PENGANTAR HUKUM TEKNOLOGI INFORMASI

Mila Jumarlis, Menhya Snae, Andi Firmansyah,
Vidya Devia Ardania, Azry Yusuf,
Jimmy Herawan Moedjahedy , Andi Ismayana Wahid,
Karman Jaya, Mirfan, Fatri Sagita, Febria Gupita, Sigit Handoko,
Suci Damayanti, Muh. Fachrur Razy Mahka, Sufriaman

Daftar Isi

Bab 13
Kebijakan Nasional dan Internasional tentang Cyber Law

13.1 Konsep Kebijakan Cyber Law Nasional dan Global

Perkembangan teknologi digital telah mengubah cara individu, perusahaan, dan negara berinteraksi. Aktivitas ekonomi, komunikasi, transaksi bisnis, hingga pelayanan publik kini banyak dilakukan melalui sistem elektronik yang saling terhubung secara global. Transformasi tersebut melahirkan ruang virtual yang dikenal sebagai *cyberspace* (Dikdik et al., 2009). *Cyberspace* merupakan lingkungan digital yang memungkinkan pertukaran informasi tanpa dibatasi oleh batas-batas geografis negara (*borderless*), sehingga menghasilkan bentuk-bentuk interaksi yang berbeda dari dunia fisik (Kristanto & Baihaki, 2025). Karakteristik tersebut menyebabkan aktivitas yang dilakukan di dalam ruang siber dapat melibatkan berbagai yurisdiksi secara bersamaan.

Cyber law merupakan bidang hukum yang mengatur berbagai aktivitas manusia di ruang siber. Pada tahap awal perkembangannya, lahir *Budapest Convention on Cybercrime* yang disahkan oleh Dewan Eropa pada tahun 2001 dan berorientasi pada pengaturan serta penanggulangan berbagai bentuk kejahatan berbasis komputer, seperti akses ilegal (*unauthorized access*) terhadap sistem komputer, penyadapan ilegal (*illegal interception*), perusakan data (*data interference*), dan pelanggaran konten digital seperti pornografi anak (Council of Europe, 2001). Seiring dengan pesatnya perkembangan teknologi digital, ruang lingkup *cyber law* semakin meluas hingga mencakup pelindungan data pribadi, keamanan siber, transaksi elektronik, kecerdasan buatan (*artificial intelligence*), dan kebebasan berekspresi di ruang digital (UNODC, 2013). Selain itu, lahir pula *General Data Protection Regulation* (GDPR) yang diterbitkan oleh Parlemen Uni Eropa dan menekankan tata kelola pemrosesan data pribadi sebagai bagian

penting dari perlindungan hak individu dalam ekosistem digital (The European Parliament and The Council of the European Union, 2016).

Secara umum, ruang lingkup *cyber law* mencakup pengaturan mengenai penggunaan teknologi informasi, jaringan komputer, data elektronik, transaksi elektronik, keamanan siber, serta berbagai aktivitas yang dilakukan melalui internet. Dalam perkembangannya, *cyber law* tidak lagi berfokus semata pada penegakan hukum terhadap pelaku kejahatan siber (*cybercrime*), tetapi juga diarahkan untuk membangun tata kelola ruang siber (*cyber governance*) yang mampu menciptakan kepastian hukum, melindungi hak asasi manusia, menjaga keamanan nasional, serta mendukung pertumbuhan ekonomi digital (Wirogioto & Belgradoputra, 2026). Perluasan ruang lingkup tersebut menunjukkan bahwa regulasi di ruang siber tidak lagi hanya berorientasi pada penanggulangan kejahatan siber, tetapi juga mencakup aspek tata kelola ruang siber (*cyber governance*).

Perkembangan tersebut kemudian melahirkan konsep *cyber governance*, yaitu suatu pendekatan yang menempatkan pengaturan ruang siber sebagai tanggung jawab bersama berbagai pemangku kepentingan (*multi-stakeholder governance*), tidak hanya negara sebagai pembentuk kebijakan, tetapi juga organisasi internasional, sektor swasta, komunitas teknis, akademisi, dan masyarakat sipil. Pendekatan tersebut memperoleh pengakuan internasional melalui *Tunis Agenda for the Information Society* (United Nations, 2005), yang mendefinisikan *Internet governance* sebagai berikut:

"*Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes...*"

Berdasarkan definisi tersebut, tata kelola internet dipahami sebagai proses pengembangan dan penerapan prinsip, norma, aturan, prosedur pengambilan keputusan, serta program yang melibatkan pemerintah, sektor swasta, dan masyarakat sipil sesuai dengan peran masing-masing. Konsep tersebut kemudian menjadi fondasi berkembangnya model *multi-stakeholder governance* yang menempatkan pengelolaan ruang siber sebagai tanggung jawab bersama antara pemerintah, sektor swasta, komunitas teknis, akademisi, organisasi internasional, dan masyarakat sipil (United Nations, 2005). Model ini selanjutnya diadopsi dalam berbagai forum internasional sebagai pendekatan utama dalam penyusunan kebijakan tata kelola internet.

Perkembangan konsep *cyber law* dari instrumen penanggulangan kejahatan siber menjadi bagian dari tata kelola ruang siber menunjukkan bahwa pembentukan kebijakan di bidang siber tidak lagi dapat dilakukan secara parsial. Karakteristik ruang siber yang bersifat lintas batas menuntut adanya keterpaduan antara kebijakan nasional dengan berbagai norma, standar, dan kerja sama internasional. Oleh karena itu, pembahasan mengenai kebijakan *cyber law* tidak hanya mencakup regulasi domestik, tetapi juga harus mempertimbangkan perkembangan rezim hukum internasional yang mengatur keamanan siber, perlindungan data, dan penanganan kejahatan siber (Council of Europe, 2001; United Nations, 2005; UNODC, 2013). Dengan demikian, pemahaman mengenai evolusi konsep *cyber law* menjadi landasan penting untuk menganalisis kebijakan nasional maupun internasional dalam mewujudkan tata kelola ruang siber yang efektif, adaptif, dan kolaboratif.

13.2 Kebijakan Nasional Keamanan Siber di Indonesia

Perkembangan teknologi informasi dan komunikasi telah mendorong perubahan yang signifikan dalam berbagai aspek kehidupan masyarakat, mulai dari penyelenggaraan pemerintahan, aktivitas ekonomi, pelayanan publik, hingga interaksi sosial. Transformasi digital tersebut memberikan berbagai manfaat dalam meningkatkan efisiensi dan konektivitas, namun di sisi lain juga meningkatkan risiko terhadap keamanan ruang siber. Ancaman seperti serangan siber, kebocoran data pribadi, pencurian identitas, penyebaran perangkat lunak berbahaya (*malware*), hingga serangan terhadap infrastruktur informasi vital menunjukkan bahwa keamanan siber telah menjadi salah satu isu strategis dalam penyelenggaraan negara [chintia2018kasus; republikindonesia2023keamanansiber]. Kondisi tersebut mendorong pemerintah Indonesia untuk mengembangkan kebijakan nasional yang mampu menjamin keamanan, keandalan, dan keberlanjutan ekosistem digital.

Kebijakan nasional keamanan siber di Indonesia tidak dibangun melalui satu regulasi yang berdiri sendiri, melainkan berkembang secara bertahap seiring dengan meningkatnya kompleksitas aktivitas di ruang siber. Pada tahap awal, perhatian pemerintah lebih difokuskan pada pengakuan terhadap informasi dan transaksi elektronik sebagai bagian dari aktivitas hukum yang sah. Orientasi tersebut tercermin dalam Undang-Undang Nomor 11 Tahun

2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi tonggak awal pengaturan aktivitas elektronik di Indonesia (Republik Indonesia, 2008). Kehadiran UU ITE tidak hanya memberikan dasar hukum bagi penyelenggaraan transaksi elektronik, tetapi juga mengatur berbagai bentuk perbuatan yang dikategorikan sebagai tindak pidana di ruang siber, seperti akses tanpa hak terhadap sistem elektronik, manipulasi data elektronik, dan gangguan terhadap sistem elektronik (Republik Indonesia, 2008, 2024b).

Seiring dengan meningkatnya pemanfaatan teknologi digital, kebijakan nasional di bidang siber mengalami perkembangan yang tidak lagi berfokus pada pengaturan transaksi elektronik dan penanggulangan kejahatan siber semata. Perubahan lanskap digital, meningkatnya volume data yang diproses secara elektronik, serta munculnya berbagai model bisnis berbasis platform digital mendorong pemerintah untuk memperluas cakupan kebijakan ke arah pelindungan data pribadi, penguatan keamanan sistem elektronik, dan pembangunan ketahanan siber nasional (Republik Indonesia, 2019b, 2022a, 2023a). Perkembangan tersebut menunjukkan adanya pergeseran paradigma dari pendekatan yang bersifat *reactive law enforcement* menuju pendekatan *cyber governance* yang lebih komprehensif.

Sebagai bagian dari penguatan tata kelola keamanan siber, pemerintah membentuk Badan Siber dan Sandi Negara (BSSN). Dasar hukum kelembagaan BSSN saat ini mengacu pada Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Republik Indonesia, 2021). Pembentukan BSSN merupakan langkah strategis dalam mengintegrasikan fungsi keamanan siber nasional yang sebelumnya tersebar di berbagai lembaga.

Penguatan kebijakan nasional juga ditandai dengan lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Republik Indonesia, 2022a). Regulasi ini memperluas orientasi *cyber law* Indonesia dengan menempatkan pelindungan data pribadi sebagai salah satu hak fundamental warga negara dalam ekosistem digital. Melalui undang-undang tersebut, negara tidak hanya mengatur kewajiban pengendali dan prosesor data pribadi, tetapi juga memberikan jaminan terhadap hak-hak subjek data, termasuk hak untuk memperoleh informasi, memperbaiki data, membatasi pemrosesan data, hingga mengajukan keberatan atas penggunaan data pribadinya (Republik Indonesia, 2022a). Selanjutnya, pada tahun 2024

ditetapkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang difokuskan pada penguatan kepastian hukum di ruang digital (Republik Indonesia, 2024b).

Meskipun demikian, kebijakan nasional keamanan siber di Indonesia masih menghadapi berbagai tantangan. Dari aspek regulasi, pengaturan mengenai keamanan siber masih tersebar dalam berbagai peraturan perundang-undangan sehingga belum membentuk suatu kerangka hukum yang terintegrasi. Kondisi ini berpotensi menimbulkan tumpang tindih kewenangan antarinstansi serta menyulitkan koordinasi dalam penanganan insiden siber yang bersifat lintas sektor. Selain itu, meningkatnya ancaman berupa kebocoran data pribadi, serangan *ransomware*, penyalahgunaan kecerdasan buatan (*artificial intelligence*), dan serangan terhadap infrastruktur digital menunjukkan bahwa perkembangan teknologi sering kali lebih cepat dibandingkan perkembangan regulasi yang mengaturnya (Republik Indonesia, 2022a, 2023a, 2024b).

Oleh karena itu, arah kebijakan nasional keamanan siber di Indonesia perlu terus dikembangkan melalui harmonisasi regulasi, penguatan koordinasi kelembagaan, peningkatan kapasitas sumber daya manusia, serta penguatan kerja sama dengan sektor swasta dan komunitas internasional. Pendekatan tersebut sejalan dengan karakteristik ruang siber yang bersifat lintas batas, sehingga efektivitas kebijakan nasional tidak hanya ditentukan oleh kualitas regulasi domestik, tetapi juga oleh kemampuan Indonesia untuk beradaptasi dengan perkembangan standar dan praktik internasional dalam tata kelola keamanan siber (Republik Indonesia, 2023a; UNODC, 2013).

13.3 Peran Lembaga Negara dalam Tata Kelola Siber

Implementasi kebijakan keamanan siber tidak hanya ditentukan oleh kualitas regulasi, tetapi juga oleh efektivitas kelembagaan yang menjalankannya. Karakteristik ancaman siber yang bersifat lintas sektor dan lintas yurisdiksi menyebabkan tata kelola siber memerlukan koordinasi antarlembaga yang melibatkan berbagai institusi negara sesuai dengan tugas dan kewenangannya. Oleh karena itu, penyelenggaraan keamanan siber di Indonesia tidak bertumpu pada satu lembaga semata, melainkan dilaksanakan melalui pendekatan kelembagaan yang bersifat kolaboratif.

Dalam konteks Indonesia, beberapa lembaga negara memiliki peran penting dalam tata kelola siber, yaitu:

1. **Badan Siber dan Sandi Negara (BSSN)**

   Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, BSSN memiliki tugas untuk melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi guna membantu Presiden dalam menyelenggarakan pemerintahan (Republik Indonesia, 2021). Selain itu, BSSN berperan dalam penyusunan kebijakan keamanan siber, koordinasi antarinstansi, peningkatan kapasitas keamanan siber nasional, perlindungan infrastruktur informasi vital, serta deteksi dan respons terhadap insiden siber (Republik Indonesia, 2021, 2023a). Selain menjalankan fungsi operasional, BSSN juga berperan dalam membangun budaya keamanan siber melalui peningkatan kesadaran masyarakat, pengembangan sumber daya manusia, dan penyusunan standar keamanan sistem elektronik. Kehadiran BSSN menunjukkan bahwa keamanan siber tidak lagi dipandang semata sebagai isu teknis, melainkan sebagai bagian dari sistem keamanan nasional yang memerlukan tata kelola yang terintegrasi.

2. **Kementerian Komunikasi dan Digital**

   Kementerian Komunikasi dan Digital (Komdigi) menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi berdasarkan Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital [republikindonesia2024komdigi]. Dalam menjalankan tugas tersebut, Komdigi berwenang merumuskan dan melaksanakan kebijakan di bidang komunikasi dan digital, termasuk penyelenggaraan sistem elektronik, tata kelola ruang digital, serta pengembangan ekosistem digital nasional (Republik Indonesia, 2024a). Kewenangan tersebut didukung oleh Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang memberikan landasan hukum bagi pengaturan penyelenggaraan sistem elektronik dan pelindungan data pribadi (Republik Indonesia, 2024b; UU PDP Pelindungan Data Pribadi, 2022). Dalam konteks tata kelola siber, Komdigi berperan sebagai regulator yang menyusun kebijakan,

menetapkan standar, melakukan pembinaan, dan mengawasi penyelenggara sistem elektronik agar memenuhi ketentuan peraturan perundang-undangan.

3. Kepolisian Republik Indonesia

Kewenangan Kepolisian Negara Republik Indonesia (Polri) dalam penegakan hukum terhadap tindak pidana siber didasarkan pada Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 5 Tahun 2026 (Republik Indonesia, 2002a, 2026). Dalam melaksanakan tugas tersebut, Polri berwenang melakukan penyelidikan dan penyidikan terhadap seluruh tindak pidana, termasuk tindak pidana yang dilakukan melalui sistem elektronik sebagaimana diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Republik Indonesia, 2024b, 2025a).

Dalam pelaksanaannya, penanganan tindak pidana siber dilaksanakan oleh Direktorat Tindak Pidana Siber Badan Reserse Kriminal (Dittipidsiber) di bawah Bareskrim Polri. Unit ini bertugas melakukan penegakan hukum terhadap kejahatan siber. Secara umum, Dittipidsiber menangani dua kelompok kejahatan, yaitu *computer crime* dan *computer-related crime*, seperti akses ilegal terhadap sistem elektronik, penipuan daring, penyebaran *malware*, pencurian identitas, serangan terhadap sistem elektronik, serta tindak pidana lain yang memanfaatkan teknologi informasi (Siber Polri, 2026). Selain itu, Polri juga berperan dalam pengumpulan dan analisis alat bukti elektronik, pelacakan pelaku kejahatan siber, serta kerja sama dengan kementerian, lembaga, dan otoritas penegak hukum negara lain dalam menangani kejahatan siber yang bersifat lintas negara (Siber Polri, 2026).

4. Lembaga Sektoral

Selain ketiga institusi tersebut, sejumlah lembaga negara lainnya juga memiliki peran dalam penyelenggaraan tata kelola siber sesuai dengan karakteristik sektor yang menjadi kewenangannya. Di sektor jasa keuangan, Otoritas Jasa Keuangan (OJK) berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan berwenang mengatur dan mengawasi kegiatan pada sektor jasa keuangan, termasuk

mendorong penerapan manajemen risiko teknologi informasi dan keamanan siber oleh lembaga jasa keuangan (OJK, 2024; Republik Indonesia, 2011). Sementara itu, Bank Indonesia berdasarkan Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia sebagaimana telah beberapa kali diubah, termasuk melalui Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, memiliki kewenangan dalam menjaga keamanan dan keandalan sistem pembayaran, termasuk penyelenggaraan sistem pembayaran digital yang aman dan andal (Republik Indonesia, 1999a, 2023b).

Pada aspek pertahanan negara, Kementerian Pertahanan dan Tentara Nasional Indonesia (TNI) memiliki peran dalam penyelenggaraan pertahanan siber sebagai bagian dari sistem pertahanan negara berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara dan Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia sebagaimana telah diubah dengan Undang-Undang Nomor 3 Tahun 2025 (Republik Indonesia, 2002b, 2004, 2025b). Di sisi lain, penyelenggaraan pelindungan data pribadi tidak hanya menjadi tanggung jawab pemerintah pusat, tetapi juga seluruh penyelenggara negara yang bertindak sebagai pengendali data pribadi (Republik Indonesia, 2022a).

Keberadaan berbagai lembaga tersebut menunjukkan bahwa tata kelola siber di Indonesia mengadopsi pendekatan *multi-agency governance*, yaitu penyelenggaraan keamanan siber melalui pembagian fungsi dan koordinasi antarlembaga. Pendekatan ini memberikan fleksibilitas karena setiap institusi dapat menjalankan kewenangannya sesuai dengan bidang masing-masing. Namun demikian, model tersebut juga menghadapi tantangan berupa potensi tumpang tindih kewenangan, fragmentasi regulasi, dan kebutuhan akan mekanisme koordinasi yang lebih efektif dalam menghadapi ancaman siber yang terus berkembang (Republik Indonesia, 2023a).

Oleh karena itu, efektivitas tata kelola siber nasional tidak hanya ditentukan oleh keberadaan lembaga-lembaga yang memiliki kewenangan di bidang keamanan siber, tetapi juga oleh kemampuan membangun koordinasi, pertukaran informasi, serta pembagian kewenangan yang jelas di antara seluruh pemangku kepentingan. Dengan tata kelola kelembagaan yang terintegrasi, kebijakan keamanan siber diharapkan mampu memberikan perlindungan yang optimal terhadap kepentingan negara, pelaku usaha,

maupun masyarakat dalam memanfaatkan ruang digital (Republik Indonesia, 2023a).

13.4 Kerja Sama Internasional dalam Penanganan Kejahatan Siber

Perkembangan teknologi informasi telah menyebabkan kejahatan siber berkembang menjadi salah satu bentuk kejahatan transnasional yang memiliki karakteristik berbeda dengan kejahatan konvensional. Pelaku, korban, infrastruktur digital, maupun alat bukti elektronik dapat berada pada negara yang berbeda sehingga menimbulkan persoalan yurisdiksi, penegakan hukum, dan pelaksanaan proses penyidikan. Kondisi tersebut menunjukkan bahwa penanganan kejahatan siber tidak dapat dilakukan hanya melalui kebijakan nasional, tetapi memerlukan kerja sama internasional yang efektif sebagai bagian dari tata kelola keamanan siber global (Council of Europe, 2001; UNODC, 2013).

Karakter lintas batas (*borderless*) yang melekat pada ruang siber menyebabkan batas teritorial negara tidak lagi menjadi penghalang bagi pelaku kejahatan dalam melakukan aksinya. Serangan terhadap sistem elektronik, pencurian data, penyebaran *malware*, serangan *ransomware*, maupun penipuan berbasis internet dapat dilakukan dari suatu negara terhadap korban yang berada di negara lain dalam waktu yang sangat singkat. Selain itu, bukti elektronik yang diperlukan dalam proses penegakan hukum sering kali tersimpan pada penyedia layanan digital yang berlokasi di luar yurisdiksi negara tempat tindak pidana terjadi. Oleh karena itu, koordinasi dan kerja sama antarnegara menjadi prasyarat penting dalam meningkatkan efektivitas penanggulangan kejahatan siber (UNODC, 2013).

Salah satu instrumen internasional yang menjadi acuan utama dalam kerja sama penanganan kejahatan siber adalah *Convention on Cybercrime* atau *Budapest Convention*. Konvensi ini merupakan instrumen internasional pertama yang secara komprehensif mengatur harmonisasi tindak pidana siber, prosedur penyidikan terhadap alat bukti elektronik, serta mekanisme kerja sama internasional dalam penegakan hukum (Council of Europe, 2001). Konvensi tersebut mendorong negara-negara peserta untuk mengadopsi standar minimum mengenai kriminalisasi berbagai bentuk kejahatan siber, termasuk akses ilegal terhadap sistem komputer, intersepsi

ilegal, gangguan terhadap data dan sistem komputer, penyalahgunaan perangkat, serta berbagai tindak pidana yang berkaitan dengan konten dan pelanggaran hak cipta. Selain itu, *Budapest Convention* juga mengatur mekanisme bantuan hukum timbal balik (*mutual legal assistance*), ekstradisi, serta pertukaran informasi dalam proses penyidikan dan penuntutan lintas negara (Council of Europe, 2001).

Dalam penanganan kejahatan siber, kerja sama internasional dikembangkan melalui berbagai organisasi internasional dan forum multilateral. Organisasi-organisasi tersebut berperan dalam membangun norma, memperkuat koordinasi penegakan hukum, meningkatkan kapasitas negara, serta mengembangkan instrumen hukum internasional di bidang keamanan siber dan kejahatan siber. Beberapa organisasi dan forum yang memiliki peran penting antara lain sebagai berikut.

1. **Perserikatan Bangsa-Bangsa (PBB) atau *United Nations* (UN)**

   Di tingkat global, Perserikatan Bangsa-Bangsa (PBB) menjadi salah satu organisasi internasional yang berperan dalam mengembangkan norma, kebijakan, dan instrumen hukum mengenai keamanan siber dan penanganan kejahatan siber. Hingga saat ini, belum terdapat satu instrumen hukum internasional yang sepenuhnya mengatur seluruh aspek *cyber law*. Namun, PBB telah menginisiasi berbagai forum dan instrumen yang bertujuan memperkuat kerja sama antarnegara dalam menghadapi ancaman di ruang siber (United Nations General Assembly, 2018, 2024).

   Salah satu inisiatif tersebut adalah pembentukan *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (OEWG) melalui *United Nations General Assembly Resolution* 73/27 tahun 2018 (United Nations General Assembly, 2018) dibentuk sebagai forum yang melibatkan seluruh negara anggota PBB untuk membahas perkembangan teknologi informasi dan komunikasi dalam konteks keamanan internasional. Mandat OEWG meliputi pembahasan mengenai ancaman terhadap keamanan siber, penerapan hukum internasional di ruang siber, pengembangan norma dan prinsip perilaku negara yang bertanggung jawab (*norms of responsible State behaviour*), *confidence-building measures*, serta peningkatan kapasitas (*capacity building*) negara-negara anggota dalam menghadapi ancaman siber.

Dengan demikian, fokus utama OEWG bukanlah penegakan hukum terhadap pelaku kejahatan siber, melainkan penguatan tata kelola keamanan siber internasional dan stabilitas hubungan antarnegara di ruang siber (United Nations General Assembly, 2018).

Di sisi lain, upaya PBB dalam penanggulangan kejahatan siber diwujudkan melalui pembentukan *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* berdasarkan *United Nations General Assembly Resolution* 74/247 tahun 2019 (United Nations General Assembly, 2019). Komite ini diberi mandat untuk menyusun suatu konvensi internasional yang komprehensif mengenai penanggulangan penyalahgunaan teknologi informasi dan komunikasi untuk tujuan kriminal.

Berbeda dengan OEWG yang berorientasi pada keamanan internasional, *Ad Hoc Committee* berfokus pada harmonisasi hukum pidana, penguatan kerja sama internasional dalam penyidikan dan penuntutan kejahatan siber, pertukaran alat bukti elektronik, bantuan hukum timbal balik (*mutual legal assistance*), serta ekstradisi terhadap pelaku tindak pidana siber. Hasil dari proses tersebut adalah diadopsinya *United Nations Convention against Cybercrime* oleh Majelis Umum PBB pada 24 Desember 2024 melalui Resolusi 79/243 sebagai langkah menuju pembentukan kerangka hukum internasional yang lebih inklusif dalam penanganan kejahatan siber (United Nations General Assembly, 2024; United Nations Office on Drugs and Crime, 2024).

2. International Criminal Police Organization (INTERPOL)

Selain melalui Perserikatan Bangsa-Bangsa, kerja sama internasional dalam penanganan kejahatan siber juga dilakukan melalui *International Criminal Police Organization* (INTERPOL). Berdasarkan *Constitution of the International Criminal Police Organization* (INTERPOL), organisasi ini bertujuan untuk menjamin dan mengembangkan kerja sama timbal balik yang seluas-luasnya antara otoritas kepolisian negara anggota sesuai dengan hukum nasional masing-masing serta semangat *Universal Declaration of Human Rights*, sekaligus membentuk dan mengembangkan berbagai institusi yang efektif dalam pencegahan dan pemberantasan kejahatan internasional (ICPO-INTERPOL, 2024). Dalam konteks kejahatan siber, INTERPOL berperan sebagai fasilitator

kerja sama penegakan hukum melalui pertukaran informasi dan intelijen kriminal, koordinasi penyelidikan lintas negara, dukungan forensik digital, peningkatan kapasitas aparat penegak hukum, serta pelaksanaan operasi internasional untuk mengungkap jaringan kejahatan siber yang beroperasi lintas yurisdiksi (ICPO-INTERPOL, 2024).

Melalui *Cybercrime Directorate* dan *INTERPOL Global Cybercrime Programme*, INTERPOL juga membantu negara-negara anggotanya dalam memperkuat kemampuan investigasi digital, berbagi informasi mengenai ancaman siber, serta meningkatkan koordinasi dalam penanganan insiden dan tindak pidana siber yang bersifat transnasional. Berbeda dengan PBB yang berperan dalam pembentukan norma dan instrumen hukum internasional, INTERPOL berfokus pada aspek operasional penegakan hukum melalui koordinasi antarkepolisian negara anggota (ICPO-INTERPOL, 2024).

Dalam konteks Indonesia, kerja sama internasional dalam penanganan kejahatan siber dilakukan melalui berbagai mekanisme hukum, baik yang bersifat bilateral maupun multilateral. Dari aspek penegakan hukum, Indonesia menerapkan mekanisme *Mutual Legal Assistance* (MLA) berdasarkan Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana untuk memperoleh alat bukti, informasi, maupun bantuan proses hukum dari negara lain dalam perkara pidana, termasuk tindak pidana siber (Republik Indonesia, 2006). Selain itu, penyerahan pelaku tindak pidana yang berada di luar wilayah Indonesia dapat dilakukan melalui mekanisme ekstradisi berdasarkan Undang-Undang Nomor 1 Tahun 1979 tentang Ekstradisi beserta berbagai perjanjian ekstradisi yang telah disepakati dengan negara mitra (Republik Indonesia, 1979). Di samping itu, Indonesia juga aktif dalam kerja sama kepolisian internasional melalui INTERPOL, serta kerja sama regional melalui ASEAN dalam bidang peningkatan kapasitas, pertukaran informasi, dan penguatan respons terhadap ancaman siber lintas negara (ICPO-INTERPOL, 2024; UNODC, 2013).

Meskipun berbagai mekanisme kerja sama internasional telah berkembang, efektivitasnya masih menghadapi sejumlah tantangan. Perbedaan sistem hukum, standar pembuktian, kebijakan pelindungan data pribadi, serta kepentingan politik masing-masing negara sering kali memengaruhi proses pertukaran informasi maupun pelaksanaan bantuan hukum timbal balik.

Selain itu, perkembangan teknologi digital yang berlangsung sangat cepat menyebabkan mekanisme kerja sama internasional harus terus beradaptasi agar tetap mampu menjawab berbagai bentuk ancaman baru, seperti penyalahgunaan kecerdasan buatan (*artificial intelligence*), *deepfake*, *cryptocurrency*, dan serangan terhadap infrastruktur digital kritis (United Nations General Assembly, 2024; UNODC, 2013).

Dengan demikian, kerja sama internasional merupakan salah satu elemen yang tidak terpisahkan dari tata kelola keamanan siber modern. Sinergi antara kebijakan nasional dan mekanisme kerja sama internasional diperlukan untuk membangun sistem penegakan hukum yang efektif, memperkuat kapasitas negara dalam menghadapi ancaman siber, serta mewujudkan ruang siber yang aman, stabil, dan terpercaya bagi masyarakat internasional (Council of Europe, 2001; United Nations General Assembly, 2024).

Perdebatan mengenai kerja sama internasional dalam penanganan kejahatan siber pada dasarnya mencerminkan adanya tarik-menarik antara prinsip kedaulatan negara (*state sovereignty*) dan kebutuhan akan tata kelola global (*global cyber governance*). Di satu sisi, setiap negara memiliki kewenangan untuk mengatur dan menegakkan hukumnya sendiri di ruang siber. Di sisi lain, karakter lintas batas dari aktivitas digital menuntut adanya harmonisasi norma dan mekanisme kerja sama internasional. Dilema tersebut menjadi salah satu isu sentral dalam perkembangan *cyber law* kontemporer dan menjadi dasar bagi berbagai upaya harmonisasi kebijakan yang akan dibahas pada subbab berikutnya (United Nations General Assembly, 2018, 2024).

13.5 Perbandingan Kebijakan Cyber Law di Beberapa Negara

Perkembangan *cyber law* di berbagai negara menunjukkan bahwa tidak terdapat satu model kebijakan yang berlaku secara universal. Setiap negara membangun kerangka hukum sibernya berdasarkan sistem hukum, kepentingan nasional, tingkat perkembangan teknologi, serta tantangan keamanan yang dihadapi. Meskipun memiliki tujuan yang sama, yaitu menciptakan ruang siber yang aman, setiap negara mengembangkan pendekatan regulasi yang berbeda dalam mengatur keamanan siber,

pelindungan data pribadi, transaksi elektronik, maupun penegakan hukum terhadap kejahatan siber (Council of Europe, 2001; UNODC, 2013).

Perkembangan *cyber law* menunjukkan adanya variasi pendekatan antarnegara.

1. Amerika Serikat

Amerika Serikat mengembangkan kebijakan *cyber law* melalui pendekatan sektoral (*sectoral approach*), yaitu pengaturan yang tersebar dalam berbagai peraturan sesuai dengan karakteristik sektor yang diatur. Pelindungan data pribadi, misalnya, tidak diatur dalam satu undang-undang nasional yang berlaku umum, melainkan melalui berbagai regulasi sektoral seperti bidang kesehatan (*medical records*), keuangan (*financial information*), perlindungan anak (*children's information*), dan perlindungan konsumen (Data Privacy Framework Program, 2026; OECD, 2003). Pendekatan ini memberikan fleksibilitas yang tinggi dalam menyesuaikan kebutuhan masing-masing sektor, namun juga menimbulkan tantangan dalam mewujudkan standar perlindungan yang seragam.

2. Uni Eropa

Berbeda dengan Amerika Serikat yang menerapkan pendekatan sektoral (*sectoral approach*), Uni Eropa mengembangkan *cyber law* melalui pendekatan yang lebih terintegrasi dan harmonis. Kebijakan Uni Eropa dibangun berdasarkan prinsip bahwa pelindungan data pribadi dan keamanan siber merupakan bagian dari hak fundamental warga negara sekaligus prasyarat bagi terwujudnya pasar digital yang aman (*Digital Single Market*). Oleh karena itu, Uni Eropa mengembangkan kerangka regulasi yang berlaku secara seragam bagi negara-negara anggotanya melalui *General Data Protection Regulation* (GDPR) dan *Directive* (EU) 2022/2555 atau *NIS2 Directive* (European Parliament and Council of the European Union, 2022a; The European Parliament and The Council of the European Union, 2016). GDPR menetapkan standar yang tinggi mengenai pelindungan data pribadi, hak-hak subjek data, serta kewajiban pengendali dan pemroses data (The European Parliament and The Council of the European Union, 2016). Sementara itu, *NIS2 Directive* memperkuat tata kelola keamanan siber dengan mewajibkan negara anggota menyusun strategi keamanan siber nasional, menerapkan manajemen risiko siber, memperluas pelindungan

terhadap sektor-sektor kritis, serta meningkatkan mekanisme kerja sama dan pertukaran informasi antarnegara anggota Uni Eropa (European Parliament and Council of the European Union, 2022a).

Pendekatan tersebut diperkuat melalui *EU Cybersecurity Strategy for the Digital Decade* yang diterbitkan oleh European Commission dan High Representative of the Union for Foreign Affairs and Security Policy pada tahun 2020. Strategi ini menegaskan bahwa keamanan siber merupakan salah satu fondasi transformasi digital Uni Eropa, sehingga diperlukan peningkatan ketahanan siber (*cyber resilience*), perlindungan terhadap infrastruktur kritis, penguatan kapasitas respons terhadap insiden siber, serta kerja sama internasional dalam menjaga stabilitas ruang siber (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020). Melalui strategi tersebut, Uni Eropa tidak hanya berupaya membangun sistem keamanan siber yang kuat di tingkat regional, tetapi juga mendorong terbentuknya tata kelola siber global yang terbuka, aman, dan berlandaskan penghormatan terhadap hak asasi manusia.

3. Singapura

Singapura mengembangkan kebijakan *cyber law* melalui pendekatan yang mengintegrasikan keamanan siber, perlindungan infrastruktur informasi kritis, dan pelindungan data pribadi. Pendekatan tersebut tercermin dalam *Cybersecurity Act 2018*, *Personal Data Protection Act* (PDPA), serta *Singapore Cybersecurity Strategy 2021* (Attorney-General's Chambers of Singapore, 2018, 2021; Cyber Security Agency of Singapore, 2021). *Cybersecurity Act 2018* menjadi landasan hukum dalam penyelenggaraan keamanan siber dengan memberikan kewenangan kepada *Cyber Security Agency of Singapore* (CSA) untuk melindungi *Critical Information Infrastructure* (CII), melakukan pengawasan dan audit, serta mengoordinasikan penanganan insiden siber (Attorney-General's Chambers of Singapore, 2018). Sementara itu, PDPA mengatur prinsip-prinsip pelindungan data pribadi, termasuk kewajiban organisasi dalam mengelola data serta hak-hak individu atas data pribadinya (Attorney-General's Chambers of Singapore, 2021).

4. Indonesia

Dibandingkan dengan Amerika Serikat, Uni Eropa, dan Singapura, Indonesia masih mengembangkan kerangka *cyber law* melalui berbagai regulasi yang mengatur aspek keamanan siber, transaksi elektronik, dan pelindungan data pribadi. Pengaturan tersebut antara lain tercermin dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta berbagai peraturan pelaksana mengenai penyelenggaraan sistem elektronik dan keamanan siber (Republik Indonesia, 2008, 2019a, 2022a, 2024b). Selain itu, penguatan Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 28 Tahun 2021 memperkuat aspek kelembagaan dalam penyelenggaraan keamanan siber nasional (Republik Indonesia, 2021).

Berbeda dengan Uni Eropa yang telah membangun kerangka regulasi yang terintegrasi maupun Singapura yang memiliki undang-undang khusus mengenai keamanan siber, pendekatan Indonesia masih bersifat sektoral dan tersebar dalam berbagai peraturan perundang-undangan. Kondisi tersebut menunjukkan bahwa kebijakan *cyber law* di Indonesia masih berada pada tahap penguatan dan harmonisasi regulasi. Meskipun demikian, penguatan BSSN, pengesahan Undang-Undang Pelindungan Data Pribadi, serta pembaruan Undang-Undang Informasi dan Transaksi Elektronik menunjukkan komitmen pemerintah dalam membangun tata kelola ruang siber yang lebih komprehensif (Republik Indonesia, 2021, 2022a, 2024b).

Ke depan, tantangan utama yang dihadapi Indonesia adalah memperkuat koordinasi antarlembaga, meningkatkan efektivitas implementasi regulasi, serta menyesuaikan kebijakan nasional dengan perkembangan standar dan praktik internasional di bidang keamanan siber. Perbandingan tersebut menunjukkan bahwa setiap negara mengembangkan kebijakan *cyber law* sesuai dengan kebutuhan nasionalnya. Amerika Serikat menekankan fleksibilitas melalui regulasi sektoral, Uni Eropa mengedepankan harmonisasi dan perlindungan hak-hak digital, Singapura berfokus pada ketahanan infrastruktur digital nasional, sedangkan Indonesia masih berada pada tahap penguatan kerangka regulasi dan kelembagaan. Meskipun demikian, seluruh pendekatan tersebut memiliki tujuan yang sama, yaitu menciptakan keamanan, kepastian hukum, dan kepercayaan masyarakat

dalam pemanfaatan teknologi digital (Republik Indonesia, 2023a; UNODC, 2013).

Perbedaan pendekatan kebijakan tersebut sekaligus menunjukkan bahwa perkembangan *cyber law* sangat dipengaruhi oleh sistem hukum dan prioritas kebijakan masing-masing negara. Oleh karena itu, upaya membangun kerja sama internasional di bidang keamanan siber memerlukan harmonisasi berbagai kepentingan nasional agar tercipta standar global yang tetap menghormati kedaulatan hukum setiap negara (Council of Europe, 2001; United Nations General Assembly, 2024).

13.6 Tantangan Harmonisasi Hukum Siber Internasional

Harmonisasi hukum siber internasional menghadapi berbagai hambatan yang kompleks. Pertama, perbedaan sistem hukum antarnegara menyebabkan perbedaan definisi dan ruang lingkup tindak pidana siber. Perbedaan tersebut dapat terlihat pada cara setiap negara mengatur akses ilegal, penyadapan ilegal, gangguan terhadap data, penyalahgunaan perangkat, pelindungan data pribadi, serta mekanisme pembuktian elektronik (Council of Europe, 2001; UNODC, 2013). Akibatnya, suatu perbuatan yang dikategorikan sebagai tindak pidana siber di satu negara belum tentu memiliki rumusan hukum yang sama di negara lain.

Kedua, adanya perbedaan kepentingan politik dan keamanan nasional. Banyak negara menganggap ruang siber sebagai bagian dari kedaulatan negara sehingga enggan menyerahkan kewenangan tertentu kepada mekanisme internasional. Di satu sisi, setiap negara memiliki hak untuk menjaga keamanan nasional dan mengatur aktivitas digital di wilayah hukumnya. Di sisi lain, karakter ruang siber yang bersifat lintas batas menuntut adanya kerja sama, pertukaran informasi, serta harmonisasi norma agar penanganan kejahatan siber dapat berjalan efektif (United Nations General Assembly, 2018, 2024).

Ketiga, perkembangan teknologi yang sangat cepat menyebabkan hukum sering tertinggal dibandingkan inovasi teknologi. Fenomena seperti kecerdasan buatan (*artificial intelligence*), *deepfake*, *quantum computing*, dan *cryptocurrency* menghadirkan tantangan baru yang belum sepenuhnya diakomodasi oleh instrumen hukum internasional. Teknologi tersebut dapat digunakan untuk kepentingan positif, tetapi juga dapat disalahgunakan

dalam bentuk penipuan digital, manipulasi identitas, pencucian uang, serangan terhadap sistem elektronik, maupun penyebaran informasi palsu secara terstruktur (Schmitt & Flechais, 2023; United Nations General Assembly, 2024).

Keempat, terdapat perbedaan standar pelindungan data pribadi antarnegara. Uni Eropa, misalnya, menerapkan standar pelindungan data yang sangat ketat melalui *General Data Protection Regulation* (GDPR), sementara negara lain mengadopsi pendekatan yang lebih fleksibel atau sektoral (OECD, 2003; The European Parliament and The Council of the European Union, 2016). Perbedaan standar ini dapat menimbulkan hambatan dalam transfer data lintas negara, kerja sama penegakan hukum, pertukaran alat bukti elektronik, dan pengaturan tanggung jawab penyelenggara sistem elektronik.

Kelima, masalah yurisdiksi masih menjadi persoalan utama dalam penanganan kejahatan siber. Penentuan negara yang berwenang melakukan penyidikan, penuntutan, dan pemidanaan sering kali menimbulkan konflik hukum karena pelaku, korban, server, platform digital, dan alat bukti elektronik dapat berada di negara yang berbeda. Kondisi ini menyebabkan proses penegakan hukum memerlukan mekanisme kerja sama seperti bantuan hukum timbal balik (*mutual legal assistance*), ekstradisi, pertukaran informasi, dan koordinasi antarlembaga penegak hukum lintas negara (Council of Europe, 2001; Republik Indonesia, 1979, 2006).

Selain itu, harmonisasi hukum siber internasional juga menghadapi tantangan kelembagaan. Tidak semua negara memiliki kapasitas hukum, teknologi, dan sumber daya manusia yang sama dalam menghadapi ancaman siber. Negara dengan infrastruktur digital yang lebih maju umumnya memiliki kemampuan respons insiden, forensik digital, dan regulasi yang lebih kuat, sedangkan negara berkembang masih menghadapi keterbatasan dalam penegakan hukum, perlindungan infrastruktur digital, dan pengelolaan bukti elektronik. Ketimpangan kapasitas ini dapat menghambat efektivitas kerja sama internasional karena keamanan ruang siber global sangat bergantung pada kesiapan seluruh negara yang saling terhubung (United Nations General Assembly, 2018; UNODC, 2013).

Oleh karena itu, masa depan *cyber law* internasional memerlukan peningkatan kerja sama multilateral, harmonisasi standar hukum, serta penguatan prinsip tanggung jawab bersama (*shared responsibility*) dalam

tata kelola ruang siber global. Studi komparatif menunjukkan bahwa hampir semua strategi keamanan siber nasional menempatkan kerja sama internasional sebagai elemen kunci dalam menghadapi ancaman siber yang bersifat lintas batas. Dengan demikian, harmonisasi hukum siber internasional perlu diarahkan pada keseimbangan antara penghormatan terhadap kedaulatan negara, perlindungan hak asasi manusia, kepastian hukum, dan kebutuhan praktis untuk menangani kejahatan siber secara efektif (United Nations, 2005; United Nations General Assembly, 2024).

PENGANTAR HUKUM TEKNOLOGI INFORMASI

Di era digital saat ini, perkembangan teknologi seperti kecerdasan buatan (AI), e-commerce, dan fintech telah mengubah cara manusia berinteraksi secara revolusioner. Namun, di balik segala kemudahan dan efisiensi yang ditawarkan, ekosistem digital menyimpan bom waktu berupa ancaman siber yang nyata—mulai dari kebocoran data pribadi, penipuan digital, hingga pelanggaran hak cipta transnasional. Ketika dunia maya bergerak tanpa batas geografis, di manakah hukum harus berpijak untuk melindungi hak-hak Anda? Buku ini hadir sebagai kompas esensial yang menjembatani dinamika laju inovasi teknologi dengan kepastian regulasi yang mengaturnya.

Secara sistematis, buku ini mengupas tuntas kerangka hukum siber terkini, termasuk implementasi UU ITE terbaru dan UU PDP. Pembaca akan diajak mendalami pelindungan data pribadi, forensik digital, kekayaan intelektual, serta analisis kasus-kasus riil teknologi informasi yang terjadi di Indonesia.

Ditulis dengan bahasa yang lugas dan mudah dipahami, buku ini menjadi referensi wajib bagi mahasiswa, praktisi hukum, pelaku usaha digital, serta siapa saja yang ingin beraktivitas di dunia maya secara aman dan bertanggung jawab. Bersiaplah menjadi warga digital yang cerdas dan sadar hukum di era transformasi digital!

yash media.
Follow Us:
yashmedia.id
IKAPI

HUKUM
ISBN 978-634-7327-91-8
9 786347 327918