Schedule Essential Services Singapore Cybersecurity Act.

kenyamanan penggunanya, serta meningkatkan kualitas dan standar penyedia jasa tersebut di samping mengevaluasi kinerja pemberi jasa tersebut dari waktu ke waktu.[145] *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.[146]

Secara garis besar, Undang-Undang ini menitikberatkan pentingnya pengaturan standar mengenai keamanan siber, pertukaran informasi, dan tata kelola insiden keamanan siber.[147] 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.[148] Selanjutnya, CSA juga dapat memerintahkan audit kepatuhan keamanan siber kepada sektor Infrastruktur Informasi Kritikal. CSA juga dapat

[145] Kevin Iskandar Putra, "Belajar Dari Tata Kelola Keamanan Siber Singapura", Center For Digital Society, Case Study Series 44, Januari 2019, hlm 3.
[146] Singapore Cybersecurity Act.
[147] Kevin Iskandar Putra, Op.Cit., hlm. 4.
[148] Article 3 - 9 Singapore Cybersecurity Act.

memerintahkan sektor Infrastruktur Informasi Kritikal tersebut untuk memberikan informasi yang relevan tentang keamanan siber mereka.[149]

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.[150] Apabila terdapat kasus di luar negeri yang menyebabkan atau memberikan risiko tinggi terhadap ancaman siber Singapura, maka Kepolisian 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

[149] Article 22 Singapore Cybersecurity Act.
[150] Article 27 Singapore Cybersecurity Act.

menanggapi insiden keamanan siber.[151] 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.[152]

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 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.[153]

[151] Cybersecurity Act.
[152] Kevin Iskandar Putra, Op.CIt, hlm. 6.
[153] *Article 51, Personal Data Protection Act* 2012

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.[154] Hal ini menyebabkan kekurangan bahan bakar dan membutuhkan pembayaran tebusan sebesar $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

[154]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.

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.[155] 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.[156]

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 pembaruan untuk persyaratan dan bahasa tersebut

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

kepada Dewan FAR dan lembaga terkait lainnya.[157] 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.[158]

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.[159] 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

[157] *Article 2 (b) Executive Order on Improving the Nation's Cybersecurity United States 14028*
[158] *Article 2(c) Executive Order on Improving the Nation's Cybersecurity United States 14028*
[159] *Article 2 Executive Order on Improving the Nation's Cybersecurity United States 14028*

Nasional (APNSA).[160] Dengan penggunaan teknologi tersebut, diharapkan dapat memungkinkan Pemerintah Federal untuk 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*.[161]

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.[162] 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,

[160] *Article 3* Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[161] *Article 3 Executive Order on Improving the Nation's Cybersecurity United States 14028*
[162] Bagian 4 Executive Order *on Improving the Nation's Cybersecurity United States 14028*

mekanisme pengecekannya, persyaratan, dan ketentuan lainnya guna memastikan bahwa vendor tersebut telah tepat dan memenuhi kriteria untuk dapat digunakan dalam lingkup pemerintah federal.[163] Setiap tahunnya, menteri perdagangan harus berkonsultasi dengan pimpinan lembaga lain yang relevan dan harus 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.[164]

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,

[163] Bagian 4 Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[164] Article 5 Executive Order *on Improving the Nation's Cybersecurity United States 14028*

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.[165] 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.

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.[166] 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

[165] Pasal 6 Executive Order *on Improving the Nation's Cybersecurity United States 14028*
[166] Pasal 7 Executive Order *on Improving the Nation's Cybersecurity United States 14028*

ini, agar dapat dilindungi secara maksimal dan mampu untuk menangani risiko maupun insiden siber.[167]

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 Infrastruktur Informasi Kritikal dan data penting milik negara. Oleh karenanya, RUU KKS menjadi langkah strategis dalam hal memperkuat kewenangan Badan Siber dan Sandi Negara. Badan Siber dan Sandi Negara 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 Infrastruktur Informasi Kritikal dalam memastikan bahwa Infrastruktur Informasi Kritikal negara terlindungi dari serangan siber. Oleh karenanya, RUU KKS dibutuhkan juga sebagai langkah peningkatan kewenangan Badan Siber dan Sandi Negara dalam memberikan otoritas yang lebih besar dalam melakukan penanggulangan dan penindakan terhadap ancaman siber.

Melalui RUU KKS, Badan Siber dan Sandi Negara dapat memperkuat kewenangannya dengan diberikannya otoritas untuk melakukan pemantauan dan deteksi dini terhadap ancaman siber. RUU KKS juga dapat memperluas kewenangan Badan Siber dan Sandi Negara

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

dalam memfasilitasi koordinasi antar berbagai lembaga pemerintah dalam penanganan insiden siber. Hal ini tentunya tidak hanya berdampak pada kewenangan represif Badan Siber dan Sandi Negara melainkan juga menjadi langkah bagi kewenangan preventif Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara, maka peran Badan Siber dan Sandi Negara 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 diharapkan juga dapat membantu Badan Siber dan Sandi Negara dalam membuka peluang bagi kerjasama dengan negara lain dalam bidang keamanan siber .

Dalam regulasi yang berlaku saat ini, pengembangan peran Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara untuk menjalankan tugas baru yang sesuai dengan pengembangan perannya.

Oleh karenanya, RUU KKS sangat penting untuk memperkuat kewenangan Badan Siber dan Sandi Negara dan meningkatkan kemampuan Indonesia dalam menghadapi ancaman siber. Dengan landasan hukum yang kuat, Badan Siber dan Sandi Negara dapat lebih

efektif dalam melindungi keamanan nasional, mendorong pertumbuhan ekonomi digital, dan meningkatkan kerjasama 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 Badan Siber dan Sandi Negara 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 Infrastruktur Informasi Kritikal hingga perlindungan 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, Badan Siber dan Sandi Negara, 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.

Perancangan Undang-Undang ketahanan dan keamanan siber di Indonesia, yang saat ini tengah didorong oleh Badan Siber dan Sandi Negara, berpotensi menimbulkan tumpang tindih kewenangan 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 tumpang tindih adalah karena adanya pengaturan yang bersifat *overlapping* dengan Undang-Undang yang sudah ada, seperti UU ITE. RUU KKS memberikan wewenang besar kepada Badan Siber dan Sandi Negara 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 tumpang tindih 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 Badan Siber dan Sandi Negara. 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.

Namun, 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 Perlindungan 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 tumpang tindih 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 oleh Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara, 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.

Selain itu, RUU KKS juga berpotensi untuk meningkatkan transparansi dan akuntabilitas dalam pengelolaan anggaran terkait keamanan siber. Dengan adanya regulasi yang jelas, Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara dalam melakukan evaluasi kinerja dan pengawasan terhadap penggunaan anggaran.

Pembentukan RUU KKS tidak hanya akan memperkuat lembaga Badan Siber dan Sandi Negara dalam menjalankan kewenangannya, tetapi juga memberikan dampak positif terhadap pengelolaan keuangan negara. Melalui peningkatan kapasitas dan kewenangan Badan Siber dan Sandi Negara, 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:

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

2. **Peningkatan Kapasitas Badan Siber dan Sandi Negara dan Lembaga Terkait**

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

   - Pengembangan sistem dan perangkat pemantauan serta investigasi insiden siber;
   - Perekrutan tenaga ahli siber yang kompeten untuk melakukan pengawasan dan audit keamanan siber; dan
   - 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:

   - Biaya penerapan regulasi dan standar baru terkait keamanan siber , yang memerlukan investasi dalam teknologi dan audit berkala; dan
   - 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:

- Mengurangi risiko serangan siber yang merugikan, yang dapat menyebabkan kerugian ekonomi besar bagi pemerintah dan sektor swasta;
- Menghindari kebocoran data yang bisa menimbulkan biaya kompensasi dan pemulihan besar, serta merusak reputasi pemerintah; dan
- 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 perlindungan Infrastruktur Informasi Kritikal 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[168]. Tanpa perlindungan 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 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

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

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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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 perlindungan 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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara, 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 Badan Siber dan Sandi Negara 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, Badan Siber dan Sandi Negara kemudian didefinisikan sebagai “Lembaga Pemerintah Non-Kementerian”. Berdasarkan Pasal 2 Peraturan Presiden ini, tugas Badan Siber dan Sandi Negara adalah melaksanakan keamanan

siber, sementara persandian menjadi salah satu fungsi dalam lingkup kerja Badan Siber dan Sandi Negara.

Beberapa bulan setelah pendirian Badan Siber dan Sandi Negara, 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 Badan Siber dan Sandi Negara. Perubahan ini menandai adanya evolusi peran Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara dalam mengembangkan struktur kelembagaan dan fungsinya, seiring dengan meningkatnya kebutuhan keamanan siber di tingkat nasional maupun internasional.

Evolusi peran Badan Siber dan Sandi Negara semakin terlihat jelas dengan diterbitkannya Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara yang memperluas tugas dan fungsi Badan Siber dan Sandi Negara. Berdasarkan Pasal 2 Peraturan Presiden ini, tugas Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara. Dengan diundangkannya Peraturan Presiden terbaru yaitu Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Sandi dan Siber Negara, persandian menjadi tugas utama dari Badan Siber dan Sandi Negara.

Perluasan tugas ini memberikan perluasan terhadap fungsi yang dimiliki oleh Badan Siber dan Sandi Negara, 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 Badan Siber dan Sandi Negara, pengelolaan barang milik negara yang menjadi tanggung jawab Badan Siber dan Sandi Negara, pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan Badan Siber dan Sandi Negara, 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 Badan Siber dan Sandi Negara kini memiliki peran strategis yang lebih luas dalam kebijakan dan tata kelola siber Indonesia.

Untuk memastikan efektivitas Badan Siber dan Sandi Negara dalam menjalankan fungsinya, diperlukan harmonisasi antara berbagai peraturan yang mengatur Badan Siber dan Sandi Negara, baik dalam lingkup keamanan siber maupun persandian. Transformasi Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara mencerminkan adaptasi pemerintah Indonesia terhadap tantangan era digital. Dalam kerangka regulasi yang ada saat ini, pengembangan peran Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara 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 Badan Siber dan Sandi Negara

untuk melaksanakan tugas tambahan yang sejalan dengan pengembangan peran baru dari Badan Siber dan Sandi Negara.

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 perlindungan Infrastruktur Informasi Kritikal. 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 Infrastruktur Informasi Kritikal 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 tersebut. 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.

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.[169] 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.[170]

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

[169] Teguh Prasetyo, "Membangun Hukum Nasional Berdasarkan Pancasila", Jurnal Hukum dan peradilan, Vol. 3 Nomor 3, 2014, hlm. 216.
[170] 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.[171] 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

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

harus dapat menciptakan kerangka kerja yang memfasilitasi kolaborasi antara Badan Siber dan Sandi Negara, kementerian terkait lembaga penegak hukum, hingga sektor swasta agar tercapai tujuan Indonesia yang lebih cepat 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.[172]

Perkembangan dunia teknologi saat ini memberikan ancaman yang semakin nyata dan mengkhawatirkan. Pesatnya perkembangan teknologi memberikan manfaat sekaligus ancaman yang besar terhadap dunia siber.[173] 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

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

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 pada dasarnya sudah menjadi kewajiban bagi negara ini dalam memperkuat hukum yang dapat menjamin pelindungan bagi masyarakat dari segala bentuk ancaman siber.[174] 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 perlindungan 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.[175] 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.

B. Landasan Sosiologis

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

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

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.[176] 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[177].

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.[178] Serangan ini menyebabkan gangguan pada layanan publik penting seperti pendaftaran peserta didik baru dan layanan imigrasi, menunjukkan betapa rentannya Infrastruktur Informasi Kritikal tanpa perlindungan 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, 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

---

[176] 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.

[177] 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

[178] 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

menggarisbawahi kebutuhan akan sistem backup dan *Disaster Recovery Plan* (DRP) yang kuat untuk ketahanan siber di masa depan.[179]

Kedua, keamanan siber berkaitan erat dengan kepercayaan publik terhadap Infrastruktur Informasi.[180] 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 Perlindungan 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.[181] Selain itu, peningkatan penggunaan media sosial dan internet di Indonesia tidak dibarengi dengan peningkatan literasi digital/teknologi di masyarakat sehingga akan semakin memperbesar peluang pihak tidak bertanggungjawab dalam melakukan ancaman kejahatan siber.

---

[179] *Ibid,* hlm.208

[180] 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

[181] 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.

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.

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 Badan Siber dan Sandi Negara yang belum mampu menjangkau seluruh aspek keamanan siber, baik dalam ranah publik maupun privat. Selain itu, Badan Siber dan Sandi Negara 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 Nomnor 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.[182] 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.

[182] 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 Infrastruktur Informasi Kritikal 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 siber di era digital saat ini.

Badan Siber dan Sandi Negara seharusnya ditingkatkan menjadi lembaga negara yang lahir dari Undang-Undang atau merupakan kementerian yang langsung berada di bawah Presiden. Badan Siber dan Sandi Negara juga 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.

B. Arah dan Jangkauan Pengaturan

1. Arah Pengaturan

Arah pengaturan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber menekankan perlunya 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 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. Jangkauan ini meliputi pelindungan terhadap Infrastruktur Informasi Kritikal, pengamanan data dan informasi, serta pengelolaan risiko siber yang dapat mempengaruhi stabilitas nasional. Selain itu, RUU ini mengatur tanggung jawab Penyelenggara Infrastruktur Informasi sebagai PSE dalam memastikan keamanan data pelanggan dan efektivitas sistem yang digunakan. Dengan perkembangan ancaman siber yang dinamis, pengaturan 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 ekonomi, pertahanan, dan sosial.

C. Ruang Lingkup dan Materi Muatan

Adapun ruang lingkup materi muatan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber adalah sebagai berikut:

1. Pengaturan penyelenggaraan Keamanan dan Ketahanan Siber

Pemerintah bertanggung jawab melindungi negara, warga negara, Infrastruktur Informasi Kritikal, dan aset nasional dari ancaman serta serangan siber domestik maupun global melalui pembentukan Badan Siber dan Sandi Negara. Badan Siber dan Sandi Negara mengoordinasikan lembaga negara dan pemangku kepentingan untuk menyelenggarakan keamanan dan ketahanan siber, termasuk pelindungan terhadap Infrastruktur Informasi Kritikal, penerapan standar keamanan nasional, audit keamanan, serta pengembangan teknologi dan sumber daya manusia. Dalam pelaksanaannya, penyelenggaraan keamanan siber mengutamakan pelindungan hak asasi manusia, data pribadi, ketertiban sosial, inovasi teknologi, dan pertumbuhan ekonomi digital. Pemerintah juga menetapkan strategi nasional keamanan siber yang melibatkan kementerian dan lembaga terkait serta memprioritaskan pencegahan kejahatan, penegakan hukum, peningkatan literasi digital, dan pengembangan ekosistem digital kondusif.

Produsen Produk dengan Elemen Digital (PDED) diwajibkan memenuhi standar keamanan dan melakukan asesmen terhadap produk mereka sesuai dengan tingkat risiko. Produk dengan risiko menengah hingga tinggi harus melalui sertifikasi dan pengujian oleh lembaga yang ditunjuk pemerintah, disertai dokumentasi kerentanan serta pembaruan keamanan secara

berkala tanpa biaya kepada pengguna. Pelaporan insiden siber menjadi kewajiban penyedia layanan teknologi dan penyelenggara Infrastruktur Informasi Kritikal, dengan pelaporan insiden *ransomware*, ancaman signifikan, atau pelanggaran keamanan harus dilaporkan dalam batas waktu tertentu. Pemerintah juga mewajibkan produsen PDED menyediakan mekanisme distribusi pembaruan keamanan dan melaksanakan pengungkapan kerentanan yang terkoordinasi untuk meningkatkan respons terhadap ancaman siber.

Badan Siber bertugas memantau, mengevaluasi, dan mengoordinasikan penanggulangan ancaman siber dengan kementerian, lembaga, dan pihak terkait melalui forum antarlembaga. Upaya ini melibatkan pertukaran informasi, pengembangan kebijakan keamanan, serta peningkatan kapasitas penanganan insiden. Penyelenggara Infrastruktur Informasi Kritikal wajib menerapkan kerangka kerja keamanan siber yang diakui internasional dan melaporkan pelanggaran atau insiden secara transparan untuk meningkatkan akuntabilitas. Pemerintah juga mengawasi kepatuhan industri melalui audit, asesmen investigatif, dan pelaporan berkala dengan tujuan untuk memastikan pengelolaan keamanan siber yang efektif dan terintegrasi.

2. Pelindungan Siber

Pelindungan Siber merupakan upaya terpadu untuk melindungi Infrastruktur Informasi Kritikal, infrastruktur lainnya, serta produk dan/atau layanan digital (PDED) dari ancaman, serangan, atau gangguan siber. Penyelenggara Infrastruktur Informasi bertanggung jawab penuh atas pelindungan infrastruktur yang dimiliki, dikelola, dan

dioperasikan, dengan cakupan yang mencakup jaringan internet, pusat data, sistem elektronik, layanan digital, infrastruktur telekomunikasi, hingga komputasi awan. Infrastruktur ini harus memenuhi standar keamanan yang ditetapkan oleh Badan Siber dan Sandi Negara melalui Peraturan Presiden, dengan penekanan pada perencanaan, pembangunan, pengoperasian, pemeliharaan, dan pengawasan sesuai standar keamanan dan ketahanan siber. Penyelenggara wajib mengelola risiko, membuat mitigasi, serta melaksanakan langkah-langkah identifikasi, proteksi, audit, dan asesmen mandiri maupun wajib sesuai dengan ketentuan peraturan perundang-undangan.

Penyelenggara Infrastruktur Informasi Kritikal diwajibkan mendaftarkan diri ke Badan Siber dan Sandi Negara serta melaksanakan audit keamanan siber secara berkala, mencakup penerapan kebijakan, efektivitas kontrol keamanan, kepatuhan terhadap regulasi, hingga pengelolaan insiden dan pelindungan data. Hasil audit harus dilaporkan setidaknya 1 (satu) kali dalam setahun, dan penyelenggara diwajibkan memiliki rencana mitigasi risiko serta simulasi pemulihan pasca-insiden secara berkala. Untuk mendorong kepatuhan, pemerintah dapat memberikan penghargaan atau insentif kepada penyelenggara yang berhasil memenuhi standar keamanan siber. Badan Siber dan Sandi Negara juga bertanggung jawab melakukan pengawasan terhadap pelaksanaan keamanan oleh penyelenggara Infrastruktur Informasi Kritikal, termasuk memberikan rekomendasi, menetapkan sektor strategis, dan memberlakukan sanksi administratif bagi pihak yang tidak mematuhi standar.

Pengelolaan infrastruktur kritikal melibatkan langkah-langkah tata kelola, audit, pengelolaan risiko, serta pengukuran tingkat kematangan keamanan. Setiap badan publik yang

mengelola Infrastruktur Informasi Kritikal diwajibkan memiliki rencana pemulihan yang komprehensif dan menjalankan audit independen dengan hasil yang dilaporkan ke Badan Siber dan Sandi Negara dalam waktu 30 (tiga puluh) hari setelah selesai. Infrastruktur Informasi Kritikal yang mempengaruhi stabilitas nasional, ekonomi, atau layanan umum memerlukan pelindungan berkelanjutan melalui pemantauan ancaman, pembaruan sistem keamanan, dan penerapan deteksi ancaman yang memadai. Semua langkah ini bertujuan untuk memastikan keamanan, ketahanan, dan kesinambungan infrastruktur kritikal demi mendukung stabilitas dan kesejahteraan nasional.

3. Kesiapsiagaan dan Ketahanan Siber

Kesiapsiagaan dan Ketahanan Siber mencakup langkah-langkah komprehensif yang melibatkan kepatuhan terhadap persyaratan PDED, identifikasi ancaman dan kerentanan melalui pemantauan berkelanjutan, serta deteksi ancaman siber secara dini. Penanganan insiden siber harus dilakukan secara cepat dan efektif dengan prosedur yang telah ditetapkan, termasuk manajemen krisis melalui koordinasi lintas kementerian dan lembaga terkait, penerapan rencana kontingensi, serta penanggulangan dan pemulihan pasca-insiden melalui mitigasi dampak dan pemulihan sistem yang terdampak. Mitigasi risiko keamanan dan ketahanan siber juga menjadi tanggung jawab seluruh pengguna PDED dan kementerian/lembaga terkait sesuai dengan ketentuan yang peraturan perundang-undangan. Pemerintah dan Penyelenggara Sistem Elektronik wajib mengantisipasi insiden siber dengan langkah-langkah terarah, seperti pembentukan tim tanggap insiden, manajemen krisis,

serta forum berbagi informasi yang bertujuan meningkatkan kesiapsiagaan dan ketahanan siber secara nasional.

Tim tanggap insiden siber dibentuk untuk menangani insiden siber dan terdiri atas kementerian, lembaga, dan pihak terkait lainnya yang ditunjuk pemerintah, dengan tanggung jawab melapor kepada Kepala Badan. Setiap badan publik yang mengalami insiden siber diwajibkan segera melaporkan kejadian tersebut, melakukan tindakan pemulihan, serta bekerja sama dalam penyelidikan insiden. Dalam situasi krisis, status Krisis Siber dapat ditetapkan oleh Presiden berdasarkan usulan Kepala Badan Siber dan Sandi Negara, dengan pembentukan gugus tugas Krisis Siber yang melaporkan perkembangan secara berkala. Setelah kondisi terkendali dan layanan minimum sistem elektronik kembali tersedia, gugus tugas akan mengusulkan pengakhiran status krisis kepada Presiden. Ketentuan lebih lanjut terkait kesiapsiagaan dan ketahanan siber diatur dalam Peraturan Pemerintah.

4. Pengembangan dan Peningkatan Kapasitas

Badan Siber dan Sandi Negara bertanggung jawab mengoordinasikan pengembangan dan peningkatan kapasitas dalam bidang keamanan siber melalui berbagai upaya, termasuk peningkatan kesadaran, literasi, pelatihan, penelitian, dan pengembangan infrastruktur. Dalam hal ini, sektor swasta yang mengelola Infrastruktur Informasi Kritikal diwajibkan bekerja sama dengan pemerintah untuk melaksanakan pelatihan, simulasi respons insiden siber, serta peningkatan pengetahuan tentang ancaman siber. Pemerintah juga memfasilitasi pengembangan ilmu pengetahuan, teknologi, riset, dan inovasi untuk mendukung keamanan dan ketahanan siber yang

berkelanjutan. Dalam mendukung upaya ini, Badan Siber dan Sandi Negara bekerja sama dengan kementerian terkait untuk melaksanakan program peningkatan kualitas sumber daya manusia dan pendidikan di bidang keamanan siber. Selain itu, pemerintah menetapkan standar nasional keamanan siber yang wajib dilaksanakan oleh penyelenggara atau pemilik Infrastruktur Informasi, dengan koordinasi antar lembaga terkait. Setiap penyelenggara infrastruktur Siber juga diwajibkan menyusun kebijakan keamanan yang mencakup penerapan standar, manajemen risiko, serta respons dan mitigasi insiden siber.

Penggunaan kecerdasan buatan (AI) untuk meningkatkan kapasitas keamanan siber didukung oleh pemerintah dengan memastikan bahwa penggunaannya berlandaskan etika, transparansi, dan di bawah pengawasan manusia. AI yang digunakan pada Infrastruktur Informasi Kritikal harus memenuhi ketentuan dan dilaporkan kepada Badan Siber dan Sandi Negara, sementara implementasinya diatur untuk meminimalkan dampak negatif yang mungkin timbul. Badan Siber dan Sandi Negara mengawasi, mengevaluasi, dan jika diperlukan, mengambil tindakan terhadap penggunaan AI dalam pengelolaan Infrastruktur Informasi Kritikal. Langkah ini bertujuan untuk memastikan bahwa kecerdasan buatan menjadi alat yang aman dan efektif dalam meningkatkan perlindungan siber tanpa mengorbankan aspek keamanan atau etika.

5. Keamanan Rantai Pasokan

Penyelenggaraan Keamanan dan Ketahanan Siber mengutamakan penggunaan produk dan jasa industri dalam negeri yang memenuhi standar sesuai dengan ketentuan

peraturan perundang-undangan. Produk dan jasa yang dihasilkan oleh industri ini wajib memiliki sertifikasi dari lembaga sertifikasi yang diakui oleh Badan Siber dan Sandi Negara, sebagai bukti pemenuhan standar Keamanan dan Ketahanan Siber yang berlaku. Selain itu, pemerintah juga mengakui sertifikasi internasional yang setara atau lebih tinggi dari standar nasional. Dalam mendukung keamanan rantai pasokan, perangkat lunak yang digunakan untuk fungsi kritikal harus memenuhi standar keamanan, dengan pengembang dan pemasok wajib menerapkan kontrol keamanan yang memadai dan transparansi. Pengguna perangkat lunak tersebut harus secara rutin melakukan evaluasi dan audit untuk memastikan kepatuhan terhadap persyaratan keamanan.

Penyedia produk dan layanan yang terkait dengan Infrastruktur Informasi Kritikal memiliki tanggung jawab untuk memenuhi standar keamanan yang telah ditetapkan, termasuk melakukan penilaian risiko terhadap potensi kerentanan serta melaporkan setiap insiden yang berpotensi membahayakan keamanan siber. Badan Publik yang mengelola Infrastruktur Informasi Kritikal wajib melaksanakan penilaian risiko ancaman siber secara berkala, menyusun rencana pemulihan, dan memastikan ketahanan operasional pasca insiden. Pedoman pengelolaan risiko dan pemulihan yang ditetapkan oleh Badan Siber dan Sandi Negara harus dipatuhi oleh sektor-sektor berisiko tinggi. Untuk memastikan efektivitas pengelolaan risiko, organisasi yang mengelola Infrastruktur Informasi Kritikal wajib melatih personel utama mereka dalam manajemen insiden siber dan pemulihan bencana.

6. Kelembagaan

Badan Siber dan Sandi Negara memiliki kedudukan strategis yang bertanggung jawab langsung kepada Presiden, dengan tugas utama menyelenggarakan keamanan dan ketahanan siber serta sandi negara. Badan Siber dan Sandi Negara merumuskan dan menetapkan kebijakan, strategi, serta standar keamanan siber; melaksanakan pembinaan dan pengawasan terhadap badan publik, mengidentifikasi, mendeteksi, dan menangani ancaman serta insiden siber, dan mengelola pusat manajemen krisis siber. Badan Siber dan Sandi Negara juga berwenang menyelenggarakan operasi keamanan siber, meminta data terkait keamanan siber, menjalin kerja sama dengan pihak internasional, serta menegakkan hukum sesuai dengan ketentuan peraturan perundang-undangan. Selain itu, Badan Siber dan Sandi Negara ini memiliki tanggung jawab khusus dalam pelaksanaan persandian negara yang meliputi pengamanan data dan informasi menggunakan metode kriptografi yang sistematis dan profesional. Untuk melaksanakan tugasnya, Badan Siber dan Sandi Negara menyusun norma, standar, prosedur, dan kriteria di bidang keamanan siber serta menjalankan fungsi literasi, pendidikan, dan peningkatan kapasitas sumber daya manusia.

Badan Siber dan Sandi Negara memiliki peran penting dalam kerja sama dengan penegak hukum, lembaga internasional, dan sektor swasta untuk menangani kejahatan siber lintas negara, termasuk melacak dan menuntut pelaku serangan siber. Penyedia layanan internet dan platform digital diwajibkan bekerja sama dengan penegak hukum untuk mengungkap identitas pelaku dan menghentikan distribusi serangan siber. Badan Siber dan Sandi Negara juga diberi kewenangan melakukan intersepsi

atau penyadapan sebagai bagian dari proses penegakan hukum terhadap insiden keamanan siber yang signifikan. Selain itu, Badan Siber dan Sandi Negara memberdayakan berbagai pihak, termasuk akademisi, pelaku usaha, dan masyarakat, dalam menyelenggarakan literasi keamanan siber dan mengelola pendidikan kedinasan untuk meningkatkan kapasitas sumber daya manusia di bidang ini. Tata cara pelaksanaan wewenang Badan Siber dan Sandi Negara dan penyelenggaraan sandi negara diatur lebih lanjut dengan Peraturan Pemerintah.

7. Kerja Sama Internasional

Badan Siber dan Sandi Negara memiliki kewenangan untuk menjalin kerja sama internasional dalam rangka memperkuat keamanan dan ketahanan siber nasional. Kerja sama ini mencakup pertukaran informasi, penelitian, pengembangan kebijakan, dan penanganan ancaman siber transnasional yang dapat mempengaruhi lebih dari satu negara. Kerja sama dilaksanakan berdasarkan perjanjian internasional, kesepakatan regional atau bilateral, serta konvensi internasional yang telah diratifikasi atau diaksesi oleh Indonesia. Selain itu, Badan Siber dan Sandi Negara bekerja sama dengan badan publik penyelenggara atau pemilik Infrastruktur Informasi internasional, baik dari kalangan pemerintah, non-pemerintah, maupun perusahaan multinasional. Dalam melaksanakan kerja sama ini, Badan Siber dan Sandi Negara memprioritaskan kepentingan nasional, politik luar negeri, ketentuan perundang-undangan, dan prinsip hukum internasional.

Untuk memajukan kepentingan siber Indonesia di tingkat global, Badan Siber dan Sandi Negara berpartisipasi dalam berbagai program internasional, termasuk perumusan konsep,

norma, dan panduan keamanan siber secara bilateral, regional, atau multilateral. Pemerintah juga terlibat dalam memecahkan masalah keamanan siber di forum internasional, membangun kemitraan dengan berbagai negara dan Penyelenggara Sistem Elektronik atau pemilik Infrastruktur Informasi, serta meningkatkan kapasitas keamanan siber kawasan. Dalam pelaksanaan diplomasi siber, Badan Siber dan Sandi Negara bekerja sama dengan kementerian dan lembaga terkait, termasuk kementerian yang bertanggung jawab dalam urusan luar negeri. Untuk memperkuat diplomasi siber, pemerintah dapat menunjuk atase keamanan dan ketahanan siber di perwakilan luar negeri. Semua langkah ini dilakukan dalam rangka mencegah penyalahgunaan siber, meningkatkan ketahanan nasional, dan mendiseminasikan kebijakan keamanan siber Indonesia di tingkat internasional.

8. Partisipasi Masyarakat

Masyarakat dapat berpartisipasi secara langsung maupun tidak langsung dalam mendukung terselenggaranya Keamanan dan Ketahanan Siber. Kemudian ketentuan tentang bentuk partisipasi masyarakat ditetapkan dalam Peraturan Badan Siber dan Sandi Negara.

9. Ketentuan Sanksi

Terhadap materi yang telah diatur dalam Undang-Undang, maka terhadap pelanggaran pada ketentuan Undang-Undang ini 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. Sanksi yang diatur dalam Undang-Undang ini dapat berupa sanksi pidana dan sanksi administratif.

Dalam Undang-Undang ini, penerapan 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 peraturan-perundang-undangan. Dalam pemberian sanksi administratif disesuaikan dengan besaran pelanggaran yang dilakukan. Selain itu, ketentuan sanksi administratif juga dapat ditentukan berdasarkan klasifikasi jenis pelanggaran yang dilakukan. Pemberian sanksi administratif dapat diberikan oleh lembaga yang diatur secara khusus untuk memberikan sanksi tersebut.

10. Ketentuan Peralihan

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. 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 perlindungan 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, Penyelenggaraan Keamanan dan Ketahanan Siber, Pelindungan Siber, Kesiapsiagaan dan Ketahanan Siber, Pengembangan dan Peningkatan Kapasitas, Keamanan Rantai Pasokan, Kelembagaan, Kerjasama Internasional, Partisipasi Masyarakat, Penyidikan, Pelanggaran Administratif, Sanksi Administratif, Ketentuan Pidana, Ketentuan Peralihan, Ketentuan Penutup.

B. Saran

1. Indonesia memerlukan pengaturan yang komprehensif di bidang keamanan dan ketahanan siber. Regulasi ini diharapkan mampu melindungi Infrastruktur Informasi Kritikal 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 siber di era digital saat ini.
2. Badan Siber dan Sandi Negara seharusnya ditingkatkan menjadi lembaga negara yang lahir dari Undang-Undang atau merupakan kementerian yang langsung berada di bawah Presiden. Badan Siber dan Sandi Negara juga 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 Cybercrime

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

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

Personal Data Protection Act (PDPA)

Peraturan Badan Siber dan Sandi Negara 2014.

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. Cybersecur. 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.

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

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

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.

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.

National Cyber Security Index Report 2023.

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 Perlindungan 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 Perlindungan 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. "Perlindungan 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)

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 Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber ," Jurnal Multidisiplin Indonesia, Vol. 2, Nomor 3, Maret 2023.

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 Cybercrime": Konvensi Pertama PBB Tentang Kejahatan Siber (Bagian I), <https://tekNomorkompas.com/read/2024/08/19/09445517/un-convention-against-cybercrime-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.

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.

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.

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.

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.

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.