AKASA LAW CENTER

HUKUM CYBER

TANTANGAN DAN SOLUSI DI ERA DIGITAL

Editor:
Prof. Dr. Yasmirah Mandasari Saragih, S.H., M.H.
Pebi Wahyudin M. Faisal, S.A.P.

AKASA LAW CENTER

HUKUM CYBER

TANTANGAN DAN SOLUSI DI ERA DIGITAL

Sumardi Efendi, S.H.I., M.Ag.
Dr. Andi Zulfa Majida, M.H.
Dr. Joice Soraya, S.H., M.Hum.
Prof. Dr. Hamidah Abdurrachman, S.H., M.Hum.
Dr. Suci Lestari Halim, S.H., M.H.
Amirah Dwi Subarkah, S.H., M.H.
Dessy Puspita Tjahjadi
Dr. Ani Purwati, S.H., M.H.
Muhammad Arif Rahman, S.H.
Dr. Subaidah Ratna Juita, S.H., M.H.
Bagus Hermanto, S.H., M.H.

Editor:
Prof. Dr. Yasmirah Mandasari Saragih, S.H., M.H.
Pebi Wahyudin M. Faisal, S.A.P.

HUKUM CYBER

TANTANGAN DAN SOLUSI DI ERA DIGITAL

Sumardi Efendi, S.H.I., M.Ag.

Dr. Andi Zulfa Majida, M.H.

Dr. Joice Soraya, S.H., M.Hum.

Prof. Dr. Hamidah Abdurrachman, S.H., M.Hum.

Dr. Suci Lestari Halim, S.H., M.H.

Amirah Dwi Subarkah, S.H., M.H.

Dessy Puspita Tjahjadi

Dr. Ani Purwati, S.H., M.H.

Muhammad Arif Rahman, S.H.

Dr. Subaidah Ratna Juita, S.H., M.H.

Bagus Hermanto, S.H., M.H.

Editor:

Prof. Dr. Yasmirah Mandasari Saragih, S.H.

Pebi Wahyudin M. Faisal, S.A.P.

AKASA

PT. ADIKARA CIPTA AKSA

2026.0000ALC

Sumardi Efendi, S.H.I., M.Ag.; Dr. Andi Zulfa Majida, M.H. ; Dr. Joice Soraya, S.H., M.Hum.; Prof. Dr. Hamidah Abdurrachman, S.H., M.Hum.; Dr. Suci Lestari Halim, S.H., M.H.; Amirah Dwi Subarkah, S.H., M.H.; Dessy Puspita Tjahjadi; Dr. Ani Purwati, S.H., M.H.; Muhammad Arif Rahman, S.H.; Dr. Subaidah Ratna Juita, S.H., M.H.; Bagus Hermanto, S.H., M.H.

HUKUM CYBER: TANTANGAN DAN SOLUSI DI ERA DIGITAL

Cetakan ke-1, Juli 2026

Hak Penerbitan pada PT Adikara Cipta Aksa, Jakarta

Editor : Prof. Dr. Yasmirah Mandasari Saragih, S.H.
Pebi Wahyudin M. Faisal, S.A.P.
Setter : Kartika Septiani, S.H.
Desain Cover : Aretha Putri, S.H.

Dicetak di Akasa Printing

PT. ADIKARA CIPTA AKSA
Kantor Pusat
Ruko Mahkota Mas Blok C, Jl. MH Thamrin, Cikokol, Kecamatan Tangerang Kota, Kota Tangerang Banten, 15117
Telepon : (+62) 821 669 576 72 (Lim)
E-mail : adikaraciptaaksa@gmail.com – www.adikaraciptaaksa.co.id

Perpustakaan Nasional RI: Katalog Dalam Terbitan (KDT)

Hukum Cyber: Tantangan dan Solusi di Era Digital
Sumardi Efendi, S.H.I., M.Ag.; Dr. Andi Zulfa Majida, M.H. ; Dr. Joice Soraya, S.H., M.Hum.; Prof. Dr. Hamidah Abdurrachman, S.H., M.Hum.; Dr. Suci Lestari Halim, S.H., M.H.; Amirah Dwi Subarkah, S.H., M.H.; Dessy Puspita Tjahjadi; Dr. Ani Purwati, S.H., M.H.; Muhammad Arif Rahman, S.H.; Dr. Subaidah Ratna Juita, S.H., M.H.; Bagus Hermanto, S.H., M.H. Cetakan Pertama, Juli 2026. Jakarta Pusat: Adikara Cipta Aksa, 2026. 222 hlm. 1,8 cm. ISBN: 978-634-05-2349-2 (PDF)

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas terselesaikannya buku *Buku Hukum Cyber: Tantangan dan Solusi di Era Digital* ini. Perkembangan teknologi digital telah membawa perubahan besar dalam kehidupan masyarakat, sekaligus menghadirkan tantangan hukum yang semakin kompleks dan dinamis.

Buku ini disusun untuk memberikan pemahaman komprehensif mengenai prinsip, regulasi, dan praktik hukum siber, baik dalam konteks nasional maupun internasional. Berbagai isu penting seperti kejahatan siber, perlindungan data pribadi, keamanan transaksi digital, tanggung jawab platform, hingga regulasi kecerdasan buatan dibahas secara sistematis dan analitis.

Kami berharap buku ini dapat menjadi referensi yang bermanfaat bagi mahasiswa, akademisi, praktisi hukum, pembuat kebijakan, dan seluruh pihak yang berkepentingan dalam membangun sistem hukum yang adaptif dan berkeadilan di era digital.

Kami menyadari buku ini masih memiliki keterbatasan, sehingga kritik dan saran sangat kami harapkan demi penyempurnaan di masa mendatang.

Jakarta, 13 Februari 2026

Tim Penulis

DAFTAR ISI

BAB 1

PENGANTAR HUKUM SIBER DAN TRANSFORMASI DIGITAL

Sumardi Efendi, S.H.I., M.Ag.

A. Evolusi Teknologi Digital dan Dampaknya terhadap Hukum

Perkembangan teknologi digital merupakan salah satu fenomena paling revolusioner dalam sejarah peradaban manusia. Transformasi ini tidak hanya mengubah cara manusia berinteraksi, bekerja, dan mengakses informasi, tetapi juga memengaruhi struktur sosial, ekonomi, politik, dan hukum secara mendasar. Teknologi digital telah mengalami evolusi panjang, dimulai dari inovasi-inovasi sederhana dalam komputasi hingga munculnya ekosistem digital yang kompleks berbasis internet, kecerdasan buatan (*artificial intelligence*), *big data*, dan *blockchain*.[1] Perjalanan evolusi ini memunculkan tantangan baru bagi dunia hukum, yang dituntut untuk menyesuaikan kerangka peraturannya agar mampu merespons perubahan yang terjadi dengan cepat, sekaligus tetap menjaga prinsip keadilan, kepastian, dan kemanfaatan hukum.

Awal dari era digital dapat ditelusuri pada perkembangan komputer generasi pertama di pertengahan abad ke-20, yang beroperasi menggunakan tabung vakum (*vacuum tubes*) dan berukuran sangat besar.[2] Pada masa ini, komputer digunakan terbatas untuk keperluan militer dan penelitian ilmiah. Perkembangan berlanjut dengan munculnya komputer generasi kedua yang menggunakan transistor, diikuti generasi ketiga yang memanfaatkan sirkuit terpadu (*integrated circuits*), sehingga

[1]Syarifah Fitrah Ramadhani, Singularity: Interaksi Manusia Dan Mesin Dalam Teknologi Informasi (Padang: Takaza Innovatix Labs, 2024). hlm. 21.

[2] Walter Isaacson, *The Innovators: Kisah Para Peretas, Genius, Dan Maniak Yang Melahirkan Revolusi Digital* (Yogyakarta: Bentang Pustaka, 2016). hlm. 54.

ukuran perangkat menjadi lebih kecil, lebih cepat, dan lebih efisien. Lompatan besar terjadi pada generasi keempat dengan pemanfaatan mikroprosesor yang memungkinkan komputer menjadi perangkat yang relatif terjangkau untuk masyarakat umum. Transformasi ini membuka jalan bagi revolusi personal computer (PC) pada 1980-an, yang memicu digitalisasi dokumen, data, dan proses bisnis.

Era berikutnya ditandai dengan lahirnya internet pada akhir 1980-an dan awal 1990-an. Internet menghubungkan jutaan perangkat komputer di seluruh dunia, memfasilitasi pertukaran informasi secara instan dan masif. Kemunculan *World Wide Web* (WWW) menjadikan internet semakin mudah diakses, dengan konten yang dapat diakses secara grafis dan interaktif.[3] Fenomena ini melahirkan apa yang dikenal sebagai "masyarakat informasi" (*information society*), di mana informasi menjadi komoditas berharga yang dapat diproduksi, didistribusikan, dan dikonsumsi secara digital. Pada tahap ini, hubungan hukum mulai teruji oleh isu-isu baru, seperti perlindungan hak cipta digital, keamanan data, dan penyalahgunaan teknologi untuk tindak kejahatan siber.

Memasuki abad ke-21, evolusi teknologi digital mengalami percepatan luar biasa melalui konvergensi teknologi informasi, telekomunikasi, dan media. Munculnya ponsel pintar (*smartphone*) dan jaringan nirkabel berkecepatan tinggi mengubah gaya hidup manusia secara drastis. Akses internet tidak lagi terbatas pada komputer meja, melainkan berada di genggaman tangan. Media sosial, aplikasi pesan instan, dan platform berbagi konten melahirkan bentuk interaksi sosial baru yang bersifat real-time, lintas batas negara, dan melampaui batasan ruang dan waktu. Perubahan ini membawa dampak hukum yang signifikan, di antaranya perlunya regulasi terkait penyebaran informasi palsu (*hoaks*), ujaran kebencian (*hate speech*), dan perlindungan privasi pengguna.[4]

Teknologi digital juga mengalami transformasi besar melalui lahirnya *cloud computing* yang memungkinkan penyimpanan dan pengolahan data di pusat data

[3]Catur Nugroho, *Cyber Society: Teknologi, Media Baru, Dan Disrupsi Informasi* (Jakarta: Kencana, 2020). hlm. 92.

[4] Chitra Imelda et al., *Transformasi Hukum* (Padang: CV. Gita Lentera, 2025). hlm. 81.

yang terhubung secara global. Konsep ini memberikan efisiensi biaya dan fleksibilitas tinggi bagi individu maupun perusahaan, namun pada saat yang sama menimbulkan permasalahan yurisdiksi hukum. Pertanyaan mengenai siapa yang bertanggung jawab atas pelanggaran data pribadi ketika data disimpan di server lintas negara menjadi tantangan baru bagi hukum internasional dan nasional. Selain itu, teknologi big data memungkinkan pengumpulan, analisis, dan pemanfaatan data dalam skala masif, yang dapat digunakan untuk inovasi, tetapi juga rawan disalahgunakan untuk manipulasi opini publik atau profilisasi yang melanggar hak asasi manusia.

Kemajuan selanjutnya terlihat pada pengembangan *Internet of Things* (IoT), di mana berbagai perangkat fisik seperti kendaraan, peralatan rumah tangga, dan mesin industri terhubung ke internet untuk saling bertukar data. IoT membuka peluang besar dalam otomasi, efisiensi energi, dan kenyamanan hidup, tetapi juga menciptakan risiko keamanan siber yang luas. Perangkat yang terhubung dapat menjadi titik masuk bagi serangan siber yang berpotensi membahayakan keselamatan pengguna atau merugikan secara ekonomi. Hal ini mendorong pembuat kebijakan untuk mempertimbangkan regulasi keamanan perangkat dan perlindungan data yang lebih ketat.

Di sisi lain, kemunculan teknologi *blockchain* membawa paradigma baru dalam pencatatan transaksi yang terdesentralisasi dan sulit dimanipulasi. *Blockchain* menjadi fondasi bagi mata uang kripto (*cryptocurrency*) seperti Bitcoin dan Ethereum, serta berbagai aplikasi *smart contract* yang memungkinkan perjanjian otomatis tanpa perantara.[5] Meskipun memberikan transparansi dan efisiensi, penggunaan mata uang kripto juga memunculkan tantangan hukum seperti potensi pencucian uang, pendanaan terorisme, dan kesulitan dalam pengawasan transaksi lintas batas. Hal ini menuntut pembentukan regulasi yang seimbang antara mendukung inovasi teknologi dan mencegah penyalahgunaan.

Kecerdasan buatan (*artificial intelligence*/AI) dan pembelajaran mesin (*machine learning*) juga merupakan tonggak penting dalam evolusi teknologi

[5]Arkas Viddy, Erick Karunia, and Rafiqoh, *Crypto & Blockchain: Masa Depan Keuangan Global* (Padang: Takaza Innovatix Labs, 2025). hlm. 1.

digital. AI digunakan dalam berbagai sektor seperti kesehatan, keuangan, pendidikan, hingga penegakan hukum. Namun, penggunaan AI menimbulkan pertanyaan hukum yang kompleks, misalnya tentang akuntabilitas jika sistem AI membuat keputusan yang merugikan, bias algoritmik yang dapat melanggar prinsip kesetaraan, dan perlindungan terhadap hak kekayaan intelektual yang dihasilkan AI. Pengaturan yang jelas diperlukan untuk memastikan bahwa AI digunakan secara etis, aman, dan bertanggung jawab.[6]

Evolusi teknologi digital tidak hanya mengubah substansi hukum, tetapi juga memengaruhi cara hukum ditegakkan. Pemanfaatan *e-government* dan *e-court* telah mempercepat proses administrasi pemerintahan dan peradilan.[7] Sistem peradilan elektronik memungkinkan pendaftaran perkara, pembayaran biaya perkara, dan persidangan dilakukan secara daring, yang meningkatkan efisiensi dan akses terhadap keadilan. Namun, perubahan ini juga membutuhkan pembaruan kerangka hukum acara agar dapat mengakomodasi bukti digital, tandatangan elektronik, dan prosedur persidangan virtual.

Secara sosiologis, percepatan teknologi digital menimbulkan fenomena disrupsi hukum. Banyak regulasi yang lahir pada era pra-digital menjadi usang atau tidak relevan untuk mengatur perilaku di dunia maya. Sebaliknya, teknologi berkembang lebih cepat daripada proses legislasi, sehingga menciptakan kesenjangan hukum (*legal gap*).[8] Kondisi ini menuntut pendekatan hukum yang adaptif dan proaktif, termasuk pembentukan undang-undang yang bersifat teknologi-netral (*technology neutral law*) agar tetap relevan meskipun terjadi perubahan teknologi di masa depan. Selain itu, kolaborasi antara negara, sektor swasta, akademisi, dan masyarakat sipil menjadi kunci dalam merumuskan kebijakan hukum siber yang efektif.

Evolusi teknologi digital juga membawa implikasi terhadap penegakan hukum pidana. Kejahatan siber seperti peretasan, pencurian identitas, penipuan daring, dan

---

[6] Anton D. Varma, *Kecerdasan Buatan (AI) Dan Hukum Di Masa Depan: Sebuah Pengantar* (Yogyakarta: Deepublish, 2024). hlm. 2.

[7] Riris Katharina, *Pelayanan Publik & Pemerintahan Digital Indonesia* (Jakarta: Yayasan Pustaka Obor Indonesia, 2020). hlm. 11.

[8] Yose Indarta, *Cyber Law: Dimensi Hukum Dalam Era Digital* (Padang: Pustaka Galeri Mandiri, 2025). hlm. 55.

eksploitasi seksual anak secara online semakin kompleks dan lintas batas negara. Penegakan hukum memerlukan kerja sama internasional, pemahaman teknis yang memadai, dan pemanfaatan teknologi investigasi digital (*digital forensics*). [9] Tantangan terbesar adalah menemukan keseimbangan antara perlindungan keamanan publik dan penghormatan terhadap kebebasan sipil, termasuk hak atas privasi dan kebebasan berekspresi.

Dari perspektif hukum perdata, kontrak elektronik (*e-contract*) dan tanda tangan digital menjadi instrumen yang semakin umum digunakan dalam transaksi bisnis. Keabsahan, kekuatan pembuktian, dan mekanisme penyelesaian sengketa dalam kontrak elektronik memerlukan pengaturan yang jelas agar memberikan kepastian hukum.[10] Demikian pula, perlindungan konsumen dalam transaksi daring memerlukan perhatian khusus, terutama terkait kewajiban platform e-commerce dalam menjamin keamanan transaksi dan keaslian produk.

Pada bidang hukum administrasi, teknologi digital mendorong perubahan signifikan dalam pelayanan publik. Pemerintah dituntut menyediakan layanan berbasis digital yang transparan, akuntabel, dan inklusif. Namun, digitalisasi layanan publik juga menimbulkan risiko penyalahgunaan data oleh aparatur negara atau pihak ketiga. Oleh karena itu, undang-undang perlindungan data pribadi menjadi sangat penting untuk menjaga kepercayaan publik terhadap layanan digital pemerintah.

Selain itu, perkembangan teknologi digital memengaruhi dimensi etika hukum. Munculnya fenomena seperti *deepfake*, disinformasi, dan manipulasi media berbasis AI menimbulkan pertanyaan tentang batas kebebasan berekspresi, integritas informasi, dan tanggung jawab platform digital. Pembuat kebijakan dihadapkan pada dilema antara melindungi kebebasan berekspresi dan mencegah penyalahgunaan teknologi untuk tujuan yang merugikan masyarakat.

Dalam konteks global, evolusi teknologi digital memperlihatkan perlunya harmonisasi hukum antarnegara. Karena sifat teknologi yang lintas batas,

[9]Budiyanto, *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia* (Banten: PT Sada Kurnia Pustaka, 2025). hlm. 52.

[10]Yapiter Marpi, *Perlindungan Hukum Terhadap Konsumen Atas Keabsahan Kontrak Elektronik Dalam Transaksi E-Commerce* (Tasikmalaya: PT. Zona Media Mandiri, 2020). hlm. 161.

perbedaan standar hukum antar yurisdiksi dapat menghambat kerja sama penegakan hukum dan perlindungan hak. Organisasi internasional seperti Perserikatan Bangsa-Bangsa (PBB), Uni Eropa (UE), dan ASEAN mulai mengembangkan kerangka kerja sama dan standar regulasi untuk menghadapi tantangan hukum siber secara kolektif.[11] Indonesia sendiri telah merespons perkembangan ini melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Rancangan Undang-Undang Perlindungan Data Pribadi, meskipun implementasinya masih menghadapi berbagai tantangan.

Dengan demikian, evolusi teknologi digital merupakan proses yang terus berlangsung dan membawa dampak luas terhadap berbagai aspek hukum. Tantangan yang dihadapi tidak hanya bersifat teknis, tetapi juga filosofis, karena menyangkut penafsiran ulang nilai-nilai hukum dalam konteks dunia digital. Prinsip-prinsip hukum klasik seperti keadilan, kepastian, dan kemanfaatan tetap relevan, tetapi perlu diterjemahkan ke dalam kerangka yang sesuai dengan dinamika teknologi. Oleh karena itu, pengembangan hukum siber dan regulasi terkait transformasi digital harus dilakukan secara berkelanjutan, partisipatif, dan berbasis pada pemahaman mendalam terhadap perkembangan teknologi.

Akhirnya, dapat disimpulkan bahwa hukum tidak boleh tertinggal oleh teknologi. Sebaliknya, hukum harus mampu menjadi panduan yang fleksibel dan visioner, sehingga dapat mengarahkan perkembangan teknologi digital ke arah yang mendukung kemajuan peradaban, perlindungan hak asasi manusia, dan keberlanjutan sosial-ekonomi. Evolusi teknologi digital memang tak terelakkan, tetapi dampaknya terhadap hukum dapat dikelola dengan baik melalui regulasi yang adaptif, kerja sama lintas sektor, dan komitmen terhadap nilai-nilai kemanusiaan yang universal.

B. Dasar-Dasar Hukum Siber

Kemajuan teknologi digital telah membuka berbagai kemungkinan baru dalam komunikasi, transaksi, serta interaksi sosial manusia. Namun, bersamaan dengan

[11] Evi Dwi Hastri et al., *Hukum Internasional Era Society 5.0* (Sumedang: CV. Mega Press Nusantara, 2025). hlm. 15.

peluang tersebut, lahir pula tantangan besar yang tidak dapat dihindari—yaitu meningkatnya pelanggaran hukum di ruang siber.[12] Hukum tradisional yang berbasis pada dunia fisik menjadi tidak cukup lagi untuk mengatur realitas baru ini. Maka, lahirlah konsep hukum siber (*cyber law*) sebagai cabang hukum yang secara khusus menangani isu-isu hukum dalam dunia maya.

Dalam konteks ini, penting untuk memahami dasar-dasar hukum siber, mencakup pengertian, ruang lingkup, jenis-jenis pelanggaran yang diatur, serta peran regulasi nasional dan internasional dalam menegakkan hukum di era digital. Pemahaman yang komprehensif mengenai aspek-aspek ini menjadi sangat krusial agar sistem hukum dapat berjalan secara adil dan efektif dalam mengatur kehidupan masyarakat digital.

1. Pengertian dan Ruang Lingkup Hukum Siber

Hukum siber, atau *cyber law*, merupakan bidang hukum yang mengatur aktivitas di dunia maya (*cyberspace*), khususnya yang berkaitan dengan penggunaan teknologi informasi, jaringan komputer, dan internet.[13] Hukum ini mencakup segala peraturan, undang-undang, dan prinsip hukum yang berlaku untuk kegiatan yang melibatkan perangkat digital, informasi elektronik, serta komunikasi digital.

Secara umum, hukum siber mengatur berbagai aspek, mulai dari keamanan informasi, transaksi elektronik, perlindungan data pribadi, hingga pelanggaran pidana yang dilakukan melalui jaringan internet. Tujuan dari hukum siber adalah memberikan perlindungan hukum kepada individu dan entitas dalam melakukan aktivitas digital, serta menjaga keteraturan dan keadilan dalam ruang siber.[14]

Hukum siber memiliki cakupan yang sangat luas karena dunia digital sendiri terus berkembang. Berikut beberapa ruang lingkup utama dalam hukum siber:

---

[12]Widyastuti Andriyani et al., *Technology, Law And Society* (Makassar: Tohar Media, 2023). hlm. 1.

[13]Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Jakarta: Kencana, 2022). hlm. 50.

[14] Muhammad Husni Abdulah Pakarti et al., *Hukum Siber: Menyikapi Tantangan Hukum Di Era Digital* (Jambi: PT Nawala Gama Education, 2025). hlm. 26.

a. Transaksi Elektronik, mengatur legalitas dan keabsahan transaksi yang dilakukan secara digital, termasuk penggunaan tanda tangan elektronik dan kontrak digital.
b. Kejahatan Siber (*Cybercrime*), mencakup berbagai pelanggaran pidana seperti peretasan, penipuan digital, pencurian data, dan penyebaran *Malware*.
c. Perlindungan Data Pribadi, mengatur pengumpulan, penyimpanan, dan pengelolaan data pribadi oleh individu maupun korporasi agar tidak disalahgunakan.
d. Hak Kekayaan Intelektual Digital, melindungi karya intelektual dalam bentuk digital, seperti *software*, musik, video, dan konten digital lainnya dari pembajakan atau distribusi ilegal.
e. Etika dan Tanggung Jawab Pengguna Internet, termasuk dalam hal penyebaran berita bohong (hoaks), ujaran kebencian, dan *cyberbullying*.
f. Keamanan Informasi, mengatur perlindungan sistem informasi dari akses tidak sah, perusakan, dan kehilangan data akibat serangan siber.
g. Yurisdiksi dan Tata Cara Penegakan Hukum, karena internet tidak mengenal batas negara, hukum siber juga mencakup mekanisme kerja sama internasional dalam menegakkan hukum lintas batas.

2. Jenis-Jenis Pelanggaran Siber

Hukum siber muncul sebagai respons terhadap meningkatnya berbagai jenis kejahatan dan pelanggaran yang dilakukan di ruang digital. Beberapa jenis pelanggaran siber yang paling umum antara lain:

a. *Hacking* (Peretasan)

Hacking merupakan kegiatan memperoleh akses tidak sah ke dalam sistem komputer atau jaringan. Seorang hacker bisa masuk ke sistem untuk mencuri data, merusak sistem, atau mengubah informasi tanpa izin. Di banyak negara, aktivitas *hacking* dianggap sebagai pelanggaran pidana dan dapat dikenai hukuman berat.[15]

[15] Tomi Wicaksono Putra, Hamidah Abdurrachman, and Hamzani Achmad Irwan, *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking* (Pekalongan: NEM, 2023). hlm. 50.

Jenis-jenis *hacking* antara lain:

1) *White hat hacker*: Melakukan peretasan secara etis untuk tujuan keamanan.
2) *Black hat hacker*: Meretas untuk tujuan kriminal seperti pencurian data atau kerusakan sistem.
3) *Grey hat hacker*: Beroperasi di antara legal dan ilegal, seringkali dengan niat baik tetapi tanpa izin.

b. Pencurian Data

Pencurian data merupakan tindakan mengambil informasi digital secara ilegal, biasanya dari perusahaan, lembaga pemerintah, atau individu. Data yang dicuri bisa berupa data pelanggan, nomor kartu kredit, informasi login, dan lain-lain. Kasus-kasus ini sangat berbahaya karena bisa menimbulkan kerugian besar baik secara ekonomi maupun privasi.

c. *Malware* dan *Ransomware*

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, menyusup, atau mengganggu sistem komputer. Salah satu jenis *Malware* yang populer adalah *Ransomware*, yang mengenkripsi data pengguna dan meminta tebusan (ransom) untuk mengembalikannya.

d. Penipuan Online (*Phishing* dan *Scam*)

Phishing merupakan upaya untuk memperoleh data sensitif seperti kata sandi dan informasi kartu kredit dengan menyamar sebagai entitas terpercaya. Biasanya dilakukan melalui email palsu, website tiruan, atau pesan teks.

Scam adalah bentuk penipuan digital lainnya yang bertujuan memanipulasi korban agar mengirimkan uang atau data pribadi melalui tipu daya.

e. *Cyberbullying*

Cyberbullying adalah tindakan intimidasi, pelecehan, atau penghinaan yang dilakukan melalui media digital seperti media sosial, email, atau pesan instan. Dampaknya bisa sangat serius, terutama bagi anak-anak dan remaja, karena dapat menyebabkan gangguan psikologis hingga tindakan bunuh diri.

f. Penyebaran Konten Ilegal

Penyebaran konten yang melanggar hukum, seperti pornografi anak, kekerasan ekstrem, ujaran kebencian, dan berita palsu, juga termasuk dalam pelanggaran siber. Hukum siber mengatur bagaimana konten semacam ini dikendalikan dan siapa yang bertanggung jawab atas penyebarannya.

g. Pelanggaran Hak Cipta Digital

Dengan mudahnya distribusi digital, pembajakan karya intelektual menjadi sangat umum. Misalnya, pengunduhan film secara ilegal, distribusi *software* bajakan, atau penggunaan musik tanpa izin di platform digital. Pelanggaran ini berdampak serius terhadap pemilik hak cipta dan industri kreatif secara keseluruhan.

3. Peran Regulasi Nasional dan Internasional dalam Penegakan Hukum Siber

Di banyak negara, hukum siber diatur secara khusus melalui undang-undang atau peraturan tersendiri. Di Indonesia, misalnya, terdapat:

a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah beberapa kali direvisi. UU ini menjadi dasar hukum untuk mengatur transaksi digital, kejahatan siber, dan pelanggaran melalui internet.
b. Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada 2022. UU ini mengatur hak dan kewajiban dalam pengelolaan data pribadi serta sanksi bagi pelanggar.
c. Peraturan Pemerintah, Peraturan Menteri, dan Surat Edaran terkait teknis pelaksanaan hukum siber, seperti sistem tanda tangan digital, sistem keamanan informasi, dan pengawasan konten digital.

Namun, salah satu tantangan terbesar dalam penegakan hukum siber di tingkat nasional adalah keterbatasan sumber daya, baik dari segi teknologi, infrastruktur, maupun kompetensi aparat penegak hukum. Oleh karena itu, kerja sama internasional menjadi sangat penting.

Karena sifat internet yang lintas batas, hukum siber tidak bisa hanya ditegakkan secara nasional. Diperlukan standar dan kerja sama internasional untuk menjamin

efektivitasnya. Beberapa bentuk kerja sama dan regulasi internasional yang penting antara lain:

a. *Budapest Convention on Cybercrime* (2001)

Merupakan perjanjian internasional pertama yang khusus mengatur kejahatan siber. Konvensi ini memberikan kerangka kerja bagi negara-negara untuk menyelaraskan hukum nasional, meningkatkan kerja sama internasional, dan memperkuat upaya penyidikan lintas negara.

b. *General Data Protection Regulation* (GDPR) – Uni Eropa

Regulasi ini menjadi standar emas dalam perlindungan data pribadi dan menginspirasi banyak negara (termasuk Indonesia) dalam menyusun UU PDP. GDPR mengatur bagaimana data dikumpulkan, diproses, dan disimpan oleh perusahaan serta memberikan hak khusus kepada individu.

c. Interpol dan *ASEAN Cybersecurity Cooperation*

Interpol dan berbagai forum regional seperti ASEAN telah membentuk unit siber untuk memfasilitasi pertukaran informasi dan kerja sama penegakan hukum antarnegara dalam menghadapi kejahatan siber.

4. Tantangan Penegakan Hukum Siber

Meski sudah ada kerangka hukum nasional dan internasional, penegakan hukum siber menghadapi banyak kendala, antara lain:

a. Anonimitas pelaku: Pelaku kejahatan siber seringkali menggunakan identitas palsu dan teknologi penyamaran.
b. Perbedaan hukum antarnegara: Negara yang satu bisa menganggap suatu aktivitas sebagai pelanggaran, sementara negara lain tidak.
c. Kurangnya kapasitas teknis: Penegak hukum sering kali tidak memiliki kemampuan teknis memadai untuk menyelidiki dan membuktikan pelanggaran digital.
d. Kecepatan perkembangan teknologi: Perkembangan teknologi jauh lebih cepat dibandingkan proses legislasi hukum.

Hukum siber hadir sebagai jawaban atas tantangan yang dibawa oleh era digital. Dengan semakin kompleksnya aktivitas manusia di dunia maya, keberadaan kerangka hukum yang mengatur keamanan, privasi, transaksi, dan perilaku digital

menjadi sangat penting. Hukum siber mencakup berbagai aspek, mulai dari perlindungan data hingga kejahatan digital seperti peretasan dan penipuan online.[16]

Namun, hukum siber tidak dapat berdiri sendiri. Karena ruang digital tidak mengenal batas, maka dibutuhkan regulasi nasional yang kuat, disertai kerja sama internasional yang efektif. Penegakan hukum siber juga menuntut pengembangan kapasitas penegak hukum dan kesadaran masyarakat terhadap hukum digital. Dengan pendekatan yang menyeluruh, hukum siber dapat menjadi pilar penting dalam menjaga keadilan dan ketertiban di era digital.

C. Transformasi Digital di Bidang Hukum

Kemajuan teknologi digital tidak hanya berdampak pada sektor ekonomi, pendidikan, dan kesehatan, tetapi juga secara signifikan mengubah wajah sistem hukum. Transformasi digital dalam bidang hukum adalah suatu keniscayaan di tengah tuntutan efisiensi, transparansi, serta akses yang lebih luas terhadap keadilan. Digitalisasi ini mencakup berbagai aspek, mulai dari layanan hukum daring, sistem pengadilan elektronik (*e-court*), hingga penggunaan teknologi canggih seperti forensik digital dan *blockchain* dalam proses penegakan hukum.[17]

Namun, perubahan ini tidak terjadi tanpa tantangan. Penerapan teknologi dalam sistem hukum juga memunculkan berbagai isu baru yang bersifat etis, hukum, dan sosial. Oleh karena itu, penting untuk memahami bagaimana digitalisasi mengubah praktik hukum serta apa saja konsekuensi yang perlu diperhatikan ke depan.

1. Digitalisasi Layanan Hukum dan Pengadilan Elektronik (*E-court*)

a. Digitalisasi Layanan Hukum

Digitalisasi layanan hukum adalah upaya untuk menyederhanakan dan mempermudah akses masyarakat terhadap bantuan hukum dengan memanfaatkan teknologi informasi. Layanan hukum digital memungkinkan masyarakat untuk mengakses informasi hukum, berkonsultasi dengan pengacara, mengurus dokumen

[16]Kurniawan Tri Wibowo, *Aspek Hukum Dalam Dunia Digital* (Banten: Sada Kurnia Pustaka, 2025). hlm. 50.

[17]Nur Arifudin et al., *Pengantar Ilmu Hukum* (Padang: CV. Gita Lentera, 2024). hlm. 33.

hukum, bahkan mengakses bantuan hukum secara online tanpa harus bertatap muka secara fisik.[18]

Di Indonesia, sejumlah platform legal tech telah bermunculan dan menawarkan berbagai layanan hukum secara digital, seperti:

1) Konsultasi hukum online
2) Pembuatan dan validasi dokumen hukum digital
3) Pendaftaran merek dagang dan hak kekayaan intelektual secara online
4) Mediasi daring
5) Pembelajaran hukum melalui platform e-learning

Digitalisasi ini membantu menjangkau masyarakat yang sebelumnya kesulitan memperoleh layanan hukum, baik karena jarak geografis, keterbatasan biaya, atau hambatan birokrasi.

b. *E-court*: Pengadilan Elektronik

Salah satu bentuk paling signifikan dari transformasi digital di bidang hukum adalah penerapan sistem pengadilan elektronik atau *e-court*. Di Indonesia, Mahkamah Agung telah mengembangkan dan menerapkan *e-court* sejak tahun 2018 sebagai bagian dari reformasi birokrasi dan pelayanan publik.[19]

Fitur utama dari sistem *e-court* mencakup:

1) Pendaftaran perkara secara online
2) Pembayaran biaya perkara secara elektronik (*e-payment*)
3) Pemanggilan pihak melalui email atau sistem elektronik
4) Sidang secara virtual (*e-litigation*)
5) Pengunggahan dan pertukaran dokumen digital

Dengan *e-court*, proses hukum menjadi lebih efisien, hemat waktu, dan transparan. Masyarakat tidak lagi harus datang langsung ke pengadilan hanya untuk

[18]Sanusi et al., *Hukum Implikasi Teknologi Dalam Perubahan Hukum* (Malang: Literasi Nusantara Abadi Group, 2023). hlm. 37.

[19] *E Court* merupakan inovasi transformatif dalam sistem peradilan Indonesia yang diimplementasikan melalui Peraturan Mahkamah Agung (PERMA) Nomor 3 Tahun 2018 tentang Administrasi Perkaradi Pengadilan Secara Elektronik yang kemudian disempurnakan melalui PERMA Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik, dan terakhir diperbarui dengan PERMA Nomor 7 Tahun 2022 tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik.

mendaftarkan perkara atau membayar biaya perkara. Bahkan dalam kondisi pandemi seperti COVID-19, sistem *e-court* terbukti menjadi solusi efektif untuk menjaga kelangsungan proses peradilan tanpa melanggar protokol kesehatan.

Namun demikian, *e-court* juga menimbulkan tantangan, seperti kebutuhan akan infrastruktur yang memadai, pelatihan teknologi bagi hakim dan advokat, serta jaminan keamanan informasi dan data pribadi para pihak.

2. Pemanfaatan Teknologi dalam Penegakan Hukum: *Digital Forensics* dan *Blockchain*

a. *Digital Forensics* (Forensik Digital)

Forensik digital adalah cabang ilmu forensik yang berfokus pada identifikasi, pelestarian, analisis, dan presentasi bukti elektronik atau digital dalam proses hukum.[20] Dalam era digital, banyak bukti tidak lagi bersifat fisik (seperti dokumen atau barang bukti konvensional), tetapi berbentuk data digital seperti email, pesan WhatsApp, metadata, file log sistem, hingga rekaman kamera CCTV.

Forensik digital sangat penting dalam penanganan kasus-kasus seperti:

1) Kejahatan siber (*cybercrime*)
2) Penipuan berbasis internet
3) Pencurian data
4) Penyebaran konten ilegal
5) Pelacakan aktivitas ilegal melalui perangkat digital

Proses forensik digital umumnya melibatkan beberapa tahap:

1) Identifikasi: Menentukan perangkat atau media penyimpanan yang relevan.
2) Pengamanan: Menjaga integritas data agar tidak berubah.
3) Analisis: Menelusuri aktivitas digital dan menemukan pola atau bukti spesifik.
4) Dokumentasi dan pelaporan: Menyusun hasil analisis sebagai alat bukti hukum di pengadilan.

[20]M. Salim et al., *Pengantar Forensik Digital* (Agam: Yayasan Tri Edukasi Ilmiah, 2025). hlm. 81.

Kelebihan forensik digital adalah kemampuannya menelusuri jejak aktivitas digital yang tampaknya telah dihapus, serta memberikan bukti kuat dalam kasus yang sulit dibuktikan secara konvensional.[21]

b. *Blockchain* dalam Sistem Hukum

Blockchain adalah teknologi pencatatan digital yang terdistribusi, aman, dan tidak dapat diubah tanpa konsensus dari seluruh jaringan.[22] Awalnya dikenal dalam konteks *cryptocurrency* seperti Bitcoin, teknologi ini kini mulai diterapkan dalam sistem hukum karena keunggulannya dalam hal transparansi, keamanan, dan auditabilitas.

Beberapa potensi penerapan *blockchain* dalam hukum antara lain:

1) Smart contracts: Kontrak digital yang dapat dieksekusi otomatis berdasarkan ketentuan yang telah disepakati oleh para pihak.
2) Registrasi aset dan properti: Pencatatan kepemilikan properti atau barang berharga yang tidak dapat dimanipulasi.
3) Pembuktian dokumen: Menyimpan cap waktu (*timestamp*) untuk membuktikan keaslian dokumen digital.
4) Transparansi dan akuntabilitas: Dalam proses pengadaan barang publik atau lelang aset negara.

Dengan teknologi ini, sistem hukum dapat menciptakan ekosistem yang lebih transparan, efisien, dan minim korupsi. Namun, penerapannya masih menghadapi hambatan dari sisi regulasi dan pemahaman teknologi oleh para aktor hukum.

3. Tantangan Etika dan Hukum dalam Penerapan Teknologi Digital di Sistem Hukum

Meskipun transformasi digital membawa berbagai manfaat, implementasinya dalam sistem hukum juga menimbulkan tantangan serius, terutama dari aspek etika dan hukum. Berikut adalah beberapa tantangan utama:

[21]Hudan Studiawan and I. Kadek Agus Ariesta Putra, *Forensik Digital: Analisis Dan Investigasi Pada Sistem Android* (Yogyakarta: Andi, 2025). hlm. 17.

[22]Dodi Setiawan et al., *Blockchain* (Sumedang: Mega Press Nusantara, 2025). hlm. 2.

a. Privasi dan Perlindungan Data

Salah satu isu paling krusial dalam digitalisasi hukum adalah perlindungan data pribadi. Dalam sistem *e-court*, forensik digital, dan layanan hukum online, terjadi pengumpulan dan penyimpanan data pribadi yang sangat sensitif. Jika data ini bocor, disalahgunakan, atau diakses pihak tidak berwenang, maka bisa terjadi pelanggaran hak privasi individu.

Regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) menjadi sangat penting sebagai dasar hukum untuk mengatur tata kelola data digital. Namun implementasinya membutuhkan pengawasan ketat, kesiapan teknis, serta kesadaran hukum yang tinggi dari seluruh pihak terkait.

b. Ketimpangan Akses dan Kesenjangan Digital

Tidak semua masyarakat memiliki akses yang sama terhadap teknologi digital. Di wilayah terpencil atau kalangan masyarakat kurang mampu, keterbatasan akses internet, perangkat, dan literasi digital menjadi hambatan dalam mendapatkan keadilan digital.

Jika tidak diantisipasi, digitalisasi justru dapat memperbesar kesenjangan hukum antara masyarakat yang melek teknologi dan mereka yang tertinggal. Oleh karena itu, transformasi digital harus disertai dengan kebijakan inklusif, program pelatihan digital, serta pemberdayaan hukum masyarakat berbasis teknologi.

c. Netralitas Teknologi dan Potensi Bias

Meskipun teknologi sering dianggap objektif, kenyataannya banyak sistem digital yang dibangun berdasarkan algoritma atau data yang mengandung bias. Misalnya, algoritma yang digunakan dalam penilaian risiko pidana (seperti sistem predictive policing) dapat secara tidak adil mendiskriminasi kelompok tertentu.

Isu ini memunculkan tantangan etika yang besar: bagaimana memastikan teknologi hukum tidak menciptakan ketidakadilan baru? Perlu ada transparansi dalam perancangan sistem, audit berkala, dan keterlibatan publik dalam pengawasan.

4. Pertanggungjawaban Hukum dalam Sistem Otomatis

Dengan hadirnya sistem otomatis seperti *smart contract* dan AI dalam penegakan hukum, muncul pertanyaan hukum yang belum terjawab dengan jelas:

siapa yang bertanggung jawab jika terjadi kesalahan? Apakah pembuat algoritma, pemilik sistem, pengguna, atau pihak ketiga?

Kasus ini menunjukkan perlunya pembaruan dalam prinsip-prinsip tanggung jawab hukum di era digital, agar dapat mengakomodasi situasi yang tidak pernah muncul dalam sistem hukum konvensional.

5. Keamanan Siber dan Ancaman Serangan Digital

Sistem hukum digital sangat rentan terhadap serangan siber. Peretasan terhadap sistem *e-court*, penyebaran *Malware* dalam layanan hukum online, atau sabotase terhadap bukti digital dapat merusak integritas proses hukum. Oleh karena itu, sistem keamanan informasi (*cybersecurity*) yang kuat wajib diterapkan, termasuk penggunaan enkripsi, autentikasi berlapis, dan audit sistem secara berkala.

Transformasi digital dalam bidang hukum merupakan langkah penting menuju sistem hukum yang lebih efisien, transparan, dan inklusif. Digitalisasi layanan hukum, penerapan *e-court*, serta pemanfaatan teknologi seperti forensik digital dan *blockchain* membuka jalan bagi masa depan hukum yang lebih responsif terhadap kebutuhan masyarakat modern.

Namun, perubahan ini juga membawa tantangan yang tidak ringan. Perlindungan privasi, keadilan akses, netralitas teknologi, serta keamanan sistem digital harus menjadi perhatian utama dalam setiap kebijakan dan implementasi digitalisasi hukum. Tidak hanya pembuat kebijakan, tetapi juga seluruh pelaku hukum hakim, jaksa, pengacara, akademisi, dan masyarakat sipil perlu berperan aktif dalam mengawal transformasi ini agar menghasilkan sistem hukum digital yang adil, aman, dan berkelanjutan.

BAB 2

PRINSIP DAN ASAS HUKUM SIBER

Dr. Andi Zulfa Majida, M.H.

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah mengubah secara fundamental cara manusia berinteraksi, bertransaksi, bekerja, dan berpartisipasi dalam ruang publik. Transformasi digital ini melahirkan lanskap sosial baru yang ditandai oleh ketergantungan yang semakin tinggi terhadap sistem elektronik, keterhubungan lintas wilayah, serta peredaran data dalam volume yang sangat besar dan bersifat global. Di satu sisi, digitalisasi memberikan peluang signifikan bagi peningkatan efisiensi administrasi, pertumbuhan ekonomi digital, dan perluasan akses informasi. Namun di sisi lain, ruang siber juga menghadirkan potensi risiko yang kompleks, seperti kejahatan siber, ancaman terhadap privasi, manipulasi informasi, serta penyalahgunaan data pribadi. Kompleksitas ini menempatkan hukum siber sebagai bidang hukum yang paling dinamis, sekaligus menuntut hadirnya kerangka normatif yang komprehensif dan adaptif.

Sebagai bidang hukum yang relatif baru, hukum siber tidak dapat hanya bertumpu pada instrumen regulasi positif. Karakter ruang siber yang lintas batas, cepat berubah, dan kerap kali tidak sepenuhnya sesuai dengan kategori yuridis konvensional menuntut adanya dasar normatif berupa prinsip dan asas hukum yang mampu memandu pembentukan, penafsiran, serta praktik implementasinya. Prinsip dan asas tersebut berfungsi sebagai kompas normatif yang memberikan arah dalam

merespons perkembangan teknologi, sekaligus menjamin perlindungan hak asasi manusia, kepastian hukum, serta keadilan di tengah percepatan inovasi digital.

Sebagaimana ditegaskan oleh Lessig[23], "*cyberspace is a world where architecture, not traditional law, determines how people can behave*". Pernyataan ini menyoroti bahwa perilaku dalam ruang digital tidak dibatasi oleh teritori fisik, tetapi oleh kode, algoritma, dan struktur perangkat lunak yang membentuk lingkungan interaksi. Oleh karena itu, pendekatan hukum terhadap ruang siber tidak dapat disamakan sepenuhnya dengan pendekatan hukum dalam ruang fisik, melainkan harus mempertimbangkan arsitektur teknologi yang melandasinya.

Pada saat yang sama, ruang digital membuka peluang bagi munculnya bentuk-bentuk kejahatan baru. Goodman[24] menegaskan bahwa "*every new technology creates new frontiers for crime*", menunjukkan bahwa inovasi teknologi hampir selalu diikuti oleh modus pelanggaran yang semakin kompleks mulai dari peretasan, pencurian identitas, pemerasan digital, hingga serangan terhadap infrastruktur kritis dan eksploitasi data pribadi.

Kondisi tersebut juga dialami Indonesia. Meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU No. 19/2016 dan UU No. 1/2024) telah membentuk fondasi regulasi siber, perkembangan teknologi yang bergerak cepat sering kali menciptakan kesenjangan pengaturan. Svantesson[25] menekankan bahwa "*law always lags behind technological innovation*", yang menggambarkan realitas bahwa hukum bergerak secara linear sementara inovasi digital berkembang secara eksponensial.

Dalam situasi seperti ini, keberadaan prinsip dan asas hukum menjadi sangat penting. Yoo menyatakan bahwa "*principles function as the stable compass when positive laws struggle to keep pace with innovation*". Prinsip memberikan arah normatif dan memastikan bahwa pembentukan serta penerapan hukum tetap berpijak pada nilai-nilai fundamental, sekalipun teknologi terus berubah.

---

[23] Lessig, L. (1996). Reading the constitution in cyberspace. *Emory Lj*, *45*, 869.

[24] Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Anchor.

[25] Svantesson, D. J. B. (2018). Enter the quagmire–the complicated relationship between data protection law and consumer protection law. *Computer law & security review*, *34*(1), 25-36.

Dalam praktik hukum siber, prinsip-prinsip seperti legalitas, kepastian hukum, proporsionalitas, akuntabilitas, netralitas teknologi, perlindungan privasi, serta asas pembuktian elektronik menjadi landasan yang tidak hanya bersifat teoretis tetapi juga operasional. Hal ini semakin penting ketika berhadapan dengan bukti digital yang memiliki karakteristik berbeda dari bukti konvensional. Kerr.[26] Mengingatkan bahwa "digital evidence challenges traditional legal doctrines in ways that demand a rethinking of foundational principles". Tanpa fondasi normatif yang jelas, penegakan hukum siber berpotensi menimbulkan ketidakpastian, tumpang tindih kewenangan, maupun pelanggaran terhadap hak-hak dasar yang semestinya dilindungi.

B. Prinsip dan Asas dalam Hukum Siber

Pembahasan mengenai prinsip dan asas dalam hukum siber merupakan fondasi penting untuk memahami bagaimana hukum merespons dinamika ruang digital. Meskipun teknologi berkembang sangat cepat, kerangka normatif tidak boleh kehilangan orientasi nilai, karena pada akhirnya hukum bekerja untuk menjaga keadilan, kepastian, dan perlindungan hak asasi manusia.

Ronald Dworkin mengingatkan bahwa prinsip hukum tidak semata instrumen teknis, melainkan nilai moral yang menjadi landasan bagi sistem hukum. Ia menegaskan, "principles are standards that must be observed… because they are requirements of justice or fairness" Lessig.[27] Dalam konteks hukum siber yang serba cepat dan serba baru, keberadaan prinsip menjadi jangkar normatif yang memastikan bahwa inovasi teknologi tidak menggerus keadilan.

1. Pengertian Prinsip dan Asas dalam Hukum

Pemisahan antara prinsip dan asas sering kali dianggap sederhana, padahal keduanya memiliki peran normatif yang berbeda dalam sistem hukum. Prinsip berfungsi sebagai nilai dasar yang mencerminkan orientasi moral dan filosofis suatu

[26] Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Colum. L. Rev.*, *105*, 279.

[27] Lessig, L. (1996). Reading the constitution in cyberspace. *Emory Lj*, *45*, 869.

bidang hukum. Sebaliknya, asas hukum lebih bersifat teknis–operasional sebagai pedoman dalam menerapkan aturan positif.

Satjipto Rahardjo menegaskan peran sentral asas dalam sistem hukum ketika ia menyatakan bahwa "asas hukum adalah jantung dari sistem hukum, karena dari sanalah aturan hukum memperoleh makna dan arah" .[28] Dengan kata lain, asas menjadi penghubung antara nilai-nilai abstrak dalam prinsip dengan implementasi konkret dalam praktik penegakan hukum.

Dalam ruang siber, prinsip dan asas mendapatkan relevansi yang lebih besar. Lawrence Lessig mengingatkan bahwa perilaku di dunia digital tidak hanya dikendalikan oleh hukum negara, tetapi juga oleh arsitektur teknologi. Ia menyatakan "code is law".[29] Artinya, hukum siber tidak dapat dilepaskan dari cara teknologi bekerja. Prinsip dan asas diperlukan sebagai parameter normatif untuk menilai apakah desain platform, algoritma, dan mekanisme pengelolaan data telah sejalan dengan nilai keadilan.

2. Karakteristik Ruang Siber

Ruang siber memiliki karakter yang berbeda secara fundamental dari dunia fisik. Ia tidak mengenal batas geografis, memiliki struktur yang desentralistik, serta memungkinkan anonimitas yang lebih mudah dimanipulasi. Karakteristik ini mengubah cara kerja banyak konsep hukum, khususnya yurisdiksi, pertanggungjawaban, dan perlindungan privasi.

Johnson dan Post menggambarkan fenomena ini dengan sangat jelas: "*the Internet defies geographical boundaries; it is a borderless realm that cannot be governed by traditional territorial doctrines*". Pernyataan ini mencerminkan bagaimana hukum konvensional menghadapi kesulitan ketika berhadapan dengan aktivitas siber.

Ruang siber memiliki sejumlah karakter utama yang memengaruhi pembentukan prinsip dan asas hukum siber. Pertama, a-sentralisasi dan distribusi membuat internet tidak dikendalikan oleh satu otoritas tunggal. Struktur ini

[28] Rahardjo, S. (2006). *Membedah hukum progresif*. Penerbit Buku Kompas.
[29] Lessig, L. (1996). Reading the constitution in cyberspace. *Emory Lj*, *45*, 869

menantang konsep kedaulatan tradisional dan mendorong negara untuk mengembangkan model regulasi yang kolaboratif dan lintas yurisdiksi.

Kedua, kecepatan perubahan teknologi jauh melampaui kemampuan hukum untuk meresponsnya. Owen Fiss menekankan ketimpangan ini dengan menyatakan bahwa *"law is reactive, whereas technology is inherently proactive"*.[30] Akibatnya, hukum sering tertinggal ("*regulatory lag*") ketika teknologi seperti AI atau blockchain memunculkan persoalan baru.

Ketiga, anonimitas pengguna menimbulkan tantangan verifikasi dan penegakan hukum. Kerr menulis bahwa *"anonymity online complicates enforcement of traditional legal norms"*. [31] Identitas digital yang mudah dimanipulasi menyebabkan pembuktian dan atribusi menjadi lebih sulit.

Keempat**,** interkonektivitas global membuat tindakan seseorang di satu negara dapat berdampak instan di negara lain. Kondisi ini menciptakan persoalan yurisdiksi dan menuntut harmonisasi hukum lintas negara agar kejahatan siber tidak memanfaatkan celah antarwilayah.

Secara keseluruhan, karakteristik tersebut menunjukkan bahwa hukum siber memerlukan prinsip-prinsip baru yang lebih adaptif, fleksibel, dan tidak terikat pada batas-batas teritorial sebagaimana hukum konvensional.

3. Perbedaan Prinsip dan Asas dalam Hukum Siber

Dalam kerangka hukum siber, prinsip dan asas memiliki hubungan komplementer, tetapi tetap berbeda baik secara tingkat abstraksi maupun fungsi.

Henry Sidgwick memberikan analogi yang relevan dengan membedakan antara prinsip dan aturan. Ia menulis, "*principles are guides of thought, while rules are guides of action*". Jika diterapkan dalam konteks hukum siber, prinsip memberikan arah moral atau nilai dasar, sedangkan asas menjadi pedoman teknis untuk menerjemahkan nilai tersebut ke dalam tindakan konkret.

Solum menegaskan relevansi prinsip ketika aturan tertulis tidak lagi memadai akibat percepatan teknologi. Ia menyatakan, "*principles provide coherence in a*

[30] Fiss, O. (2003). *The law as it could be*. NYU Press.

[31] Kerr, L. (2017). The Legitimate Scope of Criminal Law: A Question for Legal History?. *Critical Analysis L.*, *4*, 11.

system where rules may be incomplete or outdated due to rapid technological change".[32] Pernyataan ini menegaskan bahwa hukum siber bergantung pada prinsip lebih daripada bidang hukum lain, karena perubahan teknologi sering kali mendahului keberadaan regulasi.

4. Pembentukan dan Penegakan Hukum Siber

Prinsip dan asas menjadi kerangka kontrol normatif terhadap perkembangan hukum siber, baik dalam aspek legislatif maupun penegakan hukum. Dalam pembentukan hukum, prinsip berfungsi sebagai orientasi nilai untuk menjamin bahwa regulasi digital tetap sejalan dengan asas keadilan, demokrasi, dan perlindungan HAM. Sementara itu, asas berperan mengarahkan bagaimana hukum tersebut diterapkan dalam praktik misalnya asas proporsionalitas dalam pengawasan digital atau asas keandalan sistem (reliability) dalam pengelolaan data elektronik.

Joel Reidenberg menekankan urgensi perumusan prinsip ketika ia menyatakan bahwa "*the articulation of principles is essential for shaping coherent and consistent information policy*".[33] Tanpa prinsip yang jelas, kebijakan digital akan cenderung reaktif dan tidak konsisten, bahkan bisa mengabaikan perlindungan hak-hak warga negara di ruang digital.

Dalam penegakan hukum, asas memainkan peran kritis. Misalnya: Asas proporsionalitas membatasi kewenangan penyadapan. Asas akuntabilitas digital memastikan penyelenggara sistem elektronik bertanggung jawab atas kebocoran data, Asas integritas informasi menjamin sahnya alat bukti elektronik di pengadilan, Dengan demikian, prinsip dan asas adalah instrumen penting agar hukum siber tidak jatuh pada penyalahgunaan kekuasaan atau ketidakpastian regulasi.

C. Prinsip-Prinsip Dasar dalam Hukum Siber

Prinsip-prinsip dasar dalam hukum siber berfungsi sebagai landasan etik, normatif, dan metodologis bagi negara dalam mengatur aktivitas digital yang

[32] Solum, L. B. (2019). Artificially intelligent law. *BioLaw Journal-Rivista di BioDiritto*, (1), 53-62.

[33] Reidenberg, J. R. (2005). Technology and internet jurisdiction. *University of Pennsylvania law review*, *153*(6), 1951-1974.

semakin kompleks. Dalam literatur hukum modern, prinsip-prinsip ini dipandang sebagai mekanisme untuk menjaga keseimbangan antara inovasi teknologi dan perlindungan hak asasi manusia. Mereka bukan hanya wacana akademik, tetapi pedoman praktis dalam merumuskan kebijakan publik, menyusun regulasi, serta menangani perkara-perkara kejahatan siber. Beberaoa prinsip yang berlaku yaitu:

1. Prinsip Legalitas

Prinsip legalitas merupakan pondasi utama dalam hukum pidana, termasuk hukum siber. Asas ini memastikan bahwa tidak ada perbuatan yang dapat dipidana tanpa dasar hukum yang telah ditetapkan sebelumnya. Dalam konteks dunia digital yang berubah sangat cepat, prinsip legalitas berfungsi sebagai pagar agar negara tidak menerapkan hukum secara sewenang-wenang.

Andi Hamzah secara tegas menulis bahwa "asas legalitas merupakan benteng pertama untuk mencegah kesewenang-wenangan negara". [34] Kutipan ini menegaskan pentingnya legalitas sebagai perlindungan fundamental bagi warga negara.

Di sisi lain, perkembangan teknologi kerap mengungguli kecepatan pembentukan regulasi. Lawrence Lessig menggambarkan fenomena ini secara lugas: "*the law is always running after technology, always one step behind*".[35] Pernyataan ini menunjukkan bahwa hukum siber dituntut lebih adaptif agar tidak tertinggal dari inovasi digital.

Di Indonesia, asas legalitas tercermin dalam Pasal 2 dan Pasal 3 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Tantangannya adalah bagaimana memastikan aturan tersebut tetap relevan untuk menghadapi jenis-jenis kejahatan siber baru seperti serangan AI, ransomware, hingga manipulasi data biometrik.

2. Prinsip Kepastian Hukum

Kepastian hukum sangat diperlukan agar para pelaku aktivitas digital—mulai dari individu, perusahaan, hingga pemerintah—memiliki kejelasan mengenai

[34] Hamzah, A. (2017). *Hukum Pidana Indonesia*. Sinar Grafika.
[35] Lessig, L. (1996). Reading the constitution in cyberspace. *Emory Lj*, *45*, 869

konsekuensi hukum dari tindakan mereka. Tanpa kepastian, ruang digital dapat berubah menjadi arena kriminalisasi yang tidak terprediksi.

Satjipto Rahardjo mengingatkan bahwa "hukum harus memberikan pegangan yang jelas bagi manusia, bukan membuat mereka berjalan dalam kabut"[36]. Ungkapan "kabut" ini sangat relevan dalam konteks digital ketika aturan mengenai konten ilegal, bukti elektronik, atau transaksi online sering kali ditafsirkan secara berbeda oleh aparat.

Beberapa kasus UU ITE menunjukkan bahwa ketidakpastian dapat menjadi sumber kriminalisasi berlebihan, terutama terkait pasal penghinaan atau pencemaran nama baik. Oleh sebab itu, kepastian hukum bukan hanya nilai normatif, tetapi kebutuhan praktis agar masyarakat merasa aman dalam beraktivitas di ruang digital.

3. Prinsip Proporsionalitas

Prinsip proporsionalitas menuntut adanya keseimbangan antara tujuan negara, seperti menjaga keamanan siber, dan perlindungan hak-hak warga negara. Dalam konteks ini, tindakan seperti pemblokiran konten, penyadapan, atau pembatasan platform harus dilakukan secara terukur dan berdasarkan kebutuhan yang nyata.

Cass Sunstein memberikan analogi yang sangat kuat ketika menjelaskan prinsip ini: "*proportionality is the moral logic that prevents the state from using a hammer to kill a fly*".[37] Analogi "menggunakan palu untuk membunuh lalat" menggambarkan bahaya kebijakan digital yang berlebihan dan tidak terukur.

Dalam praktik, proporsionalitas menjadi penting ketika negara melakukan pengawasan komunikasi digital atau penindakan terhadap konten bermasalah. Tindakan tersebut harus memiliki dasar hukum yang kuat, dilakukan dengan cara yang paling minimal, dan dapat diuji melalui mekanisme akuntabilitas.

4. Prinsip Netralitas Teknologi

Prinsip netralitas teknologi menuntut agar regulasi tidak bergantung pada teknologi tertentu sehingga tetap berlaku meskipun inovasi digital terus berubah.

---

[36] Rahardjo, S. (2006). *Membedah hukum progresif*. Penerbit Buku Kompas

[37] Sunstein, C. (2008). Democracy and the Internet. *Information technology and moral philosophy*, *93*.

Teknologi berkembang cepat, dan regulasi yang terlalu teknis akan cepat menjadi usang.

Bert-Jaap Koops menegaskan bahwa "*technology-neutral regulation is essential to ensure that laws survive the turbulence of innovation*".[38] Kutipan ini menekankan bahwa hukum harus bersifat generik dan fleksibel.

Pendekatan netralitas teknologi tercermin dalam UU ITE yang menggunakan istilah seperti Informasi Elektronik dan Dokumen Elektronik tanpa merujuk pada platform spesifik. Dengan begitu, undang-undang tetap dapat diterapkan, baik pada email, media sosial, big data, maupun kecerdasan buatan.

5. Prinsip Perlindungan Privasi

Privasi menjadi salah satu isu paling penting dalam hukum siber modern. Di era ketika data menjadi komoditas, kontrol atas informasi pribadi harus diberikan kepada individunya.

Helen Nissenbaum menjelaskan bahwa "*privacy is not about secrecy, but about appropriate informational flows*".[39] Dengan kata lain, privasi bukan hanya soal merahasiakan data, tetapi memastikan bahwa data mengalir sesuai konteks dan tidak disalahgunakan.

Di Indonesia, prinsip ini diterapkan melalui Undang-Undang Perlindungan Data Pribadi. Namun, tantangan muncul ketika perusahaan teknologi dan lembaga pemerintah memiliki kemampuan besar untuk memproses data. Prinsip perlindungan privasi menjadi pedoman agar pemrosesan data dilakukan secara sah, terbatas, dan transparan.

6. Asas-Asas Hukum Siber dalam Perspektif Hukum Indonesia

Asas hukum dalam konteks siber di Indonesia tidak hanya bersumber dari undang-undang, tetapi juga berkembang dari praktik, putusan pengadilan, dan dinamika sosial. Maria Farida menyebut bahwa "asas hukum adalah pikiran dasar yang berada di balik setiap aturan hukum, yang memberi arah dan makna bagi

[38] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[39] Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.

penerapannya".[40] Asas-asas inilah yang memberi "roh" pada hukum siber nasional. Beberapa asas ini antara lain:

a) Asas Akuntabilitas

Asas akuntabilitas mengharuskan setiap pelaku digital baik individu, perusahaan, maupun pemerintah untuk bertanggung jawab terhadap tindakan dan dampak penggunaan teknologi. Graham Greenleaf [41] menegaskan bahwa "*accountability ensures that data controllers cannot hide behind the complexity of digital systems to escape responsibility*". Kutipan ini menegaskan bahwa semakin kompleks sistem digital, semakin besar pula urgensi akuntabilitas.

Dalam UU Perlindungan Data Pribadi (UU No. 27/2022), asas ini tampak melalui kewajiban pengendali data untuk memastikan pemrosesan data berlangsung secara sah, transparan, dan aman.

b) Asas Kehati-hatian (*Due Care/Due Diligence*)

Asas ini menuntut setiap pengelola data dan sistem elektronik untuk memastikan bahwa setiap proses dilakukan secara hati-hati dan tidak menimbulkan kerugian. Luciano Floridi[42] mengingatkan bahwa "*negligence can cause harm at a scale unimaginable in the offline world*". Kelalaian kecil saja dapat menyebabkan kebocoran data dalam skala masif.

Asas kehati-hatian terlihat dalam kewajiban audit, manajemen risiko, penggunaan enkripsi, hingga perlindungan data pada layanan berbasis cloud.

c) Asas Keterbukaan

Asas keterbukaan bertujuan memastikan bahwa pengguna mengetahui untuk apa data mereka dikumpulkan dan bagaimana data tersebut digunakan. De Hert dan Papakonstantinou menyatakan bahwa "*transparency is the most critical gateway through which individuals understand and control the use of their personal data*". Tanpa keterbukaan, masyarakat tidak dapat mengendalikan informasi pribadinya.

---

[40] Soeprapto, M. F. I. (2018). *Ilmu Perundang-undangan 2: Proses dan Teknik Penyusunan*. PT Kanisius.

[41] Greenleaf, G. (2014). *Asian data privacy laws: trade & human rights perspectives*. Oup Oxford.

[42] Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, *27*(1), 1-3.

UU PDP menegaskan kewajiban penyelenggara sistem elektronik untuk menginformasikan tujuan pengumpulan data, jangka waktu penyimpanan, serta pihak ketiga yang terlibat.

d) Asas Keamanan

Asas keamanan adalah kewajiban untuk melindungi sistem dan data dari serangan siber. Microsoft menyebut bahwa "cybersecurity today is no longer just a technical mandate, but a fundamental legal and ethical duty for all organizations". Artinya, keamanan adalah kewajiban moral dan hukum, bukan sekadar masalah teknis. Penerapan asas keamanan tampak pada penggunaan enkripsi, otentikasi berlapis, pemantauan sistem, serta kewajiban pelaporan insiden siber.

e) Asas Kepentingan Publik

Asas ini menegaskan bahwa setiap kebijakan digital harus berpihak pada keamanan dan kesejahteraan masyarakat. Julia Powles[43] menulis bahwa "public interest must remain the compass that guides digital governance, especially when private tech actors exert immense power over public life". Dengan kata lain, regulasi harus melindungi masyarakat, bukan sekadar kepentingan komersial. Asas ini terlihat dalam kebijakan anti-hoaks, penanganan konten ilegal, dan kebijakan keamanan siber nasional.

D. Integrasi Prinsip dan Asas dalam Kebijakan dan Regulasi Siber Indonesia

Integrasi prinsip dan asas hukum siber dalam regulasi nasional merupakan langkah penting untuk memastikan bahwa perkembangan teknologi digital di Indonesia berjalan sejalan dengan nilai hak asasi manusia, keamanan nasional, dan kepentingan publik. Prinsip maupun asas yang telah dibahas pada bagian sebelumnya harus diterjemahkan ke dalam kebijakan konkret agar tidak berhenti sebagai konsep abstrak. Hal ini sejalan dengan rekomendasi Organisation for Economic Co-operation and Development (OECD), yang menegaskan bahwa "principles must be embedded into policies to ensure they guide behaviour, shape

[43] Zenz, A., & Powles, J. (2024). Resisting technological inevitability: Google Wing's delivery drones and the fight for our skies. *Philosophical Transactions A*, *382*(2285), 20240107.

enforcement, and influence organizational culture".[44] Dengan kata lain, asas hukum siber harus diintegrasikan pada seluruh tingkatan peraturan, mulai dari undang-undang hingga kebijakan teknis.

Indonesia menunjukkan perkembangan signifikan dalam dekade terakhir, terutama melalui revisi UU ITE, penerbitan Undang-Undang Perlindungan Data Pribadi (UU PDP), dan penguatan strategi keamanan siber nasional. Upaya tersebut memperlihatkan kesadaran bahwa ruang digital yang aman dan berkeadilan hanya bisa dibangun melalui regulasi yang mencerminkan asas proporsionalitas, akuntabilitas, netralitas teknologi, dan perlindungan hak privat.

1. Integrasi dalam UU ITE dan Perubahannya

UU ITE beserta dua kali revisinya (2016 dan 2024) merupakan bukti nyata integrasi asas legalitas, kepastian hukum, dan proporsionalitas. Salah satu perubahan signifikan adalah upaya mengurangi multitafsir dalam pasal pencemaran nama baik yang selama ini dianggap tidak proporsional.

Dalam kajiannya, Rohmy, A.M menyatakan bahwa "perubahan pasal-pasal sensitif dalam UU ITE merupakan usaha pemerintah untuk menata kembali prinsip proporsionalitas dan menghindari kriminalisasi yang tidak perlu".[45] Kutipan ini menunjukkan bahwa asas proporsionalitas dan keadilan substantif menjadi pertimbangan penting dalam revisi UU ITE.

Revisi lainnya juga mempertegas asas akuntabilitas dan kepastian hukum dalam penyelenggaraan sistem elektronik, khususnya terkait kewajiban penyedia platform untuk menindaklanjuti laporan masyarakat secara lebih transparan.

2. Integrasi dalam UU Perlindungan Data Pribadi (UU No. 27/2022)

Undang-Undang PDP adalah salah satu tonggak terbesar dalam sejarah hukum digital Indonesia. UU ini menjadi instrumen yang secara eksplisit membangun asas-asas penting seperti transparansi, akuntabilitas, keamanan informasi, minimalisasi data, dan pembatasan tujuan.

---

[44] Canton, H. (2021). Organisation for economic co-operation and development—OECD. In *The Europa Directory of international organizations 2021* (pp. 677-687). Routledge.

[45] Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE dalam Perspektif Perkembangan teknologi informasi dan komunikasi. *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam*, *7*(2), 309-339.

Menurut Sinta Dewi, "UU PDP menempatkan asas akuntabilitas sebagai fondasi, sebab tanpa akuntabilitas tidak mungkin terjadi perlindungan data yang efektif dan berkeadilan bagi individu". Pernyataan ini menegaskan bahwa asas-akuntabilitas tidak hanya menjadi hiasan normatif, tetapi menjadi pilar utama yang menentukan keberhasilan implementasi UU PDP.

Selain itu, asas transparansi terlihat jelas dalam kewajiban pengendali data untuk memberi tahu subjek data mengenai tujuan pengumpulan data, jangka penyimpanan, potensi risiko, hingga hak-hak mereka sebagai pemilik data. Dengan demikian, subjek data ditempatkan sebagai aktor aktif, bukan sekadar objek yang dikumpulkan datanya.

3. Integrasi dalam Kebijakan Keamanan Siber Nasional

Indonesia melalui Badan Siber dan Sandi Negara (BSSN) telah mengembangkan kerangka kebijakan keamanan siber nasional yang menegaskan pentingnya asas kehati-hatian, keamanan, dan kepentingan publik.

Dalam Laporan Tahunan Keamanan Siber Nasional, BSSN (2025) menegaskan bahwa "keamanan siber harus menjadi kewajiban bersama, bukan hanya tugas pemerintah; setiap penyelenggara sistem wajib membangun budaya keamanan sejak tahap perancangan sistem".[46] Pernyataan ini menunjukkan integrasi asas keamanan (security by design) dan asas tanggung jawab kolektif (*shared responsibility*).

Secara global, pendekatan ini sejalan dengan apa yang disampaikan oleh Kello, yang menyatakan bahwa "*cybersecurity has moved from technical concern to national security priority*".[47] Dengan demikian, integrasi asas keamanan dalam kebijakan nasional bukan hanya kebutuhan teknis, tetapi juga kebutuhan strategis negara.

4. Integrasi dalam Penegakan Hukum Siber

Penegakan hukum siber membawa tantangan tersendiri karena sifat bukti digital yang mudah berubah, mudah dipindahkan, dan sering kali tersebar di lintas

[46] Maharani, M. A., & Atman, W. (2025). Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik*, *2*(3), 344-354.

[47] Kello, L. (2017). Cyber security: gridlock and innovation.

yurisdiksi. Asas akurasi, keandalan, dan proporsionalitas menjadi sangat penting dalam proses penyidikan digital.

E Army menegaskan bahwa "*perubahan pola kejahatan menuntut perubahan asas pembuktian; bukti elektronik kini bukan lagi bukti tambahan, tetapi bukti primer dalam banyak kasus siber*".[48] Kutipan ini mencerminkan pergeseran penting dalam epistemologi penegakan hukum, di mana bukti digital kini dianggap sebagai bukti utama yang menentukan arah penegakan hukum.

Integrasi asas-asas tersebut tampak dalam penyempurnaan tata cara penyitaan, pemeriksaan, dan validasi bukti digital, termasuk penggunaan metode forensik digital yang lebih akuntabel.

5. Tantangan Integrasi Asas dalam Regulasi Nasional

Meskipun kemajuan signifikan telah dicapai, masih terdapat berbagai tantangan dalam mengintegrasikan asas hukum siber ke dalam kebijakan nasional. Tantangan utama termasuk disharmonisasi antarregulasi, perbedaan perspektif antarinstansi, rendahnya literasi digital, dan tingginya laju inovasi teknologi.

Duggan dan West mengingatkan bahwa "regulation will always lag behind innovation, but strong principles help narrow the gap".[49] Pernyataan ini sangat relevan untuk konteks Indonesia, karena pembaruan hukum sering berjalan lebih lambat dibanding perkembangan AI, Internet of Things, blockchain, hingga fenomena deepfake.

Oleh karena itu, penguatan asas hukum siber perlu dilakukan secara berkelanjutan agar regulasi nasional tetap relevan, mampu melindungi hak masyarakat, dan adaptif terhadap perkembangan teknologi global.

E. Tantangan Implementasi Prinsip dan Asas dalam Ruang Siber

Implementasi prinsip dan asas hukum dalam ruang siber menghadapi tantangan yang kompleks, terutama karena karakteristik dunia digital yang bergerak sangat cepat, dinamis, dan lintas batas. Teknologi berkembang jauh lebih cepat

[48] Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.

[49] Duggan, A. J. (2010). Roman, canon and common law in twelfth-century England: the council of Northampton (1164) re-examined. *Historical Research*, *83*(221), 379-408.

dibandingkan kemampuan hukum untuk menyesuaikan diri. Seperti dinyatakan Kerr [50], "law is always playing catch-up with technology." Ungkapan ini menggambarkan realitas bahwa inovasi digital sering muncul sebelum kerangka hukum siap mengaturnya, sehingga menimbulkan kekosongan norma, ketidakpastian hukum, dan kerentanan terhadap penyalahgunaan.

Beberapa jenis tantangan utama dalam implementasi prinsip hukum siber, baik yang berkaitan dengan aspek teknologi, kapasitas kelembagaan, hingga persoalan etika dan kesadaran public, antara lain:

1. Kesenjangan antara inovasi teknologi dan pembentukan regulasi menjadi tantangan paling mendasar. Teknologi seperti kecerdasan buatan generatif, blockchain, deepfake, serta Internet of Things berkembang dalam hitungan bulan, sedangkan pembentukan regulasi memerlukan waktu panjang dan proses politik yang tidak sederhana. Kondisi ini menimbulkan legal vacuum dan ketidakpastian bagi aparat penegak hukum maupun pelaku industri. Kerr[51] mempertegas persoalan ini dengan pernyataannya, "technology evolves at a pace that the law cannot realistically mirror, leaving gaps that criminals and opportunistic actors are quick to exploit." Pernyataan ini menunjukkan bahwa celah hukum menjadi ruang subur bagi manipulasi, penipuan, dan tindak kejahatan siber.
2. Tidak semua aparat penegak hukum memiliki kemampuan teknis yang memadai untuk menangani perkara siber. Pembuktian dalam kasus digital membutuhkan keahlian khusus seperti membaca log file, memverifikasi metadata, atau melakukan disk imaging secara forensik. Minimnya laboratorium forensik digital yang mutakhir juga memperburuk situasi. UNODC[52] menegaskan bahwa, "without adequate technical capacity, digital investigations risk being incomplete, inaccurate, or legally flawed." Tanpa dukungan teknis dan pemahaman komprehensif, asas-asas hukum seperti

[50] Kerr, L. (2017). The Legitimate Scope of Criminal Law: A Question for Legal History?. *Critical Analysis L.*, *4*, 11.

[51] ibid

[52] Citaristi, I. (2022). United Nations Office on Drugs and Crime—UNODC. In *The Europa Directory of International Organizations 2022* (pp. 248-252). Routledge.

akuntabilitas, kehati-hatian, dan keandalan bukti sulit diterapkan secara konsisten.

3. Internet memungkinkan aktivitas terjadi lintas negara secara instan. Pelaku dapat berada di negara A, server di negara B, dan korban di negara C. Sementara itu, hukum pidana tetap terikat pada batas yurisdiksi yang jelas. Prosedur kerja sama internasional seperti Mutual Legal Assistance memerlukan waktu, sehingga sering kali data digital sudah terhapus sebelum dapat diperoleh. Brenner[53] menyatakan, "cybercrime is the first form of crime that genuinely transcends territory, rendering traditional jurisdictional frameworks insufficient." Kondisi ini menuntut pendekatan yurisdiksi yang lebih fleksibel serta kerja sama internasional yang lebih kuat.
4. Tingkat literasi digital masyarakat yang masih rendah menjadi titik lemah perlindungan hukum siber. Banyak pengguna internet tidak memahami keamanan dasar seperti penggunaan kata sandi kuat, bahaya tautan mencurigakan, atau konsekuensi berbagi data pribadi secara sembarangan. Molnar dan Gill menyebutkan bahwa, "public ignorance about digital security remains one of the most exploited vulnerabilities in cybercrime." Tanpa peningkatan literasi digital, perlindungan hukum tidak dapat berjalan efektif, sekalipun regulasi sudah kuat.
5. Perkembangan kecerdasan buatan dan analisis data besar (big data) menimbulkan isu etika baru yang tidak mudah dijawab oleh instrumen hukum klasik. Banyak platform digital menggunakan algoritma black box yang tidak transparan, sehingga sulit dinilai keadilannya. UNODC menekankan bahwa, "transparency is essential to maintain public trust, especially when digital investigations involve intrusive measures." Tantangan etika inilah yang sering berbenturan dengan asas non-diskriminasi, akuntabilitas, dan keadilan dalam penggunaan teknologi.
6. Akses terhadap teknologi digital tidak merata di seluruh lapisan masyarakat. Wilayah rural tertinggal dalam hal infrastruktur internet, sementara sebagian

[53] Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. UPNE.

kelompok sosial seperti masyarakat miskin, difabel, dan lansia memiliki hambatan tambahan dalam mengakses atau memahami layanan digital. Zulkarnain[54] menyebut kesenjangan ini sebagai "tantangan sosial yang secara tidak langsung melemahkan efektivitas hukum." Kesenjangan ini membuat penerapan asas keadilan dan non-diskriminasi dalam hukum siber sulit tercapai secara menyeluruh.

F. Implementasi Prinsip dan Asas Hukum Siber dalam Berbagai Konteks Penegakan Hukum

Penerapan prinsip dan asas hukum siber dalam praktik tidak hanya menuntut penguasaan teori, tetapi juga kemampuan memahami dinamika teknologi yang berubah cepat. Di lapangan, aparat penegak hukum, regulator, dan pemangku kepentingan kerap menghadapi situasi yang memerlukan interpretasi prinsipil untuk menjawab kekosongan, ketidakjelasan, atau ketertinggalan norma. Dalam konteks inilah asas-asas hukum seperti legalitas, proporsionalitas, akuntabilitas, serta perlindungan privasi memainkan peran fundamental.

Kuner[55] mengingatkan bahwa "*principles act as a stabilizing force in an environment where technologies evolve faster than laws*". Pernyataan ini menegaskan bahwa prinsip-prinsip hukum bertindak sebagai jangkar normatif yang menjaga arah penegakan hukum ketika regulasi tertinggal dari inovasi digital yang bergerak cepat mulai dari penggunaan kecerdasan buatan, eksploitasi data biometrik, hingga ancaman serangan siber lintas negara.

Dalam konteks Indonesia, implementasi prinsip dan asas hukum siber dapat dilihat dalam beberapa sektor utama sebagaimana berikut:

[54] Aprilia, G. P., & Zulkarnain, Z. (2024). Tinjauan Hukum Pidana Islam dan Hukum Informasi dan Transaksi Elektronik terhadap Kejahatan Penagihan Pinjaman Online. *Jurnal Mediasas: Media Ilmu Syari'ah dan Ahwal Al-Syakhsiyyah*, *7*(2), 483-494.

[55] Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). The EU general data protection regulation: a commentary. *Updat. Sel. Artic.(May 4, 2021)*.

1. Penyelidikan dan Penyidikan Tindak Pidana Siber

Penyidikan terhadap tindak pidana siber menghadirkan tantangan teknis mulai dari enkripsi end-to-end, penggunaan server asing, hingga anonimitas pelaku. Di sinilah asas legalitas dan proporsionalitas perlu diterapkan secara seimbang.

Kerr (2018) menekankan bahwa "*the challenge is not merely collecting digital evidence, but ensuring that such collection respects legal limits and individual rights*".[56] Artinya, meskipun negara memiliki kewenangan untuk mengambil data, langkah tersebut harus tetap tunduk pada batas-batas hukum dan penghormatan terhadap hak asasi manusia.

Penerapan asas proporsionalitas tampak dalam mekanisme penyadapan atau permintaan data kepada penyelenggara sistem elektronik. Penggunaan upaya paksa harus dilakukan secara selektif dan berbasis kebutuhan, mengikuti prinsip necessity dan least intrusive means yang telah menjadi standar internasional, terutama setelah berkembangnya rezim perlindungan data seperti GDPR.

2. Pembuktian Elektronik di Pengadilan

Bukti elektronik hanya dapat dipercaya sejauh proses pengumpulannya dapat dipertanggungjawabkan. Karena itu, asas akuntabilitas dan integritas sistem menjadi pilar utama.

Yeboah-Boateng dan Akomea-Frimpong [57] menyatakan bahwa "*digital evidence is only as credible as the process through which it is collected, preserved, and presented*". Kutipan ini menggambarkan bahwa kesalahan kecil dalam prosedur digital forensik dapat menggugurkan barang bukti di pengadilan.

Dalam praktik di Indonesia, tantangan ini kerap muncul pada kasus penipuan online, pencemaran nama baik digital, hingga transaksi elektronik. *Chain of custody* harus terdokumentasi secara jelas sejak proses penyitaan, pemeriksaan, hingga pemaparan di persidangan. Dengan demikian, asas akuntabilitas tidak hanya menjadi tuntutan etis, tetapi prasyarat yuridis agar bukti dapat diterima hakim.

---

[56] Kerr, L. (2017). The Legitimate Scope of Criminal Law: A Question for Legal History?. *Critical Analysis L.*, *4*, 44

[57] Yeboah-Ofori, A., Yeboah-Boateng, E., & Yankson, H. G. (2019, May). Relativism digital forensics investigations model: a case for the emerging economies. In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)* (pp. 93-100). IEEE.

3. Perlindungan Privasi dalam Sistem Elektronik

Meningkatnya insiden kebocoran data seperti kasus SIM card, data e-commerce, serta data kesehatan menunjukkan bahwa perlindungan privasi masih belum optimal di Indonesia. Dalam konteks ini, asas perlindungan privasi harus diperlakukan sebagai kewajiban struktural, bukan sekadar kewajiban administratif.

Tufekci[58] menegaskan bahwa "*privacy is no longer merely an individual concern; it has become a structural requirement for functioning democracies*". Pernyataan ini menunjukkan bahwa tanpa perlindungan privasi yang memadai, kepercayaan publik terhadap institusi mudah runtuh.

Pendekatan privacy by design perlindungan sejak perancangan sistem telah menjadi standar global dan penting diterapkan oleh pengendali data di Indonesia. Meskipun belum sepenuhnya termuat dalam UU ITE, pendekatan ini kini menjadi salah satu prinsip utama dalam rezim perlindungan data modern.

4. Penanganan Hoaks, Disinformasi, dan Manipulasi Konten

Perkembangan hoaks dan disinformasi sering menimbulkan dilema antara kepastian hukum dan kebebasan berekspresi. Regulasi yang terlalu ketat dapat mengancam kebebasan berpendapat, sementara regulasi yang terlalu longgar membuka ruang bagi manipulasi informasi yang dapat merusak demokrasi.

Dalam laporan pentingnya, Bradshaw dan Howard menyatakan bahwa *"information manipulation thrives where regulatory frameworks are inconsistent or overly punitive*".[59] Dengan kata lain, kebijakan yang tidak tepat justru memicu penyalahgunaan.

Indonesia menghadapi persoalan ini dalam konteks penerapan pasal-pasal tertentu dalam UU ITE yang dianggap multitafsir. Karena itu, asas proporsionalitas dan asas kehati-hatian (due diligence) sangat diperlukan agar penegakan hukum tidak bersifat sewenang-wenang.

---

[58] Tufekci, Z. (2018). It's the (democracy-poisoning) golden age of free speech. *Wired*, *16*(01), 2018.

[59] Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media manipulation. *The computational propaganda project*, *1*, 1-26.

5. Kerja Sama Internasional dalam Penanganan Kejahatan Siber

Kejahatan siber bersifat lintas negara. Pelaku, server, dan korban sering berada di yurisdiksi berbeda. Karena itu, implementasi asas international cooperation dan asas yurisdiksi sangat penting.

Broadhurst et al menegaskan bahwa "no nation can effectively fight cybercrime alone; cooperation is not optional, it is imperative".[60] Pernyataan ini menjelaskan pentingnya kerja sama antarnegara, terutama untuk jenis kejahatan seperti phishing, fraud, dan eksploitasi seksual anak berbasis digital (CSAM).

Indonesia telah membangun kerja sama melalui INTERPOL, ASEAN Cybercrime Working Group, serta Mutual Legal Assistance Treaty (MLAT). Namun perbedaan standar hukum dan lambatnya proses birokrasi sering menghambat efektivitas implementasi asas ini.

G. Tantangan dan Prospek

Perkembangan teknologi digital yang berlangsung sangat cepat menimbulkan konsekuensi besar bagi pembentukan, penerapan, dan penegakan hukum siber di Indonesia. Ruang digital kini menjadi arena interaksi sosial, ekonomi, dan politik yang tidak lagi dibatasi dimensi fisik. Namun, transformasi ini juga menghadirkan berbagai tantangan mendasar, baik dari aspek regulasi, kelembagaan, maupun kapasitas sumber daya manusia. Di balik tantangan tersebut, terdapat pula peluang strategis untuk memperkuat prinsip dan asas hukum siber agar lebih adaptif, responsif, dan berorientasi pada perlindungan hak asasi manusia. Beberapa tantangan yang dihadapi adalah:

1. Kesenjangan antara Kecepatan Teknologi dan Pembaruan Hukum

Salah satu persoalan mendasar adalah ketimpangan antara perkembangan teknologi dan kemampuan sistem hukum dalam merespons perubahan tersebut. Inovasi seperti artificial intelligence (AI), Internet of Things (IoT), big data analytics, biometric surveillance, dan algoritma pengambilan keputusan berkembang dalam tempo yang jauh lebih cepat dibanding proses legislasi.

---

[60] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

Leenes dan Koops[61] menegaskan bahwa "*law often lags behind innovation, creating gaps that can undermine legal certainty and public trust*". Kondisi ini terlihat nyata di Indonesia, di mana sejumlah teknologi telah digunakan luas tanpa kerangka hukum yang memadai. Akibatnya, asas legalitas, kepastian hukum, dan foreseeability seringkali sulit diwujudkan secara optimal.

2. Lemahnya Infrastruktur Perlindungan Data Pribadi

Meskipun Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) tahun 2022, implementasinya masih menghadapi kendala serius. Berbagai insiden kebocoran data besar seperti kasus BPJS, SIM card, dan data kesehatan menunjukkan lemahnya standar keamanan di banyak lembaga publik maupun swasta.

O'Hara dan Hall[62] mengingatkan bahwa "*privacy is only as strong as the weakest link in the infrastructure that is supposed to protect it*". Pernyataan ini relevan dengan konteks Indonesia: satu celah keamanan dapat berdampak pada jutaan warga.

3. Keterbatasan Kapasitas Aparat Penegak Hukum

Penegakan hukum siber membutuhkan kualifikasi teknis yang tinggi, mulai dari digital forensics, traceability analysis, hingga pemahaman algoritma. Belum semua aparat memiliki kapasitas tersebut, sehingga banyak investigasi berjalan lambat atau tidak tuntas.

Wall[63] menyebutkan bahwa "*the sophistication of cybercrime continues to outpace the investigative capacity of many law enforcement agencies*". Keterbatasan ini memengaruhi implementasi asas due process of law dan prinsip akurasi dalam pembuktian.

4. Tantangan Yurisdiksi dalam Kejahatan Siber Transnasional

Karakter lintas batas ruang siber membuat yurisdiksi nasional sering tidak memadai. Server dapat berada di luar negeri, pelaku di negara lain, sementara

[61] Koops, B. J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. *International Review of Law, Computers & Technology*, *28*(2), 159-171.

[62] O'hara, K., & Hall, W. (2018). Four internets: The geopolitics of digital governance.

[63] Wall*, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1-2), 45-63.

korban berada di Indonesia. Koordinasi internasional, perbedaan sistem hukum, dan keterbatasan instrumen hukum global memperumit proses penegakan hukum.

Svantesson[64] menguraikan bahwa "jurisdiction is the Achilles' heel of cyber regulation", karena konflik yurisdiksi merupakan hambatan utama dalam kasus siber transnasional. Indonesia masih membutuhkan kerja sama internasional yang lebih sistematis, termasuk melalui MLAT dan forum global lainnya.

5. Potensi Overkriminalisasi dalam UU ITE

Beberapa pasal UU ITE, khususnya terkait pencemaran nama baik dan informasi yang dianggap meresahkan, kerap dianggap multitafsir. Ketidakjelasan ini dapat membuka ruang penyalahgunaan atau overkriminalisasi.

Rachlinski[65] mengingatkan bahwa "overbroad regulations in digital spaces risk chilling effects on freedom of expression". Tantangan ini menuntut rekonstruksi norma agar tetap melindungi masyarakat tanpa mengorbankan kebebasan berekspresi.

Walaupun berbagai tantangan masih mengemuka, terdapat peluang besar bagi Indonesia untuk memperkuat kerangka hukum siber, baik melalui reformasi regulasi, peningkatan kapasitas kelembagaan, maupun kolaborasi internasional. Beberapa prospek berikut menunjukkan arah perkembangan yang menjanjikan, seperti:

a. Regulasi Berbasis Hak (Rights-Based Digital Governance)

Arah pengaturan ruang digital global kini bergerak menuju pendekatan berbasis hak asasi manusia. Indonesia mengikuti tren ini melalui UU PDP, revisi UU ITE, dan kebijakan penyelenggara sistem elektronik yang lebih transparan.

Schwartz (2019) menekankan bahwa "a rights-based digital governance provides a normative foundation that prevents abuse and supports democratic accountability". Pendekatan ini memperkuat asas privasi, akuntabilitas, dan transparansi di ruang digital.

---

[64] Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press.

[65] Rachlinski, J. J. (2010). Evidence-based law. *Cornell L. Rev.*, *96*, 901.

b. Penguatan Standar Perlindungan Data

Implementasi UU PDP mendorong adopsi standar yang lebih ketat terkait: prinsip minimasi data, prinsip akuntabilitas, prinsip persetujuan (consent), prinsip keamanan pemrosesan data. Jika standar ini diterapkan secara konsisten, maka kualitas tata kelola data nasional dapat meningkat signifikan dan risiko kebocoran data dapat ditekan.

c. Modernisasi Penegakan Hukum melalui Digital Forensics dan AI

Investasi pada teknologi digital forensics, sistem analisis otomatis, dan pemanfaatan AI memberi peluang besar untuk meningkatkan efektivitas penegakan hukum.

Bowles dan Baer mencatat bahwa "digital forensics will increasingly rely on automation to keep up with the volume and complexity of digital evidence". Dengan modernisasi infrastruktur dan peningkatan kapasitas penyidik, proses penyelidikan akan menjadi lebih cepat dan akurat.

d. Kolaborasi Internasional yang Semakin Menguat

Kejahatan siber transnasional hanya dapat dihadapi melalui kerja sama lintas negara. Indonesia sudah aktif dalam ASEAN, INTERPOL, dan berbagai forum internasional lainnya.

Broadhurst et al [66] menegaskan bahwa "global cooperation is the only meaningful strategy to counter borderless cybercrime". Semakin kuat kolaborasi internasional, semakin efektif penerapan asas yurisdiksi dan asas kerja sama global.

e. Pengembangan Kerangka Etika Digital Nasional

Selain hukum positif, etika digital menjadi panduan moral masyarakat dalam ruang siber, terutama ketika hukum belum mengatur secara eksplisit. Etika digital dapat memperkuat asas akuntabilitas, kehati-hatian, proporsionalitas, dan perlindungan HAM.

[66] Broadhurst, K., & Gray, N. (2022). Understanding resilient places: Multi-level governance in times of crisis. *Local Economy*, *37*(1-2), 84-103.

Nissenbaum[67] menjelaskan bahwa “ethical principles often guide behavior where legal norms are silent or insufficient”. Kerangka etika digital nasional dapat menjadi pelengkap penting dalam membangun budaya hukum siber Indonesia yang sehat.

[67] Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In *The ethics of information technologies* (pp. 141-178). Routledge.

BAB 3

REGULASI KEAMANAN DAN KEJAHATAN SIBER

Dr. Joice Soraya, S.H., M.Hum.

A. Kerangka Hukum Keamanan Siber di Indonesia

Keamanan siber telah menjadi kebutuhan fundamental dalam menjaga kedaulatan digital negara di tengah pesatnya perkembangan teknologi informasi dan komunikasi. Indonesia sebagai negara dengan pengguna internet terbesar di Asia Tenggara menghadapi tantangan serius dalam membangun arsitektur hukum yang mampu memberikan perlindungan komprehensif terhadap ancaman siber yang semakin kompleks dan masif. Kerangka hukum keamanan siber di Indonesia merupakan sistem yang terintegrasi dan saling berkaitan antara berbagai peraturan perundang-undangan yang mengatur aspek teknologi, informasi, dan keamanan nasional.

Fondasi utama pengaturan keamanan siber di Indonesia dimulai dari konstitusi sebagai *grundnorm* tertinggi dalam hierarki peraturan perundang-undangan. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 memberikan legitimasi konstitusional terhadap perlindungan data pribadi dan keamanan informasi melalui Pasal 28G ayat 1 yang menjamin hak atas perlindungan diri, keluarga, kehormatan, martabat, dan harta benda, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan.[68] Interpretasi progresif terhadap ketentuan konstitusional ini mencakup pula perlindungan terhadap ancaman siber yang dapat mengancam keamanan personal maupun kolektif masyarakat dalam ruang digital.

[68] Indonesia, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G ayat (1).

Implementasi mandat konstitusional tersebut diwujudkan melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menjadi pilar utama regulasi keamanan siber di Indonesia.[69] Undang-undang ini mengatur secara komprehensif mengenai penyelenggaraan sistem elektronik yang aman, andal, dan bertanggung jawab sebagaimana diatur dalam Pasal 15 yang mewajibkan setiap penyelenggara sistem elektronik untuk menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Ketentuan ini memberikan dasar hukum bagi pemberlakuan standar keamanan siber minimal yang harus dipenuhi oleh setiap entitas yang mengelola sistem elektronik, baik sektor publik maupun privat.

Pengaturan mengenai tindak pidana siber dalam Undang-Undang Informasi dan Transaksi Elektronik mencerminkan keseriusan negara dalam menangani kejahatan di ruang digital. Pasal 30 hingga Pasal 37 mengkriminalisasi berbagai bentuk perbuatan yang mengancam keamanan siber, mulai dari akses ilegal terhadap komputer dan sistem elektronik, intersepsi ilegal, gangguan terhadap data dan sistem, penyalahgunaan perangkat dan kata sandi, hingga manipulasi data elektronik.[70] Formulasi delik-delik siber dalam undang-undang ini mengadopsi prinsip-prinsip yang terdapat dalam Konvensi Budapest tentang Kejahatan Siber tahun 2001, meskipun Indonesia belum meratifikasi konvensi tersebut secara formal.

Kompleksitas ancaman siber yang tidak hanya berdimensi kriminal tetapi juga menyangkut keamanan nasional mendorong lahirnya Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital sebagai instrumen hukum khusus yang mengatur pelindungan aset informasi strategis negara.[71] Peraturan ini mendefinisikan infrastruktur informasi vital sebagai sistem elektronik yang bersifat strategis dan apabila terganggu, rusak, atau hancur akan berdampak

[69] Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016, LN No. 251 Tahun 2016, TLN No. 5952.

[70] Ibid., Pasal 30-37.

[71] Indonesia, Peraturan Presiden tentang Pelindungan Infrastruktur Informasi Vital, Perpres No. 82 Tahun 2022.

serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan negara, serta perekonomian nasional. Pengaturan ini mencerminkan paradigma keamanan siber yang telah berkembang menjadi strategi pertahanan nasional dalam menghadapi ancaman *cyber warfare* dan *cyber terrorism*.

Perlindungan data pribadi sebagai elemen krusial dalam ekosistem keamanan siber mendapatkan legitimasi hukum yang lebih kuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.[72] Undang-undang ini mengatur secara komprehensif mengenai hak-hak subjek data, kewajiban pengendali dan prosesor data pribadi, serta mekanisme pengamanan data pribadi yang harus diimplementasikan untuk mencegah kebocoran, kerusakan, atau penyalahgunaan data. Pasal 56 undang-undang ini secara tegas mewajibkan pengendali data pribadi dan prosesor data pribadi untuk melakukan upaya yang memadai untuk melindungi data pribadi yang dikelolanya dari kehilangan, penyalahgunaan, akses tidak sah, serta pengubahan dan pengungkapan data pribadi yang tidak sah.

Koordinasi antar lembaga dalam penanganan insiden siber diatur melalui Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.[73] Badan Siber dan Sandi Negara diberikan kewenangan untuk melakukan koordinasi, integrasi, dan sinkronisasi di bidang keamanan siber dan persandian dalam rangka meningkatkan efektivitas penyelenggaraan keamanan siber nasional. Kelembagaan ini berfungsi sebagai *national cyber security authority* yang bertanggung jawab dalam perumusan kebijakan, standar, dan koordinasi penanganan insiden siber nasional.

Aspek penegakan hukum terhadap kejahatan siber memerlukan kapasitas khusus dari aparat penegak hukum mengingat karakteristik kejahatan siber yang bersifat lintas batas, tanpa jejak fisik, dan memerlukan keahlian teknis yang tinggi. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan

[72] Indonesia, Undang-Undang tentang Pelindungan Data Pribadi, UU No. 27 Tahun 2022, LN No. 163 Tahun 2022, TLN No. 6833, Pasal 56.

[73] Indonesia, Peraturan Presiden tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, Perpres No. 133 Tahun 2017.

Transaksi Elektronik mengatur secara detail mengenai standar teknis keamanan sistem elektronik, sertifikasi keamanan, dan audit sistem elektronik yang harus dipenuhi oleh penyelenggara sistem elektronik.[74] Regulasi ini memberikan panduan implementatif bagi pelaku usaha dan instansi pemerintah dalam membangun sistem elektronik yang aman dan andal sesuai dengan standar nasional dan internasional.

Sektor keuangan sebagai salah satu infrastruktur vital perekonomian memiliki regulasi keamanan siber yang lebih spesifik melalui Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.[75] Regulasi ini mewajibkan bank untuk menerapkan manajemen risiko teknologi informasi secara komprehensif termasuk di dalamnya pengelolaan keamanan siber yang mencakup aspek *confidentiality*, *integrity*, dan *availability* dari data dan sistem perbankan. Pendekatan regulasi berbasis risiko ini menunjukkan evolusi pemikiran bahwa keamanan siber bukan hanya masalah teknis tetapi merupakan bagian integral dari tata kelola korporasi yang baik.

Standarisasi keamanan siber di Indonesia juga mengacu pada Standar Nasional Indonesia yang diterbitkan oleh Badan Standardisasi Nasional. SNI ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi telah diadopsi sebagai standar nasional yang menjadi acuan bagi organisasi dalam membangun sistem manajemen keamanan informasi yang komprehensif.[76] Adopsi standar internasional ini memfasilitasi interoperabilitas dan harmonisasi praktik keamanan siber Indonesia dengan praktik global, sekaligus meningkatkan kepercayaan internasional terhadap sistem keamanan informasi yang dikelola oleh entitas Indonesia.

Meskipun Indonesia telah memiliki berbagai instrumen hukum yang mengatur keamanan siber, masih terdapat beberapa tantangan dalam implementasinya. Pertama, fragmentasi regulasi yang tersebar di berbagai peraturan perundang-

[74] Indonesia, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, PP No. 71 Tahun 2019, LN No. 185 Tahun 2019, TLN No. 6400.

[75] Otoritas Jasa Keuangan, Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, POJK No. 11/POJK.03/2022.

[76] Badan Standardisasi Nasional, Standar Nasional Indonesia tentang Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Persyaratan, SNI ISO/IEC 27001:2013.

undangan sektoral berpotensi menimbulkan inkonsistensi dan tumpang tindih kewenangan antar lembaga. Kedua, kecepatan perkembangan teknologi seringkali melampaui kecepatan pembaruan regulasi sehingga menimbulkan kekosongan hukum terhadap ancaman siber yang menggunakan teknologi terkini. Ketiga, kapasitas teknis dan pemahaman hukum siber di kalangan aparat penegak hukum dan pengadilan masih perlu ditingkatkan untuk memastikan penegakan hukum yang efektif.

Harmonisasi dan sinkronisasi berbagai regulasi keamanan siber menjadi kebutuhan mendesak untuk menciptakan sistem hukum yang koheren dan efektif. Pembentukan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber yang saat ini sedang dalam proses pembahasan diharapkan dapat menjadi solusi untuk mengintegrasikan berbagai aspek keamanan siber ke dalam satu kerangka hukum yang holistik dan komprehensif. Kerangka hukum keamanan siber Indonesia juga harus responsif terhadap dinamika geopolitik siber global dengan mempertimbangkan ratifikasi Konvensi Budapest tentang Kejahatan Siber sebagai instrumen internasional utama dalam kerjasama penanggulangan kejahatan siber lintas batas.[77]

Pengembangan kerangka hukum keamanan siber ke depan harus mengadopsi pendekatan yang holistik dan adaptif terhadap perkembangan teknologi. Prinsip regulasi berbasis risiko dan berbasis prinsip dapat menjadi pendekatan yang lebih fleksibel dan adaptif dalam menghadapi dinamika teknologi. Pendekatan multi-stakeholder yang melibatkan pemerintah, sektor swasta, akademisi, masyarakat sipil, dan komunitas teknis dalam perumusan kebijakan keamanan siber akan menghasilkan regulasi yang lebih komprehensif dan implementatif. Penguatan kelembagaan keamanan siber, peningkatan literasi keamanan siber, dan pembentukan ekosistem respons insiden siber yang tangguh menjadi faktor kritis dalam efektivitas kerangka hukum keamanan siber Indonesia di masa mendatang.

[77] Council of Europe, Convention on Cybercrime, ETS No. 185 (Budapest: Council of Europe, 2001).

B. Tipologi Kejahatan Siber dan Pengaturannya dalam Peraturan Perundang-undangan

Kejahatan siber merepresentasikan transformasi fundamental dari bentuk-bentuk kejahatan konvensional yang bermigrasi ke ruang digital sekaligus melahirkan modus operandi baru yang sama sekali tidak memiliki padanan dalam dunia fisik. Kompleksitas tipologi kejahatan siber menuntut pemahaman mendalam terhadap karakteristik, modus operandi, dan dampak yang ditimbulkan agar pengaturan hukum dapat merespons secara efektif dan proporsional. Klasifikasi kejahatan siber dalam peraturan perundang-undangan Indonesia dapat dikategorikan berdasarkan objek serangan yaitu kejahatan terhadap integritas sistem dan data, kejahatan yang memanfaatkan konten ilegal, kejahatan menggunakan teknologi sebagai instrumen tindak pidana lain, dan kejahatan yang mengancam keamanan nasional.

Akses ilegal terhadap sistem komputer merupakan bentuk paling fundamental dari kejahatan siber yang diatur dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[78] Ketentuan ini mengkriminalisasi setiap orang yang dengan sengaja dan tanpa hak mengakses komputer dan sistem elektronik milik orang lain dengan cara apapun. Rumusan delik ini mencakup berbagai bentuk aktivitas mulai dari *hacking* sederhana hingga intrusi sistem kompleks menggunakan teknik eksploitasi kerentanan keamanan. Pemidanaan diperberat apabila dilakukan terhadap sistem yang dilindungi pengaman khusus atau mengakibatkan kerugian bagi pihak lain.

Intersepsi ilegal dan gangguan terhadap data merupakan kejahatan yang menyasar kerahasiaan dan integritas informasi elektronik sebagaimana diatur dalam Pasal 31 hingga Pasal 33 Undang-Undang Informasi dan Transaksi Elektronik.[79] Intersepsi ilegal melarang penyadapan, pengubahan, atau penghentian informasi

[78] Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016, LN No. 251 Tahun 2016, TLN No. 5952, Pasal 30.

[79] Ibid., Pasal 31-33.

yang sedang ditransmisikan tanpa hak, mencakup modus seperti *eavesdropping* dan *man-in-the-middle attack*. Gangguan data mengkriminalisasi perbuatan mengubah, merusak, menghilangkan, atau membuat tidak dapat diakses data elektronik milik orang lain, termasuk serangan *defacement*, penyebaran *malware*, dan *denial of service attack*. Kejahatan ini sangat merugikan karena dapat melumpuhkan sistem elektronik dan menimbulkan kerugian ekonomi signifikan.

Penyalahgunaan perangkat dan manipulasi data diatur dalam Pasal 32A dan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik sebagai delik persiapan dan delik pemalsuan digital.[80] Pasal 32A melarang produksi, penjualan, atau kepemilikan perangkat keras atau lunak yang dirancang khusus untuk memfasilitasi kejahatan siber, termasuk kepemilikan kata sandi atau kode akses ilegal. Pasal 35 mengkriminalisasi manipulasi data dengan tujuan membuat informasi palsu terlihat otentik, menargetkan kejahatan pemalsuan digital yang digunakan untuk penipuan perbankan, pemalsuan dokumen resmi, atau manipulasi transaksi elektronik. Kriminalisasi tahap persiapan ini penting untuk mencegah kejahatan sebelum menimbulkan dampak lebih besar.

Kejahatan konten ilegal mencakup pencemaran nama baik, penyebaran konten asusila, perjudian, dan ujaran kebencian sebagaimana diatur dalam Pasal 27 dan Pasal 28 Undang-Undang Informasi dan Transaksi Elektronik.[81] Pencemaran nama baik melalui media elektronik diatur dalam Pasal 27 ayat 3 dengan mempertimbangkan karakteristik media digital yang memungkinkan penyebaran informasi secara masif dan cepat. Penyebaran konten yang melanggar kesusilaan, perjudian, penghinaan berbasis SARA, dan ancaman kekerasan juga dikriminalisasi untuk melindungi kepentingan hukum kolektif masyarakat. Penyebaran berita bohong atau *hoax* yang menimbulkan kerugian konsumen dan informasi yang menimbulkan kebencian berbasis SARA diatur dalam Pasal 28 untuk mencegah dampak negatif penyalahgunaan media digital.

Penipuan dan pemerasan siber merupakan transformasi kejahatan konvensional menggunakan modus digital yang sangat merugikan masyarakat.

[80] Ibid., Pasal 32A dan Pasal 35.
[81] Ibid., Pasal 27 dan Pasal 28.

Meskipun Undang-Undang Informasi dan Transaksi Elektronik tidak secara spesifik mengatur penipuan siber, Pasal 378 dan Pasal 372 Kitab Undang-Undang Hukum Pidana tentang penipuan dan penggelapan tetap dapat diterapkan dengan memasukkan unsur penggunaan sarana elektronik.[82] Modus penipuan siber sangat dinamis, mulai dari *phishing*, penipuan belanja daring, hingga skema investasi bodong menggunakan platform digital. Pemerasan siber seperti *ransomware attack* yang mengenkripsi data korban dan meminta tebusan dapat dijerat menggunakan Pasal 368 KUHP tentang pemerasan dengan mempertimbangkan penggunaan sarana elektronik.

Kejahatan terhadap anak dalam ruang digital mendapat pengaturan khusus mengingat kerentanan anak sebagai korban. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi dan Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak mengkriminalisasi pembuatan, penyebarluasan, dan kepemilikan materi pornografi yang melibatkan anak dengan ancaman pidana berat.[83] Eksploitasi anak secara ekonomi atau seksual termasuk melalui media elektronik, *grooming*, dan *cyberbullying* juga dilarang untuk memberikan perlindungan komprehensif bagi anak dari kejahatan siber.

Kejahatan yang mengancam keamanan nasional mencakup terorisme siber, spionase siber, dan serangan terhadap infrastruktur kritis. Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme mengatur penggunaan teknologi informasi untuk penyebaran propaganda terorisme, perekrutan dan pelatihan teroris, serta koordinasi aksi terorisme melalui media elektronik.[84] Spionase siber

---

[82] Indonesia, Kitab Undang-Undang Hukum Pidana [Wetboek van Strafrecht], diterjemahkan oleh Moeljatno (Jakarta: Bumi Aksara, 2008), Pasal 378, Pasal 372, dan Pasal 368.

[83] Indonesia, Undang-Undang tentang Pornografi, UU No. 44 Tahun 2008, LN No. 181 Tahun 2008, TLN No. 4928; Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak, UU No. 35 Tahun 2014, LN No. 297 Tahun 2014, TLN No. 5606.

[84] Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme, UU No. 5 Tahun 2018, LN No. 92 Tahun 2018, TLN No. 6216.

yang mengancam kedaulatan dan kepentingan ekonomi nasional diatur dalam Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara, mencakup aktivitas pengumpulan informasi rahasia negara atau rahasia bisnis menggunakan metode *advanced persistent threat* yang disponsori negara asing.[85]

Kejahatan sektor keuangan mencakup kejahatan perbankan elektronik, pencucian uang menggunakan mata uang kripto, dan pelanggaran hak kekayaan intelektual digital. Kejahatan perbankan elektronik dengan modus *skimming* kartu ATM, *phishing* kredensial perbankan, dan *social engineering* diatur melalui Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan yang memberikan kewenangan pengaturan dan pengawasan keamanan sistem perbankan.[86] Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang mengantisipasi penggunaan teknologi dalam pencucian uang dengan memasukkan penyelenggara jasa keuangan berbasis teknologi sebagai pihak pelapor.[87] Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta mengatur perlindungan ciptaan dalam format digital dan melarang distribusi ilegal konten berhak cipta melalui internet dengan mekanisme *notice and takedown*.[88]

Kesenjangan antara tipologi kejahatan siber yang terus berkembang dengan pengaturan hukum yang ada menimbulkan tantangan serius dalam penegakan hukum. Modus kejahatan siber baru seperti *deepfake*, manipulasi algoritma, kejahatan berbasis kecerdasan buatan, dan eksploitasi teknologi *blockchain* belum diatur secara eksplisit dalam peraturan perundang-undangan. Fleksibilitas interpretasi hukum pidana diperlukan untuk menangani kejahatan baru dengan tetap menghormati asas legalitas dan kepastian hukum. Pembaruan legislasi secara berkala menjadi kebutuhan mendesak untuk memastikan hukum pidana siber tetap

[85] Indonesia, Undang-Undang tentang Intelijen Negara, UU No. 17 Tahun 2011, LN No. 52 Tahun 2011, TLN No. 5218.

[86] Indonesia, Undang-Undang tentang Otoritas Jasa Keuangan, UU No. 21 Tahun 2011, LN No. 111 Tahun 2011, TLN No. 5253.

[87] Indonesia, Undang-Undang tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, UU No. 8 Tahun 2010, LN No. 122 Tahun 2010, TLN No. 5164.

[88] Indonesia, Undang-Undang tentang Hak Cipta, UU No. 28 Tahun 2014, LN No. 266 Tahun 2014, TLN No. 5599.

relevan dan efektif dalam menghadapi perkembangan teknologi dan modus kejahatan yang terus berevolusi.

C. Mekanisme Penegakan Hukum Terhadap Kejahatan Siber

Penegakan hukum terhadap kejahatan siber memerlukan mekanisme khusus yang berbeda dengan penegakan hukum konvensional mengingat karakteristik unik dari kejahatan di ruang digital. Sifat kejahatan siber yang tidak mengenal batas teritorial, meninggalkan jejak digital yang mudah dihapus, memerlukan keahlian teknis tinggi, serta melibatkan yurisdiksi multipel menuntut adaptasi sistem peradilan pidana agar dapat merespons secara efektif. Mekanisme penegakan hukum kejahatan siber di Indonesia mencakup tahapan penyelidikan dan penyidikan, penuntutan, pemeriksaan di pengadilan, hingga eksekusi putusan dengan memperhatikan kekhususan alat bukti elektronik dan prosedur hukum acara yang disesuaikan dengan konteks digital.

Penyelidikan dan penyidikan kejahatan siber dilakukan oleh Kepolisian Negara Republik Indonesia melalui Direktorat Tindak Pidana Siber Bareskrim Polri sebagai leading sector dengan didukung unit-unit siber di tingkat Polda dan Polres. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan kewenangan khusus kepada penyidik untuk melakukan penyelidikan dan penyidikan terhadap tindak pidana di bidang teknologi informasi dengan kewenangan penangkapan, penahanan, penggeledahan, dan penyitaan terhadap sistem elektronik.[89] Pasal 43 undang-undang ini memperluas konsep alat bukti untuk mengakomodasi informasi elektronik, dokumen elektronik, hasil cetak informasi elektronik, dan hasil cetak dokumen elektronik sebagai alat bukti yang sah di samping alat bukti konvensional dalam Kitab Undang-Undang Hukum Acara Pidana.[90]

[89] Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016, LN No. 251 Tahun 2016, TLN No. 5952, Pasal 42.

[90] Ibid., Pasal 43.

Forensik digital memegang peranan krusial dalam mengungkap kejahatan siber karena proses pengumpulan, preservasi, analisis, dan presentasi bukti elektronik harus dilakukan sesuai standar ilmiah yang dapat dipertanggungjawabkan di pengadilan. Kepolisian Republik Indonesia telah membentuk Pusat Laboratorium Forensik Digital yang dilengkapi dengan perangkat dan personel terlatih dalam melakukan pemeriksaan forensik terhadap berbagai jenis perangkat elektronik.[91] Proses forensik digital meliputi identifikasi barang bukti, akuisisi data dengan metode yang memastikan integritas data original tetap terjaga, analisis data untuk menemukan jejak digital yang relevan, dan pembuatan laporan forensik sebagai alat bukti. Chain of custody atau rantai penjagaan barang bukti harus dijaga ketat untuk memastikan barang bukti elektronik tidak mengalami perubahan yang dapat menggugurkan nilai pembuktiannya.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur tata cara permintaan informasi elektronik dan dokumen elektronik kepada penyelenggara sistem elektronik dalam rangka penegakan hukum.[92] Penyidik dapat meminta penyelenggara sistem elektronik untuk memberikan informasi yang tersimpan dalam sistem elektroniknya atau informasi yang dikirim atau diterima oleh sistem yang dioperasikannya. Kewajiban penyelenggara sistem elektronik untuk memberikan data kepada penyidik harus diimbangi dengan perlindungan terhadap privasi dan kerahasiaan data pengguna yang tidak terkait dengan perkara yang diselidiki. Kendala teknis seperti enkripsi data, penggunaan jaringan anonim, dan teknik anti-forensik seringkali menghambat proses penyidikan sehingga diperlukan investasi berkelanjutan dalam peningkatan kapasitas teknis dan pengadaan peralatan forensik yang canggih.

Penuntutan perkara kejahatan siber dilakukan oleh Kejaksaan Republik Indonesia setelah berkas perkara dinyatakan lengkap. Jaksa penuntut umum harus memiliki pemahaman memadai tentang teknologi informasi agar dapat menyusun

[91] Kepolisian Negara Republik Indonesia, Peraturan Kapolri tentang Tata Cara Penanganan Barang Bukti Digital, Perkap No. 10 Tahun 2021.

[92] Indonesia, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, PP No. 71 Tahun 2019, LN No. 185 Tahun 2019, TLN No. 6400, Pasal 83-87.

dakwaan yang tepat dan melakukan pembuktian efektif di persidangan.[93] Tantangan utama dalam penuntutan adalah menerjemahkan bukti-bukti teknis yang kompleks ke dalam narasi hukum yang dapat dipahami oleh majelis hakim yang mungkin tidak memiliki latar belakang teknis mendalam. Pasal 5 ayat 1 Undang-Undang Informasi dan Transaksi Elektronik menyatakan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah sebagai perluasan dari alat bukti konvensional.[94] Pembuktian dengan bukti elektronik memerlukan verifikasi autentisitas, integritas, dan reliabilitas data elektronik dengan bantuan keterangan ahli forensik digital untuk menjelaskan kepada majelis hakim mengenai bagaimana bukti elektronik diperoleh, dianalisis, dan kesimpulan yang dapat ditarik.

Permasalahan yurisdiksi menjadi tantangan signifikan dalam penegakan hukum kejahatan siber mengingat sifat internet yang borderless. Pasal 2 Undang-Undang Informasi dan Transaksi Elektronik mengatur asas yurisdiksi ekstrateriorial dimana undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum baik di dalam maupun di luar wilayah Indonesia yang memiliki akibat hukum di Indonesia atau merugikan kepentingan Indonesia.[95] Prinsip yurisdiksi ini memberikan dasar hukum bagi penegakan hukum Indonesia terhadap kejahatan siber yang dilakukan dari luar negeri tetapi pelaksanaannya menghadapi kendala praktis karena memerlukan kerjasama internasional dalam penangkapan pelaku dan pengumpulan bukti di yurisdiksi negara lain.

Kerjasama internasional dalam penegakan hukum kejahatan siber dilakukan melalui mekanisme bantuan hukum timbal balik atau mutual legal assistance dan ekstradisi. Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Hukum Timbal Balik dalam Masalah Pidana memberikan landasan hukum bagi Indonesia untuk melakukan kerjasama dengan negara lain dalam penyidikan, penuntutan, dan pemeriksaan perkara pidana termasuk kejahatan siber.[96] Mekanisme ini

[93] Kejaksaan Republik Indonesia, Peraturan Jaksa Agung tentang Tata Cara Penanganan Perkara Pidana Siber, Perja No. 15 Tahun 2020.

[94] Indonesia, UU No. 19 Tahun 2016, Pasal 5 ayat (1).

[95] Ibid., Pasal 2.

[96] Indonesia, Undang-Undang tentang Bantuan Hukum Timbal Balik dalam Masalah Pidana, UU No. 1 Tahun 2006, LN No. 18 Tahun 2006, TLN No. 4607.

memungkinkan penyidik Indonesia meminta bantuan negara lain untuk melakukan penggeledahan, penyitaan, atau pemblokiran aset digital yang berada di yurisdiksi negara tersebut. Namun proses bantuan hukum timbal balik seringkali memakan waktu lama dan terkendala oleh perbedaan sistem hukum antar negara.

Peranan Badan Siber dan Sandi Negara dalam penegakan hukum mencakup koordinasi dan dukungan teknis kepada aparat penegak hukum. Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara memberikan kewenangan kepada BSSN untuk melakukan deteksi, pemberian peringatan dini, dan penanganan insiden siber yang mengancam keamanan siber nasional.[97] BSSN bekerja sama dengan Kepolisian, Kejaksaan, dan instansi terkait dalam mengkoordinasikan respons terhadap insiden siber berskala nasional dan memberikan dukungan teknis analisis forensik kepada aparat penegak hukum.

Mekanisme pemblokiran konten ilegal menjadi instrumen penting dalam pencegahan dan penindakan kejahatan siber. Peraturan Pemerintah Nomor 71 Tahun 2019 mengatur kewenangan Menteri Komunikasi dan Informatika untuk melakukan pemblokiran terhadap informasi elektronik yang memiliki muatan yang melanggar ketentuan peraturan perundang-undangan terhadap situs perjudian, pornografi, konten terorisme, atau layanan yang memfasilitasi kejahatan.[98] Mekanisme ini efektif sebagai langkah preventif namun menghadapi kritik terkait potensi penyalahgunaan untuk membatasi kebebasan berekspresi dan kurangnya transparansi dalam proses pemblokiran.

Perlindungan korban dan saksi dalam perkara kejahatan siber diatur dalam Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban yang memberikan hak-hak kepada korban untuk mendapatkan perlindungan fisik dan psikis, kerahasiaan identitas, dan kompensasi atas kerugian yang diderita.[99] Restitusi dan

[97] Indonesia, Peraturan Presiden tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, Perpres No. 133 Tahun 2017, Pasal 10.

[98] Indonesia, PP No. 71 Tahun 2019, Pasal 97-100.

[99] Indonesia, Undang-Undang tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, UU No. 31 Tahun 2014, LN No. 293 Tahun 2014, TLN No. 5602.

kompensasi bagi korban kejahatan siber masih menjadi permasalahan karena banyak putusan pengadilan yang tidak memerintahkan pembayaran ganti rugi meskipun kerugian korban sangat besar. Pasal 38 Undang-Undang Informasi dan Transaksi Elektronik mengatur kemungkinan gugatan perdata atas kerugian yang ditimbulkan, namun proses terpisah dari proses pidana dan memerlukan waktu serta biaya tambahan.[100]

Tantangan dalam penegakan hukum kejahatan siber berkaitan dengan keterbatasan sumber daya baik jumlah personel terlatih, peralatan forensik memadai, maupun anggaran untuk penanganan perkara yang memerlukan biaya tinggi. Rasio antara jumlah penyidik siber dengan jumlah laporan kejahatan siber sangat tidak berimbang sehingga banyak kasus tidak dapat ditangani optimal.[101] Investasi dalam pembangunan kapasitas aparat penegak hukum, pengadaan teknologi forensik, dan pembentukan ekosistem penegakan hukum yang terintegrasi antara Kepolisian, Kejaksaan, Pengadilan, dan lembaga terkait menjadi prioritas untuk meningkatkan efektivitas penegakan hukum kejahatan siber. Mekanisme penegakan hukum yang adaptif, didukung sumber daya memadai, dan terintegrasi dengan kerjasama internasional akan menjadi kunci keberhasilan Indonesia dalam memerangi kejahatan siber yang terus berkembang.

D. Harmonisasi Regulasi Siber Nasional dan Konvensi Internasional

Harmonisasi regulasi siber nasional dengan konvensi internasional merupakan kebutuhan mendesak dalam menghadapi realitas kejahatan siber yang bersifat transnasional dan tidak mengenal batas yurisdiksi negara. Karakteristik ruang siber yang borderless menuntut adanya kesamaan pemahaman dan pendekatan hukum antar negara agar penegakan hukum dapat berjalan efektif melalui mekanisme kerjasama internasional. Harmonisasi hukum tidak berarti penyeragaman total sistem hukum nasional dengan standar internasional, melainkan proses penyesuaian

[100] Indonesia, UU No. 19 Tahun 2016, Pasal 38.

[101] Bareskrim Polri, Laporan Tahunan Direktorat Tindak Pidana Siber Tahun 2022 (Jakarta: Kepolisian Negara Republik Indonesia, 2023), 45-58.

substansi hukum nasional dengan prinsip-prinsip dan norma-norma internasional yang telah disepakati sambil tetap menghormati kedaulatan dan kekhasan sistem hukum masing-masing negara. Indonesia perlu melakukan harmonisasi regulasi siber nasionalnya dengan berbagai instrumen hukum internasional untuk memfasilitasi kerjasama penegakan hukum lintas batas dan meningkatkan kredibilitas sistem hukum siber nasional di mata komunitas internasional.

Konvensi Budapest tentang Kejahatan Siber tahun 2001 merupakan instrumen hukum internasional pertama dan paling komprehensif yang mengatur mengenai kejahatan siber dan kerjasama internasional dalam penanganannya. Konvensi yang diinisiasi oleh Dewan Eropa ini telah diratifikasi oleh 68 negara dan menjadi standar global dalam pengaturan kejahatan siber. Konvensi Budapest mengklasifikasikan kejahatan siber ke dalam empat kategori utama yaitu kejahatan terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer; kejahatan terkait komputer seperti pemalsuan dan penipuan; kejahatan terkait konten seperti pornografi anak; dan pelanggaran hak cipta dan hak terkait. Konvensi ini juga mengatur kewenangan prosedural dalam penyidikan kejahatan siber termasuk preservasi data, penggeledahan dan penyitaan data komputer, intersepsi komunikasi elektronik, dan yurisdiksi. Aspek kerjasama internasional diatur mencakup ekstradisi, bantuan hukum timbal balik, dan pembentukan jaringan kontak dua puluh empat jam untuk respons cepat terhadap permintaan bantuan dalam penanganan insiden siber.

Indonesia hingga saat ini belum meratifikasi Konvensi Budapest meskipun substansi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah banyak mengadopsi prinsip-prinsip yang terdapat dalam konvensi tersebut. Pengaturan mengenai akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat dalam Undang-Undang Informasi dan Transaksi Elektronik sejalan dengan ketentuan Pasal 2 hingga Pasal 6 Konvensi Budapest. Keselarasan substansi ini menunjukkan bahwa Indonesia secara de facto telah menerapkan standar internasional dalam regulasi kejahatan siber meskipun belum terikat secara de jure melalui ratifikasi formal.

Pertimbangan untuk meratifikasi Konvensi Budapest menghadapi beberapa kendala politik dan yuridis. Pertama, kekhawatiran bahwa ratifikasi akan membuka akses terlalu luas bagi penegak hukum asing untuk mengakses data yang tersimpan di server Indonesia tanpa kontrol yang memadai. Kedua, ketentuan mengenai akses lintas batas terhadap data yang tersimpan dalam komputer sebagaimana diatur dalam Pasal 32 Konvensi Budapest dianggap berpotensi melanggar kedaulatan negara dan privasi warga negara Indonesia. Ketiga, Konvensi Budapest tidak secara spesifik mengatur mengenai perlindungan terhadap serangan siber yang disponsori negara atau cyber warfare yang menjadi ancaman serius bagi keamanan nasional Indonesia. Keempat, proses ratifikasi memerlukan political will yang kuat dari pemerintah dan persetujuan DPR yang hingga saat ini belum menjadi prioritas dalam agenda legislasi nasional.

Meskipun belum meratifikasi Konvensi Budapest, Indonesia aktif dalam berbagai forum kerjasama regional dan internasional dalam penanggulangan kejahatan siber. Association of Southeast Asian Nations telah mengembangkan ASEAN Cybersecurity Cooperation Strategy yang bertujuan meningkatkan kapasitas negara-negara anggota dalam menghadapi ancaman siber dan memfasilitasi kerjasama dalam penanganan insiden siber lintas batas. ASEAN Computer Emergency Response Team juga telah dibentuk sebagai mekanisme koordinasi regional dalam respons terhadap insiden siber yang mempengaruhi multiple negara anggota. Perserikatan Bangsa-Bangsa melalui United Nations Office on Drugs and Crime aktif dalam mendorong harmonisasi hukum kejahatan siber global melalui berbagai program capacity building dan fasilitasi dialog antar negara. Pada tahun 2019, Majelis Umum PBB membentuk Ad Hoc Committee untuk merumuskan konvensi internasional yang komprehensif mengenai penanggulangan kejahatan siber yang diharapkan dapat menjadi instrumen hukum global yang lebih inklusif.

Harmonisasi regulasi siber Indonesia dengan standar internasional juga mencakup aspek perlindungan data pribadi. General Data Protection Regulation yang diberlakukan Uni Eropa sejak tahun 2018 telah menjadi standar global dalam perlindungan data pribadi dan mempengaruhi perkembangan regulasi perlindungan

data di berbagai negara termasuk Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengadopsi banyak prinsip yang terdapat dalam GDPR seperti prinsip lawfulness, fairness, dan transparency dalam pemrosesan data, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, serta accountability. Pengaturan mengenai hak-hak subjek data seperti hak akses, hak untuk memperbaiki data, hak penghapusan, dan hak portabilitas data dalam Undang-Undang Pelindungan Data Pribadi juga sejalan dengan ketentuan GDPR. Harmonisasi dengan standar GDPR penting untuk memfasilitasi arus data lintas batas dengan negara-negara yang mensyaratkan pengakuan bahwa negara tujuan memiliki standar perlindungan data yang memadai.

Kerjasama bilateral Indonesia dengan berbagai negara dalam penanganan kejahatan siber dilakukan melalui mutual legal assistance treaty dan memorandum of understanding mengenai kerjasama keamanan siber. Indonesia telah menandatangani MLAT dengan beberapa negara seperti Australia, Tiongkok, Korea Selatan, dan negara-negara ASEAN yang memfasilitasi pertukaran informasi dan bantuan penegakan hukum dalam kasus-kasus kejahatan siber yang melibatkan lebih dari satu yurisdiksi. Melalui mekanisme MLAT, Indonesia dapat meminta bantuan negara lain untuk melakukan penggeledahan, penyitaan data elektronik, atau pemblokiran aset digital yang berada di server luar negeri dan sebaliknya berkewajiban memberikan bantuan serupa kepada negara mitra sesuai dengan prinsip resiprositas dalam hukum internasional.

Tantangan dalam harmonisasi regulasi siber berkaitan dengan keseimbangan antara kebutuhan kerjasama internasional dengan perlindungan kedaulatan nasional dan hak-hak warga negara. Prinsip kedaulatan data yang dianut Indonesia melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mewajibkan penyelenggara sistem elektronik untuk menempatkan pusat data dan disaster recovery center di wilayah Indonesia mencerminkan kehati-hatian dalam membuka akses data kepada pihak asing. Ketentuan ini bertujuan memastikan bahwa data warga negara Indonesia dapat diakses dan dilindungi oleh hukum Indonesia, namun di sisi lain dapat menghambat

kerjasama penegakan hukum internasional yang memerlukan akses cepat terhadap data yang tersimpan di server Indonesia. Harmonisasi juga harus mempertimbangkan perbedaan konteks sosial, budaya, dan sistem hukum antar negara, terutama dalam pengaturan konten yang dianggap ilegal yang dapat berbeda-beda tergantung pada nilai-nilai dan norma sosial yang dianut.

Peran Indonesia dalam forum-forum internasional seperti G20, APEC, dan BRICS memberikan kesempatan untuk berkontribusi dalam pembentukan norma-norma internasional di bidang keamanan siber. Indonesia dalam kepemimpinannya di G20 tahun 2022 telah mendorong agenda keamanan siber dan ekonomi digital sebagai salah satu prioritas dengan menekankan pentingnya pendekatan multistakeholder dan inklusif dalam tata kelola siber global. Keterlibatan aktif Indonesia dalam pembentukan norma internasional memungkinkan Indonesia untuk memastikan bahwa kepentingan dan perspektif negara berkembang terakomodasi dalam kerangka hukum internasional yang sedang berkembang.

Langkah konkret yang perlu dilakukan Indonesia dalam memperkuat harmonisasi regulasi siber mencakup kajian mendalam mengenai implikasi ratifikasi Konvensi Budapest, penguatan kapasitas kelembagaan dalam penanganan bantuan hukum timbal balik terkait kejahatan siber, pengembangan mekanisme pertukaran informasi intelijen siber dengan negara-negara sahabat, dan partisipasi aktif dalam perumusan konvensi PBB tentang kejahatan siber untuk memastikan instrumen hukum global mencerminkan keseimbangan antara keamanan siber, hak asasi manusia, dan kedaulatan negara. Evaluasi berkala terhadap efektivitas kerjasama internasional dalam penanganan kejahatan siber perlu dilakukan untuk mengidentifikasi kendala-kendala dalam implementasi dan merumuskan langkah-langkah perbaikan. Harmonisasi regulasi siber nasional dengan konvensi internasional merupakan proses yang berkelanjutan dan dinamis yang memerlukan komitmen politik kuat, alokasi sumber daya memadai, dan pendekatan yang seimbang antara keamanan nasional, perlindungan hak warga negara, dan kerjasama internasional untuk membangun rezim hukum siber yang efektif dan sejalan dengan standar internasional

BAB 4

HUKUM PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL

Prof. Dr. Hamidah Abdurrachman, S.H., M.Hum.

A. Data Pribadi

1. Definisi Data Pribadi

Semakin berkembangnya zaman maka semakin berkembang pula teknologi yang dipergunakan oleh setiap orang, apalagi dengan kehadirannya Internet di tengah-tengah masyarakat. Karena itu jarak tidak lagi menjadi batasan yang menghalangi setiap orang dalam mempergunakan teknologi tersebut guna mengakses informasi yang dibutuhkannya. Di era generasi ini, informasi yang diakses sangatlah beragam jenis dan tujuan serta sarana penyedianya. Tak jarang informasi yang diakses pengguna internet (Netizen) bersifat formal-kedinasan dan tak sedikit juga Netizen mengakses informasi yang berifat informal hanya sekedar untuk menambah wawasan dan hiburan. Penyedia informasi tersebutpun beragam, mulai dari yang menyediakan data berbentuk dokumen atau *file copy* akses terbuka dan akses terbatas, informasi terbuka bagi pembaca, foto, video singkat serta yang berbentuk video panjang.

Penyedia informasi tersebut dalam menyediakan data tidak selalu mengunggah data tersebut sendiri ke layanannya. Tak jarang Netizen dapat mengunggahnya secara langsung ke situs layanan yang telah disediakan pengembang atau penyedia layanan. Tentu hal semacam ini sangat membantu penyedia layanan untuk mempermudah setiap orang dalam mengakes informasi/data yang dibutuhkan melalui situs penyedia layanan teretentu, yang dengan demikian semakin banyak Netizen yang mengakses situs penyedia layanan tersebut maka nama penyedia situs

layanan tersebut akan semakin dikenal oleh Netizen dan meningkatkan pendapatan mereka. Namun seringkali data yang diunggah tersebut bukan asli milik yang mengunggah akan tetapi milik orang lain atau data yang diunggah masih terdapat privasi keterkaitan pihak tertentu sehingga memerlukan persetujuan dari yang bersangkutan sebelum menggungah data tersebut ke situs penyedia layanan informasi, karena data tersebut tergolong kedalam data pribadinya.

Data pribadi dapat diartikan sebagai "data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik" sebagaimana tertuang dalam Pasal 1 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Memaknai "data tentang orang perseorangan" dalam mengunggah informasi/data ke internet utamanya media sosial (medsos) perlu dipastikan muatan dari data tersebut apakah terdapat hal ikhwah tentang orang /perseorangan individu lain atau tidak. Misalnya foto bersama yang didalamnya terdapat orang lain, meskipun foto tersebut diambil dari kamera/perangkat yang kita miliki.

2. Klasifikasi Data Pribadi

Data pribadi tidak terdiri dari satu jenis saja, akan tetapi memiliki beragam jenis, menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, klasifikasi dari data pribadi diatur dalam Pasal 4, yang pada intinya bahwa data pribadi terbagi menjadi yang bersifat spesifik dan yang bersifat umum. Alasan data pribadi yang bersifat spesifik disebutkan terlebih dahulu adalah karena "data pribadi yang bersifat spesifik" lebih menunjukan "data tentang orang/perseorangan" sebagaimana disebutkan dalam Pasal 1. Klasifikasi dari "data pribadi yang bersifat spesifik" diantaranya data keuangan pribadi, informasi kesehatan, genetika, biometric, dokumen anak, catatan kejahatan, dan/ atau data yang lain sesuai ketentuan perundang-undangan.

Namun bukan berarti "data yang bersifat umum" dikesampingkan dari kategori data pribadi. Data yang bersifat umum juga termasuk kedalam objek data pribadi dari "data tentang orang/perseorangan" yang data tersebut kemudian terklasifikasikan seperti nama lengkap, jenis kelamin atau *genital sex*, informasi

kewarganegaraan, agama seseorang, status tentang perkawinan, serta data yang dipadukan ketika seseorang diidentifikasi.

B. Perlindungan Data Pribadi

1. Definisi Perlindungan Data Pribadi

Semua tindakan yang diambil untuk melindungi informasi pribadi selama proses pengolahan guna menjaga hak konstitusional mereka yang memberikan informasi tersebut secara kolektif disebut sebagai perlindungan data pribadi.[102] Sifat dinamis dari perlindungan data pribadi berarti bahwa perlindungan data pribadi akan selalu dihadapkan pada tantangan dan dipengaruhi oleh perkembangan teknologi serta prosedur korporasi yang baru. Pertumbuhan komunikasi, informasi, dan teknologi merupakan salah satu faktor yang menyebabkan kejahatan dan penggunaan data pribadi secara tidak sah.[103]

Mosi tentang perlindungan data pribadi menunjukkan bahwa setiap individu memiliki kebebasan untuk memilih apakah akan berbagi atau saling bertukar data pribadi mereka. Selain itu, setiap individu juga berhak memutuskan dengan syarat atau ketentuan apa informasi pribadi mereka dapat diberikan.[104] Di era digital ini perlindungan data pribadi merupakan suatu teknologi juga hukum guna memastikan hak dan privasi masyarakat. Masalah-masalah baru yang timbul akibat kemajuan teknologi, seperti kebocoran data maupun kejahatan siber, mengharuskan pembaruan terus-menerus terhadap undang-undang dan kampanye untuk memberikan kesadaran terhadap masyarakat luas. Pada dasarnya, setiap orang berhak mengelola data mereka sendiri, termasuk pilihan untuk membagikannya dan batasan yang diterapkan pada penggunaannya. kemajuan teknologi dan

---

[102] Hukum Online, "Dasar Hukum Perlindungan Data Pribadi", Hukum Online.com, https://www.hukumonline.com/berita/a/dasar-hukum-perlindungan-data-pribadi-lt638d55f57a6d0/?page=1

[103] Wahyudi Jafar dan M. Jodi Santoso, *Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipnya,* (t,tp : ELSAM, 2019) hal.1 https://elsam.or.id/storage/files/2/Policy%20Brief%20Perlindungan%20Data%20Pribadi%20KOnsep,%20instrumen%20dan%20prinsipnya%20oke.pdf

[104] Dhoni Martien, *Perlindungan Hukum Data Pribadi,* (Makassar : Mutiara Ilmu, 2023) https://repo.jayabaya.ac.id/4619/2/Perlindungan%20Hukum%20Data%20Pribadi.pdf

perlindungan hak individu harus selalu menghadirkan keseimbangan diantara keduanya.

2. Subjek Perlindungan Data Pribadi

Subjek Data Pribadi (SDP) berhak mendapatkan informasi mengenai kejelasan identitas, dasar hukum kepentingan, alasan pengumpulan dan penggunaan data pribadi, serta pertanggungjawaban pihak yang mengajukan permintaan. SDP mempunyai hak terhadap data pribadi mereka untuk dilengkapi, diperbarui, dan/atau diperbaiki kesalahan dan/atau ketidakatepatan data pribadi dirinya. SDP harus diberikan hak guna memperoleh akses dan mendapatkan data pribadi-nya. SDP juga berhak menyudahi pemrosesan, meniadakan, dan/ atau menghancurkan data pribadi mereka jika merasa privasi atau haknya terganggu.

SDP berhak untuk mengubah keputusannya terkait pengolahan data pribadi yang telah diserahkan kepada pihak ketiga atau penyedia layanan. SDP berhak untuk menolak keputusan yang dibuat hanya berdasarkan pengolahan otomatis, seperti profiling, jika keputusan tersebut memiliki dampak signifikan terhadap subjek data pribadi atau memiliki konsekuensi hukum. SDP berwenang untuk menunda atau membatasi pengolahan data pribadi dengan cara yang sesuai dengan tujuan pengolahannya. SDP berhak mengajukan gugatan dan meminta ganti rugi atas pelanggaran yang melibatkan pengolahan data pribadi miliknya.

SDP berhak menerima dan menggunakan informasi pribadi tentang dirinya sendiri dari pengendali data pribadi dalam format yang kompatibel dengan struktur dan/atau format yang dapat dibaca oleh sistem elektronik. Selama sistem yang digunakan dapat berinteraksi secara aman satu sama lain sesuai dengan aturan perlindungan data pribadi, SDP diperbolehkan untuk menggunakan dan mengirimkan data pribadi tentang dirinya sendiri kepada pengendali data pribadi lainnya, Yang kesemua hak SDP tersebut sebagaimana diatur dalam Pasal 8 sampai dengan Pasal 13 Undang-Undang Perlindungan Data Pribadi.

Akan tetapi ada beberapa pengecualian hak bagi SDP yang diatur dalam Pasal 15 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yaitu antara lain “kepentingan pertahanan dan keamanan nasional, kepentingan proses penegakan hukum, kepentingan umum dalam rangka penyelenggaraan negara

kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara atau kepentingan statistik dan penelitian ilmiah."

C. *Cybercrime* terhadap Data Pribadi

1. Definisi *Cybercrime*

Cybercrime merupakan salah satu jenis kejahatan internasional yang terus berkembang. Partisipasi beberapa kelompok kriminal terorganisir menambah kompleksitas kejahatan yang dilakukan di internet. Karena sifat virtual dari pusat kejahatan, korban kejahatan siber dapat berasal dari berbagai belahan dunia, dengan dampak yang luas. Cybercrime sering kali termasuk dalam salah satu kategori berikut: pelanggaran yang berkaitan dengan komputer, pelanggaran yang berkaitan dengan konten, pelanggaran yang berkaitan dengan hak cipta dan hak terkait, atau pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer.[105]

Girasa mendefinisikan cybercrime sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama. Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer, khususnya internet, dan dapat meliputi kejahatan terhadap sistem komputer maupun penggunaan komputer sebagai alat kejahatan[106]

2. *Cybercrime* terhadap Data Pribadi

Seiring dengan semakin banyaknya orang yang memanfaatkan teknologi informasi dalam kehidupan sehari-hari, jumlah jenis kejahatan siber pun meningkat dengan cepat. Phishing dan spear-phishing, yang merupakan penipuan yang melibatkan pengiriman email atau pesan SMS palsu yang seolah-olah berasal dari organisasi terpercaya seperti bank, situs e-commerce, atau otoritas pajak, merupakan teknik yang paling umum digunakan. Tujuannya adalah untuk menipu

[105] Ferinda K Fachri, "Mengenali Perbedaan Antara Cybercrime dengan Cyber Security" hukumonline.com, https://www.hukumonline.com/berita/a/mengenali-perbedaan-antara-cybercrime-dengan-cyber-security-lt63655251889f6/?page=2

[106] Ronal, "Tinjauan Yuridis Terhadap Cybercrime": 1-14, https://media.neliti.com/media/publications/149003-ID-none.pdf

korban agar mengungkapkan informasi login atau data pribadi yang dapat dimanfaatkan. Ancaman seperti ransomware dan malware juga ada. Tanpa sepengetahuan korban, malware—seperti virus, trojan, atau spyware—dapat menyusup ke perangkat mereka. Sementara ransomware mengunci data berharga korban dan meminta tebusan untuk membebaskannya, spyware mencatat aktivitas pengguna, termasuk ketukan keyboard, untuk mencuri data.

Pelanggaran privasi data terjadi ketika data pribadi dalam suatu sistem diambil, disalin, atau diakses oleh pihak yang tidak berwenang. Hal ini biasanya terjadi ketika suatu bisnis atau organisasi tidak memiliki langkah keamanan yang memadai, yang meninggalkan celah yang dapat dimanfaatkan oleh peretas. Namun, kejahatan siber juga memanfaatkan psikologi manusia melalui rekayasa sosial, yaitu menipu korban agar secara sukarela mengungkapkan informasi pribadi. Dengan memanfaatkan kepercayaan korban, taktik ini sering digunakan melalui percakapan telepon (vishing) atau koneksi media sosial.

Bahaya selanjutnya adalah penyadapan, di mana pelaku kejahatan menyadap data yang dikirimkan melalui jaringan, terutama di jaringan Wi-Fi publik yang tidak aman. Karena hal ini dapat mengungkapkan informasi pribadi pengguna tanpa sepengetahuan mereka, perilaku ini sangat berbahaya. Pencurian identitas adalah jenis kejahatan lain yang sangat berbahaya. Dalam hal ini, kegiatan ilegal seperti mengajukan pinjaman online, mendaftar kartu SIM baru, atau melakukan bentuk penipuan lainnya dilakukan menggunakan informasi pribadi seseorang, seperti Nomor Identitas Nasional (NIK) atau Nomor Kartu Keluarga (KK).Secara menyeluruh, berbagai bentuk kejahatan siber ini menunjukkan bahwa kejahatan siber tidak hanya bergantung pada teknologi canggih, tetapi juga pada kesalahan manusia dan kelemahan sistem keamanan. Oleh karena itu, untuk mengurangi bahaya dan dampak ancaman siber ini, diperlukan penggunaan teknologi perlindungan data, penerapan aturan keamanan digital yang ketat, dan peningkatan kesadaran masyarakat.

D. Cybersecurity

1. Definisi Cybersecurity

Setidaknya terdapat tiga faktor penting cybersecurity yang perlu untuk dicapai yaitu, otorisation, autentification dan nonrepudiation yang mana ketiga hal tersebut merupakan instrumen yang dipergunakan guna menjaga keamanan sistem oleh perancang dan terelavansi dengan integrity, secrecy serta availability. Memahami keenam konsep ini dan bagaimana mereka saling terhubung satu sama lain turut membantu profesionalitas keamanan dalam perancangan dan implementasi sistem yang semakin aman. Masing-masing komponen penting dalam menunjang keseluruhan keamanan, jika ditemukan kegagalan pada salah satu komponen dapat memicu probabilitas kompromi yang akan dialami oleh sistem.[107]

Cybersecurity sendiri memiliki arti sebagai upaya atau praktik dalam melindungi jaringan komputer, perangkat, aplikasi, serta data, dan sistem dari berbagai serangan siber, termasuk phishing, malware, akses ilegal, dan serangan yang dapat menyebabkan gangguan atau kerusakan sistem. Tujuannya adalah untuk melindungi operasi sistem digital dari serangan siber dan menjaga kerahasiaan, integritas, serta ketersediaan informasi.[108]

Dalam konteks data pribadi, keamanan siber dapat didefinisikan sebagai upaya untuk melindungi jaringan, perangkat, aplikasi, data, dan sistem dari berbagai ancaman siber, termasuk malware, phishing, dan akses tidak sah, guna menjaga ketersediaan, kerahasiaan, dan integritas informasi. Tiga persyaratan utama—otorisasi, autentikasi, dan non-repudiasi—yang erat terkait dengan konsep ketersediaan, kerahasiaan, dan integritas harus dipenuhi untuk mencapai hal ini. Karena kegagalan salah satu dari enam prinsip ini dapat meningkatkan risiko pelanggaran keamanan, penting untuk memahami bagaimana konsep-konsep ini saling terhubung. Profesionalisme dalam desain dan implementasi sistem sangat penting untuk membangun perlindungan data yang kokoh.

---

[107] Hanafi, *Dasar Cyber Security dan Forensic,* (Sleman:Deeppublish, 2022) hal. 17 https://eprints.amikom.ac.id/id/eprint/18330/1/Dasar%20Cyber%20Security.pdf

[108] Data Academy, "Cyber security atau Keamanan Siber: Pengertian, Jenis, dan Ancamannya" datacademy.co.id, https://dataacademy.co.id/cyber-security-atau-keamanan-siber-pengertian-jenis-dan-ancamannya/

2. Cybersecurity dalam Perlidungan Data Pribadi

Dalam memberikan kepastian keamanan informasi di era digital, cybersecurity dan perlindungan data pribadi bekerja secara bersamaan dan saling terkait erat. Melindungi privasi dan kendali individu atas informasi mereka merupakan tujuan dari perlindungan data pribadi, sementara cybersecurity berfungsi sebagai mekanisme pertahanan untuk mencegah akses tidak sah, kebocoran, atau penyalahgunaan data tersebut. Dalam hal ini, cybersecurity merupakan landasan teknis yang menjamin penerapan prinsip-prinsip perlindungan data secara efektif, termasuk kerahasiaan, integritas, dan ketersediaan informasi.

Perkembangan teknologi seperti *cloud*, artificial intelligent atau kecerdasan buatan, dan *Internet of Things* (IoT) meningkatkan risiko serangan siber, sehingga memerlukan pendekatan cybersecurity yang terus diperbarui, seperti enkripsi data, otentikasi multi-faktor, dan sistem deteksi intrusi. Tanpa cybersecurity yang kuat, upaya melindungi informasi pribadi rentan terhadap serangan seperti ransomware, phishing, atau peretasan, yang dapat mengancam hak individu. Di sisi lain, pemerintah didorong untuk mengadopsi standar cybersecurity yang lebih ketat oleh undang-undang, seperti Undang-Undang PDP dan GDPR (*General Data Protection Regulation*).

Beberapa aspek berikut merupakan langkah *Cybersecurity* dalam memberikan proteksi terhadap data pribadi. Langkah yang pertama yaitu mencegah terjadinya kebocoran data, dalam pencegahan tersebut c*ybersecurity* diharapkan mampu memblokir illegal access atau terjadinya peretasan data pribadi hingga tersebar (kebocoran data). Kemudian enkripsi data, ketika data pribadi seseorang telah dienkripsi maka secara otomatis data tersebut telah diberikan kepastian keamanan tinggi dari pihak yang hendak menyalahgunakannya. Selanjutnya adalah audit serta monitoring, monitoring rutin terhadap sistem operasi dari *cybersecurity* ditujukan untuk memvalidasi apakah prosedur *cybersecurity* yang diterapkan masih relevan dengan regulasi yang berlaku dan mengkonfirmasi apakah prosedur tersebut masih berfungsi dengan baik atau tidak. Terakhir melacak dan menemukan Insiden, *cybersecurity* berperan dalam mendeteksi insiden atau tindak kejahatan secara

efisien dan sehingga proses penanganan represifnya bisa ditindaklanjuti secara cepat.[109]

Oleh karena itu, harmonisasi prosedur cybersecurity dengan kerangka hukum perlindungan data tidak hanya meningkatkan keamanan informasi tetapi juga meningkatkan kepercayaan publik terhadap penggunaan teknologi digital. Perlindungan data pribadi dan cybersecurity saling terkoneksi dikarenakan adanya pedoman etika dan hukum yang ditetapkan untuk pengelolaan data, sementara yang menyediakan kemampuan teknis untuk mengurangi risiko. Dalam tujuan penyediaan akses internet yang aman dan yang melindungi privasi Netizen, koherensi antara *cybersecurity* dan perlindungan data pribadi juga sangat diperlukan.

E. Forensik Digital dan Cybersecurity

1. Perbedaan Forensik Digital dan Cybersecurity

Tujuan, metode, dan bidang kerja dari cybersecurity dan forensik digital memiliki perbedaan yang signifikan. Dengan mengambil langkah-langkah proaktif seperti implementasi firewall, sistem enkripsi, dan manajemen kerentanan, cybersecurity bertujuan mencegah, mengidentifikasi, serta mengurangi serangan siber. Fokus utamanya adalah melindungi infrastruktur digital dari ancaman potensial di masa depan. Di sisi lain, bidang reaktif dan investigatif forensik digital bertanggung jawab untuk mengumpulkan, menganalisis, dan melindungi bukti digital setelah terjadi pelanggaran keamanan, seperti peretasan, kebocoran data, atau kejahatan siber lainnya. Forensik digital lebih berfokus pada penyelesaian kasus daripada pencegahan, karena menggunakan teknik khusus untuk memastikan integritas bukti, mengidentifikasi asal serangan, dan mendukung proses hukum.

Meskipun forensik digital sering kali berkaitan dengan proses hukum, di mana temuan penyelidikan dapat digunakan sebagai bukti di pengadilan, cybersecurity beroperasi di bidang teknis-operasional untuk mengurangi risiko. Selain itu,

[109] Elitery "Penerapan Keamanan Siber dalam Menunjang UU Perlindungan Data Pribadi" elitery.com, https://elitery.com/articles/penerapan-keamanan-siber-dalam-menunjang-uu-perlindungan-data-pribadi/

forensik digital terutama berfokus pada metode pemulihan data, analisis log, dan pelacakan aktivitas digital, sedangkan cybersecurity mencakup aturan dan prosedur keamanan yang lebih umum. Namun, kedua bidang ini dapat bekerja secara bersamaan, yang mana forensik digital membantu dalam mengidentifikasi kelemahan keamanan setelah suatu peristiwa terjadi, yang dengan itu memungkinkan developer untuk meningkatkan sistem mereka dengan lebih efisien, sementara cybersecurity membangun lapisan pertahanan di Indonesia sednri forensik digital dan cybersecurity dapat dipelajari melalui Pendidikan khusus *Computer Hacking Forensic Investigator* (CHFI) atau dengan menempuh pendidikan jenjang master / magister di Telkom University pada Program Studi Magister Keamanan Siber dan Forensik Digital.

Studi Keamanan Siber dan Forensik Digital berfokus mengkaji operasi keamanan dan manajemen insiden, tata kelola dan manajemen risiko forensik, tantangan keamanan dalam penegakan hukum dan kejahatan siber, forensik digital, kriptografi, steganografi, keamanan blockchain, privasi dan hak digital, network security, keamanan perangkat lunak, investigasi dan analisis intelijen: teori dan metode (OSINT), forensik multimedia, analisis data forensik, dan pengumpulan data forensik di dunia siber. Diharapkan bahwa setelah menempuh program studi Keamanan Siber dan Forensik Digital akan memperoleh keterampilan yang diperlukan untuk menerapkan teknologi dan pengetahuan dalam menyelesaikan masalah-masalah sosial di bidang akademis, hukum, dan kegiatan kriminal, terutama dalam melindungi data pribadi.[110]

2. Forensik Digital dalam Perlindungan Data Pribadi

Pada intinya pebedaan dari forensik digital dan cybersecurity adalah forensik digital merupakan Langkah untuk memberikan perlindungan terhadap data pribadi setelah terjadinya tindak kejahatan terhadap data pribadi seseorang, sedangkan cybersecurity adalah Langkah pencegahan guna mencegah tindak kejahatan yang menargetkan data pribadi seseorang sebagai objek kejahatannya. Korelasi keduanya dalam memberikan perlindungan terhadap data pribadi memiliki fungsi

[110] Fakultas Informatika, "S2 Cyber Security and Digital Forensic" telkomuniversity.ac.id https://smb.telkomuniversity.ac.id/program/s2-cyber-security-and-digital-forensic/

yang berbeda. cybersecurity proaktif menggunakan alat seperti firewall, enkripsi, deteksi ancaman, dan kontrol akses yang ketat untuk mencegah kebocoran data. Tujuannya utama adalah menciptakan sistem yang tahan terhadap serangan siber, sehingga informasi pribadi sulit untuk disusupi atau dieksploitasi. Forensik digital, di sisi lain, bersifat investigatif dan reaktif digunakan setelah terjadi insiden keamanan, seperti peretasan atau kebocoran data.

Peran forensik digital dalam melindungi data pribadi setiap orang adalah untuk menentukan asal mula kebocoran, mengumpulkan bukti hukum, dan membantu pemulihan data, spesialis forensik digital memeriksa bukti digital seperti log sistem, metadata, atau jejak peretas. Untuk itu forensik jaringan merupakan salah satu cabang keilmuan forensik digital yang dipergunakan diantaranya. Hal ini dikarenakan dalam forensik jaringan melibatkan pengumpulan bukti dari jaringan dan mengevaluasinya dengan pemahaman tentang serangan jaringan. Tujuan utamanya adalah merekonstruksi peristiwa serangan intrusi jaringan dan mengidentifikasi pelaku. Deteksi serangan dan keamanan jaringan merupakan dasar dari forensik. Perubahan data detik demi detik menjadi fokus utama forensik jaringan. Salah satu jenis penyelidikan forensik jaringan adalah menyelidiki serangan siber atau peretasan. Namaun untuk mempertahankan keotentikan bukti digital yang digunakan dalam persidangan merupakan tantangan utama dalam forensik jaringan karena bukti digital bersifat folatil (mudah / cepat berubah).[111] Dengan kata lain, forensik digital berfungsi sebagai "mikroskop" yang menunjukkan bagaimana kebocoran terjadi dan siapa yang bertanggung jawab, sedangkan keamanan siber berfungsi sebagai "perisai" yang melindungi data sejak awal.

Kedua bidang ini bekerja secara bersamaan forensik digital memberikan pertanggungjawaban dan pembelajaran pasca-kejadian untuk memperkuat pertahanan ke depannya, sementara keamanan siber mengurangi risiko. Menggabungkan keduanya tidak hanya menjamin pencegahan tetapi juga

[111] Synthiana Rachmie "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website" *LITIGASI (e-Journal)*, 21, no. 1, (2020): 104-127, http://dx.doi.org/10.23969/litigasi.v21i1.2388

penegakan hukum dan peningkatan sistem jika dilakukan atau ditemukan sebuah pelanggaran atau tindak kejahatan terhadap data pribadi seseorang.

F. Tanggung Jawab Hukum Pengendali dan Prosesor Data Pribadi

Perlindungan data pribadi dalam sistem hukum Indonesia menempatkan dua entitas utama sebagai pihak yang memegang peran sentral dalam pemrosesan data, yaitu pengendali dan prosesor data pribadi.[112] Keduanya merupakan aktor hukum yang memiliki posisi strategis dalam sistem digital yang semakin kompleks dan dinamis. Dengan meningkatnya penggunaan sistem elektronik dalam kehidupan sehari-hari, kehadiran keduanya menjadi tak terelakkan, baik dalam skala individual, institusional, maupun korporasi.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur secara jelas definisi serta tanggung jawab hukum dari kedua pihak ini. Berdasarkan Pasal 1 angka 4 dan 5, pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri atau bersama-sama menentukan tujuan dan kendali atas pemrosesan data pribadi. Sementara itu, prosesor data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang memproses data pribadi atas nama pengendali data pribadi.

Kedudukan hukum antara pengendali dan prosesor tidaklah setara dalam hal otoritas terhadap data.[113] Pengendali merupakan pihak yang memiliki kewenangan penuh untuk menentukan arah pemrosesan, dari tahap pengumpulan, penyimpanan, pemanfaatan, hingga penghapusan data pribadi. Sebaliknya, prosesor menjalankan instruksi atau perintah teknis dari pengendali, yang biasanya dituangkan melalui kontrak atau perjanjian pemrosesan data.[114] Perbedaan ini menjadikan pengendali

---

[112] Nirwana, D., Nurjannah, E., Marpaung, C. R. A., & Wijaya, H. A. (2024). Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital. *JIIP-Jurnal Ilmiah Ilmu Pendidikan*, *7*(7), 7364-7373.

[113] Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum Lex Generalis*, *2*(8), 649-662.

[114] Pakpahan, J. M. (2024). Kesadaran Urgensi Peran Pengendali Dan Prosesor Data Pribadi Dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat*, *10*(1), 119-137.

sebagai subjek hukum utama dalam pemrosesan data, sementara prosesor merupakan pelaksana administratif dan teknis yang tunduk pada batasan yang ditetapkan pengendali.

Pengendali data pribadi memiliki sejumlah kewajiban hukum yang sangat penting dan tidak dapat ditangguhkan. Pasal 20 Undang-Undang PDP menyatakan bahwa setiap pemrosesan data pribadi wajib memiliki dasar yang sah. Dasar tersebut dapat berupa persetujuan, perjanjian, pemenuhan kewajiban hukum, pelaksanaan tugas dalam kepentingan publik, atau kepentingan yang sah dari pengendali data. Kewajiban ini menunjukkan bahwa pengendali tidak dapat sembarangan memproses data pribadi tanpa landasan hukum yang valid.

Lebih lanjut, Pasal 29 mengatur bahwa pengendali bertanggung jawab menjamin keakuratan dan keutuhan data pribadi. Hal ini menunjukkan bahwa tanggung jawab pengendali mencakup tidak hanya aspek legalitas, tetapi juga kebenaran substansi dari data yang diproses. Selain itu, Pasal 35 mewajibkan pengendali untuk menjaga keamanan data pribadi dari gangguan yang mengakibatkan kegagalan pelindungan data. Tindakan perlindungan ini dapat mencakup pengamanan fisik, teknis, dan administratif, seperti penggunaan sistem enkripsi, firewall, hingga kebijakan akses terbatas.

Pasal 36 memberikan kewajiban menjaga kerahasiaan data pribadi. Setiap pihak yang menangani data, baik pengendali maupun prosesor, dilarang menyebarluaskan atau membuka akses terhadap data pribadi tanpa persetujuan yang sah. Ketentuan ini berlaku tidak hanya pada saat data diproses, tetapi juga sesudahnya, yang menunjukkan perlindungan jangka panjang terhadap integritas data.

Pengendali juga bertanggung jawab terhadap hak-hak subjek data pribadi. Berdasarkan Pasal 32, pengendali wajib memberikan akses kepada subjek data untuk melihat, memperbaiki, menghapus, atau menarik kembali persetujuan atas data pribadi miliknya. Hak-hak ini merupakan bentuk perlindungan hukum yang kuat bagi individu atas pengelolaan data miliknya, serta menempatkan pengendali sebagai pihak yang wajib memfasilitasi pelaksanaan hak tersebut.

Dalam hal terjadi insiden pelanggaran data atau kebocoran informasi, pengendali memiliki kewajiban untuk memberitahukan kejadian tersebut kepada subjek data dan otoritas pelindungan data. Kewajiban ini diatur dalam Pasal 46, yang menyebutkan bahwa pemberitahuan harus dilakukan paling lambat 3 x 24 jam sejak diketahui terjadinya pelanggaran. Ketentuan ini mengandung makna pentingnya transparansi dan tanggung jawab dalam situasi darurat yang menyangkut privasi publik.

Tanggung jawab hukum prosesor juga diatur secara eksplisit dalam undang-undang ini. Pasal 51 menyebutkan bahwa prosesor hanya dapat memproses data berdasarkan instruksi pengendali. Apabila prosesor bertindak di luar ruang lingkup perintah atau menggunakan data untuk tujuan lain, maka ia dianggap bertindak sebagai pengendali dan akan menanggung seluruh akibat hukum atas tindakan tersebut. Artinya, batas tanggung jawab prosesor adalah kepatuhan terhadap perintah yang sah dan spesifik dari pengendali.

Prosesor juga wajib menerapkan langkah-langkah teknis dan prosedural yang sesuai untuk melindungi data dari akses tidak sah, gangguan, atau manipulasi. Meskipun tidak memiliki kewenangan untuk menentukan tujuan pemrosesan, prosesor memiliki tanggung jawab atas keamanan operasional dan teknis dalam pelaksanaan pemrosesan. Ketidakmampuan dalam menjaga standar teknis ini dapat berakibat pada tanggung jawab hukum, terutama jika mengakibatkan kerugian pada subjek data.

Untuk menjamin kepatuhan terhadap ketentuan hukum, undang-undang ini juga mengatur berbagai bentuk sanksi bagi pengendali dan prosesor yang melakukan pelanggaran. Pasal 57 menyebutkan jenis-jenis sanksi administratif, antara lain teguran tertulis, penghentian sementara aktivitas pemrosesan, penghapusan data, dan denda administratif. Sanksi ini dijatuhkan oleh otoritas yang ditunjuk untuk mengawasi pelaksanaan Undang-Undang PDP dan dimaksudkan untuk memberikan efek korektif terhadap pelanggaran yang terjadi.

Selain sanksi administratif, Undang-Undang PDP juga mengatur ketentuan pidana dalam Bab XIV. Pasal 67 menyatakan bahwa setiap orang yang dengan sengaja memperoleh atau mengungkapkan data pribadi yang bukan miliknya secara

melawan hukum dapat dipidana dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak lima miliar rupiah. Jika pelanggaran dilakukan oleh korporasi, Pasal 70 memperkenankan pengenaan pidana denda hingga sepuluh kali lipat dari maksimal denda untuk individu, serta pidana tambahan seperti pembekuan usaha, pencabutan izin, hingga pembubaran badan hukum.

Pasal 58 dan 59 menegaskan bahwa lembaga yang dibentuk oleh Presiden sebagai otoritas pelindungan data memiliki wewenang untuk menyelenggarakan pengawasan, pemeriksaan, hingga penjatuhan sanksi administratif. Keberadaan lembaga ini sangat penting dalam pelaksanaan fungsi pengawasan yang independen dan tidak tumpang tindih dengan fungsi lembaga lain.

Bagi subjek data yang mengalami kerugian akibat pelanggaran, terdapat hak untuk menuntut ganti rugi kepada pengendali atau prosesor yang bertanggung jawab. Gugatan perdata ini dapat diajukan ke pengadilan dan menuntut penggantian kerugian secara materiil maupun imateriil. Meskipun proses pembuktiannya tidak selalu mudah, keberadaan hak ini memberikan jaminan hukum terhadap hak privasi yang telah dilanggar.

Implementasi tanggung jawab hukum pengendali dan prosesor dalam praktik memerlukan kesiapan kelembagaan, peningkatan kapasitas teknis, serta integrasi sistem pengawasan yang efektif. Pengendali dan prosesor harus memastikan bahwa setiap aktivitas pemrosesan telah terdokumentasi, setiap alur kerja memiliki standar operasional prosedur yang jelas, dan setiap karyawan yang terlibat telah memperoleh pelatihan tentang pelindungan data pribadi.

Tidak kalah pentingnya adalah transparansi terhadap pihak ketiga. Apabila pengendali atau prosesor bekerja sama dengan vendor atau pihak eksternal lain, maka perjanjian kerja sama tersebut harus secara tegas memuat klausul tanggung jawab atas pelindungan data. Pengendali wajib memastikan bahwa pihak ketiga juga patuh terhadap ketentuan peraturan perundang-undangan.

Perkembangan teknologi informasi yang sangat pesat, seperti penggunaan kecerdasan buatan, big data, serta sistem berbasis cloud, memberikan tantangan baru bagi pengendali dan prosesor dalam menegakkan tanggung jawabnya. Oleh karena itu, keberlanjutan pemutakhiran kebijakan dan prosedur menjadi

keniscayaan. Tanpa pembaruan yang konsisten, sistem perlindungan yang sudah ada akan tertinggal dan menjadi rentan terhadap kebocoran maupun eksploitasi.

Keseluruhan pengaturan dalam Undang-Undang Pelindungan Data Pribadi memberikan landasan hukum yang kuat bagi perlindungan hak privasi individu. Pengendali dan prosesor data pribadi tidak lagi hanya bertindak atas dasar kepentingan bisnis atau administratif, melainkan memikul tanggung jawab hukum yang nyata dan dapat dikenakan sanksi apabila lalai atau menyimpang. Kepatuhan terhadap peraturan ini bukan hanya soal legalitas, tetapi juga merupakan bentuk penghormatan terhadap martabat dan hak dasar setiap warga negara.

BAB 5

HAK KEKAYAAN INTELEKTUAL DALAM *CYBERLAW*

Dr. Suci Lestari, S.H., M.H.

A. Pendahuluan

Hak Kekayaan Intelektual (selanjutnya disingkat HKI) merupakan hak yang muncul dari kegiatan pemikiran yang dilakukan oleh individu atau sekelompok orang, yang nantinya menghasilkan sebuah karya intelektual. Kegiatan pemikiran adalah aktivitas yang dilakukan dengan mengandalkan kemampuan berpikir, ketrampilan, dan keahlian dari individu atau kelompok.

Karya intelektual adalah produk yang dihasilkan dari kegiatan pemikiran dan menjadi dasar untuk mendapatkan perlindungan HKI. Dengan begitu, individu yang melakukan aktivitas intelektual tapi tidak menghasilkan karya intelektual tidak akan mendapatkan perlindungan dari HKI. Secara umum, HKI memberikan perlindungan pada gagasan, tetapi gagasan itu harus diwujudkan dalam suatu bentuk yang dapat dilihat oleh orang lain sebagai hasil dari aktivitas intelektual tersebut. Meskipun bentuk tersebut tidaklah yang dilindungi oleh HKI.

Perlindungan HKI akan menciptakan hak eksklusif, yang berarti hanya pemilik hak yang boleh menggunakan hak HKI-nya atau memberikan izin kepada orang lain untuk memanfaatkannya, biasanya disertai dengan imbalan. Hak eksklusif ini adalah kompensasi untuk semua usaha yang telah dilakukan atau dikorbankan oleh pemilik karya intelektual. Pengeluaran atau pengorbanan tersebut meliputi biaya, waktu, tenaga, pikiran, dan uang. Perlindungan hukum hanya

diberikan kepada pencipta, perancang, atau penemu yang dengan kecerdasan intelektualnya menciptakan sesuatu yang belum ada sebelumnya. Perlindungan hukum HKI ini mencakup keseimbangan antara hak dan kewajiban, baik bagi pemilik maupun masyarakat yang memanfaatkannya.

Harsono Adisumarto [115] mendefinisikan bahwa istilah "property" merujuk pada kepemilikan yang melarang orang lain menggunakan hak itu tanpa izin dari pemiliknya. Sementara itu, istilah "intellectual" berhubungan dengan aktivitas intelektual berdasarkan kreativitas dan pemikiran dalam bentuk ekspresi karya sastra, seni, dan ilmu, serta dalam bentuk penemuan yang bersifat immaterial; dan istilah "intelektual" harus dicantumkan pada setiap karya atau penemuan yang berasal dari kreativitas berpikir manusia.

Dengan demikian, inti dari HKI ini sendiri berakar pada pandangan yang sangat mendasar di mana karya-karya intelektual yang dihasilkan oleh manusia, dalam proses pembuatannya tentu memerlukan keterampilan atau keahlian khusus, ketekunan, serta membutuhkan banyak usaha dan pengorbanan.

Berdasarkan Pasal 499 Kitab Undang-undang Hukum Perdata, hak kekayaan intelektual (HKI) adalah jenis benda yang tidak dapat dilihat atau bersifat tidak berwujud. Kitab Undang-undang ini membagi benda menjadi beberapa jenis, termasuk benda yang bisa dilihat dan yang tidak bisa dilihat. Sebagai benda yang tidak terlihat, kepemilikan HKI tidak dapat dibuktikan melalui penguasaan fisik seperti benda yang bisa dilihat. Kepemilikan HKI muncul saat sebuah ide telah diterjemahkan menjadi karya atau produk yang bisa dilihat oleh publik sebagai bukti nyata adanya penciptaan intelektual dari pikiran seseorang. Hak atas hasil kreativitas intelektual ini sangat abstrak jika dibandingkan dengan hak atas benda nyata, tetapi kedua hak ini memiliki sifat yang sama yaitu hak yang mutlak. Selain itu, ada perbandingan bahwa setelah benda tidak berwujud tersebut dikeluarkan dari pikiran seseorang, maka itu bisa menjadi sebuah karya sastra, ilmu pengetahuan, seni, atau dalam bentuk pendapat. Bentuknya yang nyata dapat memberikan keuntungan

[115] Dalam Insan Budi Maulana dkk, *Hak Kekayaan Inteletual* (Depok : Rajawali Buana Pusaka, 2024), hlm. 3.

secara finansial. Ini yang menjelaskan mengapa hak ini dimasukkan ke dalam hukum tentang harta benda.

Kepemilikan HKI jelas berbeda dengan kepemilikan benda yang terlihat. Seringkali, batasan-batasan ini sulit dipahami oleh sebagian orang, terutama dalam masyarakat negara-negara berkembang seperti Indonesia. Dalam konteks masyarakat yang lebih individualistis seperti di negara-negara Barat, perkembangan HKI tidak mengalami banyak hambatan dan justru menjadi elemen penting dalam kemajuan ilmu pengetahuan, industri, perdagangan, bahkan dalam pertumbuhan ekonomi dan penghasilan devisa negara.

B. Relevansi HKI dalam Cyberlaw

Perkembangan terkini dalam teknologi informasi sangat mengesankan, sehingga dunia dianggap tanpa batas. Begitu juga dengan peradaban manusia dan semua aspeknya yang sangat dipengaruhi. Kecanggihan dunia maya digambarkan sebagai pedang bermata dua, karena dampaknya membawa dua hasil, yaitu untuk kesejahteraan dan peradaban manusia serta menjadi alat yang efektif untuk melakukan tindakan kriminal di dunia maya.

Perubahan cepat dalam teknologi digital telah memberikan pengaruh besar terhadap perlindungan hukum untuk kekayaan intelektual. Di zaman digital ini, kekayaan intelektual, seperti hak cipta, paten, dan merek, menjadi semakin mudah disalahgunakan dan dilanggar. Internet mempermudah penyebaran karya, penggandaan digital, anonimitas pelaku, dan akses global lintas yurisdiksi, sehingga risiko pelanggaran HKI meningkat.[116]

Hak kekayaan intelektual terbagi menjadi 2 (dua) golongan besar yaitu :

1. Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan.

[116] https://www.upcounsel.com/breach-of-intellectual-property

2. Hak Kekayaan Industri yang terdiri dari merek, PVT, desain sirkuit terpadu, desain industri, paten

Merek adalah tanda yang dapat ditampilkan secara grafis berupa gambar, logo, nama, kata, huruf, angka, susunan warna, dalam bentuk 2 (dua) dimensi dan/ atau 3 {tiga) dimensi, suara, hologram, atau kombinasi dari 2 (dua) atau lebih unsur tersebut untuk membedakan barang dan atau jasa yang diproduksi oleh orang atau badan hukum dalam kegiatan perdagangan barang dan/ atau jasa.

Perlindungan Varietas Tanaman yang selanjutnya disingkat PVT, adalah perlindungan khusus yang diberikan negara, yang dalam hal ini diwakili oleh Pemerintah dan pelaksanaannya dilakukan oleh Kantor Perlindungan Varietas Tanaman, terhadap varietas tanaman yang dihasilkan oleh pemulia tanaman melalui kegiatan pemuliaan tanaman.

Desain Tata Letak adalah kreasi berupa rancangan peletakan tiga dimensi dari berbagai elemen, sekurang-kurangnya satu dari elemen tersebut adalah elemen aktif, serta sebagian atau semua interkoneksi dalam suatu Sirkuit Terpadu dan peletakan tiga dimensi tersebut dimaksudkan untuk persiapan pembuatan Sirkuit Terpadu.

Desain Industri adalah suatu kreasi tentang bentuk, konfigurasi, atau komposisi garis atau warna, atau garis dan warna, atau gabungan daripadanya yang berbentuk tiga dimensi atau dua dimensi yang memberikan kesan estetis dan dapat diwujudkan dalam pola tiga dimensi atau dua dimensi serta dapat dipakai untuk menghasilkan suatu produk, barang, komoditas industri, atau kerajinan tangan.

Paten adalah hak eksklusif yang diberikan oleh negara kepada inventor atas hasil invensinya di bidang teknologi untuk jangka waktu tertentu melaksanakan sendiri invensi tersebut atau memberikan persetujuan kepada pihak lain untuk melaksanakannya.

Hak atas kekayaan intelektual (HKI) sebagai dasar utama dalam hukum siber menjadi fokus perhatian dunia internasional yang diterapkan dalam regulasi.

C. Bentuk HKI dalam Cyberlaw

1. Hak Cipta

Hak Cipta, antara lain berupa karya tulis, musik, video, software. Ciptaan yang ada dalam kelompok ini mencakup buku, artikel, jurnal, dan banyak jenis tulisan lainnya. Hak cipta memberikan perlindungan kepada karya tulisan dari peniruan atau pemakaian tanpa izin, sehingga penulis tetap menerima penghargaan atas karya yang mereka buat. Perlindungan ini meliputi karya yang dicetak maupun yang berbentuk digital.

Lagu, karya musik, dan kata-kata dalam lagu adalah bagian dari karya yang dilindungi. Hak cipta memastikan bahwa artis atau penulis lagu menerima imbalan saat karya mereka digunakan di berbagai media, baik secara langsung maupun melalui internet. Perlindungan ini tetap berlaku meskipun musik tersebut diubah susunannya. Video adalah salah satu jenis karya yang dilindungi oleh hak cipta. Pembuat video memiliki hak eksklusif mengenai pembuatan dan penyebaran konten videonya. Perangkat lunak atau aplikasi komputer adalah salah satu jenis karya yang memiliki perlindungan. Hak cipta meliputi kode program, tampilan antarmuka, dan bagian-bagian lain yang terdapat dalam perangkat lunak itu.

2. Merek

Merek, antara lain berupa nama usaha, logo, slogan. Contoh dari merek yang sudah terdaftar termasuk nama, lambang, kata-kata promosi, atau tanda yang telah secara resmi dilindungi secara hukum. Mendaftarkan merek sangat penting untuk menjaga hak eksklusif pemilik dan menghindari penyalahgunaan oleh orang lain.

3. Paten

Paten, antara lain berupa inovasi teknologi dan metode teknis. Kemajuan teknologi digital yang cepat telah merombak cara inovasi di seluruh dunia dan memicu munculnya banyak penemuan yang berhubungan dengan perangkat lunak, kecerdasan buatan (AI), Internet of Things (IoT), blockchain, dan big data.

4. Desain Industri

Desain Industri, berupa tampilan estetika produk. Penampilan visual ini dapat terdiri dari wujud, susunan, garis, warna, atau gabungan dari elemen-elemen tersebut yang secara keseluruhan menghasilkan estetika unik pada produk.

D. Bentuk Pelanggaran HKI Digital

1. Pembajakan Film/Musik *Online*

Pembajakan film akan diblokir situsnya oleh Kemenkoinfo berdasarkan Peraturan Bersama Menkumham No. 14 tahun 2015 dan Menkominfo No. 26 tahun 2015 tentang Pelaksanaan Penutupan Konten dan atau Hak Akses Pengguna Pelanggaran Hak Cipta dan atau Hak Terkait Dalam Sistem Elektronik.[117]

Contoh umum pelanggaran hak cipta daring[118]:

a. Anda mengunduh aplikasi di ponsel cerdas Anda yang memungkinkan Anda untuk 'mengambil' audio dari video musik YouTube mana pun dan menyimpan audio tersebut secara permanen dalam koleksi musik Anda.
b. Anda membuat salinan MP3 dari sebuah lagu karena CD yang Anda beli secara eksplisit mengizinkan Anda untuk melakukannya. Tetapi kemudian Anda mengunggah salinan MP3 Anda ke internet, menggunakan jaringan berbagi file, sehingga jutaan orang lain dapat mengunduhnya.
c. Sekalipun Anda tidak menawarkan rekaman secara ilegal kepada orang lain, Anda bergabung dengan jaringan berbagi file dan mengunduh salinan tidak sah dari semua musik berhak cipta yang Anda inginkan secara gratis dari komputer anggota jaringan lain.
d. Untuk mendapatkan akses ke musik berhak cipta di komputer anggota jaringan lain, Anda membayar biaya untuk bergabung dengan jaringan berbagi file yang tidak berwenang untuk mendistribusikan atau membuat salinan musik berhak cipta. Kemudian Anda mengunduh salinan tidak resmi dari semua musik yang Anda inginkan.
e. Anda mentransfer musik berhak cipta menggunakan layanan pesan instan.
f. Anda memiliki komputer dengan perangkat pembakar CD, yang Anda gunakan untuk membakar salinan musik yang telah Anda unduh ke CD yang dapat ditulis untuk semua teman Anda.

---

[117] https://www.komdigi.go.id/berita/pengumuman/detail/22-situs-diduga-pembajak-film-diblokir-kemenkominfo dan https://www.hukumonline.com/berita/a/memahami-perbedaan-pembajakan-dan-pemanfaatan-lagu-tanpa-izin-di-era-digital-lt686b64ffab7de/

[118] https://www.riaa.com/resources-learning/about-piracy/

g. Seseorang yang tidak Anda kenal mengirimkan email berisi salinan lagu berhak cipta, yang kemudian Anda teruskan kepada teman-teman Anda.
h. Menonton film di situs yang menayangkan film tanpa izin produser film/pembajakan film.

2. Plagiarisme Online

Plagiarisme adalah saat seseorang mengambil ide atau karya orang lain dan mengklaimnya sebagai milik pribadi. Plagiarisme sering terjadi karena akses yang mudah, di mana di internet sangat sederhana untuk menyalin, menempel, dan mempublikasikan tanpa izin atau mencantumkan sumber. Seringkali, orang yang melakukannya tidak menyadari bahwa ini adalah tindakan yang melanggar etika. Budaya "yang penting selesai" dan "yang penting cepat" membuat banyak orang lupakan betapa pentingnya orisinalitas. Di dunia akademis dan profesional, dorongan untuk terus menghasilkan karya terkadang membuat seseorang mencari cara yang lebih mudah.

Saat waktu terbatas dan ide tidak muncul, menyalin karya orang lain menjadi godaan yang besar. Hal yang sama berlaku di dunia konten digital—dari influencer hingga penulis artikel, dorongan untuk selalu "memperbarui" membuat plagiarisme tampak sebagai solusi yang cepat. Tidak semua pengguna internet memahami benar apa itu plagiarisme. Banyak yang berpikir bahwa selama sesuatu terdapat di internet, maka diperbolehkan untuk digunakan tanpa mencantumkan sumber. Ini menunjukkan betapa pentingnya pendidikan tentang literasi digital dan etika dalam penggunaan informasi dengan cara yang bertanggung jawab. Plagiarisme bukan sekadar tentang pelanggaran aturan, tetapi juga mengenai integritas. Ketika seseorang terbukti menyalin, reputasinya bisa hancur. Dalam skala yang lebih besar, plagiarisme yang meluas dapat merusak budaya berpikir kritis dan kreativitas—dua hal yang sangat penting untuk membangun masa depan yang inovatif dan beradab. Beruntung, teknologi juga dapat berfungsi sebagai alat untuk melawan plagiarisme. Beragam alat untuk mendeteksi plagiarisme seperti Turnitin, Grammarly, atau Copyscape saat ini banyak dipakai dalam pendidikan dan dunia jurnalistik.

Namun, hal yang lebih krusial daripada alat tersebut adalah kesadaran dan keinginan untuk bersikap jujur dalam setiap karya. Plagiarisme di ranah daring bukan hanya masalah teknis semata, tetapi juga mencerminkan kurangnya rasa menghargai terhadap hasil dan proses berpikir orang lain. Di tengah tumpukan informasi yang melimpah, sebenarnya keaslian semakin bernilai. Oleh karena itu, penting untuk menciptakan budaya yang menghargai karya orang lain, menyebutkan sumber, dan berkarya dengan jujur demi menjaga martabat dunia digital.[119]

3. Cybersquatting

Cybersquatting diatur dalam Uniform Domain-Name Dispute-Resolution Policy (UDRP) dan PANDI. Nama domain merujuk pada suatu nama yang khas yang diberikan untuk mengenali server komputer seperti web server atau fasilitas email serta internet. Penggunaan merek sebagai nama domain oleh orang lain tanpa izin dapat terjadi karena tidak ada pemeriksaan terhadap kesamaan saat mendaftar nama domain. Nama domain membantu pengguna di internet saat mengakses server, dan juga digunakan untuk mengingat nama server yang diakses tanpa perlu menghafal rangkaian angka yang rumit yang dikenal sebagai alamat IP.

Para pemilik domain yang tidak sah memanfaatkan kekurangan dalam aturan pendaftaran nama domain yang berdasarkan sistem siapa cepat dia dapat ((first come first served). Ancaman terhadap merek dalam bidang teknologi informasi sebagai nama domain dalam praktik cybersquatting menunjukkan bahwa risiko yang dihadapi oleh pemilik merek tidak hanya muncul di dunia fisik dalam bentuk pelanggaran merek tradisional seperti pemasaran yang tidak sah atau penggunaan merek untuk produk palsu, tetapi juga ada di dunia maya dalam bentuk cybersquatting yang merupakan pelanggaran baru terhadap merek di internet. Beberapa penipuan di dunia maya bahkan memanfaatkan nama domain itu untuk membuat situs palsu, melakukan penipuan, atau mengumpulkan informasi pengguna. Selain itu, terdapat juga domaintypo/ typosquatting, yaitu pendaftaran

[119] https://business-law.binus.ac.id/2015/04/01/plagiarisme-pelanggaran-hak-cipta-bagian-3-dari-3-tulisan/ dan https://louis.pressbooks.pub/understandingplagiarism/chapter/plagiarism-and-the-internet/

nama domain yang merupakan salah ketik atau kesalahan penulisan dari nama domain yang legal dan terkenal, yang dapat merugikan pemilik merek.[120]

Untuk perselisihan mengenai nama domain . com, . net, atau . org, tata cara yang diterapkan adalah Kebijakan Penyelesaian Sengketa Nama Domain Uniform (UDRP), yang mana penyelesaiannya difasilitasi oleh berbagai penyedia layanan. Mulai dari Asian Domain Name Dispute Resolution Centre/ Pusat Penyelesaian Sengketa Nama Domain Asia (ADNDRC), Canadian International Internet Dispute Resolution Centre/ Pusat Penyelesaian Sengketa Internet Internasional Kanada (CIIDRC), The Czech Arbitration Center for Internet Disputes/ Pusat Arbitrase Ceko untuk Sengketa Internet, Forum Arbitrasi Nasional, sampai dengan Organisasi Kekayaan Intelektual Dunia (WIPO). Tetapi bila perselisihannya khusus berkaitan dengan domain . id, maka cara penyelesaian perkaranya diatur dalam Kebijakan PANDI mengenai Penyelesaian Konflik Nama Domain (KPPND) Versi 8.0.

Pengelola Nama Domain Internet Indonesia (PANDI) merupakan instansi yang mengelola nama domain di Indonesia dan bertanggung jawab membuat kebijakan terkait pengelolaannya. Salah satu tugas PANDI adalah menyelesaikan masalah yang timbul terkait nama domain. Penyelesaian Perselisihan Nama Domain (PPND) adalah masalah yang diajukan oleh orang yang merasa tidak setuju dengan pendaftaran nama domain yang dianggap telah didaftarkan oleh pihak lain secara tidak sah. PPND dikelola oleh PANDI dan merupakan cara penyelesaian sengketa secara online yang diharapkan lebih mudah, murah, dan sederhana. Dengan PPND, pemilik Merek terdaftar berhak menggunakan nama domain yang sesuai dengan Merek yang mereka miliki. Jenis masalah yang ditangani oleh PPND termasuk perselisihan nama domain yang berhubungan dengan merek dan perselisihan nama domain yang berhubungan dengan nama terdaftar. Agar berhasil dalam mengajukan perselisihan nama domain yang berhubungan dengan merek, pemohon (yang mengajukan klaim) harus menunjukkan 3 (tiga) kriteria berikut secara bersamaan:

[120] https://id.kaspersky.com/resource-center/preemptive-safety/cybersquatting

a. Nama domain harus sama atau mirip dengan merek yang telah terdaftar dan dimiliki oleh pemohon.
b. Termohon (pihak yang memiliki nama domain yang dipermasalahkan) tidak memiliki hak atau kepentingan yang sah atas nama domain tersebut.
c. Nama domain harus sudah terdaftar atau digunakan oleh termohon dengan niat buruk.

Tindakan niat buruk bisa terlihat jika nama domain didaftarkan untuk mencegah penggunaan nama domain tersebut, atau didaftarkan untuk mengganggu bisnis yang ada, atau untuk menarik pengguna internet ke situs lain demi keuntungan yang tidak sah, atau dimaksudkan untuk menjual, menyewakan, atau menyerahkan kepada Pemohon yang merupakan pemilik merek untuk mendapatkan keuntungan materiil.[121]

4. *Deepfake*

Deepfake adalah praktik mengganti imaji atau suara dari sumber resmi menjadi rekaan. Kecerdasan buatan generatif seperti ChatGPT membuka jalan bagi munculnya berbagai aplikasi kreasi imaji yang hanya berbasis data latihan (*training data*), tanpa mengandaikan benda konkretnya. *Deepfake* adalah salah satu dampak negatif dari kecerdasan generatif yang masih sangat sulit untuk dikendalikan, karena perangkat legalnya masih belum tersedia. Upaya yurisprudensi atau penafsiran hakim masih menjadi satu-satunya jalan untuk mengatasi kebuntuan juridis semacam ini.[122]

5. Penyalahgunaan Kecerdasan Buatan (AI *Misuse*)

Salah satu masalah yang timbul adalah penyalahgunaan Artificial Intelligent (kecerdasan buatan), yang terdiri dari dua hal penting: deepfake pornografi dan pencurian informasi pribadi. Deepfake pornografi menggambarkan kekhawatiran tentang pemalsuan video yang menggunakan teknologi kecerdasan buatan untuk membuat konten pornografi palsu yang sulit untuk dibedakan dari yang asli. Di sisi lain, pencurian informasi pribadi melibatkan penyalahgunaan kecerdasan buatan

[121] https://affa.co.id/tidak-bisa-mendapatkan-nama-domain-yang-sama-dengan-merek-anda-ini-langkah-langkah-yang-dapat-anda-lakukan/
[122] https://marinews.mahkamahagung.go.id/artikel/kejahatan-siber-deepfake-di-era-kecerdasan-buatan-0hb

dalam meretas sistem untuk mencuri dan menyalahgunakan data pribadi seseorang. [123]

6. Penggunaan Merek Tanpa Izin di Marketplace

Marketplace seperti Amazon, eBay, atau platform lokal sering kali menjadi tempat untuk menjual barang palsu dengan merek terkenal. Pembeli yang tidak tahu sering kali membeli barang palsu, yang bisa merusak citra merek asli. Salah satu contohnya adalah penjualan barang kecantikan palsu dengan merek ternama yang mengandung bahan-bahan berbahaya. Barang semacam ini tidak hanya merusak kepercayaan para pembeli, tetapi juga dapat menimbulkan masalah hukum bagi perusahaan asli jika pembeli mengalami kerugian atau cedera. Untuk menghadapi masalah ini, perusahaan perlu memantau marketplace secara teratur. Banyak platform marketplace besar memiliki aturan untuk melindungi merek, seperti Amazon Brand Registry, yang memberi kesempatan kepada pemilik merek untuk melaporkan dan menghapus barang palsu.[124]

E. Regulasi Indonesia

1. Undang-Undang No. 28 Tahun 2014 Tentang Hak Cipta

Hak cipta sebagai salah satu aspek dalam kekayaan intelektual terkait dengan perlindungan atas produk yang merupakan buah pikiran manusia. Wilayah hak cipta mencakup perlindungan terhadap karya sastra dan seni, seperti tulisan, musik, karya seni visual seperti lukisan, serta karya yang berbasis teknologi seperti perangkat lunak, basis data elektronik, dan lainnya. Karya-karya ini yang disebut sebagai Ciptaan, ketika dipublikasikan di media internet dalam format digital, tetap memperoleh perlindungan. Hal ini dijelaskan dalam Pasal 1 angka 11 yang menyatakan bahwa pengumuman adalah proses membaca, menyiarkan, memamerkan suatu ciptaan menggunakan berbagai alat baik elektronik maupun non-elektronik, atau melakukan dengan cara apapun agar ciptaan tersebut dapat diakses, didengar, atau dilihat oleh orang lain. Pasal tersebut menjelaskan bahwa

[123] https://inspera.com/ai/examples-of-ai-misuse-in-education/

[124] https://siplawfirm.id/menelusuri-pelanggaran-merek-di-marketplace-siapa-yang-bertanggungjawab/?lang=id

perlindungan hak cipta mencakup konten digital tanpa memandang bentuk atau cara penyebarannya. Informasi yang dilindungi oleh hak cipta dalam bentuk analog tetap dilindungi ketika beralih ke bentuk digital. Misalnya, sebuah artikel, lagu, gambar, atau foto yang disebarluaskan melalui media internet masih akan mendapatkan perlindungan sebagai karya cipta.

2. UU No. 20 Tahun 2016 Tentang Merek Dan Indikasi Geografis

Undang-undang ini harus diubah agar sesuai dengan kemajuan teknologi informasi, dengan menambahkan bagian-bagian yang secara khusus menangani masalah seperti cybersquatting, penggunaan merek dalam kata kunci digital, pemakaian merek sebagai konten di media sosial tanpa izin, serta pemalsuan digital terhadap produk bermerek.

Merek bukan hanya sekadar label atau simbol; itu adalah gambaran dari bisnis yang menunjukkan nilai, kepercayaan, dan citra. Dalam dunia maya, merek lebih mudah terancam oleh masalah, seperti penggunaan yang tidak sah, peniruan, atau penyalahgunaan. Melindungi merek dengan baik tidak hanya menjaga harta perusahaan tapi juga melindungi pembeli dari produk tiruan atau penipuan. Pembeli lebih cenderung percaya pada merek yang dikenal baik. Oleh karena itu, menjaga reputasi merek di zaman digital sangat penting. Perusahaan yang tidak dapat melindungi merek mereka akan berisiko tidak hanya mengalami kerugian uang tetapi juga kehilangan dukungan dari pelanggan.

3. UU No. 13 Tahun 2016 *jo*. UU No. 65 Tahun 2024 Tentang Paten

Perkembangan teknologi informasi yang cepat telah menghasilkan banyak inovasi di berbagai sektor, termasuk perangkat lunak. Software memegang peranan yang sangat krusial dalam kehidupan sehari-hari, baik untuk perorangan maupun bisnis. Namun, dengan kemajuan teknologi yang terus berkembang, sangat penting bagi para inovator dan pengembang perangkat lunak untuk melindungi karya dan inovasi yang mereka buat. Salah satu cara untuk melindungi hak kekayaan intelektual perangkat lunak adalah dengan mendaftarkan paten.

Paten memberikan hak eksklusif kepada pemilik untuk mengatur penggunaan, pembuatan, dan penjualan suatu inovasi. Hal ini diatur dalam Pasal 19 ayat (1) yang menyatakan: “Pemegang paten memiliki hak eksklusif untuk melaksanakan paten

yang mereka miliki, memberikan izin kepada orang lain untuk melaksanakan paten tersebut, dan melarang orang lain yang tidak mendapatkan izin untuk:

a. Dalam hal paten-produk: membuat, menggunakan, menjual, mengimpor, menyewakan, menyerahkan, atau menyediakan untuk dijual atau disewakan produk yang diberi paten;
b. Dalam hal paten-proses: menggunakan proses yang dipatenkan untuk memproduksi barang atau melakukan tindakan lainnya sebagaimana disebutkan di poin a; dan
c. Dalam konteks hak paten metode, sistem, dan aplikasi: memanfaatkan metode, sistem, dan aplikasi yang sudah mendapatkan hak paten untuk menghasilkan produk atau melakukan tindakan lain seperti yang dijelaskan dalam huruf a."

Namun, tidak semua jenis perangkat lunak dapat dilindungi oleh hak paten. Melalui UU ini, terdapat peraturan yang mengatur perlindungan hak paten untuk perangkat lunak atau program komputer, seperti yang diatur dalam Pasal 4 huruf d , yang menyatakan bahwa invensi tidak mencakup program komputer, kecuali jika invensi tersebut diterapkan pada komputer. Dalam pasal ini, yang dimaksud dengan program komputer adalah program yang hanya terdiri dari kode tanpa memiliki fitur teknis, efek teknis, atau solusi untuk masalah. Solusi untuk masalah yang melibatkan program komputer yang menggunakan komputer, jaringan komputer, atau perangkat yang dapat diprogram lainnya bisa disebut sebagai invensi, yang selanjutnya dikenal sebagai invensi yang diterapkan pada komputer. Contoh masalah yang melibatkan program komputer yang bisa dianggap sebagai invensi adalah:

a. Perangkat lunak yang dipakai untuk menavigasi menggunakan sistem penentuan posisi global (GPS) pada kendaraan roda empat;
b. Perangkat lunak yang dipakai untuk memastikan jarak yang aman dari kendaraan di depan dengan menyesuaikan kecepatan kendaraan secara otomatis; dan
c. Perangkat lunak yang dipakai untuk mengatur koneksi listrik alat-alat rumah tangga dari jauh lewat internet.

Berbeda dengan pendaftaran hak cipta untuk perangkat lunak yang bisa digunakan untuk berbagai jenis kreasi, pada hak paten, program yang bisa didaftarkan dan mendapatkan hak eksklusif sebagai sebuah penemuan adalah program komputer yang dapat menyelesaikan suatu masalah dan menjadi solusi untuk hal tertentu, seperti yang dinyatakan dalam Pasal 4 huruf d UU Paten. Dalam hal ini, perangkat lunak tersebut juga harus memenuhi tiga syarat utama paten, yaitu harus baru, inovatif dan tidak mudah ditemukan oleh para ahli di bidangnya, serta dapat diterapkan di dunia industri.

Jika inovasi telah memenuhi persyaratan yang ditetapkan dalam UU Paten, pencipta bisa mempertimbangkan untuk mengajukan permohonan paten untuk melindungi hak eksklusif mereka. Dalam Pasal 24 ayat (1) dan (2) UU Paten, dijelaskan bahwa paten diberikan berdasarkan permohonan dan harus diajukan secara tertulis kepada Menteri Kemenkumham dalam bahasa Indonesia dengan membayar biaya melalui sistem *Online Single Submission* (OSS) lewat situs Direktorat Jenderal Kekayaan Intelektual (DJKI).

Mengajukan paten untuk perangkat lunak mungkin memerlukan waktu dan biaya yang tidak sedikit. Namun, keuntungan jangka panjang yang didapat sebanding dengan usaha yang dikeluarkan. Melindungi inovasi perangkat lunak adalah langkah penting untuk menjaga keberlangsungan dan perkembangan dalam industri teknologi yang semakin pesat.

4. UU No. 31 Tahun 2000 Tentang Desain Industri

Dalam hal hak atas desain industri, ada beberapa hal penting yang membuat suatu desain bisa dilindungi, yaitu:

a. Aspek Kebaruan: Desain yang diajukan haruslah baru dan belum pernah diterbitkan sebelumnya. Ini berarti desain tersebut tidak boleh sama atau mirip dengan desain yang sudah ada sebelumnya.
b. Kemampuan untuk diproduksi secara massal: Desain yang dapat dilindungi harus bisa diproduksi dalam jumlah besar dan dapat dijual di pasaran.

c. Nilai Estetika: Desain perlu memiliki daya tarik yang tinggi, terlihat mencolok, dan mampu menarik perhatian konsumen. Aspek estetika desain menjadi salah satu pertimbangan penting.
d. Dapat diamati secara langsung: Desain harus bisa dilihat dengan jelas tanpa memerlukan alat khusus, sehingga konsumen dapat dengan mudah melihat perbedaan dari produk tersebut.
e. Tidak bertentangan dengan hukum yang ada, norma agama, ketertiban umum, dan prinsip moral.

5. UU No. 11 Tahun 2008 *jo*. 19 Tahun 2016 *jo*. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik (ITE)

Tonggak penting hukum siber di Indonesia. Undang-Undang Informasi dan Transaksi Elektronik disetujui oleh Dewan Perwakilan Rakyat pada 25 Maret 2008 dan menjadi landasan hukum utama yang mengatur berbagai aktivitas di internet, mulai dari perdagangan elektronik, penyebaran data, sampai penegakan hukum terhadap kejahatan siber. Undang-undang ini memiliki 13 bab dan 54 pasal, dan terus mengalami perubahan serta penyesuaian dengan perkembangan digital yang berlangsung. UU ITE telah mengalami beberapa revisi, termasuk perubahan terkini melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE 2008.

6. PP Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik

Peraturan ini dibuat sebagai jawaban atas kemajuan teknologi informasi yang sangat cepat dan untuk mendukung perkembangan ekonomi digital serta menjaga kedaulatan negara atas informasi elektronik di wilayah Negara Kesatuan Republik Indonesia.

Peraturan ini merupakan ketentuan umum tentang pelaksanaan sistem elektronik (PSE publik dan privat). Tanggung jawab penyelenggara: perlindungan sistem, ketahanan, pemeriksaan keamanan, penyimpanan data dan pelaporan kejadian. Pengaturan tempat penyimpanan data dan lokasi pemulihan bencana. Pengelolaan transaksi secara elektronik dan keabsahan dokumen digital. Perlindungan informasi pribadi dalam sistem elektronik. Peranan pemerintah dan

kerja sama dalam keamanan siber. Pengawasan dan hukuman administratif untuk pelanggaran.

7. Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 23 Tahun 2013 tentang Pengelolaan Nama Domain

Peraturan ini diundangkan dan mulai berlaku pada tanggal 18 Oktober 2013. Beberapa hal penting dari peraturan tersebut adalah sebagai berikut:

a. Pendaftaran Nama Domain, Pendaftaran nama domain dilakukan oleh Registri atau Registrar dengan prinsip "siapa cepat dia dapat", dan tidak ada batasan jumlah nama domain yang bisa didaftarkan. Proses ini harus selesai dalam waktu 5 hari kerja. Di Indonesia, nama domain biasanya
diakhiri dengan ". id" yang menunjukkan identitas negara.

b. Pengguna Nama Domain, Peraturan pemerintah mengenai nama domain berikutnya menetapkan bahwa pengguna bertanggung jawab atas nama domain yang mereka miliki. Ini berarti pengguna harus mengikuti aturan dan menggunakan domain dengan niat baik. Selain itu, mereka juga dapat mengganti Registrar dan mengatur subdomain. Dengan begitu, nama domain dapat membantu pengguna dalam menemukan website tersebut.

c. Pengalihan Nama Domain, Pengguna dapat mentransfer nama domain ke orang lain, dan proses transfer harus dilakukan sebelum masa aktifnya habis.

d. Biaya, Registri dan Registrar berhak untuk memungut biaya untuk pendaftaran, perpanjangan, dan transfer nama domain. Di samping itu, informasi mengenai biaya harus diberitahukan dengan jelas.

e. Penyelesaian Sengketa Nama Domain, Peraturan pemerintah yang berkaitan dengan nama domain selanjutnya berhubungan dengan penyelesaian sengketa. Artinya, pihak yang dirugikan karena penggunaan nama domain secara ilegal dapat mengajukan tuntutan atau menyelesaikannya melalui mediasi.

f. Pelaporan dan Pengawasan, Sementara itu, pengelola nama domain wajib untuk melaporkan pengelolaannya secara teratur kepada menteri. Ini

karena menteri memiliki kekuasaan untuk mengawasi pengelolaan tersebut.

g. Sanksi, Registri atau Registrar yang melanggar peraturan di atas akan dikenakan sanksi administratif. Sanksi ini bisa berupa teguran tertulis hingga pencabutan nama domain jika tidak ada perbaikan dalam waktu 14 hari.

8. Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2016

Surat Edaran tentang Batasan Dan Tanggung Jawab Penyedia *Platform* Dan Pedagang (*Merchant*) Perdagangan Melalui Sistem Elektronik (*Electronic Commerce*) yang Berbentuk *User Generated Content*

a. Tujuan dari kebijakan ini adalah untuk memberikan panduan kepada Penyedia *Platform* atau Penyelenggara Sistem Elektronik serta Pedagang (*Merchant*) mengenai batasan dan tanggung jawab yang dimiliki dalam Transaksi Elektronik yang berupa perdagangan online dalam bentuk konten yang dihasilkan pengguna.

b. Sasaran dari kebijakan ini adalah:

1) Dihadirkan sistem elektronik yang aman, dapat dipercaya, dan bertanggung jawab sehingga menyebabkan berkembangnya ekosistem jual beli melalui sistem elektronik.

2) Perlindungan hukum untuk penyedia Platform, pedagang, dan Pengguna Platform dengan menjamin batasan dan tanggung jawab masing-masing dalam melakukan aktivitas perdagangan melalui sistem elektronik.

Isi dari surat edaran ini mencakup:

a) Isi yang tidak boleh diunggah pada platform UGC, antara lain:

(a) Barang dan/atau layanan yang mengandung konten negatif (seperti pornografi, perjudian, kekerasan, dan produk yang melanggar hukum)

(b) Barang dan/atau layanan yang tidak memiliki izin untuk dijual sesuai dengan hukum yang berlaku

b) Kewajiban dan tanggung jawab dari penyedia platform UGC, di antara lainnya:
   1) Menyediakan syarat dan ketentuan bagi pengguna platform UGC serta sarana untuk melaporkan
   2) Proses untuk menghapus dan memblokir konten yang dilarang
c) Kewajiban dan tanggung jawab untuk pedagang.

F. Tanggung Jawab Platform

Platform bertanggung jawab[125] atau wajib menyediakan mekanisme *takedown*, menjaga data, dan mengikuti prinsip *safe harbour*. *Safe harbor* adalah perlindungan hukum bagi penyedia layanan internet asalkan mereka mengikuti prosedur yang ditentukan dalam Digital Millennium Copyright Act ketika menerima pemberitahuan pelanggaran hak cipta. Sebuah situs berbasis *e-commerce* seperti iklan baris atau *marketplace* dapat dihentikan operasionalnya gara-gara konten yang diunggah penggunanya karena situs tersebut menggunakan UGC. *User generated content* (UGC) adalah *platform* yang memungkinkan pengguna mengunggah sendiri konten secara langsung. *Safe Harbor Policy* ini, ke depan diharapkan tidak ada lagi kesalahpemahaman, sehingga pemilik *platform* bisa berkonsentrasi penuh mengembangkan layanannya.

Salah satu poin penting dalam *Safe Harbor Policy* yang tercantum di Bagian II.B.2, disebutkan adanya perlindungan hukum bagi penyedia platform, pedagang (merchant), dan pengguna platform, dengan memastikan batasan dan tanggung jawab masing-masing dalam melakukan kegiatan perdagangan melalui sistem elektronik. Khusus penyedia platform, mereka diwajibkan menyediakan sarana pelaporan, melakukan tindakan terhadap aduan, hingga memperhatikan jangka waktu penghapusan dan/atau pemblokiran terhadap pelaporan konten yang dilarang. Aturan tersebut terdapat dalam Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2016 Tentang Batasan Dan Tanggung Jawab Penyedia Platform Dan Pedagang (*Merchant*) Perdagangan Melalui Sistem Elektronik (*Electronic Commerce*) yang Berbentuk *User Generated*

[125] https://idea.or.id/artikel/safe-harbor-policy--melindung-dan-memberi-kenyamanan-pemilik-platform-ecommerce-berbasis-user-generated-content?lang=id

Content[126] atau yang dikenal dengan sebutan *Safe Harbor Policy* atau semacam *Digital Millenium Copyright Act* (DMCA) Amerika Serikat.

G. Mekanisme Penegakan HKI

1. Kebijakan pemberitahuan dan penghapusan (*Notice and takedown)*

Kebijakan pemberitahuan dan penghapusan **(***notice and takedown)*[127] adalah sebuah mekanisme yang memungkinkan pemilik hak cipta memberikan pemberitahuan kepada penyedia layanan internet tentang adanya konten yang melanggar hak cipta, dan penyedia layanan tersebut harus menghapus konten tersebut.

Amanat Pasal 7 Trade-Related Aspects of Intellectual Property Rights (TRIPs) menjelaskan bahwa perlindungan dan penegakan hak atas kekayaan intelektual perlu mendukung inovasi serta memfasilitasi pemindahan dan penyebaran teknologi yang memberikan manfaat bagi baik pencipta maupun pengguna teknologi dan juga mendukung kesejahteraan sosial, ekonomi, serta kesetaraan hak dan kewajiban. Hal ini telah diterima dalam pasal-pasal WIPO Copyright Treaty (WCT), WIPO Performances and Phonograms Treaty (WPPT), dan Beijing Treaty untuk memberikan perlindungan hukum yang memadai dan solusi hukum yang efektif. Amerika Serikat telah menerapkan amanat ini dengan menciptakan mekanisme pemberitahuan dan penghapusan dalam DMCA 1998.

Takedown DMCA merupakan salah satu bagian paling penting yang memberi hak kepada pemilik hak cipta untuk menjaga karya mereka dari penggunaan yang tidak sah. Proses ini memungkinkan pemilik hak cipta untuk memberitahukan penyedia layanan internet bahwa ada konten yang melanggar hak cipta yang diunggah oleh pengguna mereka. Setelah mendapatkan pemberitahuan itu, penyedia layanan internet wajib melakukan tindakan untuk

---

[126] JDIH Kemkomdigi - Surat Edaran Menteri Komunikasi dan Informatika Nomor 5 Tahun 2016 tanggal 30 Desember 2016

[127] Badiah Sutianty, *Kebijakan pemberitahuan dan penghapusan (notice and takedown) sebagai sebuah kewajiban hukum untuk melakukan pencegahan pengumuman dan perbanyakan ciptaan yang melanggar hak cipta di internet = Notice and takedown policy as a legal obligation to prevent unlawful publication and dissemination of copyrighted works on internet* . https://lib.ui.ac.id/detail?id=20348957&lokasi=lokal

menghapus atau menonaktifkan akses ke konten yang dimaksud. Langkah-langkah DMCA *takedown* :

a. Pemberitahuan hak cipta: Pemilik hak cipta mengirimkan surat kepada ISP yang mencakup informasi penting, seperti penjelasan tentang karya yang dilindungi dan detail yang cukup untuk menemukan konten yang melanggar.
b. Tanggapan cepat dari ISP ; ISP diwajibkan untuk memberikan respons terhadap pemberitahuan secepatnya. Tanggapannya bisa berupa penghapusan atau menonaktifkan akses ke konten yang dilaporkan.
c. Notifikasi untuk Pengguna ; Pemberitahuan kepada pengguna yang mengunggah konten

   Kadang-kadang, ISP dapat memberitahukan pengguna yang telah mengunggah konten yang melanggar hak cipta tentang tindakan yang diambil dan memberi mereka kesempatan untuk memberikan tanggapan.
d. Counter Notification (Tanggapan atas Notifikasi): Jika seorang pengguna merasa konten yang dihapus tidak adil, mereka bisa mengajukan notifikasi balasan kepada ISP. Ini akan memicu prosedur tambahan yang perlu diikuti.

2. *Digital Millennium Copyright Act* (DMCA)

DMCA[128] adalah suatu peraturan yang diterapkan di Amerika Serikat pada tahun 1998. Undang-undang ini membuat sistem hukum untuk melindungi hak cipta dari konten digital, memberikan petunjuk tentang cara platform online beroperasi, dan memberi alat kepada pemilik hak cipta untuk membela hak-hak mereka. Beberapa tujuan utama DMCA adalah:

a. Melindungi hak cipta: DMCA memberi kesempatan bagi pemilik hak cipta untuk menjaga karya mereka agar tidak digunakan tanpa izin di dunia digital.

[128] https://www.domainesia.com/berita/dmca/

b. Mendorong inovasi dan pertumbuhan ekonomi Dengan menyediakan kerangka hukum yang jelas untuk perlindungan hak cipta, diharapkan dapat merangsang inovasi dan kemajuan ekonomi di bidang konten digital.
c. Memberikan perlindungan bagi penyedia layanan internet (ISP) Memberikan "perlindungan aman" bagi penyedia layanan internet, yang berarti penyedia tersebut tidak akan dimintai pertanggungjawaban atas pelanggaran hak cipta yang dilakukan oleh penggunanya, asalkan mereka mengikuti prosedur yang ditetapkan dalam undang-undang.

3. Pemblokiran situs oleh Kementerian Komunikasi dan Digital Republik Indonesia (Komdigi RI)

Setiap kali pemblokiran terjadi, Komdigi harus mempublikasikannya. Identifikasi dilakukan berdasarkan adanya pengaduan atau laporan yang kemudian dibahas atau melalui patroli siber[129].

4. Gugatan perdata dan pidana

Sanksi dan pelanggaran di HKI dapat berupa sanksi perdata dan atau pidana. Sanksi atas pelanggaran hak cipta berupa denda hingga Rp5 miliar dan pidana penjara hingga 10 tahun, tergantung jenis pelanggaran. Sanksi atas pelanggaran hak paten :

a. Gugatan Perdata: Apabila ada pihak yang terbukti melanggar paten dengan cara menggunakan penemuan tanpa izin, pemegang paten atau penerima lisensi berhak untuk mengajukan tuntutan ganti rugi kepada Pengadilan Niaga di daerah tempat tinggal tergugat. Namun, jika salah satu pihak tinggal di luar Indonesia, maka gugatan bisa didaftarkan di Pengadilan Niaga Jakarta Pusat sesuai dengan ketentuan dalam Pasal 143 dan Pasal 144 UU 13/2016 *jo.* UU 65/2024.

[129] https://www.komdigi.go.id/berita/sorotan-media/detail/begini-mekanisme-pemblokiran-situs-versi-kemenkominfo, https://www.dgip.go.id/index.php/artikel/detail-artikel-berita/pelindungan-hak-cipta-di-era-digital-djki-intensifkan-penegakan-hukum-dan-edukasi-publik?kategori= dan https://www.komdigi.go.id/berita/sorotan-media/detail/ini-proses-yang-ditempuh-kominfo-hingga-situs-bisa-diblokir

b. Di samping itu, dalam Pasal 153 UU 13/2016 jo. UU 65/2024 disebutkan bahwa selain penyelesaian sengketa yang telah disebutkan dalam Pasal 143, pihak-pihak dapat menyelesaikan masalah melalui arbitrase atau metode penyelesaian sengketa alternatif sesuai dengan peraturan yang berlaku.
c. Denda dan hukuman pidana, yang diatur dalam Pasal 161 UU 13/2016 jo. UU 65/2024:

> *"Setiap orang yang secara sadar dan tanpa hak melakukan tindakan yang dijelaskan dalam Pasal 160 untuk Paten, akan dihukum penjara maksimal 4 (empat) tahun dan/atau denda maksimum Rp1.000.000.000,00 (satu miliar rupiah). "*
>
> dan Pasal 162:
>
> *"Setiap orang yang secara sadar dan tanpa hak melakukan tindakan sebagaimana dijelaskan dalam Pasal 160 untuk Paten sederhana, akan dihukum penjara maksimal 2 (dua) tahun dan/atau denda maksimum Rp500. 000.000,00 (lima ratus juta rupiah). "*

H. Tantangan HKI Digital dan Contoh Kasus

Dapat disimpulkan dari pembahasan di atas bahwa tantangan HKI di dunia maya antara lain identitas anonim, bukti digital mudah dihapus, yurisdiksi, isu kecerdasan buatan/AI dan *deepfake*. Contoh-contoh kasus dalam HKI di dunia maya yang sudah dibahas di atas antara lain *reupload* lagu di TikTok, penjualan produk KW di *marketplace*[130], domain tiruan (*cybersquatting*), AI meniru gaya artis.

[130] https://e-journal.trisakti.ac.id/index.php/amicuscuriae/article/view/22009

BAB 6

PENYELESAIAN SENGKETA DALAM DUNIA DIGITAL

Amirah Dwi Subarkah, S.H., M.H.

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang sangat signifikan dalam kehidupan masyarakat modern. Digitalisasi telah mengubah hampir seluruh aspek kehidupan, mulai dari aktivitas ekonomi, sosial, hingga hubungan hukum antar individu dan badan hukum. Berbagai aktivitas yang sebelumnya dilakukan secara konvensional kini beralih ke sistem elektronik yang bersifat cepat, efisien, dan lintas batas wilayah. Transformasi ini tidak hanya mempermudah interaksi, tetapi juga melahirkan bentuk-bentuk hubungan hukum baru yang sebelumnya tidak dikenal dalam sistem hukum konvensional.[131]

Perubahan pola hubungan hukum tersebut tidak terlepas dari potensi timbulnya konflik dan sengketa. Sengketa dalam dunia digital muncul sebagai konsekuensi logis dari meningkatnya transaksi elektronik, penggunaan platform digital, serta pemrosesan dan pertukaran data secara daring. Sengketa ini dapat melibatkan berbagai subjek hukum, mulai dari individu, pelaku usaha, penyedia platform digital, hingga negara sebagai regulator. Karakter sengketa digital yang kompleks menuntut pendekatan penyelesaian yang berbeda dari sengketa konvensional.[132]

Berbeda dengan sengketa tradisional, sengketa digital sering kali terjadi tanpa adanya pertemuan fisik antar para pihak. Hubungan hukum dibentuk melalui sistem

[131] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Book, 2009), 23-25.

[132] Edmon Makarim, *Pengantar Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2019), 41-43.

elektronik yang bekerja secara otomatis berdasarkan algoritma dan standar teknis tertentu. Kondisi ini menimbulkan tantangan tersendiri, terutama terkait dengan pembuktian, identitas para pihak, serta penentuan yurisdiksi hukum yang berwenang menyelesaikan sengketa tersebut.[133]

Mekanisme penyelesaian sengketa konvensional yang selama ini mengandalkan proses litigasi di pengadilan sering kali dianggap kurang responsif terhadap karakteristik sengketa digital. Proses yang bersifat formal, memerlukan waktu yang panjang, serta biaya yang relatif tinggi menjadi kendala bagi para pihak yang bersengketa. Selain itu, keterbatasan pemahaman aparat penegak hukum terhadap aspek teknis teknologi informasi juga dapat memengaruhi kualitas putusan yang dihasilkan.[134]

Oleh karena itu, penyelesaian sengketa dalam dunia digital menjadi isu yang sangat penting dalam pembangunan hukum nasional. Diperlukan pengembangan mekanisme penyelesaian sengketa yang adaptif, fleksibel, dan mampu memberikan kepastian hukum serta keadilan bagi para pihak. Bab ini secara khusus membahas konsep sengketa digital, kerangka hukum yang berlaku di Indonesia, serta berbagai mekanisme penyelesaian sengketa yang dapat diterapkan di era digital.

B. Konsep Sengketa dalam Dunia Digital

Sengketa dalam dunia digital dapat didefinisikan sebagai perselisihan hukum yang timbul akibat pemanfaatan teknologi informasi dan sistem elektronik dalam berbagai aktivitas hukum. Sengketa ini lahir dari hubungan hukum yang dibentuk melalui kontrak elektronik, transaksi daring, penggunaan platform digital, maupun interaksi di ruang siber. Dengan demikian, teknologi informasi tidak hanya berfungsi sebagai sarana, tetapi juga menjadi bagian integral dari objek dan konteks sengketa.[135]

---

[133] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (Oxford: Oxford University Press, 2008), 68-71.

[134] Sudikno Mertokusumo, *Hukum Acara Perdata Indonesia* (Yogyakarta: Liberty, 2015)147-150.

[135] Abdul Halim Barkatullah, *Hukum Transaksi Elektronik* (Bandung: Nusa Media, 2017) 19-22.

Salah satu karakteristik utama sengketa digital adalah sifatnya yang lintas batas wilayah. Para pihak yang bersengketa dapat berada di lokasi geografis yang berbeda, bahkan berada di negara yang berbeda, sehingga menimbulkan persoalan mengenai hukum yang berlaku dan yurisdiksi lembaga penyelesaian sengketa. Dalam kondisi ini, prinsip-prinsip hukum internasional dan hukum perdata internasional menjadi relevan untuk menentukan kewenangan dan pilihan hukum yang digunakan.[136]

Karakteristik lain dari sengketa digital adalah ketergantungannya pada alat bukti elektronik. Informasi dan dokumen elektronik, seperti rekaman transaksi, korespondensi digital, dan data sistem, menjadi alat bukti utama dalam penyelesaian sengketa. Penggunaan alat bukti elektronik menuntut adanya standar hukum yang jelas mengenai keaslian, integritas, dan ketersediaan data agar dapat diterima sebagai alat bukti yang sah di hadapan hukum.[137]

Selain itu, sengketa digital juga memiliki dimensi risiko yang tinggi, terutama terkait dengan keamanan data dan perlindungan privasi. Kebocoran data, penyalahgunaan informasi pribadi, serta pelanggaran hak digital menjadi isu yang sering muncul dalam sengketa digital. Oleh karena itu, penyelesaian sengketa digital tidak hanya bertujuan menyelesaikan konflik antar pihak, tetapi juga melindungi kepentingan publik dan hak asasi manusia di ruang digital.[138]

Dengan karakteristik tersebut, sengketa digital memerlukan pendekatan penyelesaian yang komprehensif dan multidisipliner. Pendekatan hukum semata tidak cukup tanpa dukungan pemahaman teknologi informasi. Oleh karena itu, pengembangan konsep sengketa digital harus mempertimbangkan aspek hukum, teknologi, dan sosial secara bersamaan.

---

[136] Hikmahanto Juwana, *Hukum Perdata Internasional* (Jakarta: Raja Grafindo Persada, 2018) 87-90.

[137] Edmon Makarim, "Pembuktian Elektronik dalam Sistem Peradilan Indonesia," *Jurnal Hukum IUS QUIA IUSTUM* 25, no. 2 (2018): 229–33 229-233.

[138] Danrivanto Budhijanto, *Cyber Law dan Tantangan Penegakannya* (Bandung: Logoz Publishing, 2021) 101-104.

sudah disusun oleh BPUPKI. Pada hari itu juga, Soekarno dan Mohammad Hatta dipilih sebagai Presiden dan Wakil Presiden Republik Indonesia. Didasarkan pada pasal III aturan Peralihan UUD 1945 yang menyatakan bahwa pertama kali Presiden dan Wakil Presiden dipilih oleh PPKI. Sebagai sebuah negara baru, satu-satunya lembaga negara yang terbentuk satu hari setelah kemerdekaan adalah Presiden dan Wakil Presiden. Selain itu Pasal IV aturan peralihan UUD 1945 menyatakan sebelum MPR, DPR, dan Dewan Pertimbangan Agung dibentuk, menurut Undang-Undang Dasar ini, segala kekuasaannya dijalankan oleh presiden dengan bantuan sebuah komite nasional. Berdasarkan Pasal IV Aturan Peralihan UUD 1945, Presiden Soekarno segera mengisi struktur pemerintahan setelah proklamasi kemerdekaan. Langkah ini dimulai dengan pembentukan Partai Nasional Indonesia (PNI) pada 23 Agustus 1945.[139]

Pada 29 Agustus 1945, Presiden membubarkan PPKI dan melantik anggota Komite Nasional Indonesia Pusat (KNIP). Setelah itu, pada 2 September 1945, Soekarno dan Hatta membentuk kabinet pertama Republik Indonesia, yang berbentuk kabinet presidensial dan dipimpin langsung oleh Presiden.[140] Melihat cara pengisian lembaga negara ini, Adnan Buyung Nasution menilai struktur pemerintahan saat itu bersifat otoriter[141], dengan kekuasaan presiden yang luar biasa dan tidak terbatas, yang kemudian disebut sebagai constitutional dictatorship karena dibenarkan oleh Pasal IV Aturan Peralihan. Namun, dominasi kekuasaan presiden dalam praktik bernegara di bulan-bulan pertama kemerdekaan ini mengalami perubahan signifikan dengan dikeluarkannya Maklumat Wakil Presiden Nomor X.

> *"Bahwa Komite Nasional Indonesia Pusat, sebelum terbentuknya Majelis Permusyawaratan Rakyat dan Dewan Perwakilan Rakyat diserahi kekuasaan legislatif dan ikut menetapkan Garis-garis Besar*

[139] Adnan Buyung Nasution, *Aspirasi Pemerintahan Konstitusional Di Indonesia*, 1992.

[140] Joeniarto, *Sejarah Ketatanegaraan Republik Indonesia* (Jakarta: Bumi Aksara, 2001).

[141] Nasution, *Aspirasi Pemerintahan Konstitusional Di Indonesia*.

Haluan Negara, serta pekerjaan Komite Nasional Indonesia Pusat sehari-hari berhubung dengan gentingnya keadaan dijalankan oleh sebuah Badan Pekerja yang dipilih di antara mereka dan yang bertanggung jawab kepada Komite Nasional Indonesia Pusat".

Maklumat Wakil Presiden No. X tanggal 16 Oktober 1945 merupakan sebuah peristiwa ketatanegaraan yang krusial di awal kemerdekaan, di mana maklumat tersebut mengubah struktur kekuasaan yang ditetapkan oleh UUD 1945. Sebelumnya, UUD 1945 menetapkan sistem presidensial dengan kekuasaan besar di tangan Presiden. Namun, Maklumat No. X ini mengalihkan kekuasaan legislatif (yang seharusnya dimiliki oleh MPR dan DPR) kepada Komite Nasional Indonesia Pusat (KNIP), sehingga menempatkan KNIP sebagai lembaga yang sejajar dengan Presiden dan memungkinkan Indonesia bergerak menuju sistem parlementer. Pandangan seperti Asaat menempatkan Maklumat No. X setinggi Undang-Undang Dasar karena dianggap sebagai tindakan Presiden yang menjalankan kekuasaan MPR [142] dan mengatur hal-hal fundamental yang seharusnya diatur dalam Konstitusi, menjadikannya sebuah langkah yang kontroversial tetapi esensial dalam perkembangan demokrasi Indonesia.

Tidak berselang lama, pada 14 November 1945, pemerintah mengeluarkan Maklumat Pemerintah tentang Susunan Kabinet II (Maklumat 14 November).[143] Maklumat ini menegaskan bahwa tanggung jawab pemerintahan berada di tangan menteri, yang secara drastis mengubah sistem pemerintahan dari presidensial menjadi parlementer, dengan Sutan Sjahrir ditunjuk sebagai Perdana Menteri dan memimpin kabinet baru.

Sistem pemerintahan parlementer di Indonesia telah dimulai bahkan sebelum Maklumat 14 November 1945, diawali dengan Maklumat Pemerintah 31 Agustus 1945. Maklumat 31 Agustus 1945 yang menunda aktivitas Partai Nasional Indonesia (PNI), dilihat sebagai penolakan terhadap sistem partai tunggal yang diusung Soekarno. Puncaknya, melalui Maklumat Pemerintah 3 November 1945

[142] Moch. Mansoer Tolchah, *Pembahasan Beberapa Aspek Tentang Kekuasaan Eksekutif Dan Legislatif Negara Indonesia*, 1977.

[143] Nasution, *Aspirasi Pemerintahan Konstitusional Di Indonesia*.

yang ditandatangani Mohammad Hatta, pemerintah secara resmi mengadopsi sistem banyak partai (*multi-party system*) dengan memberikan kesempatan kepada rakyat untuk mendirikan partai politik. Dengan transisi ke sistem multi-partai ini, perubahan dari sistem presidensial menjadi sistem parlementer secara politik menjadi tak terhindarkan. Mahfud MD menyatakan:

> *"Perubahan sistem pemerintahan yang sangat fundamental ini tidak dilakukan dengan perubahan UUD, melainkan dengan Maklumat Pemerintah. Artinya terjadi lagi perubahan praktik ketatanegaraan. Jika menurut UUD 1945 presiden bertanggung jawab kepada MPR dan berkedudukan sebagai kepala negara dan kepala pemerintahan sekaligus, maka dengan adanya maklumat ini, presiden kehilangan kedudukannya sebagai kepala pemerintahan".*[144]

Jauh sebelum Mahfud MD, Tolchah Mansoer juga mengemukakan pendapat tentang perubahan sistem pemerintahan, di mana ia menganggap Maklumat 14 November sebagai perubahan yang luar biasa. Tolchah Mansoer menyatakan bahwa perubahan tersebut merupakan yang terpenting dari jiwa dan jalan UUD 1945.[145] Walaupun demikian, Muhammad Yamin menyatakan bahwa kementerian yang bertanggung jawab (kepada parlemen) tidak sesuai dengan Pasal 17 UUD 1945.[146]

Maklumat 14 November 1945 merupakan perubahan sistem pemerintahan dari presidensial menjadi parlementer tanpa mengubah UUD 1945, khususnya terkait Pasal 17 yang menyatakan menteri adalah pembantu presiden yang diangkat dan diberhentikan olehnya. Pergeseran ini menyebabkan menteri tidak lagi bertanggung jawab kepada presiden, melainkan kepada badan lain (parlemen), menjadikan Presiden hanya sebagai Kepala Negara, bukan lagi Kepala Pemerintahan, sesuai karakter parlementer. Menanggapi isu ini, pada 24 November

---

[144] Mahfud MD, *Politik Hukum Di Indonesia* (Jakarta: LP3ES, 1998).

[145] Tolchah, *Pembahasan Beberapa Aspek Tentang Kekuasaan Eksekutif Dan Legislatif Negara Indonesia*.

[146] Muhammad Yamin, *Proklamasi Dan Konstitusi Republik Indonesia* (Jakarta: Ghalia Indonesia, 1951).

1945, Kabinet II memberikan penjelasan mengenai "tanggung jawab menteri", menegaskan bahwa tanggung jawab menteri kepada presiden sebagaimana Pasal 17 UUD 1945 berarti menteri tidak langsung bertanggung jawab kepada rakyat.

Penjelasan 24 November 1945 menggagas perubahan dari sistem pemerintahan presidensial menjadi parlementer dengan tujuan utama agar menteri-menteri bertanggung jawab kepada rakyat melalui Badan Perwakilan Rakyat (KNIP), mencontoh praktik negara Barat dan didorong oleh kondisi genting pasca kemerdekaan. Dalam sistem baru ini, kabinet dibentuk oleh kepala negara, tetapi pertanggungjawaban kolektif terletak pada setiap menteri kepada Badan Perwakilan Rakyat sebagai perwujudan kedaulatan rakyat.

Secara jujur, Penjelasan 24 November mengakui bahwa perubahan pertanggungjawaban menteri ini tidak dimungkinkan secara langsung oleh UUD 1945 pada saat itu, sebab UUD 1945 secara eksplisit menetapkan bahwa tanggung jawab berada di tangan Presiden dan menteri bertanggung jawab kepada Presiden.

Untuk meletakkan dasar hukum perubahan ini, Penjelasan 24 November mendasarkannya pada kebiasaan ketatanegaraan (konvensi). A.K. Pringgodigdo berpendapat bahwa tidak tepat mendasarkan perubahan ini pada konvensi karena perubahan sistem pemerintahan ini adalah aturan baru yang disengaja, sementara konvensi adalah kelaziman yang timbul dari praktik hidup dan tidak seharusnya digunakan untuk mengubah hal yang sudah diatur jelas dalam UUD. Ismail Suny berargumen bahwa perubahan ini adalah konvensi ketatanegaraan yang melengkapi (supplement) UUD 1945, bukan mengubahnya, karena tidak ada ketentuan UUD 1945 yang melarang pertanggungjawaban eksekutif kepada parlemen. Oleh karena itu, perubahan pertanggungjawaban menteri kepada KNIP dianggap sah melalui konvensi.

Maklumat Pemerintah 14 November 1945 merupakan sebuah tonggak penting yang mengubah sistem pemerintahan Indonesia dari presidensial menjadi parlementer, meskipun tidak ada pasal UUD 1945 yang diubah secara eksplisit. Perubahan ini dilakukan dengan mengeluarkan maklumat yang menunjuk seorang Perdana Menteri dan menyatakan bahwa para menteri bertanggung jawab kepada Komite Nasional Indonesia Pusat (KNIP), bukan lagi kepada Presiden. Langkah ini

dianggap bertentangan dengan gagasan pendiri bangsa yang secara eksplisit menolak sistem parlementer dalam perumusan UUD 1945 di BPUPK. Terlepas dari perdebatan mengenai keabsahan dan kriterianya sebagai konvensi ketatanegaraan, Maklumat 14 November ini mendapat persetujuan dari KNIP dalam Sidang III (25-27 November 1945), yang membenarkan kebijaksanaan Presiden sebagai langkah yang diperlukan dan tidak dilarang UUD. Secara empiris, sejak maklumat ini dikeluarkan hingga berdirinya Republik Indonesia Serikat (20 Desember 1949), sistem pemerintahan parlementer ini berlaku di Indonesia, ditandai dengan pergantian delapan kabinet.[147]

Tabel Pergantian Kabinet Orde Lama

No.	Kabinet	Periode
1.	Syahrir I	14 November 1945 hingga 12 Maret 1946
2.	Syahrir II	12 Maret 1946 hingga 20 Oktober 1946
3.	Syahrir III	20 Oktober 1946 hingga 27 Juni 1947
4.	Amir Syarifudin I	03 Juli 1947 hingga 11 November 1947
5.	Amir Syarifudin II	11 November 1947 hingga 29 Januari 1948
6.	Hatta	29 Januari 1948 hingga 4 Agustus 1949
7.	Darurat	19 Desember 1948 hingga 13 Juli 1949
8.	Hatta II	04 Agustus 1949 hingga 20 Desember 1949

Dari catatan itu, dalam rentang waktu sekitar 50 bulan, dengan delapan kabinet, berarti secara rata-rata masing-masing kabinet hanya mampu bertahan sekitar enam bulan. Dari delapan kabinet itu, Kabinet Syahrir II adalah kabinet yang paling lama mampu bertahan, yaitu sekitar sembilan bulan. Sementara itu, Kabinet Amir Syarifuddin II adalah kabinet yang paling singkat masa pemerintahannya, yaitu kurang dari tiga bulan. Dalam keadaan genting, presiden mengambil alih dan memimpin kekuasaan pemerintahan negara

[147] Saldi Isra, *Sistem Pemerintahan Indonesia* (Depok: Rajawali Pers, 2018).

C. Kerangka Hukum Penyelesaian Sengketa Digital di Indonesia

Kerangka hukum penyelesaian sengketa digital di Indonesia bertumpu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Undang-undang ini memberikan dasar hukum bagi pemanfaatan teknologi informasi serta mengakui keabsahan informasi dan dokumen elektronik sebagai alat bukti hukum yang sah. Pengakuan ini menjadi tonggak penting dalam penyelesaian sengketa digital di Indonesia.[148]

Selain Undang-Undang ITE, penyelesaian sengketa digital juga berkaitan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Regulasi ini memberikan perlindungan hukum terhadap subjek data dan menetapkan tanggung jawab penyelenggara sistem elektronik dalam pengelolaan data pribadi. Sengketa yang timbul akibat pelanggaran data pribadi dapat diselesaikan melalui mekanisme hukum yang diatur dalam undang-undang tersebut.[149]

Penguatan kerangka hukum juga terlihat dari kebijakan Mahkamah Agung Republik Indonesia yang mengadopsi sistem peradilan elektronik melalui Peraturan Mahkamah Agung Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik. Penerapan *e-court* dan *e-litigation* menunjukkan upaya lembaga peradilan dalam menyesuaikan diri dengan perkembangan teknologi informasi dan meningkatkan efisiensi penyelesaian sengketa.[150]

Meskipun demikian, kerangka hukum penyelesaian sengketa digital di Indonesia masih menghadapi berbagai tantangan. Harmonisasi antar peraturan perundang-undangan belum sepenuhnya optimal, sehingga berpotensi menimbulkan tumpang tindih kewenangan dan ketidakpastian hukum. Selain itu,

---

[148] Indonesia, "Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik" (2008).

[149] Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi" (2022).

[150] Mahkamah Agung Republik Indonesia, "Peraturan Mahkamah Agung Nomor 1 Tahun 2019" (2019).

belum adanya regulasi khusus yang mengatur secara komprehensif mengenai *Online Dispute Resolution* juga menjadi kendala dalam pengembangan mekanisme penyelesaian sengketa digital.[151]

Oleh karena itu, pembaruan dan penguatan kerangka hukum menjadi kebutuhan mendesak agar sistem hukum nasional mampu merespons perkembangan teknologi secara efektif. Sinkronisasi regulasi, peningkatan kapasitas aparat penegak hukum, serta pengembangan mekanisme penyelesaian sengketa digital yang inovatif merupakan langkah strategis dalam mewujudkan kepastian hukum di era digital.

D. Penyelesaian Sengketa Digital melalui Jalur Litigasi

Periode setelah Dekrit Presiden 5 Juli 1959 menandai dimulainya Demokrasi Terpimpin di bawah

Penyelesaian sengketa digital melalui jalur litigasi merupakan mekanisme formal yang ditempuh melalui lembaga peradilan negara. Litigasi tetap menjadi pilihan utama dalam sengketa digital tertentu, terutama yang menyangkut kepentingan publik, tindak pidana siber, atau sengketa perdata bernilai besar. Dalam konteks ini, pengadilan berperan sebagai institusi yang memberikan kepastian hukum melalui putusan yang bersifat mengikat dan dapat dipaksakan pelaksanaannya oleh negara.[152]

Dalam sistem hukum Indonesia, pengadilan telah mulai mengakomodasi karakteristik sengketa digital melalui penerapan sistem peradilan elektronik. Kehadiran *e-court* dan *e-litigation* memungkinkan pendaftaran perkara, penyampaian dokumen, hingga persidangan dilakukan secara elektronik. Inovasi ini bertujuan meningkatkan efisiensi dan akses terhadap keadilan, khususnya bagi para pihak yang terlibat dalam sengketa berbasis teknologi informasi.[153]

---

[151] Pablo Cortés, *Online Dispute Resolution for Consumers in the European Union* (London: Routledge, 2011), 33-36.

[152] Sudikno Mertokusumo, *Penemuan Hukum* (Yogyakarta: Liberty, 2016), 89-92.

[153] Mahkamah Agung Republik Indonesia, *Cetak Biru Pembaruan Peradilan 2010–2035* (Jakarta: MA RI, 2020).

Meskipun demikian, penyelesaian sengketa digital melalui litigasi masih menghadapi berbagai tantangan. Salah satu tantangan utama adalah pembuktian. Hakim dituntut untuk menilai keabsahan alat bukti elektronik, termasuk memastikan integritas dan autentikasi data. Ketidaksamaan tingkat pemahaman teknologi informasi di kalangan aparat penegak hukum dapat memengaruhi kualitas pertimbangan hukum dalam putusan pengadilan.[154]

Selain itu, sifat sengketa digital yang lintas batas wilayah sering kali menimbulkan persoalan yurisdiksi. Penentuan pengadilan yang berwenang menjadi isu krusial, terutama dalam sengketa yang melibatkan platform digital asing atau para pihak yang berdomisili di negara berbeda. Dalam kondisi ini, prinsip-prinsip hukum perdata internasional dan kerja sama antarnegara menjadi relevan untuk menjamin efektivitas penyelesaian sengketa.[155]

Dengan berbagai keterbatasan tersebut, litigasi dalam sengketa digital tetap memerlukan pembaruan berkelanjutan. Reformasi hukum acara, peningkatan kapasitas hakim, serta dukungan infrastruktur teknologi menjadi prasyarat agar jalur litigasi dapat berfungsi secara optimal dalam menyelesaikan sengketa digital.

E. Penyelesaian Sengketa Digital melalui Jalur Non-Litigasi

Penyelesaian sengketa digital melalui jalur non-litigasi semakin mendapat perhatian sebagai alternatif terhadap proses litigasi yang formal dan memakan waktu. Jalur non-litigasi mencakup berbagai mekanisme seperti negosiasi, mediasi, konsiliasi, dan arbitrase. Dalam konteks sengketa digital, mekanisme ini dinilai lebih fleksibel dan responsif terhadap kebutuhan para pihak.[156]

Mediasi digital, misalnya, memungkinkan para pihak untuk menyelesaikan sengketa melalui perantara mediator dengan memanfaatkan teknologi komunikasi daring. Proses ini memberikan ruang dialog yang lebih terbuka dan berorientasi

---

[154] Edmon Makarim, *Hukum Pembuktian Elektronik* (Jakarta: Raja Grafindo Persada, 2020) 133-136.

[155] Hikmahanto Juwana, *Hukum Perdata Internasional* (Jakarta: Raja Grafindo Persada, 2018) 141-144.

[156] Takdir Rahmadi, *Mediasi: Penyelesaian Sengketa Melalui Pendekatan Mufakat* (Jakarta: Raja Grafindo Persada, 2017) 27-30.

pada penyelesaian damai. Selain itu, mediasi digital relatif lebih cepat dan biaya yang dikeluarkan lebih rendah dibandingkan litigasi di pengadilan.[157]

Arbitrase juga menjadi pilihan dalam sengketa digital tertentu, terutama sengketa bisnis dan transaksi elektronik lintas negara. Arbitrase memberikan keuntungan berupa kerahasiaan, kebebasan memilih arbiter yang memiliki keahlian khusus, serta putusan yang bersifat final dan mengikat. Dalam praktik internasional, arbitrase sering digunakan untuk menyelesaikan sengketa yang melibatkan kontrak elektronik dan layanan digital.[158]

Di Indonesia, penyelesaian sengketa non-litigasi memperoleh dasar hukum melalui Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa. Meskipun undang-undang ini belum secara khusus mengatur sengketa digital, ketentuan yang ada dapat diadaptasi untuk menyelesaikan sengketa berbasis teknologi informasi.[159]

Namun demikian, efektivitas penyelesaian sengketa non-litigasi dalam dunia digital tetap memerlukan penguatan regulasi dan kelembagaan. Diperlukan pedoman yang jelas mengenai prosedur, legitimasi, serta kekuatan mengikat hasil penyelesaian sengketa non-litigasi agar mekanisme ini dapat memberikan kepastian hukum bagi para pihak.

F. *Online Dispute Resolution* sebagai Mekanisme Penyelesaian Sengketa Digital

Online Dispute Resolution (ODR) merupakan bentuk inovasi dalam penyelesaian sengketa yang memanfaatkan teknologi informasi secara menyeluruh. ODR mengintegrasikan proses penyelesaian sengketa dengan platform digital, sehingga seluruh tahapan, mulai dari pengajuan sengketa hingga penyelesaian

[157] Gary Goodpaster, *Negotiation and Dispute Resolution* (New York: Aspen Publishers, 2001), 64-67.

[158] Gary Born, *International Commercial Arbitration* (Alphen aan den Rijn: Kluwer Law International, 2014), 78-81.

[159] Indonesia, "Undang-Undang Nomor 30 Tahun 1999 Tentang Arbitrase dan Alternatif Penyelesaian Sengketa" (1999).

akhir, dapat dilakukan secara daring. Mekanisme ini dinilai sangat relevan dengan karakteristik sengketa digital yang cepat dan lintas batas.[160]

ODR menawarkan berbagai keunggulan, antara lain efisiensi waktu, pengurangan biaya, serta kemudahan akses bagi para pihak. Dalam konteks masyarakat digital, ODR dapat menjadi sarana untuk memperluas akses keadilan, khususnya bagi pelaku usaha kecil dan konsumen yang sering kali menghadapi keterbatasan sumber daya untuk menempuh jalur litigasi.[161]

Dalam praktik internasional, ODR telah diterapkan secara luas, terutama dalam penyelesaian sengketa *e-commerce* dan perlindungan konsumen. Platform global seperti eBay dan PayPal menggunakan sistem ODR untuk menyelesaikan jutaan sengketa setiap tahunnya. Pengalaman ini menunjukkan bahwa ODR dapat berfungsi secara efektif apabila didukung oleh desain sistem yang transparan dan akuntabel.[162]

Di Indonesia, pengembangan ODR masih berada pada tahap awal. Belum adanya regulasi khusus yang mengatur ODR secara komprehensif menjadi tantangan utama. Meskipun demikian, peluang pengembangan ODR di Indonesia sangat besar seiring dengan meningkatnya aktivitas digital masyarakat. Negara perlu mengambil peran aktif dalam merumuskan kebijakan dan regulasi yang mendukung implementasi ODR sebagai bagian dari sistem penyelesaian sengketa nasional.[163]

Dengan demikian, ODR merupakan mekanisme yang menjanjikan dalam penyelesaian sengketa digital. Integrasi ODR ke dalam sistem hukum nasional memerlukan komitmen regulatif, kesiapan kelembagaan, serta peningkatan literasi digital masyarakat agar mekanisme ini dapat berjalan secara efektif dan berkeadilan.

---

[160] Ethan Katsh and Orna Rabinovich-Einy, *Digital Justice: Technology and the Internet of Disputes* (Oxford: Oxford University Press, 2017), 45-49.

[161] Pablo Cortés, "Developing Online Dispute Resolution for Consumers," *International Journal of Law and Information Technology* 19, no. 1 (2011): 1–24.

[162] Colin Rule, *Online Dispute Resolution for Business* (San Francisco: Jossey-Bass, 2022), 101-104.

[163] United Nations Commission on International Trade Law (UNCITRAL), *Technical Notes on Online Dispute Resolution* (New York: United Nations, 2017), 7-10.

G. Tantangan Penyelesaian Sengketa dalam Dunia Digital

Penyelesaian sengketa dalam dunia digital menghadapi berbagai tantangan yang bersifat multidimensional. Tantangan tersebut tidak hanya berasal dari aspek hukum, tetapi juga dari aspek teknis, kelembagaan, dan sosial. Kompleksitas sengketa digital menuntut sistem hukum untuk beradaptasi secara cepat, sementara perkembangan teknologi sering kali berjalan lebih cepat dibandingkan pembaruan regulasi yang ada. Kondisi ini berpotensi menimbulkan kesenjangan antara hukum dan realitas praktik di ruang digital.[164]

Salah satu tantangan utama adalah keterbatasan regulasi yang secara khusus mengatur penyelesaian sengketa digital. Meskipun Indonesia telah memiliki sejumlah peraturan yang berkaitan dengan teknologi informasi, pengaturan mengenai mekanisme penyelesaian sengketa digital masih bersifat parsial dan tersebar di berbagai regulasi. Ketiadaan regulasi yang komprehensif dapat menimbulkan ketidakpastian hukum dan perbedaan penafsiran dalam praktik.[165]

Tantangan berikutnya berkaitan dengan pembuktian dan pengelolaan alat bukti elektronik. Bukti digital memiliki karakteristik yang mudah diubah, disalin, dan dimanipulasi, sehingga menimbulkan persoalan terkait keaslian dan integritas data. Aparat penegak hukum dituntut untuk memiliki kemampuan teknis dalam menilai validitas bukti elektronik, sementara infrastruktur pendukung pembuktian digital masih belum merata di seluruh wilayah Indonesia.[166]

Selain itu, tantangan kelembagaan juga menjadi faktor penting. Lembaga penyelesaian sengketa, baik pengadilan maupun lembaga non-litigasi, belum sepenuhnya siap menghadapi lonjakan sengketa digital. Keterbatasan sumber daya manusia yang memiliki kompetensi di bidang hukum dan teknologi informasi

---

[164] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Book, 2006), 189-192.

[165] Hikmahanto Juwana, "Harmonisasi Hukum Nasional di Era Digital," *Jurnal Hukum Dan Pembangunan* 50, no. 3 (2020): 398–401.

[166] Makarim, *Hukum Pembuktian Elektronik,* 167-170.

menjadi kendala dalam penerapan mekanisme penyelesaian sengketa digital yang efektif.[167]

Di sisi lain, rendahnya literasi digital masyarakat turut memengaruhi efektivitas penyelesaian sengketa digital. Banyak pihak yang belum memahami hak dan kewajibannya dalam ruang digital, sehingga berpotensi memperbesar eskalasi sengketa. Oleh karena itu, peningkatan literasi hukum dan digital masyarakat menjadi bagian integral dalam mengatasi tantangan penyelesaian sengketa digital.

H. Perbandingan Penyelesaian Sengketa Digital di Beberapa Negara

Perbandingan praktik penyelesaian sengketa digital di beberapa negara menunjukkan adanya variasi pendekatan yang dipengaruhi oleh sistem hukum dan tingkat perkembangan teknologi. Negara-negara dengan infrastruktur digital yang maju cenderung lebih cepat mengadopsi mekanisme penyelesaian sengketa berbasis teknologi, termasuk *Online Dispute Resolution*. Pengalaman negara-negara tersebut dapat menjadi rujukan bagi Indonesia dalam mengembangkan sistem penyelesaian sengketa digital yang efektif.[168]

Uni Eropa, misalnya, telah mengembangkan kerangka hukum ODR yang terintegrasi untuk melindungi konsumen dalam transaksi elektronik lintas negara. Melalui Regulasi ODR Uni Eropa, konsumen dapat mengajukan sengketa secara daring melalui platform resmi yang disediakan oleh otoritas Eropa. Mekanisme ini bertujuan untuk memberikan penyelesaian sengketa yang cepat, murah, dan transparan.[169]

Amerika Serikat juga menunjukkan praktik yang berkembang dalam penyelesaian sengketa digital, khususnya melalui arbitrase dan mediasi daring. Berbagai platform digital swasta mengembangkan sistem ODR untuk menyelesaikan sengketa *e-commerce* dan layanan digital. Pendekatan berbasis

---

[167] Danrivanto Budhijanto, *Cyber Law: Sistem dan Permasalahan Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2020), 243-246.

[168] Cortés, *Online Dispute Resolution for Consumers in the European Union,* 91-94.

[169] "European Commission, Regulation (EU) No 524/2013 on Online Dispute Resolution for Consumer Disputes" (2013).

pasar ini memberikan fleksibilitas, namun juga menimbulkan perdebatan mengenai perlindungan konsumen dan kesetaraan posisi para pihak.[170]

Sementara itu, Singapura mengadopsi pendekatan yang mengintegrasikan ODR ke dalam sistem peradilan nasional. Negara ini mengembangkan Singapore *International Dispute Resolution Academy* sebagai pusat pengembangan kapasitas dan inovasi dalam penyelesaian sengketa digital. Pendekatan ini menunjukkan peran aktif negara dalam mendorong penyelesaian sengketa digital yang berstandar internasional.[171]

Perbandingan tersebut menunjukkan bahwa tidak terdapat satu model tunggal yang dapat diterapkan secara universal. Indonesia perlu mengembangkan model penyelesaian sengketa digital yang sesuai dengan karakteristik sistem hukum nasional, dengan tetap mengadopsi praktik terbaik dari berbagai negara.

Penyelesaian sengketa dalam dunia digital merupakan bagian penting dari pembangunan hukum nasional di era transformasi digital. Karakter sengketa digital yang kompleks dan dinamis menuntut adanya sistem penyelesaian sengketa yang adaptif, responsif, dan berorientasi pada keadilan substantif. Mekanisme penyelesaian sengketa konvensional perlu dilengkapi dengan pendekatan baru yang memanfaatkan teknologi informasi secara optimal.[172]

Penguatan kerangka hukum, baik melalui pembaruan regulasi maupun harmonisasi peraturan perundang-undangan, menjadi langkah strategis dalam menjamin kepastian hukum. Selain itu, kesiapan kelembagaan dan peningkatan kapasitas sumber daya manusia di bidang hukum dan teknologi informasi merupakan prasyarat utama bagi efektivitas penyelesaian sengketa digital.[173]

Pengembangan *Online Dispute Resolution* sebagai bagian dari sistem penyelesaian sengketa nasional menawarkan peluang besar untuk memperluas akses keadilan bagi masyarakat. Namun, pengembangan tersebut harus disertai

---

[170] Rule, *Online Dispute Resolution for Business*, 121-124.

[171] Sundaresh Menon, "Technology and the Changing Face of Justice," *Singapore Academy of Law Journal* 28, no. 1 (2016): 1–5.

[172] Katsh and Rabinovich-Einy, *Digital Justice: Technology and the Internet of Disputes,* 201-204.

[173] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Kencana, 2019), 311-314.

dengan pengaturan yang jelas mengenai legitimasi, prosedur, dan kekuatan mengikat putusan. Dengan sinergi antara regulasi, kelembagaan, dan literasi digital masyarakat, penyelesaian sengketa digital di Indonesia diharapkan mampu menjawab tantangan hukum di era digital secara berkelanjutan.[174]

[174] United Nations Commission on International Trade Law (UNCITRAL), *Technical Notes on Online Dispute Resolution,* 15-1.

BAB 7

TANGGUNG JAWAB HUKUM PLATFORM DIGITAL DAN PENYEDIA JASA INTERNET

Dessy Puspita Tjahjadi

A. Pendahuluan

Transformasi digital tengah marak dilakukan di Indonesia sebagai konsekuensi dari era revolusi digital. Hal ini sebagai konsekuensi dari perubahan lanskap perilaku ekonomi dan sosial secara mendunia, termasuk di Indonesia. Secara fundamental hal ini membawa perubahan dalam bentuk cara manusia berinteraksi dan beraktifitas. Tentunya ditujukan untuk diperolehnya kesejahteraan manusia dan penyelesaian permasalahan sosial secara holistik secara lebih baik.

Terbentuknya konvergensi digital mempercepat transformasi sektor ekonomi dan sosial Indonesia sebagai bagian dari masyarakat dunia, sekaligus memunculkan tantangan hukum baru sehubungan keamanan data, moderasi konten ilegal, serta tanggung jawab pengelola platform dan Internet Service Provider (ISP) di ranah digital.

Platform digital dan Internet Service Provider (ISP) kini menjadi tulang punggung infrastruktur digital yang menghubungkan jutaan pengguna dengan berbagai layanan elektronik.[175] Transformasi digital selain menghadirkan aspek perekonomian yang besar, juga menimbulkan kompleksitas hukum yang

[175] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843, ps. 15.

memerlukan pemahaman mendalam mengenai tanggung jawab hukum para penyelenggara layanan digital. Platform digital dan penyedia jasa internet juga memainkan peran krusial dalam memfasilitasi antara media sosial hingga transaksi lintas negara yang kini telah menjadi *common practice*. Meskipun hal ini memberikan banyak kemudahan dan mempercepat pertumbuhan ekonomi digital, interaksi sosial hingga transaksi ekonomi lintas negara melalui platform digital juga menimbulkan tantangan besar terkait aspek hukum, terutama dalam hal penentuan tanggung jawab hukum dan yuridiksi yang berlaku. Kebutuhan akan pengaturan tanggung jawab hukum yang adil, adaptif, dan relevan menjadi krusial dalam memitigasi resiko penyalahgunaan data, kebocoran privasi, dll.

Tulisan ini akan mengkaji tanggung jawab hukum dan konsekuensi hukum bagi penyedia platform digital dan jasa internet dalam menghadapi kompleksitas konvergensi digital serta bagaimana regulasi nasional dan harmonisasi hukum internasional dapat menjadi solusi dalam perlindungan hukum yang efektif.

Menyoroti hukum positif di Indonesia, dari aspek tanggungjawab hukum platform digital dan ISP diatur dalam berbagai peraturan perundang-undangan, dalam hal ini UU ITE (UU No. 11/2008) beserta perubahannya, juga UU PDP (UU No.27/2022), hingga berbagai peraturan pelaksana yang diterbitkan oleh Kementerian Komunikasi dan Informatika.[176] Kerangka hukum ini bertujuan menciptakan adanya perimbangan antara inovasi teknologi dan adanya perlindungan hak-hak fundamental pengguna.

Tantangan utama dalam menentukan tanggung jawab hukum terletak pada sifat dinamis teknologi digital yang seringkali berkembang lebih cepat daripada regulasi yang mengaturnya.[177] Hal ini menimbulkan kebutuhan untuk memahami prinsip-prinsip hukum yang fleksibel namun tetap memberi kepastian hukum bagi berbagai pihak yang terlibat dalam ekosistem digital.

[176] Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400, ps. 2.

[177] *Ibid*., ps. 13-14.

B. Kerangka Hukum Tanggung Jawab Platform Digital

1. Landasan Hukum Nasional tingkat Undang-undang

a. UU ITE dengan Perubahan-perubahannya

UU ITE berupa undang-undang pionir dalam mengatur aktivitas digital di Indonesia menetapkan dasar-dasar tanggung jawab penyelenggara sistem elektronik.

1) UU Informasi dan Transaksi Elektronik (ITE) yaitu UU No. 11/2008, kemudian direvisi oleh UU No. 19/2016 berikut UU No. 1/2024, merupakan landasan utama yang mengatur tanggungjawab penyelenggara sistem elektronik dan ISP atas konten ilegal serta keamanan ekosistem
2) Platform digital wajib menghapus atau memblokir konten ilegal berdasarkan notifikasi pemerintah; kelalaian dapat mengakibatkan sanksi pidana atau administratif hingga pembatasan operasional.
3) UU ITE menetapkan bahwa PSE (singkatan dari Penyelenggara Sistem Elektronik) memiliki tanggungjawab bersyarat (conditional liability model).
4) Pasal 15 UU ITE mengatur bahwa pihak PSE harus comply dalam pelenggaraan sistem elektronik secara handal juga aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana keharusnya. [178] Ketentuan Pasal 15 ayat (3) UU ITE memberikan pengecualian tanggung jawab bagi penyelenggara sistem elektronik atas bentuk-bentuk kerugian yang timbul akibat keadaan kahar/memaksa (force majeure) atau akibat kesalahan dan/atau kelalaian pihak pengguna sistem elektronik. [179] Namun, pengecualian ini tidak berlaku mutlak. Penyelenggara tetap dapat dimintai pertanggungjawaban apabila terbukti melakukan kelalaian dalam menjalankan kewajiban-kewajibannya yang diatur dalam perundang-undangan.
5) Penghapusan Konten Menurut UU ITE

[178] Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, Berita Negara Republik Indonesia Tahun 2020 Nomor 1373, ps. 2.

[179] *Ibid*., ps. 9.

a. Setiap PSE wajib **menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan** yang berada di bawah kendalinya berdasarkan *request* (permintaan) orang yang bersangkutan dan juga penetapan pengadilan (Pasal 26 ayat 3 UU ITE). Jadi, penghapusan konten terutama terkait informasi yang dianggap tidak benar, pelanggaran hak cipta, atau konten ilegal yang teridentifikasi secara hukum.
b. Pemerintah, terutama melalui Kementerian Kominfo, berwenang meminta pemutusan akses atau penghapusan konten yang melanggar peraturan perundang-undangan untuk mencegah penyebaran konten berbahaya atau ilegal.
c. Penghapusan konten di UU ITE lebih menitikberatkan pada konten publikasi digital yang melanggar hukum dan harus direspons oleh penyelenggara sistem elektronik sebagaimana diatur.

b. UU Perlindungan Data Pribadi (PDP)

1) UU PDP telah disahkan pada tahun 2022 memberikan dimensi baru dalam tanggung jawab platform digital, khususnya dalam pengelolaan data pribadi pengguna. Undang-undang ini mengadopsi ruh/prinsip internasional seperti "privacy by design" berikut "privacy by default" yang mengharuskan platform digital membangun sistem dengan mempertimbangkan perlindungan privasi sejak awal perancangan.[180]
2) UU No. 27/2022 tentang PDP (singkatan dari Perlindungan Data Pribadi) telah diberlakukan, juga memberikan definisi, hak, dan kewajiban bagi pengguna maupun pelaku usaha digital terkait pengelolaan serta keamanan data pribadi.
3) Implementasi UU PDP masih menghadapi tantangan berupa lemahnya kapasitas institusional, teknis, dan kesadaran masyarakat dalam memahami hak-hak sebagai subjek data.

[180] *Ibid*., ps. 15.

4) Platform digital dalam konteks UU PDP dapat berperan sebagai Pengendali Data Pribadi (Data Controller), Prosesor Data Pribadi (Data Processor), atau kombinasi keduanya.[181] Di mana setiap peran tersebut membawa kewajiban hukum yang spesifik dan sanksi bilamana ada pelanggaran.
5) Penghapusan Data Menurut UU PDP
   a) Pengendali Data Pribadi wajib **menghapus data pribadi** jika data tersebut sudah tidak diperlukan lagi untuk tujuan pemrosesan, ada permintaan dari subjek data, atau data diperoleh secara melawan hukum (Pasal 43 UU PDP).learning.
   b) Penghapusan harus dilakukan secara menyeluruh, mencakup data yang tersimpan di semua media termasuk backup serta harus memenuhi prinsip keamanan data agar data tidak dapat diakses lagi.
   c) UU PDP memberikan hak kepada subjek data (individu) untuk meminta penghapusan data ("*right to erasure*"), termasuk kewajiban pengendali data untuk memberitahu subjek data dan melaporkan pelanggaran terkait data pribadi (Pasal 44 UU PDP).
   d) Penghapusan data dalam UU PDP berfokus pada perlindungan privasi, keamanan dan hak individu dalam pengelolaan data pribadi.
   e) Penghapusan di **UU ITE** lebih bersifat hukum materiil terkait konten yang melanggar aturan, sementara di **UU PDP** penghapusan lebih teknis dan substansial terkait data.

Setiap platform digital di Indonesia wajib menaati kedua regulasi tersebut dan menyesuaikan kebijakan internal agar terhindar dari tuntutan hukum serta bisa melindungi *user* / pengguna dan reputasi bisnis di era digital.

Berdasarkan ke-2 undang-undang yang dimaksud, ditinjau dari perbedaan ke-2 Undang – undang tersebut jika ditinjau dari aspek fokus, compliances, kewajiban, sanksi, dan tanggung jawab; maka dapat diklasifikasikan secara terpenrinci.

[181] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 195, Tambahan Lembaran Negara Republik Indonesia Nomor 6820, Bab V.

Perbedaan Tanggung Jawab Platform Digital antara UU ITE & UU PDP

ASPEK	UU ITE	UU PDP
Fokus	moderasi konten ilegal	perlindungan data pribadi
Obyek dipatuhi / *compliances*	konten, transaksi elektronik	penggunaan data pribadi
Kewajiban	hapus/blokir konten, respons aduan, pelaporan ke pemerintah	minta persetujuan, lindungi data, hak akses subjek data
Sanksi	pidana, administratif, blokir/pencabutan izin	pidana, administratif, denda, pencabutan izin
Tanggungjawab	bersyarat/reaktif, *safe harbor*	akuntabilitas mutlak/ sepenuhnya

Perbedaan Pengaturan Jenis Penghapusan antara UU ITE & UU PDP:

JENIS	UU ITE	UU PDP
Objek	Konten Informasi Elektronik & Dokumen Elektronik (berkaitan dengan hukum konten)	Data Pribadi (berkaitan dengan privasi dan perlindungan data)
Dasar	Permintaan orang terkait dengan penetapan pengadilan, atau perintah pemerintah	Permintaan subjek data, tidak relevan lagi, atau data diperoleh secara tidak sah
Mekanisme	Pemutusan akses dan penghapusan oleh PSE yang mengelola konten	Penghapusan menyeluruh di semua media penyimpanan oleh pengendali data
Tujuan	Menghapus konten yang melanggar hukum atau tidak relevan	Melindungi hak privasi dan keamanan data pribadi pengguna

Kewenangan	PSE dan Pemerintah	Pengendali Data Pribadi dan hak individu sebagai subjek data

Dapat diamati bahwa perbedaan utama pengaturan penghapusan konten dalam **UU ITE** dan penghapusan data dalam **UU PDP** terletak pada objek dan mekanisme penghapusan yang diatur masing-masing.

2. Landasan Hukum Nasional tingkat Peraturan Pelaksana dan Surat Edaran

a. Peraturan Pemerintah Nomor 71 Tahun 2019

PP 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan detail operasional mengenai kewajiban penyelenggara sistem elektronik, termasuk perihal persyaratan teknis minimal sistem elektronik, kewajiban sertifikasi keamanan, dan prosedur audit dan evaluasi sistem[182]

b. Surat Edaran Menteri Kominfo Nomor 5 Tahun 2016

Surat edaran ini secara khusus mengatur tanggung jawab platform digital terhadap User Generated Content (UGC). Platform diwajibkan untuk:

1) Melakukan moderasi konten secara efektif
2) Menyediakan mekanisme pelaporan konten ilegal
3) Menindaklanjuti laporan dalam waktu yang wajar[183]

c. Regulasi Spesifik untuk OSS dan e-Commerce

1) PP No. 5 Tahun 2021 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko dan Perpu No. 2 Tahun 2022 tentang Cipta Kerja mewajibkan OSS-RBA untuk pelaku usaha, termasuk UMKM serta korporasi multinasional.

[182] Damar Juniarto, "Menyoal Aturan PSE Lingkup Privat: Ancaman bagi Kebebasan Sipil di Ruang Digital," dalam *Jurnal Hukum Digital & Masyarakat* 3, no. 1 (2021): 45-60.

[183] "Kominfo Buka Blokir Steam, Counter Strike, dan Dota," *CNN Indonesia*, 2 Agustus 2022, https://www.google.com/search?q=https://www.cnnindonesia.com/teknologi/20220802111152-185-828945/kominfo-buka-blokir-steam-counter-strike-dan-dota.

2) Peraturan Menteri Kominfo No. 5 Tahun 2020 mengatur mekanisme pelaporan dan penghapusan konten ilegal, perlindungan konsumen, serta sanksi administratif.

3. Standar Internasional dan *Best Practice* Sebagai *Benchmark* dan/atau Perbandingan Kerangka Hukum Internasional Secara Global

a) Safe Harbor, Generalis, dan Lex Specialis

Model safe harbor di Indonesia menekankan pembatasan tanggung jawab platform jika sudah melakukan langkah preventif terhadap konten ilegal; pengaturan yang serupa dengan Digital Millennium Copyright Act (DMCA, AS) dan General Data Protection Regulation (GDPR, Eropa). Pendekatan lex generalis dan lex specialis: UU ITE berlaku umum, sedangkan UU Hak Cipta, UU Perlindungan Konsumen, atau UU PDP digunakan secara khusus terhadap pelanggaran yang lebih spesifik.

b) Standar Global Perlindungan Data Pribadi

GDPR Eropa dijadikan rujukan standar pengelolaan, akses, dan penghapusan data pengguna oleh platform digital global. Amerika Serikat menerapkan DMCA dan Communications Decency Act (CDA Sec. 230) sebagai standar perlindungan serta pembatasan tanggung jawab platform digital atas konten pihak ketiga.

Indonesia juga mengadopsi berbagai standar internasional dalam mengatur tanggung jawab platform digital. Prinsip "safe harbor" yang berkembang dalam hukum Amerika Serikat melalui Digital Millennium Copyright Act (DMCA) dan Communications Decency Act Section 230 memberikan inspirasi bagi pengaturan tanggung jawab terbatas platform digital.[184] Namun, penerapan safe harbor di Indonesia memiliki karakteristik khusus yang disesuaikan dengan kondisi hukum dan sosial Indonesia, dengan memberikan perlindungan bersyarat kepada platform digital yang menjalankan kewajiban moderasi dan kepatuhan regulasi.

C. Tanggung Jawab Spesifik Platform Digital

1. Tanggung Jawab terhadap Konten Pengguna

[184] Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Ithaca: Cornell University Press, 2019).

a. Prinsip Umum Tanggung Jawab

Platform digital pada umumnya tidak dibebankan pertanggungjawaban atas konten yang diunggah/ di-upload oleh pengguna (principle of no general monitoring obligation). Namun, tanggung jawab dapat timbul dalam situasi tertentu, seperti platform mengetahui adanya konten ilegal namun tidak mengambil tindakan, platform secara aktif mendorong atau memfasilitasi konten illegal, platform gagal menerapkan sistem moderasi yang memadai[185]

b. Kewajiban Moderasi Konten

Berdasarkan SE Menkominfo No. 5 tahun 2016, platform digital memiliki kewajiban:

1) Menyediakan mekanisme pelaporan konten (notice and takedown)
2) Merespons laporan dalam waktu paling lambat 24 jam untuk konten yang jelas melanggar hukum
3) Menyediakan prosedur banding bagi pengguna yang kontennya dihapus[186]

2. Tanggung Jawab dalam PDP

a. Kewajiban Pengendali dan Prosesor Data

UU PDP mengklasifikasikan platform digital sebagai pengendali data pribadi yang memiliki kewajiban untuk memperoleh persetujuan secara sah dari subjek data, menerapkan prinsip minimalisasi data, menjamin keamanan dan kerahasiaan data, dan memberikan akses kepada subjek data untuk mengelola data pribadinya[187]

Di dalam Platform digital yang memproses data pribadi anak menghadapi kewajiban tambahan berupa harus adanya persetujuan dari orang tua atau wali, menerapkan mekanisme verifikasi usia, dan memberikan perlindungan khusus terhadap data sensitif anak[188]

b. Kewajiban Pelaporan Insiden Keamanan

---

[185] Communications Decency Act of 1996, 47 U.S.C. § 230(c)(1).

[186] *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).

[187] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102.

[188] European Commission, "Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines," press release, 25 April 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

Ketika terjadi pelanggaran data pribadi, platform digital wajib melaporkan insiden kepada otoritas dalam waktu 72 jam, memberitahukan kepada subjek data yang terdampak, dan melakukan investigasi dan remediasi[189]

3. Tanggung Jawab Platform Digital dan ISP di Indonesia

a. Tanggung Jawab Platform Digital

Tanggung jawab platform digital mencakup: pengendalian moderasi konten; penyediaan mekanisme pelaporan pelanggaran bilamana hal ini terjadi; serta penghapusan/pemblokiran konten ilegal seperti *hate speech*, pornografi, penipuan, dan pelanggaran hak cipta.

Sanksi pidana dan administratif bagi platform yang membiarkan konten ilegal—pasal 27–29 UU ITE; dan pasal pelanggaran merek di e-commerce.

1) Platform digital dapat digugat secara perdata atas kelalaian menanggulangi pelanggaran oleh pihak ketiga, berdasarkan aturan PMK (Pasal 1365 KUHPdt).
2) Tanggung Jawab Platform Digital, menurut UU ITE:

a) Platform digital diwajibkan untuk memantau, mengendalikan, dan menghapus konten ilegal seperti ujaran kebencian, pornografi, penipuan, dan pelanggaran hak cipta.
b) Harus menyediakan mekanisme pelaporan, merespons aduan pengguna, dan secara proaktif melaporkan serta menghapus konten terlarang sesuai permintaan pemerintah.
c) Jika lalai, platform dapat dikenai sanksi pidana (berupa penjara hingga enam tahun dan/atau denda sampai Rp1 miliar sesuai Pasal 27–29 UU ITE) serta sanksi administratif (denda, pemblokiran, atau pencabutan izin).
d) Model tanggung jawab UU ITE cenderung bersyarat dan reaktif; platform tidak bertanggung jawab mutlak atas pelanggaran pengguna, tetapi wajib menindaklanjuti jika diberitahu oleh otoritas.

[189] European Commission, "Commission opens formal proceedings against X under the Digital Services Act," press release, 18 December 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709.

Jadi menurut UU PDP, platform digital yang berperan sebagai pengendali data harus memperoleh persetujuan subjek data sebelum mengumpulkan, memproses, dan menyimpan data pribadi, harus menjamin keamanan data pribadi, transparansi penggunaan, dan memberikan hak kepada subjek data untuk mengakses, mengubah, menghapus, dan menarik persetujuan, jika terjadi pelanggaran atau kebocoran data, platform dapat dikenai sanksi administratif (peringatan, pembatasan, pencabutan izin, denda administratif) dan sanksi pidana (penjara hingga 5 tahun dan denda maksimal Rp 5 miliar), model tanggung jawab UU PDP lebih prospektif dan mutlak pada perlindungan hak privasi individu serta pemenuhan standar keamanan seluruh proses pengelolaan data.

b. Tanggung Jawab ISP

1) ISP wajib menyediakan akses yang aman dan menanggulangi penyebaran konten melanggar hukum secara proaktif (pemantauan sistem) dan reaktif (respon laporan).
2) Sanksi ISP meliputi administratif (peringatan, denda, pembatasan/pencabutan izin), perdata (ganti rugi pengguna yang dirugikan), dan pidana jika terbukti sengaja membiarkan distribusi konten ilegal.

4. Penerapan Safe Harbor dan Generalis di Indonesia

a) Industri UMKM dan Industri Besar

1) Safe harbor belum diatur spesifik dalam Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik—masih berpedoman pada Surat Edaran Kominfo Nomor 5 Tahun 2016 dan doktrin penafsiran umum UU ITE.
2) Secara generalis, penggunaan platform digital untuk perizinan berusaha berbasis resiko, yang disebut dengan OSS_RBA (singkatan dari Online Single Submission – Risk-Base Approach) yang dikelola oleh Kementerian Investasi/ BKPM dan terintegrasi dengan berbagai instansi pemerintah; dibuat untuk memudahkan pelaku usaha dari tingkat UMKM hingga korporasi multinasional. Tetap membebankan tanggung jawab hukum, yang berlaku terhadap badan usaha yang mendaftarkan diri, jika

dikemudian hari, diketahui melakukan upaya perizinan untuk maksud distribusi barang/jasa ilegal lewat sistem digital.

b) Perusahaan Asing dan Marketplace

1) Perusahaan asing yang beroperasi di Indonesia wajib patuh pada ketentuan hukum lokal termasuk UU ITE dan UU PDP; selain menerapkan standar internasional seperti GDPR dan DMCA.

Marketplace selaku PSE wajib menjaga hak cipta dan tidak membiarkan peredaran produk ilegal (safe harbor model)—jika lalai, tanggung jawab dapat dibebankan secara pidana maupun perdata.

D. Studi Kasus

Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa pada tahun 2023, Indonesia mengalami lebih dari 403 juta anomali lalu lintas yang mengarah pada serangan siber. Serangan-serangan ini menunjukkan bahwa ekosistem digital di Indonesia dinilai kurang kuat/ masih lemah, dan kasus kebocoran data pribadi juga kerap terjadi. Pada tahun 2022, Indonesia menghadapi serangan siber, jenis ancaman malware dari botnet, berakibat pada terjadinya kebocoran data secara massif dan bermakna. Hal ini mencetuskan pemberlakuan UU PDP Nomor 27/2022, yang efektif berlaku mulaidi bulan Oktober tahun 2024. UU yang mendasari regulasi utama dalam perlindungan data pribadi.

Berdasarkan hal tersebut, maka setiap instansi dan badan hukum wajib berbenah diri dari aspek konten digital platform nya, diantaranya:

1. Putusan Permohonan Ahli Waris Anak di Bawah Umur di Platform Digital Putusan3.mahkamahagung.go.id

Contoh penetapan perwalian anak di bawah umur yang diakses via direktori putusan Mahkamah Agung menunjukkan pentingnya perlindungan hak privat dan pengelolaan data anak dalam ekosistem digital. Dalam penetapan tersebut, pengelolaan data anak di bawah umur untuk keperluan perwalian, balik nama sertifikat, atau pengurusan hak waris wajib tunduk pada prinsip perlindungan privasi, serta regulasi PDP dan UU ITE.

Sehingga dengan kata lain, platform Direktori Putusan Mahkamah Agung (putusan3.mahkamahagung.go.id); menghadapi tantangan khusus dalam menyeimbangkan transparansi peradilan dengan perlindungan data pribadi anak. Hal ini beresiko dalam perkara yang melibatkan anak khususnya pada perkara permohonan perwalian anak yang seringkali sarat dengan data pribadi dan riwayat keluarga dan pribadi anak, seharusnya juga menerapkan anonimisasi sesuai dengan Surat Keputusan Ketua Mahkamah Agung RI Nomor 1-144/KMA/SK/I/2011.[190]

Kasus ini bisa dijadikan acuan contoh kasus nyata yang menunjukkan bahwa kegagalan anonimisasi berikut jejak digitalnya, dapat memberikan kemudahan terjadinya tindak kejahatan berupa penyalahgunaan data anak oleh pihak lain, sehingga anak yang dimohonkan penetapan perwaliannya menjadi rentan terhadap penyalahgunaan data pribadinya. Untuk kasus pidana anak seperti perudungan dll, hal ini bahkan bisa menyebabkan resiko adanya trauma psikologis pada anak yang terlibat dalam perkara. Komisi Perlindungan Anak Indonesia (KPAI) melaporkan adanya anak yang mengajukan perubahan nama secara hukum akibat trauma dari publikasi identitas dalam putusan pengadilan. [191] Praktik terbaik anonimisasi diantaranya meliputi penggantian nama dengan inisial atau istilah umum ("ANAK", "PEMOHON","TERMOHON",dll.), penghilangan informasi yang dapat mengidentifikasi, dan redaksi alamat dan detail personal lainnya.

2. Praktik "Sharenting" di Platform Sosial Media

Fenomena sharenting atau membagikan dokumentasi anak saat moment parenting oleh orang tua, telah banyak mendominasi ruang sosial media Indonesia—orang tua membagikan data/informasi anak tanpa persetujuan, menimbulkan pelanggaran privasi anak.

Kasus selebriti dan influencer seperti Rachel Vennya dan Raffi Ahmad menyoroti ketidakpahaman terhadap bahaya privasi, eksposur berlebihan, risiko pencurian identitas, serta potensi eksploitasi data anak di platform digital.

[190] Paddy Leerssen, "The Digital Services Act: A New Era of Platform Accountability," *European Journal of Digital Law* 4, no. 2 (2023): 215-235.

[191] Rogier Creemers, "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management," *Journal of Contemporary China* 26, no. 103 (2017): 85-100.

Regulasi saat ini masih minim dalam penegakan batas privasi anak di ruang digital, meski UU PDP telah memberi dasar hukum pembatasan dan perlindungan atas data anak.

Fenomena sharenting, sebagai praktik orang tua membagikan foto dan informasi anak di media sosial, menimbulkan dilema hukum baru. Platform media sosial menghadapi tantangan dalam menentukan batas-batas perlindungan anak sambil tetap menghormati kebebasan berekspresi pengguna.[192] Kini beberapa platform media sosial global telah mengembangkan kebijakan khusus untuk membatasi eksploitasi komersial terhadap anak di bawah umur melalui konten yang dibagikan orang tua. Implementasi kebijakan serupa di Indonesia masih memerlukan harmonisasi dengan UU Perlindungan Anak dan UU PDP.[193]

3. Kasus Kebocoran Data Pribadi dan Ecosystem Digital

Kasus kebocoran data e-commerce Tokopedia (2020) mengungkap kelemahan sistem keamanan, kurangnya akuntabilitas perusahaan, dan celah regulasi dalam perlindungan data pribadi pengguna digital.

Serangan siber terhadap ekosistem digital Indonesia pada 2022–2023 menunjukkan kerentanan sistem, lemahnya perlindungan siber, dan tingginya angka kebocoran data pribadi.

UU PDP dan PP terkait belum optimal dalam praktik perlindungan hak konsumen, menunjukkan pentingnya harmonisasi standar global dan penguatan literasi digital untuk semua pelaku usaha terkait OSS dan platform digital.

E. Penutup

Bab ini memberikan analisis komprehensif tentang tanggung jawab hukum platform digital dan ISP di Indonesia dan global, diperkaya studi kasus relevan serta penerapan dalam ekosistem OSS, UMKM, dan industri besar maupun perusahaan asing. Bahasan ini memetakan tantangan, solusi, serta urgensi penguatan regulasi dan literasi digital sebagai respons terhadap dinamika siber dan ekosistem digital yang terus berubah.

---

[192] *Gonzalez v. Google LLC*, 598 U.S. ___ (2023).
[193] Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512.

Perbedaan utama tanggung jawab platform digital menurut UU ITE dan UU PDP adalah fokus regulasi: UU ITE menekankan pengendalian dan moderasi konten ilegal di sistem platform, sedangkan UU PDP menitikberatkan pada perlindungan, pengelolaan, dan keamanan data pribadi pengguna dari sisi hak subjek data serta pengendali data.

Berdasarkan hal tersebut diatas, saran, rekomendasi atas hal-hal yang membutuhkan perhatian dan penelaahan lebih lanjut diantaranya:

1. Pemerintah sebaiknya memberikan kejelasan terhadap definisi "konten terlarang" yang bersifat ambigu pada UU ITE dan memberi pengaturan atas ketiadaan pengawasan independen digital.
2. Kebijakan dan penegakan hukum lintas batas serta perhatian terhadap kapasitas institusi lokal menghadapi perusahaan multinasional dan industri besar; sebagai dampak minimnya literasi digital dan kesadaran konsumen serta pelaku usaha (misalnya UMKM).
3. Ancaman terhadap kebebasan berekspresi versus regulasi moderasi konten.
4. Penataan lebih jelas tentang safe harbor dan pedoman transparansi penyelenggaraan platform digital.
5. Harmonisasi regulasi lokal dengan standar global seperti GDPR untuk perlindungan data dan hak konsumen.
6. Penguatan literasi digital, perlindungan privasi anak, serta pengawasan publik agar ecosystem digital sehat dan berkelanjutan.

BAB 8

ARSITEKTUR HUKUM KEAMANAN TRANSAKSI DIGITAL DAN INOVASI FINTECH DI ERA SIBER

Dr. Ani Purwati, S.H., M.H

A. Konseptualisasi Hukum Cyber

Perkembangan hukum cyber mengikuti kemajuan teknologi digital. Pada 1970–1980-an, istilah *computer law* digunakan karena pengaturan hukum masih berfokus pada komputer sebagai alat. Regulasi saat itu berkaitan dengan perlindungan perangkat lunak, lisensi *software*, hak cipta program komputer, serta kejahatan komputer seperti akses tanpa izin dan perusakan data. Para ahli seperti Bainbridge dan Reed memandang fase ini sebagai perluasan hukum kekayaan intelektual, perdata, pidana ke dunia komputasi.[194] Ketika internet berkembang pada 1990-an, lahirlah istilah *internet law* yang memperluas perhatian dari komputer ke jaringan global. Pada fase ini muncul isu seperti nama domain, tanggung jawab ISP, transaksi *e-commerce*, spam, pencemaran nama baik daring, kontrak elektronik,[195] tanda tangan elektronik dan alat bukti elektronik. Di Indonesia, perkembangan ini tercermin dalam UU 11/2008 tentang ITE yang kemudian diperbarui melalui UU 19/2016 dan UU 1/2024 untuk memperkuat pengaturan konten ilegal, pencemaran nama baik, hoaks serta kewajiban PSE.

---

[194] Bainbridge, D. I. (2004). *Introduction to computer law* (5th ed.). Pearson Education; Reed, C. (2000). *Internet law: Text and materials*. Butterworths

[195] Katsh, E. (1995). *Law in a digital world*. Oxford University Press; Koops, B.-J. (2010). The quest for cybercrime principles. In B.-J. Koops et al. (Eds.), *Cybercrime and jurisdiction* (pp. 27–62). T.M.C. Asser Press.

Seiring meningkatnya aktivitas digital, istilah *cyber law* muncul sebagai konsep yang lebih luas Hukum siber mencakup berbagai cabang hukum pidana, perdata, administrasi, telekomunikasi, kekayaan intelektual, dan perlindungan data selama masih terkait dengan penggunaan teknologi digital. Saat ini, fokus hukum cyber terutama mengarah pada perlindungan data pribadi dan keamanan siber. Perlindungan data diperkuat melalui UU 27/2022 tentang PDP yang berlaku penuh sejak 17 Oktober 2024 sementara keamanan siber diatur melalui PP 71/2019 tentang PSTE, Perpres 47/2023 tentang SKSN dan Peraturan BSSN 5/2024 tentang RAN Keamanan Siber. Seluruh instrumen ini membentuk kerangka tata kelola keamanan siber nasional, perlindungan infrastruktur informasi vital serta penanganan insiden siber secara koordinatif. Perkembangan tersebut menunjukkan bahwa hukum cyber Indonesia merupakan hasil integrasi dari *computer law* dan *internet law* yang kemudian berkembang menjadi rezim hukum digital modern.

1. Konsolidasi *Cyber Law*: Rezim Hukum Siber sebagai Kerangka Digital Modern

Perkembangan teknologi digital mendorong lahirnya *cyber law* sebagai konsep yang lebih luas dibanding *computer law* dan *internet law*. Jika pada tahap awal regulasi hanya mengatur perangkat komputer, lalu beralih pada persoalan internet dan transaksi elektronik, maka *cyber law* hadir sebagai rezim hukum yang menyatukan seluruh aspek hukum yang berkaitan dengan aktivitas di ruang siber. Konsep ini mencakup dimensi pidana, perdata, administrasi, telekomunikasi, kekayaan intelektual, hingga perlindungan data pribadi dan keamanan siber. Sebagai kerangka digital modern, *cyber law* tidak hanya menjawab kejahatan dan sengketa di dunia maya, tetapi juga mengatur tata kelola data, kewajiban penyelenggara sistem elektronik, standar keamanan serta hak-hak individu dalam ekosistem digital. Pendekatan ini memungkinkan hukum beradaptasi dengan teknologi yang terus berkembang seperti cloud computing, kecerdasan buatan, dan Internet of Things. Dengan demikian, *cyber law* menjadi fondasi normatif yang memastikan ruang digital tetap aman, terpercaya, dan menghormati hak-hak pengguna.

2. *Cyber Law* Indonesia: Integrasi Perlindungan Data Pribadi dan Keamanan Siber

Hukum cyber juga berhubungan erat dengan hukum teknologi informasi, perlindungan data pribadi, dan kebijakan keamanan digital. Hukum teknologi informasi melalui UU ITE, PP 71/2019 dan peraturan Kominfo menyediakan fondasi pengaturan sistem elektronik, kontrak elektronik, bukti elektronik, dan kewajiban PSE. UU PDP melengkapi fondasi tersebut dengan menetapkan prinsip-prinsip perlindungan data pribadi berdasarkan asas transparansi, tujuan tertentu, minimalisasi data, dan akuntabilitas serta menetapkan hak subjek data dan kewajiban pelaporan insiden. Kebijakan keamanan digital diperkuat melalui Perpres BSSN, Perpres SKSN, serta pedoman keamanan siber terbaru. Pemerintah juga sedang menyesuaikan PP 71/2019 agar lebih relevan dengan perkembangan teknologi seperti kecerdasan buatan dan *cloud computing*. Hukum TI mengatur infrastruktur digital, UU PDP mengatur perlindungan data, sedangkan rezim keamanan siber memastikan keamanan dan keandalan sistem. Kajian hukum cyber membutuhkan pendekatan interdisipliner.

Dari sisi hukum, analisis perlu memperhatikan hubungan antarregulasi dan perbedaan antara aturan dan praktik. Dari sisi komunikasi, hukum cyber berkaitan dengan moderasi konten, algoritme distribusi informasi, ujaran kebencian dan disinformasi. Perspektif sosiologi digital menjelaskan bagaimana masyarakat merespons kewajiban hukum di tengah rendahnya literasi digital. Dari sisi ilmu komputer, efektivitas hukum cyber ditentukan oleh penerapan standar teknis seperti enkripsi, autentikasi berlapis, *access control*, pengelolaan log, segmentasi jaringan, dan penerapan *Zero Trust Architecture (ZTA)*.[196] Semua aspek teknis ini menjadi dasar penting dalam penyusunan kewajiban hukum untuk melindungi infrastruktur informasi vital.

Dari sisi hukum, analisis perlu memperhatikan hubungan antarregulasi dan perbedaan antara aturan

[196] National Institute of Standards and Technology. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). U.S. Department of Commerce; National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations* (NIST Special Publication 800-53, Rev. 4). U.S. Department of Commerce

B. Kerangka Teoretik Hukum Siber Kontemporer: *Risk Regulation, Digital Sovereignty, Cyber Governance, Global Cyber Norms*

1. Teori Regulasi Risiko (*Risk Regulation Theory*) dalam Ekosistem Digital

Teori Regulasi Risiko dalam hukum cyber hukum modern tidak lagi cukup hanya mengatur perilaku atau menjatuhkan sanksi tetapi harus mampu mengantisipasi dan mengelola risiko yang lahir dari teknologi digital. Risiko siber bersifat lintas batas, cepat berubah, semakin kompleks sehingga sering kali sulit diprediksi oleh regulator maupun pelaku usaha. Mengacu pada gagasan *risk society* Ulrich Beck risiko digital dipahami sebagai jenis risiko baru yang tidak dapat ditangani dengan pendekatan hukum yang sekadar merespons pelanggaran.[197] Hukum cyber diarahkan untuk mengenali, menilai, dan mengurangi risiko melalui penguatan regulasi, institusi, dan standar keamanan. Risiko yang dihadapi meliputi ancaman teknis seperti malware, ransomware, dan kerentanan sistem; risiko manusia seperti *human error* dan lemahnya kontrol akses; risiko ekonomi yang berhubungan dengan dominasi platform digital; serta risiko kelembagaan akibat tumpang tindih aturan dan minimnya koordinasi antarinstansi.[198]

Pendekatan berbasis risiko bertujuan menekan kemungkinan terjadinya insiden, membatasi dampaknya, dan membagi beban tanggung jawab secara proporsional antara negara, Penyelenggara Sistem Elektronik (PSE), dan masyarakat. Di Indonesia, pendekatan ini tercermin dalam beberapa regulasi utama. UU ITE dan perubahannya melalui Pasal 15 mewajibkan PSE menjaga keamanan dan keandalan sistem elektronik. PP 71/2019 menetapkan standar keamanan minimum serta kewajiban menjaga kerahasiaan dan integritas sistem (Pasal 24–26). UU 27/2022 tentang PDP semakin memperkuat pendekatan *risk-based* dengan mewajibkan langkah teknis–organisasi (Pasal 35), pelaporan insiden kebocoran data (Pasal 46), serta *Data Protection Impact Assessment* untuk pemrosesan berisiko tinggi (Pasal 34).

---

[197] Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

[198] Clarke, R., & Knake, R. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press

Pada level kebijakan nasional Perpres 47/2023 mengatur perlindungan infrastruktur informasi vital dan mekanisme krisis, diperkuat oleh Perpres 53/2017 dan 28/2021 tentang BSSN serta peraturan mengenai Rencana Aksi Nasional Keamanan Siber. Dalam pelaksanaannya, teori ini diterjemahkan ke beberapa model regulasi, seperti model *command-and-control* yang menetapkan kewajiban teknis (misalnya enkripsi dan penyimpanan log lima tahun), model *risk-based* yang menyesuaikan kewajiban dengan tingkat risiko pengolahan data, serta instrumen berbasis pasar seperti sertifikasi keamanan. Selain itu, model ko-regulasi dan swa-regulasi juga diterapkan melalui kebijakan platform digital yang disesuaikan dengan UU ITE dan PP 71/2019.[199] Pendekatan ini menghadapi sejumlah tantangan, mulai dari keterbatasan pemahaman regulator terhadap teknologi baru, risiko *over-regulation* atau *under-regulation* hingga ketimpangan distribusi risiko yang sering lebih membebani pengguna. Penegakan hukum lintas negara juga masih menjadi hambatan besar karena sifat ruang siber yang tanpa batas. Dalam konteks akademik S3, Teori Regulasi Risiko menjadi kerangka analitis penting untuk menilai apakah regulasi Indonesia UU ITE, UU PDP, PP 71/2019 dan kebijakan BSSN sudah sesuai dengan tingkat risiko digital yang berkembang atau masih perlu diperkuat melalui integrasi konsep kedaulatan digital, *cyber governance* dan *global cyber norms* agar hukum siber Indonesia semakin adaptif dan melindungi hak masyarakat secara lebih efektif.[200]

2. Teori Kedaulatan Digital dan Implikasinya terhadap Yurisdiksi Siber

Teori Kedaulatan Digital menegaskan bahwa negara tidak lagi hanya berkuasa atas wilayah fisik, tetapi juga atas ruang digital yang mencakup data, infrastruktur, arus informasi, aplikasi, platform yang beroperasi di dalam yurisdiksinya. Negara berhak menetapkan aturan keamanan siber, mengatur pemrosesan data, mengawasi aktivitas platform asing serta melindungi warga negara dalam interaksi digital global. Konsep ini lahir dari perluasan teori kedaulatan Westphalia yang digabungkan dengan prinsip yurisdiksi teritorial dan fungsional dalam hukum

[199] Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press.

[200] Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press

internasional.[201] Pesatnya teknologi termasuk cloud, pusat data, layanan digital lintas negara menuntut negara memperluas kedaulatannya ke ranah non-teritorial.[202] Dalam konteks Indonesia berbagai regulasi menunjukkan arah penguatan kedaulatan digital. UUD 1945 Pasal 1 ayat (2) memberi dasar negara mengatur ruang digital. UU ITE memberikan landasan yurisdiksi ekstrateritorial (Pasal 2), mewajibkan keamanan sistem elektronik (Pasal 15) dan memberi kewenangan negara memutus atau mengendalikan akses terhadap konten digital (Pasal 40). PP 71/2019 mendukung kedaulatan data melalui kewajiban penyimpanan data PSE publik di Indonesia (Pasal 20) serta standar keamanan dan audit (Pasal 24–26). UU PDP memperkuat perlindungan warga negara dengan menetapkan hak subjek data (Pasal 4–9), kewajiban pengendali data (Pasal 35), dan aturan ketat transfer data ke luar negeri (Pasal 56–57). Pada sisi keamanan siber, Perpres 47/2023 menegaskan perlindungan infrastruktur vital dan mekanisme respons krisis yang dipimpin BSSN, sesuai mandat Perpres 53/2017 dan 28/2021.

Teori kedaulatan digital juga berpengaruh besar terhadap yurisdiksi siber. Pertama, yurisdiksi teritorial diperluas sehingga Indonesia dapat menindak pelanggaran digital yang berdampak di Indonesia meskipun dilakukan dari luar negeri (UU ITE Pasal 2). Kedua, yurisdiksi personal memberi negara kewenangan melindungi data warga negara yang diproses di luar negeri sesuai UU PDP. Ketiga, yurisdiksi subjektif–objektif memungkinkan penegakan hukum terhadap pelanggaran digital lintas negara. Keempat, yurisdiksi atas platform asing ditegakkan melalui kewajiban registrasi PSE asing dan kepatuhan pada aturan konten sesuai PP 71/2019 dan Permen Kominfo[203]. Penerapan kedaulatan digital juga menghadapi tantangan, seperti tumpang tindih klaim yurisdiksi antarnegara, besarnya dominasi perusahaan teknologi global, dilema antara pengendalian negara dan kebebasan internet, serta keterbatasan penegakan hukum siber.[204]

---

[201] Nye, J. S. (2010). *Cyber power*. Harvard Kennedy School. (hlm. 12–15)

[202] DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. (hlm. 25–33)

[203] Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press. (hlm. 102–118)

[204] Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677–739. (hlm. 678–700)

C. *Cyber Governance* dan *Multi-Stakeholder Approach*

Cyber governance adalah kerangka tata kelola yang mengatur bagaimana negara, sektor privat, masyarakat sipil, komunitas teknis, dan pengguna bekerja sama mengelola ruang digital yang bersifat lintas batas dan terus berkembang. Karena internet dibangun oleh banyak actor mulai dari penyedia infrastruktur hingga platform global tata kelola siber tidak dapat sepenuhnya dijalankan hanya oleh negara.[205] Ruang digital membutuhkan kombinasi regulasi nasional, standar teknis internasional, kebijakan platform digital, serta kerja sama global agar keamanan, privasi, inovasi, hak digital, dan stabilitas ekosistem digital tetap terjaga.Pendekatan multi-stakeholder diperlukan karena sebagian besar infrastruktur digital dikelola sektor privat, sedangkan standar internet dibuat oleh komunitas teknis seperti IETF, ICANN, W3C.[206] Platform global seperti Google, Meta, TikTok, dan X juga memiliki kebijakan internal yang membentuk ruang publik digital. Selain itu, ancaman siber yang bersifat global membuat kolaborasi seluruh aktor menjadi kewajiban, bukan pilihan.[207]

Dengan demikian, pemerintah berperan menyusun norma dan kebijakan, sektor privat mengelola infrastruktur, komunitas teknis menetapkan standar, masyarakat sipil mengawasi hak digital, dan pengguna memperkuat literasi digital. Indonesia menerapkan tata kelola siber berbasis model hybrid. Di tingkat nasional, Perpres 47/2023 menetapkan kerangka Strategi Keamanan Siber Nasional, termasuk perlindungan Infrastruktur Informasi Vital dan mekanisme respons krisis. Perpres 53/2017 dan 28/2021 menempatkan BSSN sebagai otoritas utama keamanan siber. Dalam perlindungan data pribadi, UU 27/2022 (UU PDP) menetapkan hak subjek data, kewajiban pengendali data, serta aturan transfer data ke luar negeri. Pada pengawasan platform digital, Permen Kominfo 5/2020 jo. 10/2021 mewajibkan PSE asing untuk registrasi, menyediakan akses pengawasan konten, dan mematuhi

[205] DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. (hlm. 1–6)

[206] Mueller, M. (2010). *Networks and states: The global politics of internet governance*. MIT Press. (hlm. 40–55)

[207] Nye, J. S. (2010). *Cyber power*. Harvard Kennedy School. (hlm. 25–28)

standar penghapusan konten tertentu. UU ITE melalui Pasal 2 dan Pasal 40 menegaskan yurisdiksi digital Indonesia termasuk kewenangan pemutusan akses.

1. Prinsip *Cyber Norms* global dan tantangan pembentukannya

Prinsip cyber norms global merupakan standar perilaku bersama yang disepakati negara dan berbagai aktor non-negara untuk menjaga ruang siber tetap aman, stabil dan bertanggung jawab. Tidak seperti hukum internasional berbasis perjanjian yang bersifat mengikat, *cyber norms* berkembang melalui *soft law* seperti kesepakatan politik, pedoman teknis, praktik negara.[208] Tujuan utamanya adalah mencegah konflik siber, mendorong penggunaan teknologi secara etis, serta melindungi hak asasi manusia dan infrastruktur digital yang bersifat lintas batas. Beberapa prinsip inti yang telah diterima secara global mencakup: penghormatan terhadap kedaulatan negara (UN Charter Pasal 2(4)); larangan menyerang infrastruktur vital sebagaimana ditegaskan dalam UN-GGE 2015; kewajiban negara mencegah aktivitas siber berbahaya dari wilayahnya; perlindungan terhadap CSIRT/CERT; kerja sama internasional dalam menangani insiden besar; perlindungan hak digital sesuai ICCPR serta kewajiban militer menggunakan kemampuan siber secara proporsional dan sesuai hukum humaniter.[209]

Pembentukan cyber norms tidak hanya dilakukan oleh negara. Perusahaan teknologi besar, komunitas teknis seperti IETF dan ICANN, serta organisasi masyarakat sipil berperan penting dalam menetapkan standar dan etika digital.[210] Di tingkat global, PBB melalui UN-GGE dan OEWG menjadi forum utama penyusunan norma ini.Indonesia mengadopsi berbagai prinsip *cyber norms* dalam regulasi nasional. Perpres 47/2023 mengatur perlindungan Infrastruktur Informasi Vital (Pasal 7–8) dan manajemen krisis siber (Pasal 17–20). UU PDP menjamin hak subjek data (Pasal 4–9) dan mengatur transfer data internasional (Pasal 56–57). UU ITE memberikan dasar yurisdiksi ekstrateritorial (Pasal 2) dan mengatur

[208] Duncan B. Hollis, *The Oxford Handbook of Cybersecurity* (Oxford: Oxford University Press, 2021), 110–114

[209] Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber norms: Legal, policy & industry perspectives*. CCDCOE. (hlm. 12–17)

[210] UN Group of Governmental Experts (UN-GGE). (2015). *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations. (hlm. 7–15).

pemutusan akses konten ilegal (Pasal 40). PP 71/2019 menetapkan kewajiban keamanan sistem elektronik (Pasal 19, 24–26).

Perpres 53/2017 dan 28/2021 memperkuat peran BSSN sebagai koordinator keamanan siber serta pengembangan CSIRT nasional. Pembentukan cyber norms masih menghadapi banyak tantangan. Perbedaan kepentingan geopolitik antara model internet terbuka (AS–Eropa) dan model *cyber sovereignty* (Tiongkok–Rusia) menjadikan konsensus sulit.[211] Belum adanya kesepakatan global tentang definisi serangan siber juga menghambat penegakan norma. Dominasi sektor privat yang memiliki sebagian besar infrastruktur digital membuat keberhasilan norma bergantung pada dukungan perusahaan besar. Tantangan lain termasuk kesulitan menentukan pelaku serangan, kesenjangan kemampuan teknis negara berkembang, tumpang tindih regulasi nasional, serta cepatnya evolusi ancaman seperti *deepfake*, penyalahgunaan AI, dan *hybrid cyber warfare*.[212]

D. Ancaman Keamanan Siber dan Kompleksitas Regulasi

1. Eskalasi Ancaman Siber dan Implikasi terhadap Hukum Pidana Regulasi Nasional

Ancaman keamanan siber terus meningkat baik dari sisi frekuensi maupun tingkat kompleksitas, sehingga menimbulkan dampak langsung terhadap hukum pidana, hukum internasional, dan desain regulasi nasional.[213] Jika sebelumnya serangan bersifat oportunistik, kini pola serangan semakin terstruktur, terkoordinasi, dilakukan oleh aktor negara (*state-sponsored*) maupun kelompok kriminal non-negara.[214] Empat ancaman yang paling dominan ialah ransomware, DDoS, phishing, dan *Advanced Persistent Threat* (APT). *Ransomware* mengenkripsi sistem dan menuntut tebusan, sehingga memicu penerapan norma

[211] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (New York: Oxford University Press, 2006), 89–95

[212] National Institute of Standards and Technology (NIST), *AI and Cybersecurity: Emerging Risks* (Washington DC: NIST, 2023), 3

[213] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 17

[214] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford: Oxford University Press, 2016), 44

pidana seperti UU ITE Pasal 30 tentang akses ilegal, Pasal 32 tentang perusakan atau perubahan data, serta Pasal 36 tentang kerugian serius, termasuk potensi tindak pidana pencucian uang melalui kripto.[215] Serangan DDoS yang menonaktifkan layanan digital masuk ke kategori gangguan sistem sebagaimana diatur UU ITE Pasal 33, sedangkan PP 71/2019 Pasal 24–26 mewajibkan PSE menjaga ketersediaan dan keandalan system khususnya bila yang diserang adalah Infrastruktur Informasi Vital (IIV) sebagaimana diatur dalam Perpres 47/2023.[216]

Phishing, sebagai rekayasa sosial untuk memperoleh data pribadi, melibatkan norma pidana UU ITE Pasal 30–32, pidana dalam UU PDP terkait pemrosesan data tanpa dasar hukum (Pasal 65–67), serta Pasal 378 KUHP tentang penipuan apabila unsur tipu muslihat terpenuhi.[217] Adapun APT adalah ancaman paling kompleks karena dilakukan dalam jangka panjang oleh kelompok profesional, sering kali terkait kepentingan negara. Serangan semacam ini dapat melibatkan UU ITE Pasal 30–36, UU Intelijen Negara, serta mekanisme manajemen krisis siber melalui Perpres 47/2023 bahkan dapat masuk ranah hukum internasional apabila melibatkan tanggung jawab negara (*state responsibility*).[218]

2. Tantangan Attribution dalam Perspektif Hukum Internasional dan Politik Global

Di tingkat global, tantangan terbesar dalam penegakan hukum siber adalah attribution, yakni proses menentukan siapa pelaku serangan.[219] Ruang siber yang lintas-batas memungkinkan serangan dilakukan melalui berbagai negara dengan metode *proxy attack*, sementara pelaku dapat menyamarkan jejak menggunakan IP spoofing, VPN berlapis, *false flag*, atau *cryptomixing*.[220] Pada saat yang sama, belum ada definisi universal mengenai serangan siber atau serangan bersenjata

[215] Europol, *Internet Organised Crime Threat Assessment 2022* (The Hague: Europol, 2022), 15

[216] National Institute of Standards and Technology (NIST), *Guide to Distributed Denial of Service (DDoS) Defense* (Gaithersburg: NIST, 2021), 8

[217] Brian Krebs, *Spam Nation* (Naperville: Sourcebooks, 2014), 72

[218] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 112

[219] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 62

[220] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W.W. Norton, 2015), 200–

dalam hukum internasional, sehingga interpretasi *use of force* menurut UN Charter masih bervariasi. Standar pembuktian untuk menetapkan tanggung jawab negara juga sangat tinggi karena harus dibuktikan bahwa serangan dilakukan oleh agen negara atau negara membiarkan serangan terjadi dari wilayahnya. Tantangan politis juga muncul karena tuduhan serangan siber dapat memicu eskalasi diplomatik, sanksi ekonomi, atau aksi balasan. Akibatnya, attribution sering kali lebih menjadi isu politik daripada proses hukum murni. Kesenjangan besar antara perkembangan teknologi digital dan kecepatan regulasi fenomena yang dikenal sebagai *regulatory lag*. Teknologi seperti AI generatif, quantum computing, IoT, blockchain hingga serangan zero-day berkembang jauh lebih cepat daripada siklus legislasi. Alhasil, regulasi cenderung bersifat reaktif dan baru dibuat setelah terjadi insiden besar, misalnya penyusunan UU PDP setelah kebocoran data masif atau penyusunan pedoman sektoral pasca serangan ransomware pada rumah sakit.

E. Kompleksitas Regulasi, *Regulatory Lag*, Fragmentasi Kebijakan Siber di Indonesia

Fragmentasi hukum juga menjadi masalah karena banyaknya aturan yang saling tumpang tindih, seperti UU ITE, UU PDP, PP 71/2019, Perpres SKSN, serta aturan sektoral OJK, BI, Kemenkes, dan Kominfo, sehingga menimbulkan ambiguitas kewenangan. Kapasitas teknis regulator pun belum merata: keterbatasan ahli forensik digital, infrastruktur keamanan, dan anggaran membuat banyak kasus sulit ditangani secara efektif.[221] Negara harus menyeimbangkan antara kebutuhan keamanan, perlindungan privasi, ekonomi digital dan ruang inovasi. Regulasi yang terlalu ketat dapat menghambat inovasi, sementara regulasi yang terlalu longgar meningkatkan risiko siber. Seluruh tantangan ini menunjukkan bahwa tata kelola keamanan siber memerlukan pendekatan adaptif, berbasis risiko, serta didukung koordinasi lintas lembaga dan kerja sama internasional.[222]

[221] DeNardis, Laura, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014), 190–196

[222] ENISA (European Union Agency for Cybersecurity), *Cybersecurity Policy Framework* (Athens: ENISA, 2021), 12

Tata kelola keamanan siber di Indonesia masih menghadapi persoalan besar berupa fragmentasi regulasi**.** Aturan-aturan terkait siber tersebar di banyak instrumen hukum. UU ITE menetapkan larangan dan sanksi atas akses ilegal (Pasal 30), perusakan data (Pasal 32), serta gangguan sistem (Pasal 33). UU PDP memberikan dasar hukum pemrosesan data pribadi dan sanksi bagi pengendali atau prosesor data yang melanggar (Pasal 65–67). PP 71/2019 mewajibkan Penyelenggara Sistem Elektronik (PSE) menjaga keamanan, kerahasiaan, dan keandalan sistem. Perpres 47/2023 mengatur mekanisme respons insiden dan pembagian peran nasional dalam Sistem Keamanan Siber Nasional (SKSN). Di luar itu terdapat pengaturan sektoral seperti POJK 38/2016, kebijakan BI terkait keamanan sistem pembayaran serta Permenkes mengenai rekam medis elektronik. Banyaknya aturan ini sering menimbulkan tumpang tindih kewenangan dan kebingungan dalam penanganan insiden siber, terutama pada sektor-sektor yang saling terhubung. Selain masalah fragmentasi, Indonesia juga menghadapi *regulatory lag* yaitu keterlambatan regulasi dalam mengikuti perkembangan teknologi.

Teknologi baru seperti AI generatif, quantum computing, IoT, dan blockchain bergerak jauh lebih cepat dibanding proses legislasi. Saat ini belum ada aturan khusus mengenai standar keamanan IoT atau penggunaan AI dalam mitigasi ancaman siber. Akibatnya, banyak isu teknis hanya ditangani melalui pedoman internal atau aturan sektoral yang sifatnya sementara. Tantangan berikutnya ketimpangan kapasitas antar-regulator. Tidak semua lembaga memiliki ahli forensik digital, analis ancaman, atau anggaran untuk membangun infrastruktur keamanan sesuai standar. Padahal UU ITE dan PP 71/2019 mengharuskan PSE menerapkan langkah pengamanan minimum. Ketika kemampuan teknis tidak merata, implementasi aturan menjadi tidak konsisten dan proses investigasi insiden pun melambat. Dari sudut pandang kebijakan publik, pemerintah harus menyeimbangkan keamanan, privasi, inovasi. Regulasi yang terlalu ketat dapat membebani pelaku usaha, terutama PSE skala kecil, namun regulasi yang terlalu longgar meningkatkan risiko serangan dan kebocoran data. Karena itu, Indonesia mulai menerapkan pendekatan *risk-based regulation*, yaitu kewajiban yang berbeda

tergantung tingkat risiko layanan, misalnya standar lebih ketat untuk Infrastruktur Informasi Vital sesuai Perpres 47/2023.

1. Perlindungan Data Pribadi sebagai Pilar Hukum *Cyber*

Perlindungan data pribadi merupakan fondasi utama hukum cyber di Indonesia, tetapi implementasi UU 27/2022 tentang Pelindungan Data Pribadi (UU PDP) masih menghadapi kendala besar. Secara normatif, UU PDP sudah mengatu**r** hak subjek data (Pasal 4–15), kewajiban pengendali data (Pasal 20–48), transfer data Internasional (Pasal 56–57) serta sanksi administratif dan pidana (Pasal 57–67). Namun aturan turunannya, termasuk standar keamanan, tata cara audit, dan pembentukan Otoritas Pengawas PDP (amanat Bab VIII), belum sepenuhnya operasional. Banyak organisasi menunda kepatuhan karena belum jelas definisi teknis seperti pemrosesan berisiko tinggi atau tindakan teknis dan organisasi. Fragmentasi regulasi digital. Kewajiban dalam UU PDP tumpang tindih dengan UU ITE misalnya Pasal 15 tentang keamanan sistem elektronik dan Pasal 40 tentang pemutusan akse serta PP 71/2019 tentang PSTE (Pasal 19 dan Pasal 24–26 tentang keamanan dan audit sistem). Regulasi sektoral seperti POJK Perlindungan Konsumen**,** aturan BI tentang data sistem pembayaran dan Permenkes tentang rekam medis elektronik memiliki definisi dan standar berbeda sehingga menimbulkan ketidakseragaman pelaporan insiden. Fragmentasi ini menunjukkan tata kelola yang belum terkoordinasi lintas sektor.

Dari sisi kelembagaan otoritas pengawas PDP yang menjadi mandat UU PDP belum sepenuhnya kuat dari aspek struktur, independensi, dan kemampuan teknis. Tanpa lembaga yang solid, penegakan sanksi administratif (Pasal 57–58) sering lemah dan banyak kebocoran data tidak diikuti penegakan yang transparan. Kondisi ini membuat UU PDP tampak lebih sebagai "simbol hukum" daripada instrumen perlindungan yang efektif. Budaya kepatuhan organisasi pun masih rendah: banyak pihak hanya menyiapkan *privacy notice* secara formalitas, tanpa menerapkan Data Protection Impact Assessment (Pasal 34)**,** tata kelola hak subjek data atau rencana respons insiden sebagaimana diwajibkan UU.

Konflik juga muncul ketika prinsip *privacy by design* bertemu inovasi digital seperti AI, Big Data, IoT. Teknologi AI dan Big Data sangat bergantung pada

kumpulan data besar, sementara UU PDP menuntut minimasi data (Pasal 21 huruf c) dan pembatasan tujuan pemrosesan (Pasal 20). IoT mengumpulkan data terus-menerus, sering tanpa pemahaman memadai dari pengguna, sehingga berpotensi menabrak kewajiban transparansi (Pasal 22) dan prinsip keamanan (Pasal 35). Keputusan otomatis berbasis algoritma di sektor finansial, kesehatan, atau ketenagakerjaan juga bertentangan dengan hak subjek data untuk menolak pemrosesan tertentu (Pasal 10 huruf f) dan hak mendapatkan penjelasan atas keputusan otomatis (Pasal 10 huruf g). Di sisi lain, model bisnis platform digital berbasis monetisasi data sering bertentangan dengan konsep *privacy by default*, sehingga berbagai praktik manipulatif seperti *dark patterns* berisiko melanggar asas fairness dan accountability.

Tantangan penegakan hukum menambah kompleksitas. Otoritas PDP masih memperkuat koordinasi dengan Kominfo, BSSN (Perpres 53/2017 dan 28/2021), OJK, BI, Kemenkes sementara mekanisme pelaporan insiden belum terpusat, meskipun UU PDP mewajibkan pelaporan insiden dalam 72 jam (Pasal 46). Di banyak instansi publik dan privat, terdapat *compliance gap*: belum tersedia DPO (tugas dan fungsi Pasal 53–54), belum dilakukan DPIA, dan kontrak pemrosesan data dengan pihak ketiga belum memuat ketentuan wajib sebagaimana diatur Pasal 51. Masyarakat juga memiliki literasi privasi rendah sehingga tidak memahami hak-haknya seperti hak perbaikan (Pasal 7 huruf b) atau hak penghapusan data (Pasal 7 huruf c). Di sisi lain, kemampuan penegakan seperti digital forensics dan audit algoritma masih terbatas sehingga banyak kasus kebocoran berhenti pada teguran. Ketegangan juga muncul antara percepatan ekonomi digital nasional termasuk program integrasi data pemerintah, telemedisin, *fintech*, dan smart city dengan tuntutan perlindungan privasi yang ketat. Jika tidak dikelola seimbang UU PDP dapat dipersepsikan sebagai hambatan inovasi atau justru membuka ruang pengabaian prinsip privasi demi kepentingan ekonomi. Karena ituperlindungan data pribadi perlu diposisikan sebagai infrastruktur kepercayaan digital (*trust infrastructure*) yang mendukung pertumbuhan teknologi secara aman dan berkelanjutan.

2. Yurisdiksi Siber dan *Cyber Sovereignty*

Isu yurisdiksi siber dan cyber sovereignty muncul karena aktivitas digital berlangsung lintas batas, menggunakan server dan jaringan global, serta melibatkan pelaku dari berbagai negara. Ruang siber yang tidak mengenal batas fisik ini menantang konsep yurisdiksi tradisional, sehingga negara mendorong kontrol lebih besar terhadap data, platform digital, dan infrastruktur strategis. Dalam konteks transboundary *cyber activities*, serangan botnet, pencurian data dari luar negeri atau pemrosesan data warga Indonesia oleh pusat data asing menimbulkan persoalan hukum terkait siapa yang berwenang mengatur dan menindak.

Indonesia merespons ketidakpastian ini melalui asas ekstrateritorial UU ITE Pasal 2, yang memungkinkan penegakan hukum terhadap perbuatan di luar negeri yang berdampak di Indonesia. Selain itu UU PDP Pasal 56–57 mengatur syarat transfer data internasional, termasuk prinsip perlindungan setara (*adequacy*) dan kerja sama antarnegara. PP 71/2019 juga mewajibkan PSE asing yang beroperasi secara masif di Indonesia untuk tunduk pada hukum nasional, sehingga yurisdiksi Indonesia dapat menjangkau entitas global yang memproses data warga Indonesia. Namun, arus data lintas negara (*cross-border data flows*) tetap menjadi tantangan besar karena membawa risiko privasi, keamanan nasional, hingga konflik standar regulasi. Pada tingkat global, tata kelola siber terpecah dalam tiga model utama. Amerika Serikat menerapkan pendekatan liberal dan pasar terbuka, tanpa undang-undang privasi federal komprehensif, sehingga aliran data global berlangsung bebas selama ada persetujuan atau kontrak. Uni Eropa melalui GDPR menempatkan privasi sebagai hak fundamental (EU Charter Art. 7–8) dan menerapkan aturan ketat termasuk privacy by design, batas transfer data internasional, serta mekanisme adequacy decision. Tiongkok menganut model cyber sovereignty melalui Cybersecurity Law 2017, Data Security Law 2021, dan Personal Information Protection Law 2021, yang memperkuat kendali negara atas data dan memberi kewajiban data localization untuk data penting. Sementara ASEAN tidak memiliki standar tunggal; Singapura (PDPA), Thailand (PDPA), dan Indonesia (UU PDP) mengikuti pendekatan campuran, sementara Vietnam lebih mirip model Tiongkok. Fragmentasi ini menyebabkan interoperabilitas terbatas dan menyulitkan kerja sama yurisdiksi.

Isu lain yang krusial adalah data localization, yaitu kewajiban penyimpanan atau pemrosesan data tertentu di dalam negeri. Indonesia menerapkan data localization untuk PSE publik sesuai PP 71/2019 Pasal 20, memperketat transfer data lintas negara melalui UU PDP Pasal 56–57, dan memasukkan data strategis sebagai bagian dari Infrastruktur Informasi Vital (IIV) dalam Perpres 47/2023. Meskipun bertujuan memperkuat keamanan nasional, penegakan hukum, dan kedaulatan digital, kebijakan ini memiliki konsekuensi ekonomi, seperti meningkatnya biaya pusat data, terbatasnya integrasi cloud global, dan potensi menurunnya minat investasi asing. Dilema kebijakan muncul ketika negara harus menyeimbangkan kepentingan keamanan dan kedaulatan dengan kebutuhan kecepatan inovasi ekonomi digital. Over-regulation berpotensi menghambat pertumbuhan digital, sementara under-regulation meningkatkan risiko kebocoran data dan ketergantungan pada platform global. Secara keseluruhan isu yurisdiksi siber dan cyber sovereignty memperlihatkan tarik-menarik antara sifat ruang digital yang lintas batas dengan dorongan negara untuk mempertahankan kontrol atas data dan infrastruktur kritis.

3. Keamanan Infrastruktur Kritis (*Critical Information Infrastructure Protection* – CIIP)

Keamanan Infrastruktur Kritis (CIIP) menjadi pilar penting dalam perlindungan ruang siber karena sektor-sektor vital seperti kesehatan, perbankan, energi, dan transportasi memiliki risiko serangan yang tinggi, mulai dari ransomware, APT, serangan pada SCADA/ICS, hingga gangguan layanan (DDoS) yang dapat mengancam keselamatan publik dan stabilitas nasional. Di sektor kesehatan, serangan pada rekam medis elektronik (RME) dan perangkat IoT medis berpotensi melumpuhkan layanan rumah sakit; sektor perbankan menghadapi risiko pembobolan dan DDoS yang memengaruhi stabilitas sistem keuangan; sektor energi rentan pada serangan terhadap sistem kendali industri; dan sektor transportasi dapat mengalami gangguan navigasi dan sistem otomatisasi.

Untuk mengatasi risiko tersebut, penyelenggara sistem elektronik tingkat tinggi diwajibkan menerapkan standar keamanan ketat sesuai PP 71/2019 Pasal 24–26 tentang kewajiban menjaga kerahasiaan, integritas, dan ketersediaan sistem

elektronik, kewajiban audit, pencatatan log, dan pelaporan insiden, UU ITE Pasal 15 mengenai kewajiban PSE menyediakan sistem yang andal dan aman serta Perpres 47/2023 Pasal 7–10 mengenai identifikasi dan perlindungan Infrastruktur Informasi Vital (IIV). Namun, terdapat kesenjangan dalam penerapan standar keamanan internasional**.** NIST SP 800-53 menyediakan kontrol teknis sangat detail sedangkan ISO/IEC 27001 lebih menekankan manajemen keamanan berbasis ISMS yang lebih umum sementara Zero Trust Architecture (NIST SP 800-207) menuntut verifikasi akses berkelanjutan dan segmentasi mikro. Perbedaan kedalaman teknis dan kesiapan organisasi menyebabkan banyak PSE hanya menerapkan standar minimal sehingga muncul gap antara regulasi nasional dan *best practice* global. Hal ini menegaskan perlunya harmonisasi kebijakan dan peningkatan kemampuan teknis untuk memperkuat keamanan infrastruktur kritis nasional.

F. Strategis Penguatan Penerapan Hukum Cyber

1. Pendekatan Regulasi Progresif

Pendekatan regulasi progresif diperlukan agar hukum mampu mengikuti perkembangan teknologi yang bergerak cepat. Pertama, *adaptive regulation* dan prinsip *technology-neutral* memungkinkan hukum tetap relevan tanpa harus diperbarui setiap kali muncul inovasi baru. Prinsip ini menekankan pengaturan pada *risiko* dan *fungsi*, bukan jenis teknologi tertentu misalnya mengatur "pemrosesan data berisiko tinggi" tanpa menyebut AI, blockchain atau IoT satu per satu. Pendekatan ini sejalan dengan UU PDP (Pasal 3 & asas-asas pemrosesan data) yang fokus pada prinsip lawfulness, fairness, minimasi, dan akuntabilitas yang berlaku untuk semua teknologi.

Kedua, harmonisasi hukum nasional dengan standar global diperlukan agar Indonesia tidak terisolasi secara digital. *Budapest Convention on Cybercrime* menyediakan model penegakan kejahatan siber lintas negara dan prosedur investigasi digital. *GDPR* menjadi rujukan untuk perlindungan data, termasuk prinsip *privacy by design*, minimasi data, dan pengaturan transfer lintas-negara. Sementara itu, *ASEAN Digital Masterplan 2025* (ADM 2025) mendorong interoperabilitas standar keamanan, e-commerce, dan tata kelola data antarnegara

ASEAN. Penyelarasan ini dapat dilakukan melalui revisi atau harmonisasi UU ITE, penguatan PP 71/2019, serta integrasi prinsip GDPR dalam UU PDP (Pasal 56–57) mengenai transfer data internasional

Ketiga, regulasi progresif memerlukan *regulatory sandbox* untuk teknologi yang inovatif namun berisiko tinggi seperti AI, blockchain, cloud computing, dan fintech. Sandbox memungkinkan pengujian teknologi baru dalam lingkungan terbatas sebelum diadopsi secara luas. Indonesia telah menjalankan sandbox melalui OJK (Inovasi Keuangan Digital) dan BI (Regulatory Sandbox Sistem Pembayaran), namun cakupan perlu diperluas untuk AI generatif, autonomous system, dan layanan berbasis data besar. Sandbox membantu mengurangi risiko, memperkuat compliance, dan mendorong inovasi yang aman.

2. Pendekatan Regulasi Progresif

Pendekatan regulasi progresif diperlukan agar hukum mampu mengikuti perkembangan teknologi yang bergerak cepat. Pertama, *adaptive regulation* dan prinsip *technology-neutral* memungkinkan hukum tetap relevan tanpa harus diperbarui setiap kali muncul inovasi baru. Prinsip ini menekankan pengaturan pada *risiko* dan *fungsi*, bukan jenis teknologi tertentu—misalnya mengatur "pemrosesan data berisiko tinggi" tanpa menyebut AI, blockchain, atau IoT satu per satu. Pendekatan ini sejalan dengan UU PDP (Pasal 3 & asas-asas pemrosesan data) yang fokus pada prinsip lawfulness, fairness, minimasi, dan akuntabilitas yang berlaku untuk semua teknologi.

Kedua, harmonisasi hukum nasional dengan standar global diperlukan agar Indonesia tidak terisolasi secara digital. *Budapest Convention on Cybercrime* menyediakan model penegakan kejahatan siber lintas negara dan prosedur investigasi digital. *GDPR* menjadi rujukan untuk perlindungan data, termasuk prinsip *privacy by design*, minimasi data, dan pengaturan transfer lintas-negara. Sementara itu, *ASEAN Digital Masterplan 2025* (ADM 2025) mendorong interoperabilitas standar keamanan, e-commerce, dan tata kelola data antarnegara ASEAN. Penyelarasan ini dapat dilakukan melalui revisi atau harmonisasi UU ITE, penguatan PP 71/2019, serta integrasi prinsip GDPR dalam UU PDP (Pasal 56–57) mengenai transfer data internasional.

Ketiga, regulasi progresif memerlukan *regulatory sandbox* untuk teknologi yang inovatif namun berisiko tinggi seperti AI, blockchain, cloud computing, dan fintech. Sandbox memungkinkan pengujian teknologi baru dalam lingkungan terbatas sebelum diadopsi secara luas. Indonesia telah menjalankan sandbox melalui OJK (Inovasi Keuangan Digital) dan BI (Regulatory Sandbox Sistem Pembayaran), namun cakupan perlu diperluas untuk AI generatif, autonomous system, dan layanan berbasis data besar. Sandbox membantu mengurangi risiko, memperkuat compliance, dan mendorong inovasi yang aman.

3. Strategi Penegakan Hukum Siber

Penegakan hukum siber membutuhkan instrumen kelembagaan, teknis, dan internasional yang kuat. Pertama, kapasitas aparat penegak hukum perlu ditingkatkan, terutama dalam digital forensics, malware analysis, cryptocurrency tracing, dan investigasi APT. Penguatan ini harus melibatkan BSSN, Kepolisian**,** OJK, BI, Kominfo, dan Kejaksaan melalui pelatihan teknis serta peralatan forensik modern.[223] Kedua, harmonisasi regulasi sangat penting mengingat banyaknya tumpang tindih antara KUHP, UU ITE, UU PDP, UU Telekomunikasi 2024, dan peraturan teknis Kominfo. Harmonisasi diperlukan agar pembuktian pidana lebih sederhana, pengaturan akses legal terhadap data digital lebih jelas, serta penanganan insiden keamanan siber tidak terfragmentasi.[224] Misalnya, integrasi definisi "akses tanpa hak" (UU ITE Pasal 30), "pemrosesan ilegal" (UU PDP Pasal 65–67), dan pengaturan barang bukti elektronik (UU ITE Pasal 5–6, KUHAP).[225] Ketiga, penanganan kejahatan siber lintas Negara membutuhkan kerja sama internasional melalui MLAT (*Mutual Legal Assistance Treaty*), *Interpol Cybercrime Directorate*, serta kerja sama regional seperti *ASEAN Cybersecurity Cooperation* dan *FIRST-CSIRT*.[226] Banyak kasus siber melibatkan server dan

[223] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 4th ed. (Amsterdam: Elsevier, 2019), 33

[224] Duncan B. Hollis, *The Oxford Handbook of Cybersecurity* (Oxford: Oxford University Press, 2021), 298–303;

[225] Susan Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Westport: Praeger, 2010), 89

[226] INTERPOL, *Global Cybercrime Strategy 2022–2025* (Lyon: INTERPOL, 2022), 10–13

pelaku di banyak negara, sehingga tanpa mekanisme MLAT, permintaan data, ekstradisi, atau joint investigation akan terhambat[227]. Indonesia juga perlu berproses menuju ratifikasi *Budapest Convention* atau setidaknya mengadopsi praktik terbaiknya agar mekanisme pembuktian digital lebih kompatibel secara global.[228]

[227] Council of Europe, *Mutual Legal Assistance in Criminal Matters Handbook* (Strasbourg: CoE, 2020), 23–29 Council of Europe, *Budapest Convention on Cybercrime: Explanatory Report* (Strasbourg: CoE, 2001), 6–10; Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart Publishing, 2018), 152

[228]

BAB 9

HUKUM CYBER DALAM PERSPEKTIF INTERNASIONAL

Dr. Ani Purwati, S.H., M.H

A. Dinamika Geopolitik Siber dan Tantangan Harmonisasi Hukum Internasional

1. Transformasi Ruang Siber Global dan Urgensi Hukum Siber Internasional

Perkembangan ruang siber global dalam dua dekade terakhir ditandai oleh meningkatnya konektivitas, digitalisasi layanan publik, dan integrasi ekonomi berbasis data sehingga memperluas interaksi antarnegara sekaligus memperbesar risiko keamanan. Transformasi digital ini mendorong negara-negara menyusun norma hukum baru untuk mengatur aktivitas siber mulai dari perlindungan data, keamanan jaringan hingga penanggulangan kejahatan siber. Dalam konteks hubungan internasional urgensi hukum siber menjadi semakin menonjol karena ruang siber bersifat lintas batas dan tidak tunduk pada teritorial fisik tradisional. Oleh sebab itu banyak negara menggunakan prinsip hukum internasional yang sudah ada seperti *state responsibility* dan *due diligence* yang tercermin dalam Pasal 2(4) UN Charter mengenai larangan penggunaan kekuatan Pasal 51 tentang hak bela diri serta norma Tallinn Manual 2.0 yang menegaskan serangan siber dapat

dikategorikan sebagai *use of force* bila dampaknya sebanding dengan serangan fisik.[229]

Penerapan norma-norma tersebut menghadapi sejumlah kendala mendasar. Salah satunya adalah ketidakpastian yurisdiksi karena banyak kejahatan siber dilakukan dari satu negara, menggunakan server di negara lain, dan menargetkan korban di yurisdiksi ketiga. Situasi ini menantang prinsip *territorial jurisdiction* dalam hukum internasional, sehingga banyak negara beralih menggunakan *objective territoriality* atau *effects doctrine* sebagaimana tercermin dalam *Budapest Convention on Cybercrime* Pasal 22 tentang yurisdiksi multi-negara.[230] Selain itu kejahatan siber lintas negara seperti ransomware, pencurian data, dan *business email compromise* terus meningkat dan melibatkan kelompok kriminal transnasional. *Budapest Convention* sebenarnya mengatur pelestarian cepat (Pasal 16–18) dan kerja sama penegakan hukum (Pasal 23–35) tetapi efektivitasnya terbatas karena tidak semua negara menjadi pihak konvensi ini.[231]

2. Fragmentasi Regulasi Global dan Divergensi Model Tata Kelola Siber

Masalah berikutnya adalah fragmentasi regulasi global karena hingga kini belum ada satu rezim hukum siber universal yang disepakati. Upaya harmonisasi yang dilakukan Perserikatan Bangsa-Bangsa melalui *Open-Ended Working Group* (OEWG) dan G*roup of Governmental Experts* (GGE**)** juga belum menghasilkan standar global yang mengikat sebab kepentingan geopolitik negara-negara besar tidak mudah dipertemukan.[232] Fragmentasi semakin terlihat melalui perbedaan tajam dalam model regulasi Amerika Serikat, Uni Eropa, Tiongkok yang menciptakan ekosistem hukum siber global yang tidak seragam. Amerika Serikat mengadopsi model liberal market berbasis sektor dengan fokus pada inovasi. AS tidak memiliki undang-undang privasi nasional yang komprehensif, tetapi

[229] Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 94–110). Cambridge University Pres

[230] Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*, ETS No. 185, Article 22

[231] Council of Europe. (2001). *Convention on Cybercrime*, Articles 16–18 & 23–35.

[232] United Nations General Assembly. (2013, 2015, 2021). *Reports of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98; A/70/174; A/76/13

menggunakan pendekatan sektoral melalui HIPAA untuk kesehatan, GLBA untuk keuangan, *CLOUD Act* untuk yurisdiksi data, dan *Cybersecurity Act* untuk aspek keamanan. Sebaliknya, Uni Eropa menempatkan data sebagai hak fundamental dan menerapkan model yang sangat ketat melalui GDPR yang mengatur prinsip pemrosesan (Pasal 5–7), keamanan data (Pasal 32), serta sanksi administratif yang berat (Pasal 83). Rezim keamanan jaringan dan layanan penting diatur lebih lanjut dalam NIS2 Directive yang menerapkan kewajiban manajemen risiko dan pelaporan insiden bagi sektor-sektor strategis.[233] Berbeda dari keduanya Tiongkok menonjol dengan pendekatan *cyber sovereignty* yang menekankan kontrol negara dan kepentingan keamanan nasional. Regulasi seperti *Cybersecurity Law* 2017, *Data Security Law* 2021, dan *Personal Information Protection Law* (PIPL) 2021 menegaskan kewajiban *data localization* (CSL Pasal 37), *security assessment* untuk transfer data (PIPL Pasal 38–43) dan pengawasan ketat terhadap operator infrastruktur penting. Pendekatan ini menimbulkan perbedaan tajam terhadap model AS dan UE, karena Tiongkok menempatkan negara sebagai pengendali utama arus data dan aktivitas digital. Ketiga model regulasi ini tidak hanya menciptakan ketidaksinkronan dalam standar global, tetapi juga menghambat interoperabilitas hukum serta mempersulit kerja sama internasional dalam menangani ancaman siber. Oleh sebab itu harmonisasi regulasi dan penguatan kerja sama internasional baik melalui penegakan hukum, standardisasi keamanan, maupun mekanisme respons insiden menjadi kebutuhan mendesak untuk membangun tata kelola ruang siber global yang aman, stabil, dan dapat dipertanggungjawabkan.

3. Evolusi *Computer Law* ke *Cyber Law* dalam Sistem Internasional

Perkembangan hukum siber internasional berlangsung melalui tiga fase besar yang mencerminkan perubahan ekosistem digital global. Pada 1970–1980-an, fokus utama terletak pada *computer law* yaitu hukum yang mengatur penggunaan komputer, penyalahgunaan perangkat keras, keamanan fisik sistem serta tindak

[233] United States. (1996). *Health Insurance Portability and Accountability Act* (HIPAA), 45 CFR §§160–164; Gramm–Leach–Bliley Act (GLBA), 15 U.S.C. §§6801–6809; CLOUD Act, 18 U.S.C. §2713 (2018).

pidana berbasis mesin seiring meningkatnya penggunaan mainframe dan komputer komersial di sektor publik dan swasta. Memasuki 1990–2000-an ketika internet mulai terhubung secara global melalui protokol TCP/IP, karakter hukum berubah menjadi *internet law*, yang mencakup nama domain, transaksi elektronik, kontrak digital, perlindungan konsumen daring, serta yurisdiksi perdagangan elektronik. Evolusi ini semakin berkembang sejak 2010 hingga 2024 dimana ruang digital telah berubah menjadi ekosistem kompleks yang mencakup data lintas negara, keamanan jaringan, platform digital berskala global, kecerdasan buatan, dan infrastruktur informasi vital. Perkembangan ini melahirkan *cyber law* sebuah rezim hukum yang memberi perhatian lebih besar pada keamanan data, privasi digital, stabilitas jaringan, serta koordinasi internasional terhadap ancaman siber. Jejak evolusi ini juga tercermin pada berbagai instrumen global seperti *Budapest Convention on Cybercrime 2001*, resolusi PBB tentang keamanan ICT, *Tallinn Manual 1.0 dan 2.0*, hingga GDPR Uni Eropa yang menjadi tonggak penting perlindungan data pribadi lintas negara.

B. *Cyber Law* Hukum Internasional Kontemporer dan Peran Organisasi Internasional

Dalam konteks hubungan internasional modern, *cyber law* berkembang menjadi cabang hukum tersendiri yang beroperasi di persimpangan antara hukum humaniter internasional, hukum HAM, keamanan internasional, hukum perbatasan digital.[234] Diskusi mengenai *state responsibility*, *due diligence*, *sovereignty in cyberspace*, serta *prohibition of intervention* kini menjadi bagian inti dari perdebatan hukum internasional mengenai ruang siber. Perkembangan ini tidak dapat dilepaskan dari peran organisasi internasional yang membentuk norma, standar teknis, dan kerangka kerja sama global. ITU menetapkan standar telekomunikasi dan protokol keamanan melalui *Global Cybersecurity Agenda*. PBB, melalui OEWG dan GGE, mengembangkan norma perilaku negara di ruang

[234] Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 1–25, 78–102). Cambridge University Press

siber serta merumuskan batas-batas tindakan yang dianggap melanggar kedaulatan digital. INTERPOL berkontribusi dalam penanggulangan kejahatan siber melalui kerja sama penegakan hukum lintas yurisdiksi dan pengembangan kapasitas investigatif. OECD di sisi lain membentuk prinsip-prinsip kebijakan digital mencakup keamanan data, privasi, tata kelola ekonomi digital yang menjadi rujukan berbagai negara.[235] Konstelasi ini menunjukkan *cyber law* telah berkembang menjadi rezim hukum transnasional yang mengatur keamanan global, stabilitas geopolitik, perlindungan data, tata kelola ruang digital secara komprehensif.

1. Instrumen *Hard Law*, Konvensi, Piagam, Standar Hukum HAM

Dalam ranah instrumen global formal (*hard law*)**,** konvensi utama yang sering dijadikan rujukan adalah *Budapest Convention on Cybercrime* 2001 yang menjadi traktat pertama yang secara khusus mengatur tindak pidana siber lintas batas. Konvensi ini menetapkan katalog delik mulai dari akses ilegal (*illegal access*, Pasal 2), intersepsi ilegal (Pasal 3), gangguan terhadap data (*data interference*, Pasal 4), gangguan terhadap sistem (*system interference*, Pasal 5), penyalahgunaan perangkat (Pasal 6), hingga penipuan dan pemalsuan komputer (Pasal 7–8), serta mengatur upaya percobaan, bantuan, dan tanggung jawab korporasi (Pasal 11–13). Di tingkat prosedural, Pasal 14–21 mengatur kewenangan khusus seperti pelestarian cepat data komputer (*preservation*), penggeledahan dan penyitaan sistem, serta pengumpulan *traffic data*, sedangkan Pasal 22 mengatur yurisdiksi multi-negara dan Pasal 23–35 mewajibkan kerja sama internasional yang luas antara aparat penegak hukum lintas negara. Dalam konteks hukum perang dan keamanan internasional, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* bukan traktat tetapi kompendium otoritatif yang merumuskan 154 *black letter rules* mengenai bagaimana hukum internasional termasuk hukum perang, kedaulatan, tanggung jawab negara, dan HAM, berlaku terhadap operasi siber baik di masa damai maupun konflik bersenjata Manual ini memaknai misalnya pelanggaran kedaulatan, penggunaan kekuatan (*use of force*) dan agresi

[235] OECD. (2015). *Digital Security Risk Management Recommendations* (pp. 3–14). OECD Publishing

di ruang siber, sehingga memberi panduan bagaimana menilai serangan siber yang menimbulkan kerusakan setara serangan kinetik

Di sisi lain, *UN Charter* memberikan dasar normatif utama bagi operasi siber antarnegara: Pasal 2 ayat (4) melarang ancaman atau penggunaan kekuatan terhadap integritas teritorial atau kemerdekaan politik negara lain yang dalam interpretasi mutakhir mencakup serangan siber terhadap infrastruktur kritis apabila dampaknya setara dengan kekerasan bersenjata. Pasal 39 memberi kewenangan kepada Dewan Keamanan untuk menentukan adanya ancaman terhadap perdamaian, pelanggaran perdamaian, atau tindakan agresi termasuk potensi insiden siber besar yang mengganggu stabilitas internasional dan Pasal 51 mengakui hak bela diri jika suatu serangan siber mencapai ambang *armed attack* misalnya menyebabkan kehancuran fasilitas vital atau korban jiwa. Di ranah HAM *International Covenant on Civil and Political Rights (ICCPR)* menjadi dasar utama standar HAM digital Pasal 17 menjamin hak atas privasi dan melarang intervensi yang sewenang-wenang atau melawan hukum terhadap *privacy, family*, *home or correspondence* yang kini ditafsirkan mencakup komunikasi elektronik, metadata dan pemrosesan data personal; Pasal 19 menjamin kebebasan berpendapat dan berekspresi, termasuk dalam bentuk komunikasi online, sementara *General Comment* No. 34 Komite HAM PBB menegaskan hak ini juga berlaku penuh di ruang digital dan pembatasannya harus memenuhi syarat legalitas, kebutuhan, dan proporsionalitas. Meskipun demikian instrumen *hard law* masih memiliki keterbatasan serius dalam ruang digital: belum ada satu konvensi global yang secara komprehensif mengatur *state behavior* di ruang siber banyak negara di luar Eropa tidak meratifikasi *Budapest Convention* Tallinn Manual bersifat non-mengikat dan penerapan norma umum seperti Piagam PBB atau ICCPR terhadap kasus-kasus teknis (misalnya *botnet*, serangan *zero-day*, operasi *false-flag*) sering menimbulkan perbedaan tafsir di antara negara, sehingga terjadi kesenjangan antara norma formal dan praktik.

2. Instrumen *Soft Law* Norma, Pedoman, Standar Multi-Pemangku Kepentingan

Di luar kerangka formal tersebut berkembang instrumen non-mengikat (*soft law*) yang berperan besar dalam membentuk norma dan kebiasaan negara. Di lingkungan PBB, *UN Group of Governmental Experts (UN-GGE)* pada 2013 (A/68/98), 2015 (A/70/174), dan 2021 (A/76/135) menghasilkan laporan konsensus yang menetapkan kerangka perilaku bertanggung jawab negara (*responsible state behavior*) di ruang siber, termasuk pengakuan bahwa Piagam PBB berlaku penuh dalam konteks ICT, pentingnya menghormati kedaulatan digital, larangan menyerang *critical infrastructure* sipil, serta kewajiban memberikan bantuan ketika diminta oleh negara korban insiden siber yang serius. Paralel dengan itu, *Open-Ended Working Group (OEWG)* yang bersifat inklusif (semua negara anggota PBB) menyusun laporan 2021 (A/75/816) dan laporan-laporan lanjutan 2022–2025 yang menegaskan kembali penerapan Piagam PBB, memperluas diskusi mengenai *confidence-building measures*, kerja sama kapasitas siber, serta membuka jalur partisipasi pemangku kepentingan non-negara dalam pembahasan keamanan siber internasional.

Di luar PBB berbagai organisasi teknis dan ekonomi mengembangkan *normative frameworks*: OECD mengeluarkan *Privacy Guidelines* (2013) dan *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* (2015) yang mendorong pendekatan berbasis risiko, teknologi-netral, dan akuntabilitas dalam kebijakan keamanan digital nasional. ENISA sebagai Badan Keamanan Siber Uni Eropa membangun kerangka sertifikasi keamanan siber dan panduan strategi keamanan nasional, termasuk panduan *cybersecurity practices for AI* dan *cybersecurity certification framework* untuk produk dan layanan ICT di pasar digital Eropa. ITU menyusun *Global Cybersecurity Agenda* dan berbagai panduan strategi keamanan siber nasional yang berisi praktik terbaik tata kelola, pembagian peran lembaga dan standar teknis. Selanjutnya ekosistem *multi-stakeholder* teknis seperti IETF**,** ICANN dan W3C mengembangkan standar protokol internet, sistem penamaan domain (DNS) dan standar web secara terbuka dan berbasis konsensus. IETF dan W3C, misalnya memproduksi *Request for*

Comments (RFC) dan standar web melalui proses terbuka yang melibatkan komunitas teknis global sementara ICANN mengelola sistem nama domain tingkat atas dan menjadi simpul penting dalam tata kelola teknis internet global berbasis model multi-pemangku kepentingan. Walaupun soft law tidak mengikat secara formal berfungsi sebagai *norm generator* dan *gap filler* yang melengkapi kekosongan *hard law* membentuk ekspektasi perilaku, serta menjadi rujukan bagi negara ketika menyusun kebijakan nasional, sehingga secara bertahap berkontribusi pada lahirnya praktik kebiasaan (*state practice*) dan *opinio juris* di bidang hukum siber internasional.

3. Prinsip-Prinsip Utama *Cyber Law Internasional*

Dalam hukum internasional modern *cyber law* dibangun di atas sejumlah prinsip dasar yang mengatur bagaimana negara bertindak, berinteraksi, dan bertanggung jawab di ruang siber global. Prinsip kedaulatan digital menegaskan negara memiliki hak penuh untuk mengatur infrastruktur, jaringan, data yang berada dalam yurisdiksinya serta melarang negara lain melakukan intervensi, pemanipulasian data atau penetrasi sistem yang mengganggu integritas digitalnya. Prinsip non-intervensi dan penggunaan kekuatan melarang tindakan siber yang bertujuan memengaruhi urusan domestik negara lain atau menimbulkan kerusakan signifikan terhadap infrastruktur vital, dan serangan dengan dampak serius dapat dikategorikan sebagai *use of force* atau *armed attack* menurut Pasal 2(4) dan 51 Piagam PBB.

Prinsip *due diligence* mewajibkan negara mencegah wilayahnya digunakan sebagai basis serangan siber yang merugikan negara lain sedangkan prinsip *state responsibility* menetapkan kapan suatu operasi dapat diatribusikan kepada negara termasuk jika dilakukan oleh kelompok yang menerima instruksi atau dukungan efektif dari pemerintah[3]. Tantangan teknis yang besar muncul dalam *atribusi* karena jejak digital mudah dipalsukan melalui *proxy*, *spoofing* atau *false-flag attacks* sehingga negara sering menggabungkan bukti teknis analisis intelijen dan motif geopolitik untuk menentukan pelaku. Prinsip perlindungan HAM digital menjamin hak atas privasi, kebebasan berekspresi, dan perlindungan data sehingga tindakan

siber negara harus memenuhi uji legalitas, kebutuhan dan proporsionalitas sebagaimana diatur dalam ICCPR dan berbagai standar internasional.[236]

Prinsip keamanan kolektif menekankan ancaman siber tidak dapat ditangani secara unilateral sehingga diperlukan kerja sama internasional dalam berbagi informasi, merespons insiden dan membangun kapasitas siber sebagaimana digunakan dalam mekanisme NATO, ASEAN dan forum PBB.[237] Sementara itu prinsip kehati-hatian (*precautionary principle*) menuntut negara bersikap waspada terhadap risiko digital baru seperti AI, IoT, komputasi kuantum sehingga kebijakan pengamanan harus diterapkan meskipun bukti ilmiah belum lengkap demi mencegah kerusakan besar terhadap sistem publik maupun infrastruktur kritis.[238] Keseluruhan prinsip ini membentuk fondasi tata kelola ruang siber global yang bertumpu pada kedaulatan, tanggung jawab negara, penghormatan HAM, stabilitas internasional, dan keamanan kolektif.

C. Arsitektur regulasi siber dunia dalam perbandingan Amerika Serikat, Uni Eropa, Tiongkok–Rusia, ASEAN

1. Model Liberal Market (Amerika Serikat)

Model liberal market Amerika Serikat menempatkan inovasi dan mekanisme pasar sebagai fondasi utama tata kelola siber sehingga perlindungan data dan privasi tidak diatur melalui satu undang-undang federal yang komprehensif melainkan melalui skema sektoral seperti HIPAA untuk data kesehatan (45 CFR §160–164)[239], GLBA untuk data keuangan (§501–§502), COPPA untuk data anak-anak (15 U.S.C. §6501–6506)[240] dan FCRA untuk data kredit (15 U.S.C. §1681)[241].

---

[236] International Law Commission (ILC), *Articles on Responsibility of States for Internationally Wrongful Acts* (2001), Art. 8

[237] United Nations, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security – Report 2021*, **pp. 10–15**; *Report 2023*, **pp. 12**

[238] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021); OECD, *Principles on AI* (2019)

[239] U.S. Department of Health and Human Services, *Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules*, 45 C.F.R. §§160–164

[240] U.S. Congress, *Gramm-Leach-Bliley Act (GLBA)*, §§501–502, Pub. L. 106–102 (1999)

[241] State of California, *California Consumer Privacy Act (CCPA) & California Privacy Rights Act (CPRA)*, Cal. Civ. Code §§1798.100–1798.199

Tidak adanya *Federal Data Protection Act* membuat perlindungan privasi sebagian besar bergantung pada hukum negara bagian, seperti CCPA/CPRA California (Cal. Civ. Code §1798.100–1798.199) sehingga menciptakan fragmentasi regulatif. Ketiadaan pengaturan privasi federal yang ketat memberi ruang besar bagi perusahaan teknologi besar seperti Google, Meta, Amazon dan Microsoft untuk menentukan sendiri standar pengumpulan data, arsitektur keamanan serta kebijakan platform, dengan pengawasan terbatas dari FTC Act §5 yang hanya menindak praktik yang menipu (*deceptive*) atau merugikan (*unfair*).[242]

Standar keamanan seperti NIST *Cybersecurity Framework* bersifat sukarela, sementara mekanisme penegakan hukum digital bergantung pada kerja sama perusahaan melalui *Stored Communications Act* (18 U.S.C. §2701–2712)[243] dan Cloud Act 2018 yang memberi akses pemerintah terhadap data tertentu.[244] Pendekatan *innovation-first* ini juga diperkuat *oleh National Cyber Strategy* yang menekankan deregulasi dan kemitraan publik–swasta[245] serta CDA §230[246], yang memberikan kekebalan hukum bagi platform atas konten pengguna sehingga memungkinkan ekspansi platform digital tanpa tanggung jawab penerbitan. Dalam konteks keamanan siber pemerintah lebih mengandalkan insentif pasar dan kolaborasi sukarela misalnya melalui *Cybersecurity Information Sharing Act* (CISA) 2015 (6 U.S.C. §1501)[247] yang mendorong pertukaran informasi ancaman antara pemerintah dan sektor swasta. Secara keseluruhan, model ini menghasilkan ekosistem digital yang sangat inovatif, tetapi juga menimbulkan ketimpangan perlindungan privasi dan dominasi kuat korporasi dalam membentuk standar siber nasional.

2. Model Hak Asasi dan Perlindungan Data (Uni Eropa)

---

[242] Federal Trade Commission, *FTC Act*, 15 U.S.C. §45 (Section 5: Unfair or Deceptive Acts or Practices)

[243] U.S. Congress, *Stored Communications Act*, 18 U.S.C. §§2701–2712

[244] U.S. Congress, *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, 2018, 18 U.S.C. §2523

[245] The White House, *National Cyber Strategy of the United States of America* (Washington, DC: White House, 2018), pp. **5–12**

[246] U.S. Congress, *Communications Decency Act (CDA)*, 47 U.S.C. §230

[247] U.S. Congress, *Cybersecurity Information Sharing Act (CISA) 2015*, 6 U.S.C. §1501

Model regulasi siber Uni Eropa dibangun atas pendekatan hak asasi manusia yang menempatkan privasi dan perlindungan data sebagai hak fundamental sehingga pilar utamanya terdiri dari GDPR, EU Cybersecurity Act, dan NIS2 Directive. GDPR 2016/679 menjadi instrumen kunci yang menetapkan prinsip-prinsip pemrosesan data pada Pasal 5 seperti *lawfulness*, *fairness, transparency* dan data *minimisation*[248] serta mengatur dasar keabsahan pemrosesan pada Pasal 6 dan perlindungan ketat untuk *special categories of data* pada Pasal 9.[249] GDPR juga memperkenalkan prinsip privacy by design and by default melalui Pasal 25 yang mewajibkan perlindungan privasi dirancang sejak awal sistem dibuat dan memastikan pengaturan standar meminimalkan pengumpulan data[250]. Hak-hak subjek data seperti akses (Pasal 15), perbaikan (Pasal 16), penghapusan (Pasal 17), dan portabilitas data (Pasal 20) diperkuat dengan kewajiban pemberitahuan pelanggaran data dalam 72 jam (Pasal 33–34) serta rezim sanksi berat hingga 20 juta euro atau 4% omzet global (Pasal 83).[251]

Di sisi keamanan siber, EU Cybersecurity Act (Regulation 2019/881) memperkuat mandat ENISA dan membangun sistem sertifikasi keamanan siber berskala Uni Eropa dengan tingkat jaminan *basic*, *substantial* dan *high* sehingga standar keamanan menjadi seragam di seluruh UE. Instrumen ketiga, NIS2 Directive (2022/2555), memperluas kewajiban keamanan bagi sektor energi, transportasi, kesehatan, infrastruktur digital, layanan cloud hingga administrasi publik melalui kategori *essential* dan *important entities* (Pasal 3–4).[252] Pasal 21 NIS2 mewajibkan penerapan manajemen risiko menyeluruh, termasuk keamanan rantai pasok, kebijakan penanganan insiden serta penggunaan kriptografi dan enkripsi sementara Pasal 23–24 menetapkan kewajiban pelaporan insiden kepada

[248] European Union, *General Data Protection Regulation (GDPR) 2016/679*, **Art. 5**, *Official Journal of the European Union L119/35 (2016)*, Recitals **39–50**

[249] European Union, *GDPR 2016/679*, **Arts. 6 and 9**, OJ L119/36–38

[250] European Union, *GDPR 2016/679*, **Art. 25**, OJ L119/51–52; lihat juga Recitals **78–79** mengenai *privacy by design*.

[251] European Union, *GDPR 2016/679*, **Arts. 15–20, 33–34, 83**, OJ L119/43–45; L119/52–54; L119/82–83

[252] European Union, *Regulation (EU) 2019/881 (EU Cybersecurity Act)*, **Arts. 46–54**, OJ L151/15–22; tingkat jaminan sertifikasi terdapat pada **Art. 52**

CSIRT dan otoritas nasional melalui *early warning* dan *incident notification*.[253] Keseluruhan instrumen ini beroperasi dalam kerangka precautionary principle, yaitu prinsip kehati-hatian yang mendorong regulator mengambil tindakan pencegahan meskipun bukti risiko belum lengkap. Prinsip ini terlihat dalam kewajiban melakukan Data Protection Impact Assessment (DPIA) untuk pemrosesan berisiko tinggi (Pasal 35 GDPR), kewajiban sertifikasi keamanan melalui *Cybersecurity Act* dan penerapan langkah manajemen risiko proaktif dalam NIS2. [254] Uni Eropa membangun sistem regulasi yang menempatkan privasi, keamanan data, dan keamanan siber sebagai fondasi utama inovasi digital, sekaligus memastikan bahwa perkembangan teknologi tetap tunduk pada standar HAM dan perlindungan data lintas batas.

3. Model *Cyber Sovereignty* (Tiongkok–Rusia)

Model *cyber sovereignty* yang diterapkan Tiongkok dan Rusia berangkat dari gagasan bahwa negara memiliki kendali penuh atas seluruh aktivitas digital dalam wilayahnya mulai dari infrastruktur, arus data, platform digital, hingga perilaku daring warga negara. Pendekatan ini menempatkan keamanan nasional, stabilitas politik, dan kedaulatan informasi sebagai prioritas utama, sehingga pemerintah mengatur secara ketat akses, penyimpanan, serta pergerakan data lintas batas. Di Tiongkok, kerangka ini dibangun melalui tiga undang-undang inti. Cybersecurity Law (CSL) 2017 mewajibkan operator jaringan menjaga keamanan sistem, melakukan *data localization*, serta menjalani *security review*. Pasal 37 menetapkan bahwa data penting yang dihasilkan oleh *Critical Information Infrastructure* (CII) harus disimpan di dalam negeri dan hanya dapat dipindahkan ke luar negeri setelah penilaian keamanan. *Data Security Law* (DSL) 2021 melengkapi CSL dengan mengklasifikasikan data menurut tingkat risikonya bagi keamanan nasional dan ekonomi, serta memperketat transfer lintas batas melalui kewajiban *risk assessment*. DSL juga melarang penyerahan data kepada otoritas asing tanpa persetujuan pemerintah, menegaskan prinsip kedaulatan data. Sementara itu

[253] European Union, *NIS2 Directive*, **Arts. 21 and 23–24**, OJ L333/90–95

[254] European Union, *GDPR 2016/679*, **Art. 35**, OJ L119/55–56; lihat pula EU Cybersecurity Act **Arts. 49–52** dan NIS2 Directive **Art. 21** untuk kerangka manajemen risiko proaktif.

Personal Information Protection Law (PIPL) 2021 mengatur perlindungan data pribadi dengan ketentuan ketat mengenai dasar keabsahan pemrosesan, perlindungan data sensitif, kewajiban perusahaan asing menunjuk perwakilan lokal, serta pembatasan ekspor data melalui persyaratan sertifikasi atau *security assessment*. Pemerintah juga diberikan wewenang luas untuk membatasi operasi perusahaan digital yang dianggap mengancam keamanan nasional. Rusia menerapkan pendekatan serupa melalui Data *Localization Law* 2015, yang mewajibkan penyimpanan data warganya pada server domestik serta *Yarovaya Law* yang memperluas kewajiban penyedia layanan untuk menyimpan metadata dan memberikan akses kepada otoritas keamanan.

Kedua negara melihat internet bukan sebagai ruang bebas global, melainkan sebagai perpanjangan kedaulatan negara yang harus tunduk pada kontrol hukum dan politik domestik. Karena itu, kontrol negara terhadap arus data mulai dari pembatasan transfer internasional, pengelolaan jalur trafik nasional, penyaringan konten, hingga penegakan standar keamanan lokal menjadi ciri utama model ini. Pendekatan *cyber sovereignty* ini bertolak belakang dengan model liberal Barat, karena menempatkan negara sebagai otoritas tertinggi dalam menentukan siapa yang boleh mengakses, memproses, atau mentransfer data di dalam ekosistem digital nasional.

4. Model Campuran Asia Tenggara (ASEAN)

Model regulasi siber di Asia Tenggara bersifat campuran (hybrid) karena menggabungkan tiga pendekatan: perlindungan hak asasi dan data pribadi ala Uni Eropa, dukungan terhadap inovasi dan iklim bisnis seperti di Amerika Serikat, serta elemen kedaulatan digital yang menguat sebagaimana model Tiongkok–Rusia. Pada tingkat regional, ASEAN belum memiliki kerangka hukum yang mengikat, tetapi menyediakan pedoman melalui ASEAN Framework on Personal Data Protection (2016), ASEAN Digital Masterplan 2025, ASEAN Data Management Framework, dan ASEAN Model Contractual Clauses (MCC) untuk transfer data lintas batas semua bersifat *soft law* sehingga negara anggota tetap bebas membangun regulasinya sendiri.

Singapura memiliki sistem paling mapan melalui *Personal Data Protection Act* (PDPA) 2012 dan *Cybersecurity Act* 2018. PDPA menetapkan 11 kewajiban utama organisasi, termasuk *accountability*, *consent*, *purpose limitation*, *protection*, pembatasan retensi data, serta kewajiban pelaporan insiden (*data breach notification*) dalam waktu 3 hari. Undang-undang ini juga mewajibkan penunjukan Data Protection Officer (DPO) dan pembatasan transfer data lintas negara melalui mekanisme perlindungan yang memadai. *Cybersecurity Act* memberi kewenangan penuh kepada Cyber Security Agency (CSA) untuk menetapkan *Critical Information Infrastructure* (CII), mewajibkan audit keamanan, *risk assessment*, pelaporan insiden, dan kepatuhan terhadap *codes of practice*, terutama bagi sektor seperti energi, transportasi, dan kesehatan. Thailand menerapkan *Personal Data Protection Act* (PDPA) 2019, yang substansinya mirip GDPR. UU ini menuntut dasar pemrosesan yang sah, persetujuan yang jelas dan spesifik, serta hak-hak subjek data seperti akses, perbaikan, dan penghapusan. *Cross-border transfer* dibatasi kecuali negara tujuan memiliki tingkat perlindungan yang memadai atau terdapat mekanisme kontraktual tertentu.

Bagian penting dari PDPA adalah *Section 37* yang mewajibkan *data controller* menerapkan langkah keamanan teknis dan organisasi yang wajar untuk mencegah akses atau pengungkapan data tanpa kewenangan, serta melaporkan insiden kepada otoritas data nasional (PDPC). Indonesia menggunakan model berlapis melalui UU ITE, PP 71/2019, UU PDP 27/2022, dan Perpres 47/2023. UU ITE mengatur tindak pidana siber, termasuk akses ilegal (Pasal 30), intersepsi tanpa hak (Pasal 31), perusakan atau perubahan data (Pasal 32), dan gangguan sistem elektronik (Pasal 33). PP 71/2019 mewajibkan Penyelenggara Sistem Elektronik (PSE) menjamin kerahasiaan, integritas, keaslian, dan ketersediaan sistem, serta mengatur kewajiban pengelolaan keamanan bagi PSE publik maupun privat. UU PDP 2022 mempertegas perlindungan data pribadi sebagai hak fundamental, mengatur prinsip pemrosesan, dasar hukum (konsen, kontrak, kepentingan sah), klasifikasi data pribadi spesifik, hak subjek data (akses, perbaikan, penghapusan, keberatan), kewajiban pengendali/pemroses, serta sanksi administratif dan pidana.

Perpres 47/2023 tentang SKSN menetapkan arsitektur nasional keamanan siber, pembagian peran antar instansi, serta mekanisme manajemen insiden yang melibatkan infrastruktur informasi vital (IIV). Namun, tumpang tindih kewenangan antara Kominfo, BSSN, kementerian teknis, dan otoritas sektor masih menjadi kendala implementatif. Dalam konteks harmonisasi regional, ASEAN menghadapi tantangan karena perbedaan tingkat kematangan regulasi, pendekatan kebijakan yang tidak seragam, serta keterbatasan kapasitas institusi pengawas di beberapa negara anggota. *ASEAN Way* yang menekankan *non-interference* dan keputusan berbasis konsensus juga memperlambat pembentukan standar regional yang mengikat layaknya GDPR di Uni Eropa. Akibatnya perusahaan yang beroperasi lintas negara harus menavigasi variasi aturan yang kompleks, sementara respons insiden siber lintas batas masih bergantung pada kerja sama *ad hoc* bukan pada satu rezim hukum kawasan. Meskipun demikian kebutuhan harmonisasi standar keamanan minimum, mekanisme transfer data lintas batas, serta kerangka manajemen risiko regional semakin mendesak mengingat meningkatnya ancaman siber dan intensifikasi ekonomi digital ASEAN.

D. Arsitektur Yurisdiksi Siber Internasional: Prinsip, Konflik, Tantangan Penegakan Hukum Global

Yurisdiksi siber menjadi isu fundamental karena ruang digital bersifat *borderless*, dimana pelaku, *server, cloud*, korban dapat berada di beberapa negara sekaligus, sehingga penentuan negara mana yang berwenang menindak suatu tindakan siber menjadi sulit. Dalam hukum internasional, negara pada prinsipnya menggunakan yurisdiksi teritorial tetapi dalam konteks siber tindakan sering kali tersebar misalnya malware dibuat di negara A, dikirim melalui server di negara B, menyerang korban di negara C, dan menyasar platform yang berkantor di negara D. Karena itu, banyak negara memperluas kewenangan dengan *objective territoriality* yakni yurisdiksi atas perbuatan di luar negeri yang menimbulkan efek signifikan di dalam negeri, sebagaimana diterapkan Amerika Serikat melalui *effects doctrine* dan Uni Eropa melalui GDPR Pasal 3 yang tetap berlaku bagi pengendali data di luar UE sepanjang memproses data subjek UE.

Di luar itu negara juga menerapkan asas kebangsaan (*nationality principle*) untuk menindak warga negaranya yang melakukan serangan siber di luar negeri serta *passive personality principle* untuk melindungi warga negaranya yang menjadi korban, misalnya dalam kasus *online fraud*, eksploitasi seksual anak, atau serangan phishing lintas negara. Tantangan semakin meningkat ketika penegakan hukum melibatkan *distributed cloud architecture*, di mana data tersimpan di berbagai yurisdiksi sehingga akses ke bukti digital harus mengikuti aturan negara tempat data berada. Uni Eropa menerapkan pembatasan ketat transfer data lintas negara melalui GDPR Pasal 44–50 yang mensyaratkan *adequacy decision*, *standard contractual clauses*, atau *binding corporate rules*, sementara Amerika Serikat melalui *CLOUD Act* 2018 memberi kewenangan ekstra-teritorial kepada aparat untuk mengakses data perusahaan AS meskipun berada di server luar negeri. Pertentangan yurisdiksi terlihat jelas dalam sengketa *Schrems II* (2020) ketika Pengadilan Eropa membatalkan EU–US *Privacy Shield* karena dianggap tidak sejalan dengan standar privasi GDPR terutama terkait akses pemerintah AS berdasarkan FISA Section 702.

Konflik lain muncul antara UE dan Tiongkok, karena aturan Tiongkok memperketat ekspor data melalui *Cybersecurity Law* Pasal 37, *Data Security Law* Pasal 24–30**,** dan PIPL Pasal 38–43**,** yang mewajibkan *security assessment* dan memungkinkan negara melarang transfer data atas dasar keamanan nasional. Selain benturan regulasiyurisdiksi siber juga terkendala mekanisme kerja sama penegakan hukum lintas negara melalui *Mutual Legal Assistance Treaty* (MLAT) yang sering lambat dan tidak efektif, sementara bukti digital sangat mudah hilang ditambah lagi kewajiban ekstradisi hanya berlaku jika terpenuhi *double criminality principle* yang tidak selalu tersedia ketika negara pelaku tidak mengkriminalisasi tindakan siber tertentu. Untuk mengatasi hambatan ini sebagian negara mengadopsi *Budapest Convention on Cybercrime* 2001 yang mengatur yurisdiksi multi-negara (Pasal 22), *expedited preservation* data (Pasal 16), serta kerja sama penegakan hukum (Pasal 23–35), namun efektivitasnya terbatas karena negara besar seperti Tiongkok, Rusia, dan sebagian besar ASEAN belum menjadi pihak. Secara keseluruhan, yurisdiksi siber tetap menjadi area paling kompleks dalam hukum internasional modern,

ditandai oleh benturan kepentingan nasional, tumpang tindih regulasi, dan ketiadaan rezim global yang mengikat; sehingga negara dan perusahaan multinasional harus menavigasi kombinasi berbagai asas yurisdiksi sambil menghadapi potensi konflik hukum antarnegara yang semakin intens.

1. *Cybersecurity* dan Hukum Humaniter Internasional

Dalam hukum internasional modern, *cyber operations* dipandang sebagai ancaman signifikan terhadap perdamaian karena kapasitasnya mengganggu stabilitas politik, ekonomi, dan keamanan negara tanpa melibatkan kekuatan bersenjata konvensional. Piagam PBB Pasal 2(4) melarang penggunaan kekuatan terhadap negara lain, dan norma ini dianggap berlaku pula untuk serangan siber yang menimbulkan kerusakan besar terhadap fungsi negara. Ketika dampaknya cukup serius misalnya mematikan jaringan listrik nasional atau merusak fasilitas nuklir serangan siber dapat dikualifikasikan sebagai *armed attack* sebagaimana dimaksud Pasal 51 Piagam PBB, sehingga memberi negara korban hak melakukan pembelaan diri. Dalam praktiknya, Dewan Keamanan PBB juga dapat menilai serangan siber sebagai ancaman terhadap perdamaian menurut Pasal 39 terutama jika menyasar layanan publik yang menopang kehidupan masyarakat. Infrastruktur vital seperti sistem energi, keuangan, kesehatan, transportasi, air minum, dan telekomunikasi menjadi target paling berbahaya karena kegagalannya dapat berakibat luas pada warga sipil. Laporan UN-GGE 2015 dan 2021 menegaskan bahwa negara tidak boleh menyerang *critical infrastructure* negara lain dan wajib mencegah penggunaan wilayahnya sebagai basis serangan yang mengancam kesejahteraan publik.

Dalam konteks konflik bersenjata hukum humaniter internasional (IHL) berlaku penuh terhadap operasi siber. Tallinn Manual 2.0 menyatakan bahwa IHL mengikat semua pihak dalam konflik, baik siber maupun kinetik, sehingga setiap serangan siber yang diperkirakan menyebabkan kerusakan fisik, gangguan serius, atau korban sipil diklasifikasikan sebagai *attack* berdasarkan Protokol Tambahan I 1977. Prinsip-prinsip fundamental IHL*distinction*, *necessity*, dan *proportionality* juga berlaku dalam ruang siber. Prinsip *distinction* mewajibkan aktor militer membedakan sasaran militer dari objek sipil, sehingga malware yang berpotensi

menyebar tanpa kontrol ke jaringan rumah sakit, air minum, atau transportasi sipil dapat melanggar IHL. Prinsip *proportionality* melarang operasi siber yang dapat menimbulkan kerusakan sipil berlebihan dibanding keuntungan militer, termasuk dampak tak langsung seperti gangguan sistem rumah sakit yang tiba-tiba kehilangan listrik. Prinsip *necessity* menuntut bahwa serangan hanya boleh dilakukan untuk mencapai tujuan militer yang sah, sehingga serangan acak atau serangan yang murni bermotif ekonomi/politik tidak dapat dibenarkan.

Pada saat yang sama, ICCPR memberikan perlindungan HAM digital termasuk hak hidup, privasi, dan komunikasi yang tetap mengikat negara bahkan dalam penanganan ancaman siber. Sejumlah insiden global menunjukkan kompleksitas penerapan hukum ini. Stuxnet (2010) merusak centrifuge fasilitas nuklir Iran melalui malware industri, dan dianggap sebagai contoh awal operasi siber yang menimbulkan kerusakan fisik nyata. WannaCry (2017) menunjukkan bahaya *malware* yang menyebar tanpa kendali, menabrak layanan kesehatan Inggris (NHS) dan mengancam nyawa pasien akibat terganggunya peralatan medis. SolarWinds (2020) mencerminkan skala dan kedalaman operasi spionase siber yang menembus jaringan lembaga pemerintah Amerika Serikat melalui *supply-chain compromise* tanpa kerusakan fisik, namun dengan implikasi besar bagi keamanan nasional. Ketiga kasus ini memperkuat pandangan bahwa ruang siber sudah menjadi domain strategis yang setara dengan darat, laut, udara, ruang angkasa serta membutuhkan standar hukum internasional yang lebih tegas dalam mengatur agresi, perlindungan warga sipil, dan respon negara terhadap serangan yang semakin canggih dan sulit diatribusikan.

2. Tantangan Masa Depan Hukum *Cyber Quantum Threat - Smart City Surveillance*

Perkembangan teknologi digital dalam dekade mendatang menghadirkan tantangan besar bagi hukum cyber internasional karena inovasi bergerak jauh lebih cepat daripada kemampuan negara dan organisasi internasional dalam menetapkan norma dan mekanisme penegakan. Salah satu tantangan paling kritis adalah *quantum computing* yang diproyeksikan mampu mematahkan algoritma kriptografi konvensional seperti RSA dan ECC hanya dalam hitungan detik. Jika teknologi ini

beroperasi pada skala penuh, seluruh sistem keamanan berbasis enkripsi mulai dari transaksi keuangan, komunikasi diplomatik, hingga perlindungan data pemerintah berisiko terbuka. Oleh sebab itu, badan standarisasi seperti NIST telah mengembangkan *post-quantum cryptography* untuk menggantikan algoritma lama. Tantangan hukum cyber adalah memastikan kewajiban transisi global terutama bagi sektor kritis yang tunduk pada instrumen seperti EU NIS2 Directive Pasal 21 yang mewajibkan manajemen risiko canggih.[255] Ancaman kedua datang dari AI generatif, deepfake, *automated cyberattacks*.

Teknologi ini tidak hanya mampu memanipulasi identitas dan informasi publik, tetapi juga memungkinkan serangan otomatis yang menganalisis pertahanan target secara *real time*.[256] *Deepfake* berpotensi mengganggu stabilitas politik, pemilu, dan kepercayaan publik terhadap institusi negara. Hingga kini belum ada rezim global yang mengatur penyalahgunaan AI untuk tujuan ofensif, meskipun Uni Eropa mulai merintis pengaturan melalui EU AI Act yang mengkategorikan sistem berbasis risiko.[257] Tantangan hukum selanjutnya adalah menentukan *liability* ketika AI menjadi instrumen serangan siapa yang bertanggung jawab pengembang, operator platform atau negara.[258] Dalam bidang keamanan *Zero Trust Architecture* (ZTA) muncul sebagai standar baru karena menggantikan model perimeter tradisional yang semakin tidak relevan. Prinsip *never trust, always verify* menuntut verifikasi berlapis terhadap setiap permintaan akses, baik dari dalam maupun luar organisasi. Amerika Serikat menjadikan ZTA sebagai kewajiban

[255] European Union, *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2)*, **Art. 21**, pp. **45–48** (ketentuan risk management untuk essential & important entities)

[256] Ben Buchanan, *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), **pp. 112–119** tentang *automated cyber operations* dan kemampuan analisis pertahanan secara otomatis

[257] European Union, *Artificial Intelligence Act (EU AI Act)*, Regulation (EU) 2024/1689, **Title II, Chapter 1**, pp. **29–37** (kerangka *risk-based classification* untuk AI)

[258] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Dordrecht: Springer, 2013), **pp. 74–85** mengenai distribusi *liability* antara pengembang, operator, dan institusi negara dalam kasus kerusakan akibat AI

nasional melalui *Executive Order* 14028 (2021) yang memerintahkan seluruh lembaga federal menerapkan arsitektur ini.[259]

Uni Eropa mengintegrasikannya dalam kerangka NIS2, sementara negara Asia seperti Singapura telah mengadopsinya melalui CSA *Zero Trust Policy Architecture*. Tantangan hukum ke depan ialah bagaimana menetapkan standar sertifikasi keamanan berbasis ZTA yang berlaku global. Pertumbuhan masif *Internet of Things* (IoT) menambah kompleksitas risiko privasi karena miliaran perangkat rumah tangga, kesehatan, industry dan transportasi mengumpulkan data personal secara terus-menerus.[260] Kerentanan perangkat IoT sering berakar dari lemahnya standar keamanan manufaktur, minimnya enkripsi, dan tidak adanya mekanisme pembaruan perangkat (*patching*).

EU mencoba mengatasi masalah ini melalui *Cyber Resilience Act* dan skema sertifikasi di bawah *EU Cybersecurity Act* Regulation (2019/881) Namun banyak negara belum memiliki regulasi serupa, sehingga IoT menjadi pintu masuk serangan botnet global seperti Mirai. Teknologi *blockchain dan cryptocurrency* memunculkan dilema antara inovasi dan risiko kejahatan digital. Karakter *pseudo-anonim cryptocurrency* memudahkan pencucian uang, pendanaan terorisme, dan pembayaran ransomware. Badan global FATF menetapkan *Travel Rule* sebagai mekanisme identifikasi transaksi aset kripto, dan Uni Eropa mengatur ekosistem aset digital melalui MiCA Regulation 2023. Implementasi tidak merata dan beberapa yurisdiksi justru menjadi tempat pelarian aktivitas ilegal. [261] Tantangannya adalah bagaimana mengharmonisasi regulasi blockchain tanpa mematikan inovasi. Isu yang semakin strategis adalah *data localization* yaitu kebijakan negara yang mewajibkan data disimpan di wilayah yurisdiksi. Tiongkok menerapkan kebijakan ketat melalui *Cybersecurity Law* Pasal 37 *Data Security Law*

[259] Cyber Security Agency of Singapore (CSA), *Zero Trust Maturity Model & Policy Architecture* (Singapore: CSA, 2021), **pp. 5–12**, khususnya tahapan implementasi dan persyaratan verifikasi berlapis

[260] Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (New York: W.W. Norton, 2018), **pp. 43–52** mengenai risiko privasi dan keamanan pada ekosistem Internet of Things (IoT)

[261] European Union, *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*, **Arts. 3–7 (definitions), Arts. 14–45 (asset-referenced tokens), Arts. 53–62 (crypto-asset service providers)**, *Official Journal of the European Union L150/40–101 (2023)*

Pasal 25–30, PIPL Pasal 38–43[262] sementara Uni Eropa membatasi transfer data internasional melalui GDPR Pasal 44–50[263] dan Amerika Serikat memberlakukan yurisdiksi ekstra-teritorial melalui *CLOUD Act* 2018.[264] Konflik regulasi antarnegara semakin sering muncul terutama ketika perusahaan multinasional berada di bawah dua rezim yang saling bertentangan dalam pengelolaan data. Di bidang tata kelola kota perkembangan *smart city* menghadirkan ancaman pengawasan massal (*mass surveillance*) melalui penggunaan kamera CCTV, sensor IoT, big data dan sistem AI yang memantau mobilitas dan interaksi warga.[265] Meskipun meningkatkan efisiensi kota, risiko penyalahgunaan data biometrik, metadata, dan pola perilaku sangat tinggi jika tidak diatur secara transparan. Hak atas privasi yang dijamin ICCPR Pasal 17 menjadi rujukan utama tetapi belum ada rejim global yang mengatur penggunaan data smart city secara komprehensif.[266]

1 Reformasi Tata Kelola Siber Dunia *Budapest Convention* dan Standardisasi Keamanan Internasional

Arah penguatan tata kelola cyber global membutuhkan konsensus internasional yang lebih kuat karena rezim hukum saat ini masih tersebar antara Piagam PBB, hukum HAM, hukum humaniter dan regulasi sektoral. Harmonisasi diperlukan bukan untuk membentuk satu konvensi besar secara sekaligus, melainkan melalui penguatan norma bertahap seperti *responsible state behaviour* yang sudah dirumuskan oleh UN-GGE (2015, 2021) dan OEWG termasuk pengakuan bahwa Piagam PBB khususnya Pasal 2(4) (larangan penggunaan kekuatan), Pasal 39 (ancaman terhadap perdamaian), dan Pasal 51 (hak membela diri) berlaku penuh di ruang siber. Selain itu, prinsip *due diligence* dan *state responsibility* sebagaimana

---

[262] *Cybersecurity Law of the People's Republic of China* (2016), **Art. 37** — kewajiban data localization bagi *critical information infrastructure operators*

[263] European Union, *General Data Protection Regulation (GDPR) 2016/679*, **Arts. 44–50**, *OJ L119/56–60* — dasar hukum transfer data internasional (*adequacy decision*, *appropriate safeguards*, *derogations*)

[264] U.S. Congress, *Clarifying Lawful Overseas Use of Data (CLOUD) Act* (2018), **18 U.S.C. §2523** — yurisdiksi ekstra-teritorial terhadap data yang disimpan oleh penyedia layanan AS.

[265] Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: PublicAffairs, 2019), **pp. 351–379**, membahas integrasi AI–IoT dalam pengawasan perkotaan dan implikasi privasi.

[266] United Nations, *International Covenant on Civil and Political Rights (ICCPR)*, **Art. 17**, *UN Treaty Series, vol. 999, p. 176 (1976)* — hak atas privasi dan perlindungan dari campur tangan sewenang-wenang

diatur dalam ARSIWA Pasal 4–11 perlu dipertegas penerapannya terhadap serangan siber lintas negara. Dalam konteks harmonisasi perlu dorongan agar lebih banyak negara mengadopsi *Budapest Convention on Cybercrime* (2001). Konvensi ini memberikan definisi umum tindak pidana siber (Pasal 2–9), kewenangan penyidikan elektronik (Pasal 14–21), dan kerangka kerja sama seperti *mutual assistance* dan *expedited preservation* (Pasal 23–35). Meskipun beberapa negara seperti Tiongkok dan Rusia mengkritik orientasi Eropanya, konvensi ini tetap menjadi rujukan global yang paling operasional dan dapat diadaptasi oleh negara berkembang sebagai standar minimum hukum pidana siber.

Penguatan *Mutual Legal Assistance Treaty* (MLAT) menjadi agenda mendesak karena proses permintaan data digital lintas negara sering lambat, padahal bukti elektronik cepat berubah. Penguatan ini mencakup penyederhanaan prosedur, penggunaan saluran aman untuk permintaan data, batas respons yang lebih ketat, serta integrasi jaringan kontak 24/7 sebagaimana direkomendasikan Budapest Convention Pasal 35. Selain itu, pembentukan *joint cyber investigation teams* diperlukan untuk menangani kasus lintas negara seperti ransomware, serangan ke infrastruktur finansial, atau operasi spionase berskala besar. Pada ranah teknis, penguatan tata kelola global perlu dilakukan melalui standardisasi keamanan, khususnya melalui standar ISO/IEC 27001, rekomendasi ITU-T X.1205, serta kerangka regional seperti *EU Cybersecurity Act* (Regulation 2019/881) dan NIS2 *Directive* 2022/2555 yang mewajibkan manajemen risiko dan pelaporan insiden (Pasal 21–24). Standardisasi juga diperlukan untuk sistem baru seperti Zero Trust, kriptografi pasca-kuantum, keamanan IoT, sertifikasi perangkat digital guna mencegah fragmentasi standar antarnegara. Perusahaan teknologi besar memegang infrastruktur kunci cloud, platform komunikasi, media sosial harus dilibatkan dalam tata kelola global. Negara perlu menetapkan kewajiban kolaboratif seperti pelaporan insiden global, mekanisme *vulnerability disclosure*, dan batasan *lawful access* yang tetap menghormati HAM sebagaimana diatur dalam ICCPR Pasal 17 (privasi) dan Pasal 19 (kebebasan berekspresi). Kerangka ini harus memastikan bahwa negara tidak sepenuhnya menyerahkan keamanan digital kepada sektor swasta namun tetap membangun akuntabilitas bersama. Pendekatan *human-rights*

centric harus menjadi dasar tata kelola siber, terutama untuk mencegah penyalahgunaan teknologi seperti pengawasan massal, penyaringan data ekstrem, dan sensor yang tidak proporsional. GDPR terutama Pasal 5 (prinsip pemrosesan data), Pasal 25 (*privacy by design*), Pasal 44–50 (transfer data internasional), menjadi model global untuk memastikan keamanan tidak mengorbankan hak-hak fundamental.

BAB 10

TANTANGAN REGULASI DALAM ARTIFICIAL INTELLIGENCE DAN BIG DATA

Muhammad Arif Rahman, S.H.

A. Pendahuluan

Inovasi dalam Era Digital Dunia tengah berada di tengah revolusi teknologi yang dimotori oleh dua kekuatan transformatif yaitu Kecerdasan Artifisial (*Artificial Intelligence* atau AI) dan *Big Data*. Kombinasi keduanya tidak hanya menjanjikan efisiensi dan inovasi yang belum pernah terjadi sebelumnya di berbagai sektor, mulai dari kesehatan, industri kreatif, hingga pendidikan, tetapi juga secara fundamental mengubah cara masyarakat, korporasi, dan negara berinteraksi. Kemampuan AI untuk menganalisis himpunan data raksasa (*Big Data*) guna mengidentifikasi pola, membuat prediksi, dan mengotomatisasi pengambilan keputusan telah menjadi pendorong utama pertumbuhan ekonomi dan kemajuan sosial.[267]

Namun, di balik potensi luar biasa ini, kemajuan teknologi menciptakan apa yang oleh para ahli hukum disebut sebagai *pacing problem*, yaitu suatu kondisi di mana laju perkembangan teknologi jauh melampaui kemampuan kerangka hukum dan regulasi konvensional untuk beradaptasi. Akibatnya, muncul suatu ruang hampa regulasi (*regulatory vacuum*) yang dieksploitasi oleh berbagai pihak, baik

[267] Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023. Lihat juga: *Jangan Disalahgunakan! Berikut Etika Penggunaan AI Berdasarkan Surat Edaran Menkominfo*. (2024). Retrieved from https://news.sah.co.id/jangan-disalahgunakan-berikut-etika-penggunaan-ai-berdasarkan-surat-edaran-menkominfo/.

untuk keuntungan komersial maupun tujuan-tujuan yang merugikan. Tantangan yang dihadapi bukan lagi sekadar masalah teknis, melainkan telah bergeser menjadi persoalan yurisprudensi yang mendasar, yang mempertanyakan kembali konsep-konsep hukum mapan seperti pertanggungjawaban (*liability*), alat bukti (*evidence*), dan proses hukum yang adil (*due process*). Isu-isu seperti pelanggaran privasi, manipulasi informasi, dan pengikisan integritas akademik hanyalah beberapa manifestasi dari risiko yang melekat pada era digital ini.

Lebih jauh lagi, tantangan regulasi ini melampaui sekadar isu perlindungan konsumen atau penegakan hukum siber. Ia menyentuh inti dari kedaulatan digital suatu negara. Kemampuan sebuah bangsa untuk mengatur aliran data lintas batas, mengawasi penerapan sistem AI yang dikembangkan oleh entitas asing, dan melindungi ruang diskursus publik dari manipulasi algoritmik (eksploitasi sistem) merupakan pilar utama kedaulatan di abad ke-21. Kasus-kasus seperti peretasan data berskala besar yang menyasar institusi negara, sebagaimana yang terjadi dalam insiden Bjorka di Indonesia, serta skandal manipulasi pemilu oleh Cambridge Analytica di luar negeri, menjadi pengingat keras bahwa kegagalan dalam meregulasi teknologi ini dapat mengancam stabilitas nasional dan integritas proses demokrasi. Ketika korporasi teknologi global mengendalikan infrastruktur data dan AI, kebijakan internal dan algoritma mereka dapat memberikan dampak yang lebih langsung terhadap warga negara dibandingkan hukum domestik itu sendiri. Oleh karena itu, upaya untuk meregulasi AI dan Big Data pada hakikatnya adalah sebuah tindakan untuk menegaskan kedaulatan negara dan melindungi fondasi demokrasi dari kekuatan eksternal yang tidak akuntabel.

B. Peta Regulasi Lanskap Digital Indonesia

Fondasi dan Keterbatasan Indonesia telah mengambil langkah-langkah signifikan untuk membangun kerangka hukum yang mengatur ruang digital. Tiga pilar utama yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), dan pedoman etika AI membentuk fondasi bagi tata kelola digital di negara ini. Namun, analisis yang lebih mendalam menunjukkan bahwa meskipun fondasi ini telah diletakkan,

arsitekturnya dirancang untuk era internet yang lebih awal dan kini menunjukkan keterbatasan yang serius ketika dihadapkan pada kompleksitas AI dan *Big Data*. Kerangka hukum yang ada cenderung bersifat reaktif, dibentuk sebagai respons terhadap krisis yang telah terjadi, bukan sebagai langkah antisipatif untuk menghadapi tantangan masa depan.

1. Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah mengalami dua kali perubahan merupakan instrumen hukum pidana utama dalam ranah siber Indonesia. UU ini memberikan landasan bagi penegakan hukum terhadap berbagai kejahatan digital, seperti penyebaran berita bohong (disinformasi), ujaran kebencian, dan peretasan, yang dampaknya dapat diperparah secara eksponensial oleh AI. Dalam konteks AI, ketentuan-ketentuan ini relevan untuk menjerat pelaku yang menyalahgunakan teknologi untuk menciptakan dan menyebarkan konten berbahaya secara masif, seperti *deepfake* atau kampanye disinformasi terotomatisasi.[268]

Meskipun demikian, UU ITE sering kali dikritik sebagai pedang bermata dua. Revisi terbaru yang disahkan pada awal tahun 2024 ternyata masih mempertahankan beberapa "pasal karet" yang problematis. Pasal-pasal seperti Pasal 27A tentang pencemaran atau penyerangan kehormatan atau nama baik, dan Pasal 28 ayat (2) tentang ujaran kebencian berdasarkan SARA, memiliki rumusan yang lentur dan multitafsir. Sifat ambigu ini menciptakan ketidakpastian hukum dan membuka peluang penyalahgunaan untuk membungkam kritik yang sah terhadap pemerintah, korporasi, atau bahkan terhadap sistem AI itu sendiri. Sebagai contoh, seorang peneliti atau jurnalis yang mengungkap adanya bias diskriminatif dalam algoritma perekrutan berbasis AI yang digunakan oleh sebuah perusahaan, secara teoretis dapat dijerat dengan Pasal 27A jika laporannya dianggap "menyerang nama baik" perusahaan tersebut. Potensi kriminalisasi semacam ini

[268] Undang-Undang Nomor 1 Tahun 2024. Lihat juga: *Revisi Kedua UU ITE: Masih Mempertahankan Pasal-Pasal Karet Yang Lama, Menambah Pasal Baru Yang Sangat Berbahaya*. (n.d.). Retrieved from https://aji.or.id/informasi/revisi-kedua-uu-ite-masih-mempertahankan-pasal-pasal-karet-yang-lama-menambah-pasal-baru.

dapat menghambat transparansi dan akuntabilitas publik, yang justru sangat vital dalam mengawasi pengembangan dan penerapan teknologi AI yang bertanggung jawab.

2. Undang-Undang Pelindungan Data Pribadi (UU No. 27 Tahun 2022) merupakan sebuah tonggak sejarah bagi hak privasi di Indonesia. Undang-undang ini, yang terinspirasi dari kerangka hukum internasional seperti GDPR Uni Eropa, memperkenalkan serangkaian hak bagi subjek data dan kewajiban yang ketat bagi pengendali dan prosesor data pribadi. Hak-hak fundamental seperti hak untuk mendapatkan akses (Pasal 7), hak untuk menghapus data atau *right to be forgotten* (Pasal 8), dan yang terpenting, hak untuk mengajukan keberatan atas pengambilan keputusan otomatis termasuk pemrofilan (Pasal 10), memberikan warga negara instrumen hukum untuk mengontrol data mereka. Di sisi lain, pengendali data diwajibkan untuk memiliki dasar hukum pemrosesan yang sah (Pasal 20), menerapkan prinsip keamanan data (Pasal 35), dan melaporkan insiden kebocoran data (Pasal 46). Namun, prinsip-prinsip ideal dalam UU PDP ini diuji secara ekstrem oleh karakteristik inheren dari *Big Data* yaitu volume, kecepatan, dan keragaman (*volume, velocity, variety*). Prinsip pembatasan tujuan (*purpose limitation*), sebagaimana diatur dalam Pasal 27 yang mewajibkan pemrosesan data dilakukan secara "terbatas dan spesifik", menjadi sulit diterapkan ketika data yang dikumpulkan untuk satu tujuan (misalnya, analisis lalu lintas pengguna aplikasi) kemudian digunakan kembali (*repurposed*) untuk melatih model AI dengan tujuan yang sama sekali baru dan tidak terduga saat pengumpulan awal. Demikian pula, implementasi hak untuk menolak keputusan otomatis (Pasal 10) menjadi sangat menantang ketika berhadapan dengan algoritma *deep learning* yang kompleks dan bersifat "kotak hitam", di mana logika di balik sebuah keputusan tidak dapat dijelaskan dengan mudah bahkan oleh pengembangnya sendiri. Kehadiran UU PDP merupakan fondasi yang sangat penting, tetapi tanpa peraturan turunan yang teknis dan detail serta

pengawasan yang efektif, fondasi ini berisiko tidak mampu menahan beban kompleksitas ekosistem *Big Data* dan AI.

3. Kementerian Komunikasi dan Informatika menerbitkan Surat Edaran (SE) Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial pada Desember 2023. SE ini berfungsi sebagai jembatan normatif untuk memandu pengembangan dan pemanfaatan AI di Indonesia sembari menunggu terbentuknya peraturan yang lebih mengikat. SE ini menguraikan sembilan prinsip etika utama yang harus diperhatikan oleh para penyelenggara sistem elektronik (PSE), yaitu Inklusivitas, Kemanusiaan, Keamanan, Aksesibilitas, Transparansi, Kredibilitas dan Akuntabilitas, Pelindungan Data Pribadi, Pembangunan dan Lingkungan Berkelanjutan, serta penghormatan terhadap Kekayaan Intelektual. Penting untuk dipahami bahwa SE ini memiliki status sebagai *soft regulation* atau regulasi lunak. Artinya, ia tidak memiliki kekuatan hukum yang memaksa dan tidak mencantumkan sanksi bagi pelanggarnya. Fungsinya lebih sebagai panduan dan acuan moral bagi industri untuk melakukan swaregulasi. Meskipun tidak mengikat secara hukum, SE ini memberikan sinyal yang jelas mengenai arah kebijakan pemerintah dan dapat menjadi rujukan bagi hakim dalam mempertimbangkan itikad baik atau buruk suatu pihak dalam sengketa yang berkaitan dengan AI. Namun, ketergantungan pada pedoman etis yang tidak dapat ditegakkan secara hukum jelas tidak memadai untuk mengatasi risiko-risiko signifikan yang ditimbulkan oleh sistem AI berisiko tinggi.

Pola kemunculan ketiga pilar regulasi ini memperlihatkan postur regulasi Indonesia yang secara konsisten bersifat reaktif. UU ITE lahir untuk merespons kejahatan siber di era awal internet. UU PDP baru disahkan setelah bertahun-tahun terjadi insiden kebocoran data massal yang puncaknya adalah kasus Bjorka pada tahun 2022, yang menciptakan tekanan publik dan politik yang masif. Demikian pula, SE tentang Etika AI diterbitkan sebagai respons langsung terhadap popularitas global generative AI seperti ChatGPT yang meledak pada akhir 2022. Rangkaian sebab-akibat ini menunjukkan bahwa regulasi di Indonesia lebih sering didorong

oleh krisis (firefighting) daripada oleh visi ke depan (foresight). Tanpa pergeseran paradigma menuju model regulasi yang lebih proaktif dan antisipatif, Indonesia akan terus berada satu langkah di belakang disrupsi teknologi berikutnya, membiarkan warga negara dan institusinya rentan terhadap risiko yang belum terpetakan.

C. Studi Kasus Global dan Nasional

Manifestasi Kegagalan dan Penyalahgunaan Analisis terhadap kerangka hukum menjadi lebih tajam ketika dihadapkan pada realitas di lapangan. Berbagai kasus yang terjadi baik di tingkat nasional maupun global bukan sekadar insiden terisolasi, melainkan manifestasi nyata dari celah regulasi, dilema etis, dan kegagalan tata kelola yang telah diidentifikasi sebelumnya. Kasus-kasus ini berfungsi sebagai studi empiris yang memvalidasi urgensi untuk mereformasi pendekatan regulasi, menunjukkan bagaimana konsep-konsep abstrak seperti "privasi data" dan "bias algoritma" dapat berujung pada kerugian konkret bagi individu dan masyarakat.

1. Krisis Keamanan dan Privasi Data

Kebocoran Data Skala Masif (Studi Kasus: Bjorka). Pada tahun 2022, Indonesia digemparkan oleh serangkaian aksi peretasan oleh aktor anonim yang menamakan dirinya "Bjorka". Aktor ini mengklaim telah berhasil membobol dan menjual data dari berbagai institusi pemerintah dan BUMN, termasuk data registrasi kartu SIM, data pemilih dari Komisi Pemilihan Umum (KPU), hingga surat-surat rahasia yang ditujukan kepada Presiden. Kasus Bjorka menjadi simbol dari kegagalan katastrofik (mengantisipasi skenario terburuk) dalam tata kelola data oleh badan publik. Insiden ini secara telanjang mempertontonkan lemahnya standar keamanan siber di lembaga-lembaga pemerintah sebelum adanya UU PDP, serta menyoroti persoalan mendasar mengenai akuntabilitas negara sebagai pengendali data pribadi jutaan warganya. Respons awal pemerintah yang cenderung defensif dan saling lempar tanggung jawab antara lembaga terkait semakin menggerus kepercayaan publik terhadap kemampuan negara dalam melindungi data warganya. Kasus ini menjadi justifikasi utama percepatan pengesahan UU PDP dan kini dapat

dilihat sebagai tolok ukur terhadap kewajiban baru yang diamanatkan oleh undang-undang tersebut, terutama kewajiban untuk menerapkan langkah-langkah keamanan yang memadai (Pasal 35) dan kewajiban pemberitahuan dalam hal terjadi kegagalan pelindungan data (Pasal 46).[269]

2. Eksploitasi Data oleh Pinjaman Online Ilegal (Pinjol)

Jika kasus Bjorka merepresentasikan kegagalan di tingkat makro, maka maraknya pinjaman online ilegal atau pinjol adalah contoh nyata dari persenjataan Big Data untuk mengeksploitasi individu di tingkat mikro. Praktik pinjol ilegal beroperasi dengan modus memberikan kemudahan pinjaman tanpa syarat yang rumit, namun dengan bunga yang mencekik dan metode penagihan yang tidak manusiawi. Model bisnis ini sepenuhnya bergantung pada penyalahgunaan data. Saat pengguna menginstal aplikasi pinjol ilegal, mereka sering kali tanpa sadar memberikan izin akses penuh terhadap data-data sensitif di ponsel mereka, seperti daftar kontak, galeri foto, dan riwayat panggilan. Data ini kemudian dipanen secara masif, melanggar prinsip-prinsip fundamental dalam UU PDP seperti minimalisasi data dan pemrosesan berdasarkan persetujuan yang sah. Data yang telah dipanen tersebut kemudian digunakan sebagai senjata untuk melakukan intimidasi, teror, dan pelecehan, tidak hanya kepada peminjam tetapi juga kepada seluruh orang dalam daftar kontaknya, ketika terjadi keterlambatan pembayaran. Fenomena pinjol ilegal menunjukkan dampak destruktif dari pemrosesan data yang tidak diregulasi, yang dapat menyebabkan kerugian finansial, tekanan psikologis berat, hingga rusaknya hubungan sosial korban.[270]

---

[269] Arisa, Nadiyah. (2023). *Analisis Framing Pemberitaan Aksi Peretasan Hacker Bjorka Di Detik.Com.* e-Proceeding of Management : Vol.10, No.4 Agustus 2023 | Page 3259. Lihat: Putri, Annisa. (2024). *Upaya Hukum dalam Strategi Perlindungan Data pada Penggunaan Internet Studi Kasus : Hacker Bjorka.* Jurnal Hukum dan Pembangunan Ekonomi, Volume 12, Nomor 1, 2024. Lihat juga: Syabila, Syifa. (2025). *Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia*. Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial dan Politik Volume. 2 Nomor. 3 Agustus 2025.

[270] Hikmawati, Puteri. *Penerapan Hukum Pidana Dalam Penanganan Kasus Pinjaman Online Ilegal.* Info Singkat: Vol. XIII, No.17/I/Puslit/September/2021. Lihat juga: Gusti.grehenson. (2024). *Pinjol Ilegal Kian Marak, Pakar UGM Desak OJK Perketat Pengawasan*. Retrieved from https://ugm.ac.id/id/berita/pinjol-ilegal-kian-marak-pakar-ugm-desak-ojk-perketat-pengawasan/.

3. Manipulasi Algoritmik dan Ancaman Demokrasi

Skandal Cambridge Analytica pada tahun 2018 menjadi titik balik kesadaran global akan potensi *Big Data* untuk mengancam proses demokrasi. Perusahaan konsultan politik ini secara tidak sah memanen data pribadi dari sekitar 87 juta pengguna Facebook melalui sebuah aplikasi kuis kepribadian. Data yang dikumpulkan meliputi profil, "likes", daftar teman, dan informasi pribadi lainnya yang kemudian dianalisis menggunakan model psikometrik (pengukuran sifat-sifat mental) untuk membangun profil psikologis dari para pemilih. Dengan profil ini, Cambridge Analytica melakukan apa yang disebut sebagai *psychographic microtargeting*, yaitu mengirimkan pesan-pesan politik yang dirancang khusus untuk mengeksploitasi kecenderungan psikologis, ketakutan, dan prasangka setiap individu, dengan tujuan akhir memengaruhi pilihan mereka dalam pemilihan Presiden Amerika Serikat tahun 2016. Kasus ini mengilustrasikan bagaimana data pribadi dapat diubah menjadi data perilaku (*behavioral data*) dan digunakan sebagai instrumen manipulasi dalam skala yang belum pernah ada sebelumnya. Ini menjadi peringatan keras bahwa kerangka hukum pemilu yang ada saat ini, termasuk di Indonesia, sama sekali belum siap untuk menghadapi ancaman kampanye politik berbasis data yang dapat mengikis diskursus publik yang rasional dan sehat.[271]

4. Integritas Akademik di Era AI Generatif

Tantangan regulasi tidak hanya terjadi di ranah politik dan ekonomi, tetapi juga merambah ke dunia pendidikan. Kemunculan model AI generatif yang canggih seperti ChatGPT telah menciptakan krisis baru terkait integritas akademik. Mahasiswa kini dapat dengan mudah menghasilkan esai, tugas, atau bahkan bagian dari karya ilmiah yang koheren dan sulit dibedakan dari tulisan manusia hanya dengan memberikan beberapa perintah sederhana. Praktik ini menciptakan bentuk plagiarisme baru yang sulit dideteksi oleh perangkat lunak pengecek plagiarisme

[271] Bofa, Maya. (2022). *Data Rights di Era Surveillance Capitalism: Skandal DataCambridgeAnalytica & Facebook dalam Pemilihan Presiden AmerikaSerikat 2016*. Hasanuddin Journal of International Affairs Volume 2, No 2, August 2022. Lihat juga: Zaelany, Faris. 2023. *Pelanggaran Privasi Dan Ancaman Terhadap Keamanan Manusia Dalam Kasus Cambridge Analytica.* Journal of International Relations, Volume 9, Nomor 1, 2023, hal 125-137.

konvensional yang bekerja dengan membandingkan teks dengan basis data karya yang sudah ada. Lebih lanjut, upaya untuk melawan plagiarisme AI ini juga menimbulkan masalah baru. Perangkat lunak pendeteksi tulisan AI terbukti tidak dapat diandalkan dan memiliki tingkat *false positive* yang signifikan, yang berisiko menyebabkan tuduhan palsu dan sanksi yang tidak adil kepada mahasiswa yang jujur. Dilema ini menuntut institusi pendidikan tinggi untuk tidak sekadar menerapkan kebijakan larangan yang reaktif, tetapi untuk merumuskan kembali pendekatan pedagogis dan aturan akademik yang secara mendasar mendefinisikan ulang makna orisinalitas dan peran etis teknologi AI dalam proses pembelajaran.[272]

Apabila ditarik benang merah dari keempat studi kasus yang berbeda ini bahwa kelalaian negara dalam kasus Bjorka, predatorisme korporat oleh pinjol ilegal, manipulasi politik oleh Cambridge Analytica, dan penyalahgunaan individual dalam plagiarisme AI, maka akan tampak sebuah pola yang sama yaitu adanya "jurang pertanggungjawaban" (*accountability gap*). Dalam setiap insiden, sangat sulit untuk menunjuk satu pihak tunggal yang secara hukum dan etis bertanggung jawab penuh atas kerugian yang terjadi. Pada kasus Bjorka, terjadi saling tunjuk antar lembaga pemerintah. Operator pinjol seringkali anonim dan berada di luar yurisdiksi. Dalam skandal Cambridge Analytica, tanggung jawab tersebar di antara pengembang aplikasi, Cambridge Analytica itu sendiri, Facebook sebagai platform, dan tim kampanye politik. Bahkan dalam kasus plagiarisme, muncul perdebatan mengenai sejauh mana tanggung jawab pengembang AI yang menciptakan alat yang memfasilitasi pelanggaran tersebut. Pola ini menunjukkan bahwa kerangka hukum tradisional, yang dibangun di atas asumsi kausalitas yang jelas dan pertanggungjawaban individual mulai goyah. Implikasi yang lebih luas adalah bahwa setiap regulasi masa depan yang efektif harus berfokus pada penciptaan rantai pertanggungjawaban yang jelas dan dapat diaudit untuk seluruh siklus hidup

[272] Perry, C. (2025). *Terduga Dituduh Salah Oleh Detektor AI: Positif Salah*. Retrieved from https://undetectable.ai/blog/id/mahasiswa-dituduh-secara-salah-oleh-detektor-ai/. Lihat: *Ketika Si Curang Diberi Ruang: Menilik Pelanggaran Hak Cipta Berupa Plagiarisme oleh Mahasiswi di Surabaya.* (2024). Retrieved from https://lk2fhui.law.ui.ac.id/portfolio/ketika-si-curang-diberi-ruang-menilik-pelanggaran-hak-cipta-berupa-plagiarisme-oleh-mahasiswi-di-surabaya/. Lihat juga: Pujiati. (2024). *7 Contoh Kasus Penyalahgunaan AI di Bidang Pendidikan.* Retrieved from https://duniadosen.com/penyalahgunaan-ai/.

sistem data dan AI, mulai dari perancangan, pengembangan, penerapan, hingga penggunaan akhir.

D. Perspektif Internasional

Indonesia tidak perlu memulai dari nol. Yurisdiksi lain, terutama Uni Eropa, telah berada di garis depan dalam upaya menciptakan kerangka hukum yang komprehensif untuk era digital. Meskipun adopsi mentah-mentah terhadap regulasi asing bukanlah solusi yang bijaksana, analisis terhadap prinsip-prinsip dan arsitektur hukum dari *General Data Protection Regulation* (GDPR) dan EU AI Act menawarkan pelajaran berharga dan model konseptual yang dapat diadaptasi untuk membangun tata kelola digital Indonesia yang lebih matang, berorientasi pada hak, dan siap menghadapi masa depan.

1. Standar Emas Pelindungan Data

General Data Protection Regulation (GDPR) (Regulasi (EU) 2016/679) secara luas dianggap sebagai standar emas global untuk pelindungan data pribadi. Kekuatan fundamental GDPR tidak hanya terletak pada ketentuannya yang detail, tetapi pada pergeseran filosofis yang mendasarinya, bahwa GDPR memosisikan pelindungan data pribadi bukan sekadar sebagai praktik tata kelola perusahaan yang baik, melainkan sebagai hak asasi manusia yang fundamental (*fundamental right*). [273] Pendekatan ini melahirkan prinsip-prinsip yang jauh lebih ketat dibandingkan kerangka hukum sebelumnya. Beberapa konsep kunci dalam GDPR yang sangat relevan untuk dipelajari antara lain:

a. Privasi by Design dan by Default

Prinsip ini mewajibkan organisasi untuk mengintegrasikan pelindungan data ke dalam setiap tahap pengembangan sistem, produk, atau layanan sejak awal, bukan sebagai tambahan di akhir. Pengaturan *default* haruslah yang paling melindungi privasi pengguna.

[273] Wolford, B. (2025). *What is GDPR, the EU's new data protection law*? Retrieved from https://gdpr.eu/what-is-gdpr/.

b. Persetujuan yang Tegas dan Spesifik (*Explicit Consent*)

GDPR menetapkan standar yang sangat tinggi untuk persetujuan. Persetujuan harus diberikan secara bebas, spesifik, terinformasi, dan tidak ambigu melalui tindakan afirmatif yang jelas. Praktik seperti kotak yang sudah dicentang (*pre-ticked boxes*) secara eksplisit dilarang.[274]

c. Hak Subjek Data yang Diperluas

Selain hak-hak yang kini juga diadopsi oleh UU PDP, GDPR memberikan penekanan kuat pada hak portabilitas data, yang memungkinkan individu untuk memindahkan data mereka dari satu penyedia layanan ke layanan lain dengan mudah, sehingga mendorong persaingan dan mencegah *vendor lock-in*.

d. Lingkup Ekstrateritorial dan Sanksi yang Memberatkan

Salah satu aspek paling berpengaruh dari GDPR adalah jangkauan ekstrateritorialnya. Regulasi ini berlaku bagi setiap organisasi di mana pun di dunia yang memproses data pribadi individu yang berada di Uni Eropa. Kekuatan penegakannya didukung oleh sanksi denda yang sangat besar, yang dapat mencapai hingga 20 juta Euro atau 4% dari total omzet tahunan global perusahaan, mana yang lebih tinggi. Mekanisme sanksi ini terbukti efektif dalam memaksa perusahaan teknologi global untuk mematuhi standar GDPR.

2. Pendekatan Berbasis Risiko

Jika GDPR mengatur "bahan bakar" era digital (data), maka *EU AI Act* (Regulasi (EU) 2024/1689) adalah upaya pertama di dunia untuk meregulasi "mesin"-nya (AI) melalui sebuah kerangka hukum yang komprehensif dan mengikat (*hard law*).[275] Alih-alih menerapkan satu set aturan yang sama untuk semua jenis AI, *AI Act* mengadopsi pendekatan berbasis risiko yang cerdas dan

[274] Pheaden. (2025). *GDPR Principles and Requirements*. Retrieved from https://pro.bloomberglaw.com/insights/privacy/the-eus-general-data-protection-regulation-gdpr/#what-is-the-gdpr.

[275] AI Act. (n.d.). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. Lihat: CITI Program. (2025). *An Overview of the EU AI Act and What You Need to Know.* Retrieved from https://about.citiprogram.org/blog/an-overview-of-the-eu-ai-act-what-you-need-to-know/. Lihat juga: Kosinski, M., & Scapicchio, M. (2025). *What is the EU AI Act?* Retrieved from https://www.ibm.com/think/topics/eu-ai-act.

proporsional. Arsitektur regulasi ini dapat digambarkan sebagai sebuah piramida dengan empat tingkatan risiko:

a. Risiko yang Tidak Dapat Diterima (*Unacceptable Risk*)

Tingkat teratas piramida ini secara tegas melarang praktik-praktik AI yang dianggap sebagai ancaman nyata terhadap keselamatan, penghidupan, dan hak-hak fundamental manusia. Contohnya termasuk sistem *social scoring* oleh pemerintah, AI yang memanipulasi perilaku manusia secara subliminal (di bawah alam sadar) hingga menyebabkan kerugian, dan eksploitasi kerentanan kelompok tertentu.

b. Risiko Tinggi (*High Risk*)

Ini adalah kategori yang paling diatur secara ketat. Sistem AI yang termasuk dalam kategori ini adalah yang digunakan dalam sektor-sektor kritis di mana kegagalan atau bias dapat menimbulkan dampak serius. Contohnya meliputi AI dalam infrastruktur kritis (transportasi, energi), rekrutmen tenaga kerja, penilaian kredit, penegakan hukum (termasuk identifikasi biometrik jarak jauh), dan administrasi peradilan. Sebelum dapat dipasarkan, sistem AI berisiko tinggi ini harus memenuhi serangkaian kewajiban yang ketat, seperti melakukan penilaian risiko, memastikan kualitas data latih yang tinggi untuk meminimalkan bias, menjaga catatan aktivitas (*logging*), menyediakan dokumentasi teknis yang detail, serta memastikan adanya pengawasan manusia yang efektif.

c. Risiko Terbatas (*Limited Risk*)

Untuk sistem AI yang memiliki risiko spesifik terkait transparansi, kewajibannya lebih ringan. Pengguna harus diberi tahu secara jelas bahwa mereka sedang berinteraksi dengan sistem AI (misalnya, *chatbot*) atau bahwa konten yang mereka lihat adalah hasil buatan atau manipulasi AI (*deepfake*).

d. Risiko Minimal (*Minimal Risk*)

Mayoritas aplikasi AI, seperti filter spam atau AI dalam video game, masuk dalam kategori ini. *AI Act* tidak memberlakukan kewajiban hukum tambahan bagi sistem-sistem ini, sehingga memungkinkan inovasi untuk berkembang bebas di area yang tidak berisiko.

Pendekatan berjenjang ini sangat relevan bagi Indonesia karena ia menawarkan model regulasi yang terarah, yang memungkinkan regulator untuk memfokuskan

sumber daya pengawasan yang terbatas pada area yang paling berisiko, tanpa harus membebani atau menghambat inovasi di area yang risikonya rendah.

3. Pendekatan Sektoral

Amerika Serikat cenderung mengadopsi model yang lebih terfragmentasi dan sektoral. Hingga saat ini, belum ada undang-undang federal tunggal yang secara menyeluruh mengatur AI. Sebaliknya, regulasi dilakukan melalui kombinasi antara penerapan hukum yang sudah ada oleh lembaga-lembaga federal sesuai sektornya (misalnya, FDA untuk AI di bidang medis) dan inisiatif legislasi di tingkat negara bagian. Beberapa negara bagian seperti Colorado dan Utah telah mengesahkan undang-undang yang mengatur penggunaan AI, terutama terkait diskriminasi algoritmik. Pendekatan ini menawarkan fleksibilitas yang lebih besar, namun juga berisiko menciptakan lanskap regulasi yang tidak konsisten dan tumpang tindih (*patchwork regulation*), yang dapat menyulitkan kepatuhan dan penegakan hukum secara nasional.[276]

Fitur Kunci	UU PDP (No. 27/2022)	GDPR (EU)	EU AI Act
Fokus Utama	Pelindungan Data Pribadi	Pelindungan Data sebagai Hak Asasi Manusia Fundamental	Regulasi AI Berbasis Risiko pada Penggunaannya
Lingkup Teritorial	Yurisdiksi Indonesia	Ekstrateritorial, berlaku bagi siapa pun yang memproses data subjek data UE	Ekstrateritorial, berlaku jika sistem AI digunakan atau outputnya digunakan di UE
Dasar Hukum Pemrosesan	6 dasar hukum (mis. persetujuan, kontrak, kewajiban hukum)	6 dasar hukum yang serupa dengan penekanan yang lebih ketat pada persetujuan	Tidak berlaku langsung; fokus pada pemenuhan kewajiban sesuai tingkat risiko

[276] TOI Education / Aug 31, 2025. (n.d.). *US Education Department is all for using AI in classrooms: Key guidelines explained*. Retrieved from https://timesofindia.indiatimes.com/education/news/ethical-use-of-ai-in-us-classrooms-how-to-stay-compliant-and-innovative/articleshow/123616928.cms.

Hak Subjek Kunci	Hak Akses, Perbaikan, Hapus, Portabilitas, Keberatan atas Keputusan Otomatis	Hak serupa dengan penekanan yang lebih kuat dan implementasi yang lebih detail	Hak atas transparansi, penjelasan, dan pengawasan manusia untuk sistem AI berisiko tinggi
Kewajiban Pengendali/Provider Kunci	Wajib melakukan Penilaian Dampak PDP (PDPIA) untuk pemrosesan berisiko tinggi	Wajib melakukan *Data Protection Impact Assessment* (DPIA) untuk pemrosesan berisiko tinggi	Wajib melakukan penilaian kesesuaian, manajemen risiko, tata kelola data, dan pengawasan manusia untuk sistem AI berisiko tinggi
Mekanisme Sanksi	Denda administratif hingga 2% dari pendapatan tahunan; sanksi pidana	Denda administratif hingga 4% dari omzet tahunan global	Denda administratif hingga 7% dari omzet tahunan global

E. Kerangka Teoretis dan Solusi Regulasi

Regulasi yang terlalu ketat berisiko mematikan inovasi, sementara regulasi yang terlalu longgar atau tidak ada sama sekali akan membuka pintu bagi penyalahgunaan dan kerugian sosial seperti yang telah diuraikan dalam studi kasus. Oleh karena itu, diperlukan sebuah paradigma regulasi yang baru yang dinamis, adaptif, dan mampu menyeimbangkan antara inovasi dan kontrol. Teori Regulasi Responsif (*Responsive Regulation*) menawarkan kerangka kerja konseptual yang kuat untuk mencapai keseimbangan tersebut.[277]

[277] Ayres, I. and Braithwaite, J. (1992) *Responsive Regulation. Transcending the Deregulation Debate.* Oxford University Press, Oxford. Lihat juga: Nunes, Rui. (2015). *A New Governance Model for Independent Regulatory Agencies.* Theoretical Economics Letters, Vol.5 No.1, January 19, 2015.

1. Teori Regulasi Responsif (Ayres & Braithwaite)

Melampaui Debat Regulasi vs. Deregulasi Dipopulerkan oleh Ian Ayres dan John Braithwaite, teori Regulasi Responsif berargumen bahwa strategi regulasi yang paling efektif adalah yang mampu merespons atau beradaptasi dengan perilaku, struktur, dan budaya dari industri atau entitas yang diregulasi. Alih-alih terjebak dalam perdebatan biner (benar atau salah) antara regulasi yang kuat versus deregulasi, teori ini mengusulkan sebuah spektrum intervensi yang fleksibel. Inti dari teori ini adalah konsep "piramida penegakan" (*enforcement pyramid*). Piramida ini menggambarkan hierarki strategi intervensi regulator.

a. Dasar Piramida

Di tingkat paling bawah dan paling luas, regulator memulai dengan dialog, persuasi, dan mendorong swaregulasi (*self-regulation*). Ini adalah pendekatan yang paling tidak intervensionis dan paling hemat biaya, yang mengasumsikan bahwa sebagian besar entitas yang diregulasi memiliki itikad baik untuk patuh.

b. Tingkat Menengah

Jika persuasi gagal atau swaregulasi terbukti tidak efektif, regulator akan "naik" ke tingkat berikutnya dalam piramida. Intervensi menjadi lebih formal dan memaksa, dimulai dari surat peringatan, kemudian pengenaan denda atau sanksi administratif.

c. Puncak Piramida

Di tingkat tertinggi, untuk pelanggaran yang paling serius atau pelaku yang berulang kali tidak kooperatif, regulator menggunakan "senjata pamungkas" yang paling berat, seperti penuntutan pidana, penangguhan, atau bahkan pencabutan izin usaha.

2. Ancaman yang Kredibel (*Credible Threat*)

Regulator harus memiliki kapasitas dan kemauan politik untuk menggunakan sanksi di puncak piramida. Pengetahuan bahwa regulator memiliki kekuatan untuk menjatuhkan sanksi berat akan mendorong sebagian besar entitas untuk patuh secara sukarela di tingkat bawah piramida, demi menghindari eskalasi yang lebih merugikan. Dengan demikian, model ini secara inheren menyeimbangkan antara

pemberian kebebasan bagi para inovator yang bertanggung jawab dan penindakan tegas terhadap pelaku yang tidak bertanggung jawab.

F. Penutup

Menuju Tata Kelola Digital yang Berkeadilan dan Akuntabel Perjalanan untuk meregulasi *Artificial Intelligence* dan *Big Data* adalah sebuah maraton, bukan sprint. Analisis dalam bab ini telah menunjukkan bahwa tantangan yang dihadapi bersifat multidimensional, mencakup aspek hukum, etika, teknis, ekonomi, hingga kedaulatan negara. Kerangka hukum Indonesia yang ada saat ini, meskipun telah memiliki fondasi melalui UU ITE dan UU PDP, menunjukkan postur yang reaktif dan belum sepenuhnya siap menghadapi kompleksitas dan kecepatan perubahan teknologi. Studi kasus baik di tingkat nasional maupun global telah memberikan bukti empiris yang tak terbantahkan mengenai risiko-risiko nyata yang timbul dari jurang regulasi mulai dari erosi privasi dan keamanan data, eksploitasi ekonomi terhadap kelompok rentan, ancaman terhadap integritas proses demokrasi, hingga pengikisan nilai-nilai fundamental dalam dunia akademik.

Menghadapi tantangan ini, pesimisme atau penolakan terhadap teknologi bukanlah pilihan yang bijaksana. Sebaliknya, Indonesia harus mengadopsi paradigma tata kelola digital yang proaktif, adaptif, dan berprinsip. Pembelajaran dari yurisdiksi lain, seperti pendekatan berbasis hak dari GDPR dan arsitektur berbasis risiko dari EU AI Act, menawarkan cetak biru yang berharga. Namun, kunci keberhasilan tidak terletak pada peniruan, melainkan pada adaptasi yang cerdas melalui kerangka Regulasi Responsif. Model piramida penegakan yang diusung oleh Ayres dan Braithwaite menawarkan jalan tengah yang pragmatis untuk menyelesaikan paradoks antara inovasi dan kontrol, memungkinkan regulator untuk bertindak fleksibel namun tetap tegas.

Pada akhirnya, membangun masa depan digital yang adil dan akuntabel menuntut sebuah komitmen kolektif. Para pembuat kebijakan dan legislator dituntut untuk memiliki visi ke depan dan keberanian politik untuk menciptakan regulasi yang adaptif. Aparat penegak hukum harus meningkatkan kapasitas teknisnya untuk mampu melakukan penuntutan yang efektif terhadap kejahatan siber generasi

baru. Industri teknologi memiliki tanggung jawab etis untuk menanamkan prinsip-prinsip seperti *privacy by design* dan akuntabilitas algoritmik ke dalam inti model bisnis mereka. Sementara itu, akademisi dan masyarakat sipil harus terus berperan sebagai pengawas yang kritis. Jalan ke depan bukanlah untuk menakuti atau melarang teknologi, melainkan untuk membentuk arah pengembangan dan penerapannya dengan kearifan, pandangan jauh ke depan, dan komitmen yang tak tergoyahkan pada supremasi hukum dan hak asasi manusia. Masa depan digital bukanlah sesuatu yang pasif untuk diprediksi, melainkan sebuah bangunan yang harus secara aktif kita rancang dan konstruksi bersama, di mana kerangka hukum berfungsi sebagai salah satu perangkat arsitektural yang paling krusial.

BAB 11

CYBERSECURITY DAN PENCEGAHAN KEJAHATAN SIBER

Dr. Subaidah Ratna Juita, S.H., M.H.

A. Pengantar

Era digital telah menciptakan peluang baru untuk interaksi manusia yang tidak lagi terikat pada ruang fisik. Aktivitas ekonomi, pemerintahan, dan sosial kini semakin tergantung pada teknologi informasi dan komunikasi (TIK). Namun, di balik kemudahan ini, muncul berbagai bentuk ancaman kejahatan siber yang dapat merugikan individu, perusahaan, maupun negara. Kejahatan siber tidak lagi sekadar tindakan kriminal konvensional yang dilakukan secara daring, tetapi telah berkembang menjadi ancaman serius terhadap keamanan nasional dan kedaulatan data negara. Perkembangan teknologi digital pada akhirnya telah membawa perubahan mendasar dalam sistem sosial, ekonomi, dan hukum di Indonesia. Namun, kemajuan ini juga disertai dengan meningkatnya ancaman kejahatan siber seperti peretasan, kebocoran data pribadi, dan penipuan digital.

Kejahatan siber (*cybercrime*) merupakan ancaman nyata bagi keamanan nasional dan stabilitas sosial ekonomi. Menurut laporan Interpol serangan siber meningkat lebih dari 80% secara global, dan Indonesia termasuk negara yang paling terdampak di kawasan Asia Tenggara. Data *Badan Siber dan Sandi Negara (BSSN)* menunjukkan bahwa pada tahun 2023 terjadi lebih dari 1,2 miliar serangan siber terhadap infrastruktur digital nasional.

[278] Kajian ini bersifat yuridis-normatif dengan menggunakan metode analisis kualitatif terhadap berbagai kasus kebocoran data yang terjadi di Indonesia, seperti insiden BPJS Kesehatan, Dukcapil, dan serangan ransomware yang menargetkan rumah sakit pemerintah. Hasil dari kajian ini menunjukkan bahwa pencegahan kejahatan siber memerlukan sinergi antara berbagai instansi, peningkatan regulasi, serta edukasi kepada publik. Salah satu faktor penyebab yang signifikan adalah rendahnya literasi digital di kalangan pengguna, kelemahan dalam infrastruktur keamanan, serta regulasi yang masih belum memadai. Oleh karena itu, pencegahan kejahatan siber harus diterapkan secara menyeluruh, tidak hanya pada aspek teknis, tetapi juga pada aspek manusia dan kelembagaan. Pencegahan kejahatan siber menjadi prioritas nasional karena dampaknya tidak hanya merugikan individu, tetapi juga mengancam integritas negara. Sebagai respon, pemerintah Indonesia telah menerbitkan berbagai regulasi, antara lain UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan UU No. 19 Tahun 2016 yang terakhir diubah dengan UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disebut UU ITE, serta memperkuat koordinasi antarinstansi dalam bidang keamanan siber.

B. Kerangka Hukum Nasional di Bidang Keamanan Siber

Cybersecurity atau keamanan siber pada dasarnya merupakan konsep perlindungan terhadap sistem informasi dari ancaman, gangguan, dan penyalahgunaan. Menurut Anderson, keamanan siber tidak hanya mencakup aspek teknis, tetapi juga sosial, hukum, dan kelembagaan. Dalam konteks hukum Indonesia, keamanan siber dipahami sebagai bagian dari keamanan nasional yang bertujuan menjaga kerahasiaan, keutuhan, dan ketersediaan informasi digital.[279]

Sementara itu, perlindungan data pribadi berangkat dari prinsip hak asasi manusia, khususnya hak atas privasi sebagaimana tercantum dalam Pasal 28G ayat

[278] Abd. Rofik Budin, "Indonesia Alami Lonjakan 13,6 Juta Serangan Siber," 2024, https://event.cloudcomputing.id/berita/lonjakan-serangan-siber-indonesia.

[279] Rudi Nasution, "Tantangan Implementasi UU Perlindungan Data Pribadi Di Indonesia," *Jurnal Hukum Dan Informasi* 9, no. 2 (2023).

(1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menyatakan:

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya."

Hak atas privasi ini kemudian menjadi dasar bagi pembentukan regulasi mengenai data pribadi. Perlindungan data tidak hanya berarti mencegah pencurian informasi, tetapi juga memastikan pengelolaan data dilakukan dengan prinsip transparansi, akuntabilitas, dan keamanan.

Kerangka hukum nasional Indonesia di bidang keamanan siber dibangun atas dasar tiga pilar utama: (1) UU ITE dan perubahannya, (2) UU Perlindungan Data Pribadi (UU PDP), dan (3) regulasi pelaksana dari BSSN dan Kominfo.

1. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Dari perspektif hukum, kerangka regulasi di Indonesia sebenarnya telah menyediakan dasar normatif yang kuat. UU ITE muncul sebagai respons terhadap kebutuhan untuk mengatur ruang siber yang berkembang dengan pesat. Sejak diberlakukan, UU ini menjadi dasar dalam penanganan berbagai kasus terkait dunia maya. Cakupan UU ITE berupa berbagai aspek, termasuk keamanan informasi, perlindungan data pribadi, transaksi elektronik, serta pencegahan kejahatan siber. Selain itu, UU ini juga mengatur tentang penyebaran informasi yang dapat dianggap menipu, merugikan, atau melanggar norma kesusilaan. UU ITE memberikan definisi yang jelas mengenai tindakan kriminal di ruang siber, seperti penipuan daring, pencurian identitas, dan distribusi konten ilegal.[280]

UU ITE menetapkan kerangka hukum untuk transaksi elektronik, mengatur hak dan kewajiban pengguna serta penyedia layanan internet, dan memberikan

[280] Risma Siti Maesaroh, "Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital," *STAATSRECHT* 4, no. 2 (2024): 258.

regulasi terkait tindak pidana di dunia maya, termasuk penyebaran konten ilegal dan pencemaran nama baik.[281] Dalam Pasal 30 ayat (1) secara tegas menyatakan:

> *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun."*

Ketentuan ini memperjelas bahwa akses tanpa izin terhadap sistem elektronik merupakan tindak pidana. Namun, realitas di lapangan menunjukkan bahwa penegakan hukum terhadap kejahatan siber masih menghadapi banyak kendala, seperti kesulitan pembuktian digital, minimnya ahli forensik siber, serta lemahnya koordinasi antarinstansi.

Sementara Pasal 46 ayat (1) mengatur sanksi pidana atas pelanggaran tersebut:

> *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)."*

Pasal ini menjadi dasar hukum terhadap berbagai bentuk peretasan (*hacking*) atau pengaksesan sistem tanpa izin. Lebih lanjut, Pasal 32 UU ITE mengatur larangan terhadap pengubahan, penghapusan, atau pemindahan informasi elektronik tanpa hak, sedangkan Pasal 33 menegaskan larangan terhadap tindakan yang mengakibatkan terganggunya sistem elektronik orang lain.

Hubungan yang kompleks antara keamanan siber dan keamanan nasional menunjukkan perlunya langkah-langkah hukum yang efektif. Serangan siber dapat mengancam infrastruktur vital, mengganggu fungsi pemerintah, dan mengekspos data sensitif, sehingga menimbulkan risiko langsung terhadap kedaulatan negara. Di Indonesia, yang tengah mengalami digitalisasi pesat dan konektivitas yang semakin luas, tantangan di bidang keamanan siber menjadi semakin kompleks. UU

[281] H.dan Agung Cucu Purnawirawan Ajamalus, "Perkembangan Hukum Cyber Di Indonesia: Tantangan Dan Peluang," *Bulletin of Community Engagement*, 2024.

ITE, yang disahkan pada tahun 2008, berfungsi sebagai dasar hukum utama dalam menangani isu ini. Namun, kritik muncul terkait dengan kecukupan dan kemampuannya untuk menghadapi ancaman siber yang terus berkembang. Oleh karena itu, memahami keunggulan dan kelemahan kerangka hukum Indonesia sangat penting untuk merumuskan rekomendasi yang sesuai dengan konteks nasional. [282]

2. Undang-Undang Perlindungan Data Pribadi (UU PDP)

Hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam membangun rezim hukum perlindungan data di Indonesia. Kehadiran UU PDP menjadi titik balik penting dalam sistem hukum nasional karena mengatur secara komprehensif tata kelola, hak, dan tanggung jawab dalam pengolahan data pribadi. Sebagai pelengkap dari UU ITE, UU PDP menegaskan hak-hak subjek data pribadi dan kewajiban pengendali data.

UU PDP ini memperluas cakupan hukum dari sekadar penindakan ke arah pencegahan, tata kelola, dan tanggung jawab pengendali data. Pasal 4 ayat (1) UU PDP menyatakan:

"Setiap orang memiliki hak atas perlindungan data pribadinya."

Kemudian, Pasal 20 ayat (1) menegaskan kewajiban pengendali data untuk menjamin keamanan data pribadi dari kehilangan, penyalahgunaan, atau akses ilegal. Apabila terjadi pelanggaran, Pasal 65 ayat (2) memberikan kewenangan kepada pemerintah untuk mengenakan sanksi administratif berupa denda paling banyak 2% dari pendapatan tahunan badan hukum terkait. Pasal 4 UU PDP menegaskan bahwa setiap individu memiliki hak atas perlindungan data pribadinya, sementara Pasal 65 menetapkan sanksi administratif dan pidana terhadap pelanggaran perlindungan data.

Ketentuan pidana juga diatur dalam Pasal 67 ayat (1) UU PDP yang berbunyi:

[282] Herni Rahmayanti, "Peran Hukum Dalam Mengatakan Serangan Cyber Yang Mengancam Keamanan Nasional," *Jurnal Hukum Dan HAM Wara Sains* 2, no. 9 (2023): 907.

"Setiap orang yang secara melawan hukum mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."

Dari perspektif hukum, UU PDP berfungsi sebagai *lex specialis* terhadap perlindungan data pribadi, melengkapi ketentuan umum dalam UU ITE. Namun, efektivitasnya sangat bergantung pada kesiapan lembaga pengawas yang ditunjuk pemerintah, sebagaimana diatur dalam Pasal 58 ayat (1) yang menyebutkan pembentukan lembaga pengawas independen untuk memastikan pelaksanaan perlindungan data pribadi. Implementasi UU PDP juga berkaitan dengan aspek tanggung jawab korporasi. Misalnya, pengendali data seperti instansi publik atau perusahaan digital memiliki kewajiban untuk melaporkan insiden kebocoran data kepada subjek data dan pemerintah. Ketentuan ini penting dalam membangun budaya akuntabilitas digital di Indonesia.

Dengan demikian, regulasi ini memperluas cakupan hukum siber dari sekadar penindakan ke arah pencegahan dan penguatan tata kelola data. Namun, upaya pencegahan kejahatan siber tidak dapat dilakukan hanya melalui regulasi hukum. Pendekatan sosial dan teknis juga sangat penting, mengingat bahwa banyak kasus pelanggaran terjadi akibat kelalaian pengguna dan rendahnya kesadaran keamanan digital. Oleh karena itu, tulisan ini menekankan pentingnya sinergi antara pendekatan hukum, sosial, dan teknologi untuk menciptakan ekosistem siber yang aman dan berkelanjutan.

3. Regulasi Pelaksana dan Peran BSSN

Badan Siber dan Sandi Negara (BSSN) sebagai lembaga negara memiliki mandat strategis untuk melindungi ruang siber nasional. Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, BSSN bertugas menyelenggarakan keamanan siber secara nasional, termasuk deteksi dini, pencegahan, serta mitigasi serangan siber terhadap infrastruktur vital informasi.

Selain itu, Peraturan BSSN Nomor 8 Tahun 2020 tentang Strategi Keamanan Siber Nasional menetapkan kebijakan strategis keamanan siber yang berfokus pada lima pilar utama, yaitu:

a. Ketahanan dan keandalan sistem informasi nasional,
b. Penguatan sumber daya manusia di bidang keamanan siber,
c. Pengembangan riset dan inovasi teknologi siber,
d. Kolaborasi antarinstansi pemerintah dan sektor swasta, serta
e. Penegakan hukum terhadap pelanggaran di ruang siber.

Melalui kerangka hukum ini, pemerintah berupaya menciptakan sistem yang menyeluruh dalam menjaga keamanan data nasional sekaligus memberikan kepastian hukum bagi masyarakat digital.

C. Analisis Kasus Empiris Berkaitan dengan *Cybersecurity* di Indonesia

1. Kasus Kebocoran Data BPJS Kesehatan (2021)

Pada Mei 2021, publik digemparkan oleh kebocoran data pribadi 279 juta peserta BPJS Kesehatan yang dijual secara daring di forum *RaidForums*. Data tersebut mencakup nama, NIK, alamat, dan status keanggotaan. Berdasarkan investigasi BSSN dan Kominfo, kebocoran tersebut diduga berasal dari kesalahan konfigurasi server dan lemahnya enkripsi sistem penyimpanan data.

Dari aspek hukum, kasus ini jelas melanggar Pasal 30 ayat (1) UU ITE tentang akses ilegal serta Pasal 67 UU PDP mengenai pengumpulan data tanpa izin. Namun, hingga kini belum ada penegakan hukum yang tuntas, menunjukkan lemahnya penerapan prinsip *accountability* dalam tata kelola data publik.

Kasus BPJS menunjukkan bahwa pencegahan kejahatan siber tidak dapat hanya mengandalkan regulasi, tetapi juga memerlukan audit keamanan berkala dan sistem pelaporan insiden yang transparan.

2. Kebocoran Data Dukcapil (2022)

Kasus lain terjadi pada tahun 2022, ketika data penduduk dari Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) mengalami kebocoran dan

diperjualbelikan secara online. Data tersebut mencakup NIK, tanggal lahir, dan status kependudukan.

Jika mengacu pada Pasal 32 ayat (1) UU ITE dan Pasal 67 ayat (1) UU PDP, tindakan ini termasuk tindak pidana siber karena adanya unsur perolehan dan penyebarluasan data pribadi tanpa hak. Namun, pemerintah menghadapi kendala dalam menentukan pelaku utama karena jejak digitalnya melibatkan server luar negeri. Hal ini menegaskan pentingnya kerja sama internasional dan harmonisasi hukum siber lintas negara, sebagaimana diamanatkan dalam Pasal 44 UU ITE yang mengatur kerja sama internasional dalam penegakan hukum terkait tindak pidana siber.

3. Serangan *Ransomware* terhadap Rumah Sakit (2022–2023)

Kasus serangan ransomware terhadap beberapa rumah sakit pemerintah dan swasta pada 2022–2023 memperlihatkan risiko besar bagi sektor kesehatan. Serangan ini menyebabkan gangguan pelayanan dan hilangnya data pasien. Menurut Badan Siber dan Sandi Negara (BSSN), sepanjang 2023 ada 347 dugaan insiden siber di Indonesia. Insiden siber ini meliputi kebocoran data, ransomware (penyanderaan data), web defacement (peretasan situs web), dan serangan DDoS (gangguan terhadap fungsi situs web). Sekitar 40% rumah sakit di Indonesia belum memiliki sistem keamanan siber yang memadai. [283]

Dalam konteks hukum, serangan ransomware memenuhi unsur tindak pidana berdasarkan Pasal 33 UU ITE, yaitu: “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang mengakibatkan terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”

Selain pelaku, lembaga pengelola data juga dapat dimintai pertanggungjawaban apabila terbukti lalai menjaga keamanan data pasien, sebagaimana diatur dalam Pasal 35 UU PDP tentang tanggung jawab pengendali data.

[283] Adi Ahdiat, “Pemerintahan, Sektor Paling Rentan Insiden Siber,” 2024, https://databoks.katadata.co.id/infografik/2024/07/02/pemerintahan-sektor-paling-rentan-insiden-siber.

Kasus ini memperlihatkan bahwa sektor kesehatan menjadi target empuk kejahatan siber karena lemahnya sistem enkripsi, kurangnya sumber daya manusia di bidang keamanan TI, dan tidak adanya standar keamanan wajib bagi sistem publik.

D. Upaya Pencegahan Kegiatan Siber

Keamanan siber telah menjadi isu yang sangat krusial di era digital saat ini, terutama dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi di berbagai sektor kehidupan. Meskipun perkembangan teknologi ini memberikan banyak keuntungan, ia juga membawa risiko besar berupa kejahatan siber (cybercrime). Di Indonesia, kejahatan siber mencakup berbagai jenis, seperti pencurian data pribadi, peretasan, penyebaran virus komputer, penipuan daring, dan pencemaran nama baik. Ancaman-ancaman ini tidak hanya mempengaruhi individu dan perusahaan, tetapi juga dapat mengancam keamanan nasional.

Pendekatan multidisipliner menunjukkan bahwa kejahatan siber tidak dapat dipandang hanya dari aspek hukum, tetapi juga merupakan fenomena sosial dan teknologi.

a. Secara hukum, Indonesia telah memiliki instrumen regulatif yang cukup kuat, namun implementasinya masih lemah karena terbatasnya kapasitas lembaga penegak hukum.
b. Secara sosial, rendahnya literasi digital masyarakat memperparah kerentanan terhadap serangan siber, terutama melalui penipuan daring (*phishing*) dan rekayasa sosial (*social engineering*).
c. Secara teknis, masih banyak lembaga publik yang belum menerapkan standar keamanan informasi berbasis ISO/IEC 27001 atau sistem manajemen keamanan informasi nasional.

Ketiga aspek ini menunjukkan bahwa pencegahan kejahatan siber harus dilakukan secara holistik. Pemerintah perlu memperkuat kapasitas BSSN dan aparat penegak hukum, meningkatkan literasi digital publik, serta mendorong adopsi teknologi keamanan mutakhir seperti *multi-factor authentication*, enkripsi data, dan sistem deteksi dini ancaman siber (SIEM).

Keamanan siber (*cybersecurity*) dan pencegahan kejahatan siber (*cybercrime*) memiliki dimensi ekonomi yang signifikan. Kejahatan siber tidak hanya merusak data atau reputasi individu dan organisasi, tetapi juga memiliki dampak luas terhadap perekonomian, baik pada tingkat mikro (individu, perusahaan) maupun makro (ekonomi negara).[284]

Pencegahan kejahatan siber di Indonesia dapat dilakukan melalui pendekatan struktural. Pencegahan struktural merupakan pendekatan yang dilakukan melalui pembentukan, penguatan, dan harmonisasi perangkat hukum serta kelembagaan yang mengatur keamanan dan ketertiban dunia maya. Pendekatan ini menitikberatkan pada sistem hukum nasional, kebijakan publik, serta koordinasi antarinstansi pemerintah dalam mengantisipasi dan menindak kejahatan siber secara komprehensif.

1. Penguatan Kerangka Hukum Nasional

Kerangka hukum nasional menjadi dasar utama dalam menegakkan dan mencegah tindak pidana siber. Indonesia telah memiliki UU ITE, sebagai landasan utama dalam mengatur perilaku masyarakat di ruang siber. Pasal 30 sampai dengan Pasal 33 UU ITE secara tegas melarang akses ilegal terhadap sistem elektronik dan data pribadi.

Di samping UU ITE, terdapat Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang memperkuat tanggung jawab penyelenggara sistem elektronik dalam menjaga keamanan data pengguna. Selain itu, pemerintah juga telah menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menjadi langkah penting dalam perlindungan hak digital warga negara.

Penguatan sistem hukum menurut Budi Rahardjo, harus bersifat adaptif terhadap perkembangan teknologi agar regulasi tidak tertinggal dari modus kejahatan siber yang terus berubah. Oleh karena itu, evaluasi dan pembaruan

[284] Handrini Ardiyanti, "Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 5, no. 1 (2016).

regulasi harus dilakukan secara berkala untuk menutup celah hukum yang mungkin dimanfaatkan pelaku.[285]

2. Pembentukan dan Penguatan Lembaga Keamanan Siber

Pencegahan kejahatan siber juga dilakukan melalui pembentukan lembaga yang secara khusus menangani isu-isu keamanan digital. Pemerintah Indonesia telah membentuk Badan Siber dan Sandi Negara (BSSN) berdasarkan Peraturan Presiden Nomor 53 Tahun 2017 yang kemudian diperbarui dengan Peraturan Presiden Nomor 133 Tahun 2017. BSSN berfungsi sebagai lembaga sentral yang bertugas menjaga kedaulatan siber, melakukan deteksi dini, mitigasi serangan, serta melakukan koordinasi antara instansi pemerintah dan sektor swasta.

Selain BSSN, unit khusus penegakan hukum juga dibentuk di bawah Direktorat Tindak Pidana Siber Bareskrim Polri untuk menangani kejahatan siber dari sisi penindakan. Lembaga ini bekerja sama dengan Interpol, ASEAN *Cybercrime* Unit, serta berbagai lembaga internasional untuk meningkatkan efektivitas pencegahan dan penegakan hukum lintas negara.

3. Koordinasi Antarinstansi dan Kolaborasi Multisektor

Kejahatan siber bersifat lintas sektor dan lintas yurisdiksi, sehingga pencegahannya memerlukan koordinasi yang kuat antarinstansi. Pemerintah telah membentuk *National Cyber Coordination Center (NCCC)* yang berfungsi mengintegrasikan kebijakan antar lembaga seperti Kominfo, Polri, BSSN, BNN, Kemhan, dan Kemenkumham. Kolaborasi multisektor ini mencakup berbagai aspek, mulai dari pertukaran informasi ancaman *(threat intelligence sharing*), penyusunan kebijakan, hingga pelaksanaan operasi siber bersama. Efektivitas pencegahan kejahatan sangat bergantung pada koordinasi struktural antar lembaga yang memiliki kewenangan berbeda namun tujuan yang sama, yakni mengurangi peluang terjadinya tindak pidana.

4. Kerja Sama Internasional di Bidang Keamanan Siber

Karakter kejahatan siber yang bersifat lintas batas membuat kerja sama internasional menjadi elemen penting dalam pencegahan. Indonesia aktif

[285] Budi Rahardjo, *Eamanan Sistem Informasi Berbasis Internet* (Bandung: PT. Insan Indonesia, 2005).

berpartisipasi dalam berbagai forum internasional seperti ASEAN *Cybersecurity Cooperation Strategy* (2023–2025*), Budapest Convention on Cybercrime (Council of Europe), serta APEC Cybersecurity Framework*. Melalui kerja sama ini, Indonesia memperoleh akses terhadap pelatihan, teknologi deteksi dini, serta jaringan informasi global yang memperkuat kapasitas nasional dalam menghadapi ancaman siber.

5. Evaluasi dan Reformasi Kelembagaan

Pencegahan kejahatan siber secara struktural memerlukan reformasi kelembagaan secara berkelanjutan. Evaluasi kinerja lembaga siber perlu dilakukan secara periodik untuk memastikan kesesuaian fungsi dan efektivitasnya dengan kebutuhan keamanan nasional.

Sementara itu Penegakan hukum terhadap kejahatan siber di Indonesia dapat dijelaskan menggunakan teori efektivitas hukum Soerjono Soekanto. Menurut Soekanto, efektivitas hukum dalam konteks ini, seperti halnya dalam bidang hukum lainnya, bergantung pada lima faktor utama, yaitu: [286]

a. Substansi hukum (aturan dan norma yang berlaku),
b. Struktur hukum (lembaga penegak hukum),
c. Kultur hukum (kesadaran masyarakat),
d. Sarana dan prasarana pendukung, serta
e. Faktor masyarakat.

Faktor Substansi Hukum (Peraturan Perundang-undangan): Mengacu pada kualitas dan kejelasan hukum materil dan formil yang mengatur kejahatan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan turunannya. Efektivitas hukum sangat bergantung pada apakah substansi hukum tersebut memadai, tidak multitafsir, dan mampu menjangkau berbagai bentuk kejahatan siber yang terus berkembang.

Faktor Penegak Hukum: Termasuk peran serta kualitas aparat penegak hukum, seperti Kepolisian, Kejaksaan, Hakim, dan lembaga terkait seperti Badan Siber dan Sandi Negara (BSSN) serta Kementerian Komunikasi dan Informatika (Kominfo).

[286] Adrian Sutedi, *Hukum Informasi Dan Transaksi Elektronik* (Jakarta: Sinar Grafika, 2020).

Efektivitas diukur dari profesionalisme, integritas, sumber daya (yang mencakup teknologi dan anggaran), dan koordinasi antar lembaga dalam penanganan kasus siber.

Faktor Sarana atau Fasilitas Penegakan Hukum: Meliputi infrastruktur fisik dan non-fisik yang mendukung proses penegakan hukum, seperti ketersediaan laboratorium forensik digital, perangkat lunak analisis, sistem database yang terintegrasi, dan anggaran operasional yang mencukupi untuk melakukan investigasi dan penyidikan kejahatan siber.

Faktor Masyarakat (Kesadaran dan Kepatuhan Hukum): Merujuk pada tingkat pemahaman, kesadaran, serta kepatuhan masyarakat terhadap hukum siber. Efektivitas penegakan hukum siber juga sangat bergantung pada partisipasi aktif masyarakat dalam mencegah kejahatan siber, melaporkan insiden yang terjadi, dan mematuhi etika serta norma penggunaan teknologi informasi yang berlaku.

Faktor Kebudayaan (Sistem Nilai yang Berlaku): Meliputi nilai-nilai budaya, norma, dan etika yang berkembang di masyarakat, termasuk dalam lingkungan digital. Faktor ini berkaitan dengan bagaimana nilai-nilai tersebut mendukung atau justru menghambat penegakan hukum, misalnya dalam hal etika berbagi informasi, privasi data, dan penghargaan terhadap hak cipta di dunia siber.

Kelima faktor ini saling terkait dan menentukan sejauh mana hukum siber di Indonesia dapat diterapkan secara efektif untuk menciptakan ruang siber yang aman dan tertib. Dalam konteks keamanan siber, kelima faktor tersebut harus berjalan beriringan. Undang-undang yang kuat akan sulit diterapkan jika aparat penegak hukum tidak memiliki kompetensi digital, atau jika masyarakat tidak menyadari pentingnya perlindungan data pribadi. Oleh karena itu, pendekatan multidisipliner menjadi sangat penting dalam memperkuat sistem keamanan siber nasional.

E. Penutup

Tulisan ini menunjukkan bahwa keamanan siber (*cybersecurity*) merupakan aspek fundamental dalam menjamin keberlangsungan sistem digital nasional, terutama setelah diberlakukannya UU ITE dan UU PDP sebagai payung hukum utama.

Pertama, rezim hukum siber di Indonesia telah membentuk kerangka yang cukup komprehensif dengan sanksi pidana dan administratif yang tegas. Namun, masih terdapat kesenjangan antara norma hukum dan praktik lapangan, khususnya dalam hal penegakan hukum, kesiapan lembaga pengawas, dan kapasitas sumber daya manusia di bidang forensik digital. Kedua, studi kasus seperti kebocoran data BPJS, data Dukcapil, serta serangan ransomware rumah sakit menunjukkan lemahnya sistem keamanan data publik dan korporasi. Insiden tersebut bukan hanya masalah teknis, tetapi juga akibat kurangnya kepatuhan terhadap prinsip perlindungan data pribadi sebagaimana diatur dalam Pasal 35 dan Pasal 67 UU PDP. Ketiga, keberhasilan pencegahan kejahatan siber membutuhkan pendekatan multidisipliner hukum, sosial, dan teknis yang saling melengkapi. Regulasi tanpa penguatan budaya keamanan digital dan kapasitas teknis tidak akan efektif. Dengan demikian, urgensi peningkatan keamanan siber bukan semata soal teknologi, tetapi juga menyangkut etika, tanggung jawab, dan tata kelola hukum digital nasional.

Pencegahan struktural terhadap kejahatan siber di Indonesia bertumpu pada tiga pilar utama: hukum yang adaptif, kelembagaan yang kuat, dan koordinasi yang efektif antarinstansi serta antarnegara. Dengan memperkuat aspek regulatif dan kelembagaan, Indonesia dapat meningkatkan resiliensi nasional terhadap ancaman siber dan membangun ekosistem digital yang aman, terpercaya, dan berkelanjutan. Langkah-langkah yang akan datang perlu difokuskan pada penguatan kerangka hukum nasional yang responsif terhadap inovasi teknologi, peningkatan kapasitas sumber daya manusia di sektor keamanan siber, penyusunan kebijakan keamanan yang lebih komprehensif, serta penyuluhan kepada masyarakat mengenai pentingnya keamanan siber untuk meminimalkan dampak kejahatan di dunia maya.

BAB 12

MASA DEPAN HUKUM SIBER: INOVASI DAN REGULASI

Bagus Hermanto, S.H., M.H.

A. Dinamika Hukum Siber dalam Lintasan Zaman: Sebuah Apersepsi

Revolusi digital yang berlangsung sejak akhir abad ke-20 telah mengubah secara fundamental cara manusia hidup, bekerja, dan berinteraksi. Internet, yang pada awalnya diciptakan sebagai sarana pertukaran data dalam konteks militer dan akademis, telah menjelma menjadi infrastruktur global yang menopang sistem ekonomi, pemerintahan, komunikasi sosial, dan budaya secara menyeluruh. Kemunculan teknologi seperti komputasi awan (*cloud computing*), kecerdasan buatan (AI), Internet of Things (IoT), blockchain, dan jaringan 5G semakin memperkuat ketergantungan manusia pada ekosistem digital[287]. Namun, kemajuan ini tidak datang tanpa konsekuensi. Munculnya kejahatan siber (*cybercrime*), penyalahgunaan data pribadi, disinformasi digital, manipulasi algoritma, dan serangan siber lintas negara menjadi ancaman nyata yang memerlukan perhatian hukum yang serius[288]. Dunia hukum—yang pada dasarnya bergerak berdasarkan preseden, prinsip-prinsip normatif, dan proses legislasi yang kompleks—seringkali tertinggal dibandingkan dengan kecepatan inovasi teknologi yang bersifat

[287]Koos, Stefan. "Digital globalization and law." Lex Scientia Law Review 6.1 (2022): 33-68.

[288]Sklair, Leslie. "The globalization of human rights." Journal of Global Ethics 5.2 (2009): 81-96.

disruptif[289]. Hal inilah yang menciptakan jurang antara kemajuan teknologi dan kesiapan hukum untuk mengaturnya.

Hukum siber (*cyber law*) sebagai cabang hukum yang menangani aktivitas di ruang digital menjadi domain yang sangat strategis dan multidisipliner tidak hanya berhubungan dengan hukum pidana (dalam konteks kejahatan digital), tetapi juga menyentuh ranah hukum perdata (kontrak elektronik, perlindungan konsumen digital), hukum administrasi (regulasi platform digital), hukum internasional (serangan siber antarnegara), serta aspek etika dan HAM digital[290]. Sejumlah urgensi pengembangan hukum siber tercermin dari beberapa hal misalnya ***pertumbuhan eksponensial teknologi digital*** tanpa payung hukum yang jelas berpotensi menimbulkan kekacauan normatif, ***peningkatan volume dan kompleksitas serangan siber,*** seperti ransomware dan pencurian identitas digital, yang menyasar sektor strategis seperti perbankan, rumah sakit, dan infrastruktur pemerintahan; ***ketidaksetaraan perlindungan hukum*** antara negara maju dan berkembang dalam mengelola data, teknologi enkripsi, dan regulasi teknologi baru dan ***ambiguitas yurisdiksi dan prinsip hukum internasional*** dalam menangani pelanggaran yang terjadi di dunia maya yang tidak mengenal batas negara. Oleh karena itu, masa depan hukum siber tidak dapat hanya bertumpu pada pendekatan konvensional. Dibutuhkan pendekatan baru yang bersifat progresif, kolaboratif, dan adaptif terhadap dinamika zaman.

Dalam kerangka filosofis, hukum siber menantang batas-batas klasik antara ruang publik dan privat, antara identitas individu dan kolektif, serta antara tanggung jawab manusia dan teknologi. Apakah AI dapat dikenakan tanggung jawab hukum? Siapa yang bertanggung jawab atas keputusan algoritma yang bias? Apakah hak untuk dilupakan (*right to be forgotten*) di ruang digital merupakan bagian dari hak asasi manusia? Pertanyaan-pertanyaan ini menunjukkan bahwa hukum siber bukan sekadar urusan teknis legalistik, tetapi juga perdebatan filosofis yang menyangkut nilai dan prinsip dasar peradaban modern. Beberapa isu utama secara filasafati yang

[289]Hermanto, B. (2023). Deliberate legislative reforms to improve the legislation quality in developing countries: case of Indonesia. The Theory and Practice of Legislation, 11(1), 1-31.

[290]Suseno, Sigid, et al. "Cybercrime in the new criminal code in Indonesia." *Cogent Social Sciences* 11.1 (2025): 2439543.

berkenaan dengan tiga nilai utama yakni prinsip kehati-hatian teknologi (*precautionary principle*): bahwa inovasi harus dilakukan dengan pertimbangan risiko hukum dan sosial, Perihal Keadilan digital yang memastikan tidak ada kelompok masyarakat yang termarginalkan oleh sistem digital yang diciptakan; serta akses yang setara terhadap teknologi hukum digital, termasuk perlindungan bagi kelompok rentan seperti anak-anak, difabel, atau warga di daerah terpencil[291].

Subtema ini bertujuan untuk mengeksplorasi secara komprehensif arah masa depan hukum siber melalui dua perspektif utama: regulasi dan inovasi. Dalam kerangka ini, regulasi dipahami bukan sebagai instrumen pembatas, melainkan sebagai alat pengarah (*steering tool*) untuk menciptakan ekosistem digital yang aman, adil, dan berkelanjutan. Di sisi lain, inovasi hukum diperlukan untuk menjembatani kesenjangan antara norma dan teknologi, termasuk melalui pendekatan *legal tech*, regulasi adaptif, dan kolaborasi multistakeholder. Secara akademik, subtema ini berkontribusi pada pengayaan literatur hukum siber yang masih berkembang, terutama dalam konteks negara berkembang seperti Indonesia yang tengah membentuk kerangka hukum digitalnya. Secara praktis, analisis ini relevan bagi pembuat kebijakan, pelaku industri digital, aparat penegak hukum, akademisi, dan masyarakat sipil dalam memahami dinamika regulasi teknologi secara mendalam dan reflektif.

B. Evolusi Hukum Siber dalam Era Reaktif menuju Era Proaktif

1. Hukum Siber pada Era Reaktif: Perkembangan Awal Hukum Siber

Hukum siber, seperti yang kita pahami sekarang, tidak muncul dalam sekejap. Pada fase awalnya, hukum terkait dengan ruang digital muncul sebagai reaksi terhadap berkembangnya teknologi informasi (TI) dan internet yang membawa tantangan-tantangan baru yang tidak terjangkau oleh hukum tradisional. Kejahatan di dunia maya atau *cybercrime* mulai terlihat pada akhir 1980-an hingga awal 1990-an, ketika komputer pribadi dan internet mulai diperkenalkan secara luas ke

[291]Rachovitsa, Adamantia. "Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue." International journal of law and information technology 24.4 (2016): 374-399.

masyarakat. Dalam fase ini, keberadaan hukum siber belum tersosialisasi dengan baik, karena dunia maya pada waktu itu masih dianggap sebagai wilayah yang terpisah dari dunia nyata, sehingga tidak ada hukum yang jelas mengaturnya. Ketika serangan siber mulai terjadi—seperti peretasan, virus komputer, atau penyalahgunaan sistem komputer—negara-negara dan masyarakat secara umum baru mulai menyadari bahwa hukum yang berlaku di dunia fisik tidak cukup untuk menangani masalah yang muncul di dunia digital[292]. Oleh karena itu, langkah pertama yang diambil oleh banyak negara adalah merespons kejadian-kejadian yang sudah terjadi, yang menandai dimulainya periode hukum siber yang bersifat reaktif.

Pendekatan reaktif dalam hukum siber mengacu pada kecenderungan untuk merespons insiden atau pelanggaran yang telah terjadi alih-alih mengantisipasi atau mencegah terjadinya kejahatan atau kerugian digital. Hukum ini bertindak hanya ketika ada bukti atau insiden yang menonjol, seperti serangan virus atau pencurian data. Dalam banyak kasus, hukum yang berlaku pada masa ini lebih berfokus pada pencarian pelaku dan penjatuhan hukuman setelah pelanggaran terjadi, tanpa upaya preventif yang jelas atau pengaturan awal yang memadai untuk mencegah potensi masalah di masa depan.

Pendekatan ini sering kali melibatkan pembentukan peraturan baru yang hanya diaktifkan ketika suatu kejadian mengharuskan adanya penanganan hukum. Dalam hal ini, hukum bersifat reaktif karena baru diterapkan setelah kerugian atau pelanggaran terjadi, dan tidak cukup cepat atau terorganisir untuk mengatasi ancaman yang berkembang dalam ekosistem digital. Sebagai contoh saat masa ini, terdapat kasus serangan Virus Komputer Salah satu ancaman yang muncul pertama kali di dunia maya adalah virus komputer. Pada tahun 1980-an dan 1990-an, virus seperti *Morris Worm* (1988) atau *ILOVEYOU* (2000) mengakibatkan kerugian besar pada sistem komputer, dengan mencuri data atau merusak infrastruktur. Serangan-serangan ini memicu perlunya regulasi yang mengatur tentang keamanan perangkat lunak dan penggunaan komputer secara bertanggung jawab. Sebagai

[292] Colombell, Mark R. "The legislative response to the evolution of computer viruses." *Richmond Journal of Law & Technology* 8.3 (2002): 18.

respons terhadap ancaman ini, beberapa negara mulai mengadopsi undang-undang terkait kejahatan komputer yang pertama kali, seperti The Computer Fraud and Abuse Act (CFAA) yang diberlakukan di Amerika Serikat pada 1986. Namun, undang-undang ini masih terbatas pada kejahatan yang sudah terjadi, dan tidak memberikan aturan preventif yang jelas tentang bagaimana mencegah serangan tersebut di masa depan. Kemudian dalam perkembangannya, terjadi kasus pencurian Identitas Digital dengan berkembangnya e-commerce pada tahun 1990-an, kasus pencurian identitas digital mulai meluas. Penggunaan kartu kredit secara online, misalnya, membuka celah bagi para penjahat untuk melakukan penipuan transaksi. Pada masa ini, hukum siber tidak memiliki regulasi yang memadai untuk menangani kejahatan tersebut, karena hukum yang ada tidak mengatur transaksi digital atau pengelolaan data pribadi secara rinci. Sebagai respons, banyak negara mulai membuat undang-undang mengenai keamanan transaksi elektronik, tetapi regulasi ini hanya berlaku setelah insiden pencurian identitas terjadi. Misalnya, beberapa negara mulai mengadopsi hukum tentang perdagangan elektronik dan perlindungan konsumen, tetapi tidak cukup untuk membentuk kerangka hukum yang dapat mencegah pencurian identitas secara sistematis.

Pendekatan reaktif ini, meskipun merupakan langkah awal dalam menanggulangi kejahatan digital, memiliki sejumlah kelemahan signifikan akibat dari pertama, keterlambatan Respons dan Kerugian yang Lebih Besar Karena hukum hanya diterapkan setelah insiden terjadi, dampaknya sering kali jauh lebih besar daripada jika hukum sudah ada untuk mencegahnya. Misalnya, serangan virus atau pencurian identitas yang tidak terdeteksi atau ditangani dengan cepat dapat merugikan korban dalam skala yang sangat besar, baik dalam hal finansial, reputasi, maupun keamanan data. Hal lainnya berkenaan dengan Tidak Ada Pengaturan yang Jelas untuk Teknologi Baru Pendekatan ini hanya memberikan perhatian kepada masalah yang sudah ada, sementara teknologi baru, seperti blockchain, kriptografi, atau kecerdasan buatan, mulai berkembang tanpa ada regulasi yang memadai. Akibatnya, banyak potensi penyalahgunaan teknologi yang tidak dapat terdeteksi oleh hukum yang ada. Kelemahan lainnya berkenaan dengan munculnya potensi Ketidakpastian Hukum Karena hukum pada periode ini lebih fokus pada reaksi

terhadap kasus tertentu, para pelaku kejahatan atau bahkan perusahaan digital yang beroperasi di wilayah abu-abu hukum sering kali tidak memiliki kejelasan tentang apa yang diperbolehkan dan apa yang tidak diperbolehkan. Hal ini menyebabkan ketidakpastian dalam ekosistem digital dan berpotensi menciptakan ruang untuk penyalahgunaan.

2. Era Kontemporer Perkembangan Hukum Siber: Regulasi Antisipatif pada Era Proaktif

Meskipun hukum siber pada periode awal didominasi oleh pendekatan reaktif, seiring dengan meningkatnya ancaman dan kompleksitas masalah yang muncul, ada pergeseran yang mulai terlihat menuju regulasi yang lebih proaktif dan preventif. Pendekatan ini mulai terlihat pada pertengahan 2000-an, dengan langkah-langkah seperti pembentukan badan pengatur yang khusus mengawasi dan mengatur penggunaan teknologi, serta kebijakan yang menekankan perlindungan data pribadi secara lebih komprehensif. Pada periode awal, hukum siber lebih banyak bersifat reaktif, di mana sistem hukum bertindak hanya ketika suatu insiden sudah terjadi, seperti serangan siber, pencurian data, atau penipuan digital. Namun, semakin berkembangnya teknologi digital, semakin jelas bahwa pendekatan reaktif tidak cukup untuk menangani tantangan yang muncul di ruang maya. Kejahatan siber berkembang pesat dan semakin kompleks, sedangkan teknologi seperti kecerdasan buatan (AI), blockchain, dan Internet of Things (IoT) memperkenalkan ancaman baru yang belum dapat diprediksi sebelumnya[293]. Untuk itu, pada pertengahan 2000-an dan seterusnya, banyak negara dan organisasi internasional mulai berpindah ke pendekatan proaktif, yang berfokus pada regulasi yang antisipatif dan pencegahan. Pendekatan ini bertujuan untuk mengatur perkembangan teknologi dan aktivitas digital dengan menetapkan aturan yang jelas di muka, bukan hanya untuk merespons kejadian-kejadian yang sudah terjadi. Regulasi yang antisipatif mengharuskan adanya perencanaan kebijakan yang lebih holistik, yang tidak hanya melihat kejahatan atau pelanggaran digital setelah terjadi,

[293]Buiten, Miriam C. "Towards intelligent regulation of artificial intelligence." *European Journal of Risk Regulation* 10.1 (2019): 41-59.

tetapi juga bagaimana mencegah potensi risiko dan dampak negatif yang mungkin timbul.

Regulasi yang antisipatif tidak hanya mengatur tindak pidana yang terjadi di dunia maya, tetapi juga berfokus pada pengendalian dan pencegahan potensi risiko yang ditimbulkan oleh perkembangan teknologi. Berikut adalah beberapa karakteristik dari regulasi antisipatif dalam konteks hukum siber yakni pertama, Pendekatan Berbasis Prinsip dan Proses Regulasi yang antisipatif menekankan prinsip dasar dalam penerapan hukum, seperti keamanan data, privasi individu, dan transparansi algoritma. Misalnya, prinsip transparansi dalam pengelolaan data pribadi menuntut perusahaan untuk memberikan penjelasan yang jelas dan mudah dipahami mengenai bagaimana data pengguna akan digunakan. Hal ini berfungsi sebagai pencegahan lebih awal terhadap potensi penyalahgunaan atau penyimpangan dalam pengelolaan data. Kedua, Regulasi yang Mengarah pada Inovasi Teknologi yang Aman Regulasi proaktif berusaha menciptakan kerangka hukum yang memungkinkan inovasi teknologi tanpa mengabaikan aspek keamanannya. Pendekatan ini melibatkan pengembangan *sandbox regulation* sebagaimana dipraktikkan Inggris dan Singapura, yang memungkinkan perusahaan fintech menguji produk mereka dalam lingkungan yang terkendali sebelum diluncurkan ke pasar umum. Hal ini memungkinkan regulator untuk mengidentifikasi potensi risiko dan kelemahan dalam teknologi tersebut, serta membuat regulasi yang lebih efektif tanpa menghambat inovasi yang memungkinkan perusahaan dan pengembang teknologi untuk menguji dan mengeksplorasi inovasi mereka dalam lingkungan yang terkendali, sambil memastikan bahwa teknologi yang diujicobakan tidak membahayakan pengguna atau merusak ekosistem digital. Ketiga, Perlindungan Data dan Privasi yang Lebih Ketat Salah satu contoh dari regulasi antisipatif yang paling terkenal adalah General Data Protection Regulation (GDPR) di Uni Eropa, yang diterapkan pada 2018. GDPR mengatur bagaimana perusahaan mengumpulkan, memproses, dan menyimpan data pribadi, dengan tujuan melindungi privasi individu dari

penyalahgunaan oleh pihak ketiga[294]. Regulasi ini mengatur prinsip seperti right to be forgotten, akses data, dan persetujuan eksplisit dalam pengumpulan data pribadi. Implementasi regulasi ini memberikan perlindungan proaktif kepada individu untuk mencegah pelanggaran data di masa depan. Keempat, Pencegahan Kejahatan Siber melalui Kode Etik dan Kebijakan Keamanan Regulasi antisipatif dalam hukum siber juga mencakup kebijakan untuk mencegah kejahatan siber, baik dari sisi pencegahan maupun mitigasi, seperti halnya pola Cybersecurity Act di Singapura yang mendorong regulasi bertujuan untuk memastikan bahwa sektor-sektor kritikal ini tidak hanya berfokus pada respons terhadap insiden, tetapi juga pada pencegahan dan mitigasi risiko yang ada, mengedukasi pengguna internet dan organisasi tentang keamanan digital melalui standar dan kode etik yang jelas, serta kewajiban untuk memiliki sistem keamanan yang terstandarisasi[295]. Regulasi ini juga mengharuskan perusahaan untuk memiliki prosedur keamanan yang efektif dalam menghadapi potensi ancaman siber. Kelima, Kolaborasi Internasional dalam Regulasi Siber Dalam menghadapi kejahatan siber yang bersifat lintas negara, pendekatan proaktif juga memerlukan kolaborasi internasional dalam penyusunan regulasi. Organisasi internasional seperti United Nations dan OECD telah berupaya untuk menciptakan kerangka kerja internasional untuk memerangi kejahatan siber. Di tingkat negara, perjanjian dan konvensi internasional seperti Budapest Convention tentang kejahatan siber bertujuan untuk memfasilitasi kerjasama antarnegara dalam hal investigasi dan penegakan hukum siber.

C. Resistensi dan Tantangan Mewujudkan Hukum Siber dalam basis Regulasi dan Inovasi

Implementasi regulasi yang proaktif dalam hukum siber memiliki potensi besar untuk menciptakan ekosistem digital yang aman dan terkelola dengan baik[296].

[294]Ringe, Wolf-Georg, and R. U. O. F. Christopher. "Regulating Fintech in the EU: the Case for a Guided Sandbox." *European Journal of Risk Regulation* 11.3 (2020): 604-629.

[295] Seng, Nicholas. "Cybersecurity regulation—types, principles, and country deep dives in Asia." *International Cybersecurity Law Review* 5.3 (2024): 387-411.

[296] Wibowo, Ari, Widya Alawiyah, and Azriadi. "The importance of personal data protection in Indonesia's economic development." *Cogent Social Sciences* 10.1 (2024): 2306751.

Dengan regulasi yang lebih anticipatory, pemerintah dan organisasi dapat mengurangi potensi kerugian yang diakibatkan oleh kejahatan siber, pencurian data, atau penyalahgunaan teknologi [297]. Namun, meskipun pendekatan ini menawarkan banyak manfaat, terdapat berbagai tantangan yang harus dihadapi dalam implementasi regulasi proaktif. Tantangan ini dapat bersifat teknis, politik, sosial, serta ekonomi [298]. Untuk memahami lebih dalam mengenai tantangan tersebut, kita akan mengeksplorasi beberapa hambatan utama yang muncul dalam upaya penerapan regulasi yang mengedepankan pencegahan dan antisipasi ini.

1. Tantangan Teknologi akibat Kecepatan Perkembangan Teknologi yang Tidak Terkendali.

Salah satu tantangan utama dalam penerapan regulasi proaktif adalah kecepatan perkembangan teknologi yang terus berubah dan berkembang dengan pesat. Teknologi baru seperti kecerdasan buatan (AI), blockchain, Internet of Things (IoT), dan komputasi kuantum dapat menghadirkan potensi yang sangat besar dalam berbagai sektor, namun juga membawa tantangan besar dalam hal regulasi[299]. Perubahan yang sangat cepat ini membuat proses pembaruan regulasi sangat sulit diimbangi dengan inovasi yang terjadi di dunia digital. Regulasi yang ada sering kali tertinggal beberapa langkah dari teknologi yang sedang berkembang. Misalnya, kecerdasan buatan (AI) dan algoritma otomatis kini banyak digunakan dalam pengambilan keputusan, dari sektor finansial hingga pemerintahan. Namun, meskipun banyak risiko yang terkait dengan penggunaan AI—seperti bias algoritma, transparansi yang rendah, dan pelanggaran privasi—banyak negara belum memiliki regulasi yang memadai untuk mengaturnya. Hal ini mengarah pada risiko ketidakadilan dan penyalahgunaan teknologi yang dapat berdampak besar pada masyarakat dan ekonomi.

---

[297]Hermanto, B., & Mas Aryani, N. (2021). Omnibus legislation asa tool of legislative reform by developing countries: Indonesia, Turkey, and Serbia practice. The Theory and Practice of Legislation,9(3), 425-450.

[298]Abdul Manan, 2013, Aspek-aspek Pengubah Hukum, 2005, Kencana Prenada Media Jakarta. Cetakan keempat.

[299] Sinaga, Blassyus Bevry, and Raia Putri Noer Azzura. "Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era Society 5.0." *Padjadjaran Law Review* 12.1 (2024): 71-82.

2. Tantangan dalam Pembentukan Kebijakan dan Kerangka Hukum

Tantangan dalam Pembentukan Kebijakan dan Kerangka Hukum dengan ditandai Kesulitan dalam Menetapkan Standar Internasional yang Konsisten, bahwa sebagian besar regulasi hukum siber mengharuskan kolaborasi internasional, karena kejahatan siber sering kali bersifat lintas batas. Misalnya, serangan siber yang dilancarkan oleh individu atau kelompok dari satu negara bisa berdampak pada perusahaan atau individu di negara lain. Oleh karena itu, perlu adanya standar yang konsisten dalam mengatur hal-hal seperti perlindungan data pribadi, keamanan jaringan, dan kerjasama dalam penegakan hukum siber. Namun, tantangan terbesar yang dihadapi adalah perbedaan regulasi antarnegara. Setiap negara memiliki kepentingan, budaya, dan prioritas yang berbeda dalam hal pengaturan teknologi dan data pribadi. Beberapa negara lebih ketat dalam hal perlindungan privasi, sementara negara lain mungkin lebih longgar untuk mendorong inovasi. Ketidaksepakatan antara negara-negara besar mengenai bagaimana mengatur ruang digital dapat menghambat upaya untuk menciptakan regulasi yang seragam di tingkat internasional. Sebagai contoh, *General Data Protection Regulation* (GDPR) yang diterapkan di Uni Eropa memiliki pengaruh global[300], tetapi negara lain, seperti Amerika Serikat, belum mengadopsi standar serupa yang dapat diterima secara internasional.

3. Tantangan Ekonomi dan Sumber Daya

Tantangan Ekonomi dan Sumber Daya dengan adanya Keterbatasan Sumber Daya dalam Implementasi Regulasi**,** penerapan regulasi proaktif yang efektif memerlukan investasi yang signifikan dalam infrastruktur dan sumber daya manusia, baik dari pemerintah maupun sektor swasta. Regulator harus memiliki tim yang terlatih untuk menangani isu-isu teknologi yang rumit dan harus mampu melakukan audit dan pengawasan secara terus-menerus terhadap sistem yang terlibat[301]. Tidak semua negara, terutama yang sedang berkembang, memiliki

[300] Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." *International Journal of Market Research* 59.6 (2017): 703-705.

[301]Bagus Hermanto, 2021, Discover Future Prospect of Indoensia Criminal Law Reform: Questioing Adat Criminal Law Existence, Material, and Formal, Legislation and Constitutional Court Decisions Framework, International Seminar with theme Challenges in Reforming Indonesia

kapasitas untuk memenuhi tuntutan tersebut. Keterbatasan anggaran dan kurangnya tenaga ahli di bidang hukum teknologi dan siber sering kali membuat implementasi regulasi proaktif menjadi sangat sulit, bahkan di negara-negara maju sekalipun. Selain itu, organisasi yang lebih kecil atau perusahaan rintisan (startup) mungkin menghadapi kesulitan dalam memenuhi regulasi yang kompleks dan biaya tinggi yang terkait dengan kepatuhan terhadap peraturan yang baru diberlakukan.

4. Tantangan Sosial dan Budaya ditandai dengan resistensi terhadap Pengawasan dan Regulasi

Pendekatan proaktif dalam regulasi hukum siber juga berpotensi menimbulkan resistensi di kalangan masyarakat dan sektor swasta. Di satu sisi, regulasi yang ketat dapat dianggap sebagai langkah yang diperlukan untuk melindungi hak-hak individu, namun di sisi lain, regulasi yang berlebihan atau terlalu ketat dapat menyebabkan penurunan inovasi, peningkatan biaya operasional, atau bahkan pengekangan kebebasan digital. Terlebih di banyak negara, ada ketakutan akan munculnya pengawasan yang berlebihan oleh pemerintah atau penyalahgunaan kekuasaan dalam pengaturan data pribadi. Hal ini dapat menyebabkan ketidakpercayaan publik terhadap lembaga pemerintah yang mengelola kebijakan siber.

5. Tantangan dalam Penegakan Hukum adanya Kesulitan dalam Penegakan dan Pemantauan Regulasi,

Setelah regulasi diterapkan, tantangan berikutnya adalah bagaimana melakukan penegakan hukum secara efektif di dunia maya. Hukum siber sering kali mengharuskan pengawasan yang berkelanjutan terhadap platform digital, transaksi daring, dan interaksi antar penggunanya. Kejahatan siber, termasuk phishing, ransomware, dan penipuan online, sering kali dilakukan oleh pelaku yang sangat terorganisir dan tersembunyi di balik lapisan teknologi yang canggih. Penegakan hukum siber tidak selalu efektif karena sifat dunia maya yang global dan tidak terpusat. Kejahatan dapat dilakukan dengan menggunakan identitas palsu atau jaringan anonim, dan pelaku sering kali bersembunyi di negara yang memiliki

Criminal Law, organized by Master of Law Program, Faculty of Law Udayana University and School of Law Melbourne University, 17 June 2021, pp. 1-20.

regulasi yang lebih longgar atau tidak ada regulasi sama sekali. Hal ini membuat yurisdiksi internasional menjadi salah satu hambatan utama dalam penegakan hukum.

D. Masa Depan Hukum Siber dalam Mengombinasi Regulasi dan Inovasi yang Prospektif

Dalam beberapa dekade terakhir, dunia maya telah berkembang pesat, menciptakan peluang dan tantangan baru dalam berbagai sektor, mulai dari ekonomi hingga politik. Di sisi lain, ancaman siber seperti peretasan, pencurian data pribadi, serangan *ransomware*, dan penyalahgunaan teknologi telah menjadi masalah global yang memerlukan perhatian serius. Sebagai respons terhadap ancaman yang terus berkembang ini, inovasi dalam hukum siber menjadi sangat penting untuk menciptakan sistem hukum yang efektif dan adaptif. Inovasi ini tidak hanya mencakup pembaruan dalam regulasi, tetapi juga melibatkan penerapan teknologi baru yang dapat memperkuat keamanan dan efisiensi penegakan hukum. Inovasi dalam hukum siber harus dapat menanggapi perubahan teknologi dengan fleksibilitas, sementara tetap menjamin keadilan, privasi, dan keamanan. Dengan demikian, regulasi dan hukum siber tidak hanya bertujuan untuk melindungi individu dan organisasi dari ancaman siber, tetapi juga untuk memfasilitasi inovasi teknologi yang aman dan bertanggung jawab.

Disisi lainnya juga perlu didorong Hukum Siber dalam basis regulasi yang futuristik dan prospektif, Di tengah pesatnya perkembangan teknologi informasi dan komunikasi, hukum siber semakin memainkan peran yang sangat penting dalam menjaga stabilitas dan keamanan dunia maya. Namun, dunia maya yang dinamis dan terus berkembang memerlukan regulasi hukum siber yang tidak hanya reaktif terhadap ancaman-ancaman baru, tetapi juga adaptif terhadap perubahan teknologi yang terus berinovasi. Oleh karena itu, menciptakan regulasi yang lebih adaptif dan integratif merupakan tantangan besar yang harus dihadapi oleh pembuat kebijakan dan regulator di seluruh dunia. Regulasi yang adaptif dan integratif tidak hanya fokus pada pengaturan dan perlindungan hak-hak individu serta data pribadi, tetapi juga harus mampu menyeimbangkan kebutuhan untuk mendukung inovasi

teknologi, memastikan kerjasama internasional, dan menjaga keamanan nasional. Dalam konteks ini, regulasi yang adaptif mengacu pada kemampuan hukum untuk menyesuaikan diri dengan perubahan cepat teknologi, sedangkan regulasi yang integratif mencakup kerjasama yang erat antara sektor publik, swasta, dan negara-negara di seluruh dunia untuk menangani ancaman siber yang sifatnya lintas batas.

Pertama, Regulasi yang Lebih Adaptif terhadap Perkembangan Teknologi Baru, Salah satu arah utama masa depan hukum siber adalah penguatan perlindungan data pribadi dan keamanan siber. Kebijakan yang lebih ketat mengenai pengumpulan, penyimpanan, dan pemrosesan data pribadi sangat penting, mengingat meningkatnya ancaman terhadap privasi individu. Setidak-tidaknya ada tiga aspek penting yang dapat dilihat dalam konteks prospektif Hukum Siber dalam ranah regulasi yakni pertama, mengadopsi regulasi yang lebih ketat terkait penggunaan data pribadi, serta memperkenalkan sanksi yang lebih berat bagi perusahaan yang gagal melindungi data pelanggan, kedua, mendorong penggunaan teknologi kriptografi dan enkripsi data untuk memperkuat keamanan data pribadi dan transaksi digital. Ketiga, mengembangkan kebijakan Zero Trust Security untuk memastikan bahwa tidak ada pihak yang dipercaya secara otomatis dalam jaringan dan sistem digital. Pengembangan Kerangka Regulasi yang Fleksibel dan Adaptif, sebagai respons terhadap inovasi teknologi yang cepat berkembang, kerangka regulasi hukum siber perlu dibuat lebih fleksibel dan adaptif. Regulasi yang terlalu kaku akan menghambat perkembangan teknologi, sementara regulasi yang terlalu longgar akan menciptakan kerentanannya terhadap potensi penyalahgunaan dan kejahatan, melalui penerapan model peraturan berbasis risiko yang memungkinkan penyesuaian regulasi secara fleksibel tergantung pada tingkat ancaman yang dihadapi dan dampak dari teknologi tersebut, menggunakan regulatory sandbox yang memungkinkan uji coba teknologi baru dalam kerangka regulasi yang aman dan terkontrol, serta mengadopsi pendekatan berbasis prinsip untuk menciptakan regulasi yang tidak menghambat inovasi teknologi namun tetap menjamin hak-hak dasar pengguna, seperti perlindungan data pribadi dan keamanan siber. Dalam hal ini, melalui basis penggunaan Regulatory Sandboxing untuk Inovasi Teknologi Baru. Salah satu inovasi yang paling menarik dalam bidang hukum siber adalah

regulatory sandboxing, sebuah konsep yang memungkinkan perusahaan dan startup untuk menguji teknologi baru dalam ruang yang terkendali dan terbatas. Konsep ini pertama kali diterapkan di sektor finansial melalui FinTech sandboxes, tetapi kini juga diterapkan dalam teknologi lain yang berisiko tinggi, seperti blockchain, kecerdasan buatan (AI), dan Internet of Things (IoT). Regulatory sandbox memberikan ruang bagi inovasi tanpa takut akan sanksi langsung jika ada pelanggaran kecil atau ketidaksesuaian dengan regulasi yang ada [302] . Ini memungkinkan pengembangan dan pengujian teknologi dengan cepat, sambil memberikan pengawasan dari pihak regulator untuk memastikan bahwa teknologi tersebut aman dan dapat dipertanggungjawabkan. Singapura dan Inggris merupakan negara yang telah sukses menerapkan konsep ini di sektor teknologi, khususnya dalam hal blockchain dan AI. Termasuk, Pengembangan Hukum untuk Kecerdasan Buatan (AI) dan Etika Teknologi, bahwa perkembangan kecerdasan buatan (AI) adalah salah satu inovasi yang paling mengubah lanskap dunia digital dan hukum. Dari sektor bisnis hingga pemerintahan, AI digunakan untuk pengambilan keputusan otomatis, analisis data besar, dan bahkan peradilan otomatis. Namun, penggunaan AI juga menghadirkan tantangan besar dalam hal transparansi, keadilan, dan akuntabilitas. Oleh karena itu, inovasi hukum dalam mengatur penggunaan AI sangat penting untuk memastikan teknologi ini tidak disalahgunakan. Contoh inovasi yang berkembang adalah penerapan peraturan tentang transparansi algoritma, yang memastikan bahwa algoritma yang digunakan dalam pengambilan keputusan dapat dipahami dan dipertanggungjawabkan oleh pihak yang terlibat. Negara-negara seperti Uni Eropa telah mengusulkan Regulasi AI yang menetapkan standar etika dan keamanan bagi penggunaan AI, serta memastikan bahwa algoritma yang digunakan tidak menyebabkan diskriminasi atau bias.

Kedua, Inovasi Teknologi untuk Penguatan Penegakan Hukum Siber, melalui tiga hal yakni pertama, Blockchain dalam Penegakan Hukum dan Bukti Digital. Salah satu inovasi yang telah mengubah cara penegakan hukum dilakukan adalah

[302] Elizaveta, Gromova, and Ivanc Tjaša. "Regulatory sandboxes (experimental legal regimes) for digital innovations in BRICS." *BRICS Law Journal* 7.2 (2020): 10-36.

blockchain. Teknologi blockchain memungkinkan pencatatan data yang tidak dapat diubah dan terdistribusi, yang sangat berguna dalam konteks bukti digital dan keamanan data. Blockchain dapat digunakan untuk menyimpan jejak digital transaksi yang aman, yang tidak bisa diubah atau dihapus tanpa persetujuan seluruh jaringan. Hal ini memberikan keamanan yang lebih tinggi dalam hal keabsahan bukti di pengadilan. Sebagai contoh, teknologi blockchain dapat digunakan untuk mencatat transaksi yang terjadi dalam dunia siber, seperti transaksi cryptocurrency, dan memberikan bukti yang sah dalam kasus-kasus kejahatan siber seperti pencucian uang atau peretasan. Estonia telah menjadi pionir dalam penerapan blockchain untuk identitas digital dan pencatatan data publik, memberikan contoh bagaimana teknologi ini dapat memperkuat keamanan dan transparansi dalam pemerintahan. Kedua, Pemanfaatan Kecerdasan Buatan dalam Penegakan Hukum Siber, penggunaan kecerdasan buatan (AI) dalam penegakan hukum siber telah meningkat dengan pesat. AI digunakan untuk mendeteksi dan menganalisis ancaman siber secara otomatis, seperti malware, serangan phishing, dan upaya peretasan. Sistem AI dapat memproses data dalam jumlah besar secara real-time dan memberikan peringatan dini sebelum ancaman menjadi serangan besar. Selain itu, AI juga dapat digunakan untuk mengidentifikasi pola dalam data digital yang dapat mengarah pada penyelidikan kejahatan siber, serta memprediksi potensi ancaman berdasarkan pola historis. Di beberapa negara, seperti Amerika Serikat, AI digunakan untuk analisis forensik digital dan untuk mendukung tim investigasi siber [303] . Ketiga, Perlindungan Data Pribadi dengan Teknologi Kriptografi, teknologi kriptografi telah menjadi tulang punggung utama dalam inovasi perlindungan data pribadi di era digital. Kriptografi memungkinkan data untuk dikendalikan dan dienkripsi, memastikan bahwa hanya pihak yang berwenang yang dapat mengaksesnya. Teknologi seperti enkripsi end-to-end telah menjadi standar dalam platform komunikasi dan transaksi digital, yang menjamin bahwa data pribadi tetap aman meskipun sistem atau jaringan terancam oleh peretas. Sebagai contoh, layanan pesan instan seperti WhatsApp dan Signal menggunakan enkripsi

[303] Mehra, Salil K. "Law and cybercrime in the United States today." *The American Journal of Comparative Law* 58.suppl_1 (2010): 659-686.

end-to-end untuk memastikan bahwa hanya pengirim dan penerima yang dapat membaca pesan yang dikirim. Hal ini sangat penting dalam konteks regulasi yang mengharuskan perlindungan data pribadi yang lebih ketat. Hal-hal harus disertai dengan Pendidikan dan pelatihan dalam bidang keamanan siber menjadi sangat penting dalam meningkatkan kapasitas sumber daya manusia di seluruh dunia untuk mengatasi ancaman yang ada. Peningkatan kemampuan dalam keamanan digital, forensik digital, dan analisis ancaman sangat dibutuhkan baik di sektor publik maupun swasta, dengan mengembangkan program pelatihan dan sertifikasi untuk profesional hukum siber dan teknolog, termasuk pengajaran tentang teknik terbaru dalam analisis forensik dan deteksi serangan siber, dan menyediakan sumber daya untuk peningkatan kapasitas di negara-negara berkembang yang mungkin kekurangan tenaga ahli dan infrastruktur untuk mengelola masalah-masalah siber yang semakin kompleks.

Ketiga, kerjasama Internasional yang Lebih Kuat, terlebih dalam menghadapi ancaman siber sering kali bersifat lintas batas negara, yang membuat penegakan hukum domestik menjadi sulit. Oleh karena itu, masa depan hukum siber akan melibatkan peningkatan kerjasama internasional yang lebih erat antara negara-negara, organisasi internasional, dan lembaga non-pemerintah untuk menangani kejahatan siber secara global. Setidaknya dengan membangun dan memperkuat perjanjian internasional yang mengatur standar keamanan siber dan perlindungan data pribadi, seperti Konvensi Budapest tentang Kejahatan Siber dan Kerangka Kerja Keamanan Siber dari Organisasi Kerjasama dan Pembangunan Ekonomi (OECD)[304]. Meningkatkan pertukaran informasi antara negara dalam menangani ancaman siber, terutama dalam penyelidikan dan pengadilan kejahatan siber yang bersifat lintas batas, serta membentuk forum internasional untuk kolaborasi dalam penanggulangan ancaman siber dan berbagi pengetahuan serta pengalaman mengenai kebijakan keamanan siber. Hal ini dapat diperkuat dengan kolaborasi antara Sektor Publik dan Swasta utamanya dalam menghadapi tantangan yang terus berkembang di dunia maya, kolaborasi antara sektor publik dan swasta menjadi

[304]Tropina, Tatiana. "'This is not a human rights convention!': the perils of overlooking human rights in the UN cybercrime treaty." *Journal of Cyber Policy* (2024): 1-21.

sangat penting. Pemerintah perlu bekerja sama dengan perusahaan teknologi untuk memastikan bahwa kebijakan yang dihasilkan dapat menciptakan lingkungan digital yang aman, sekaligus mendukung inovasi teknologi yang sehat, dalam wujud mendirikan forum kolaborasi di tingkat nasional dan internasional yang menggabungkan pemangku kepentingan dari sektor publik, swasta, dan masyarakat sipil untuk membahas masalah-masalah hukum siber dan menciptakan solusi bersama, serta mendorong perusahaan teknologi untuk menjadi mitra dalam merancang kebijakan yang bertanggung jawab terkait keamanan siber dan perlindungan data pribadi, serta memberikan insentif untuk inovasi yang dapat memperkuat ekosistem digital yang aman.

Hukum siber berada di persimpangan penting dalam menghadapi tantangan dan peluang yang muncul dengan pesatnya perkembangan teknologi informasi dan komunikasi. Di satu sisi, dunia maya telah membawa banyak kemudahan dan inovasi, seperti dalam bidang ekonomi digital, komunikasi, dan teknologi, tetapi di sisi lain, hal ini juga membuka celah bagi berbagai jenis kejahatan dan pelanggaran yang semakin canggih, seperti serangan siber, penyalahgunaan data pribadi, dan penyebaran informasi palsu. Oleh karena itu, menciptakan kerangka hukum yang relevan dan efektif untuk mengatur dunia maya bukan hanya menjadi penting, tetapi juga mendesak. Masa depan hukum siber membutuhkan kerangka yang mampu menggabungkan berbagai elemen penting, seperti keamanan, privasi, kerjasama internasional, kolaborasi sektor publik dan swasta, serta pendekatan berbasis teknologi. Agar regulasi hukum siber dapat efektif, adaptif, dan tidak menghambat inovasi, perlu ada keseimbangan antara perlindungan hak individu dan kemajuan teknologi.

Pentingnya kerjasama internasional dalam menciptakan regulasi bersama akan menjadi kunci dalam mengatasi ancaman siber yang semakin global. Begitu pula, peningkatan kapasitas dalam hal pendidikan dan pelatihan di bidang hukum siber perlu didorong secara maksimal agar profesi ini dapat menanggapi berbagai tantangan baru yang akan muncul seiring dengan perkembangan dunia maya. Dengan mengimplementasikan strategi yang mencakup pembaruan regulasi secara dinamis, pemanfaatan teknologi baru, serta kolaborasi lintas sektor, masa depan

hukum siber dapat menjadi lebih terstruktur, aman, dan efisien. Hukum siber tidak hanya akan memberikan perlindungan terhadap individu dan negara tetapi juga akan mendukung ekosistem digital yang lebih sehat, aman, dan inovatif di masa depan.

Peralihan ke pendekatan proaktif dalam regulasi hukum siber menandai langkah penting dalam pengaturan dunia maya yang lebih aman dan terkendali. Regulasi yang antisipatif berusaha untuk menciptakan perlindungan digital yang lebih baik, mencegah ancaman siber sejak dini, dan memastikan bahwa teknologi berkembang dalam batas-batas yang aman. Namun, tantangan besar tetap ada, baik dalam aspek teknis maupun internasional. Oleh karena itu, peran kolaborasi global, pembaruan regulasi yang fleksibel, serta pendidikan dan kesadaran publik sangat diperlukan untuk memastikan bahwa regulasi yang antisipatif dapat berjalan efektif dan efisien. Implementasi regulasi proaktif dalam hukum siber sangat penting untuk menciptakan ekosistem digital yang aman, transparan, dan terkelola dengan baik. Namun, tantangan yang dihadapi dalam penerapan regulasi ini sangat kompleks dan mencakup berbagai aspek—dari tantangan teknologis yang berhubungan dengan kecepatan perkembangan teknologi, hingga tantangan sosial dan budaya yang berkaitan dengan penerimaan regulasi oleh masyarakat. Untuk mengatasi tantangan tersebut, diperlukan pendekatan yang holistik, yang melibatkan kerjasama antarnegara, sektor publik dan swasta, serta transparansi dalam proses regulasi.

Regulasi proaktif yang efektif harus dapat menyeimbangkan antara melindungi hak-hak individu dan mendorong inovasi teknologi yang bermanfaat bagi masyarakat secara keseluruhan. Inovasi dalam hukum siber, baik dalam bentuk regulasi yang adaptif, penggunaan teknologi baru, maupun peningkatan metode penegakan hukum, merupakan elemen penting dalam menciptakan dunia maya yang aman dan terkelola dengan baik. Teknologi seperti AI, blockchain, dan kriptografi membuka peluang baru untuk meningkatkan efisiensi, transparansi, dan keamanan dalam sistem hukum siber. Namun, inovasi ini juga membawa tantangan dalam hal regulasi dan etika, yang memerlukan pendekatan yang hati-hati agar dapat mengoptimalkan manfaatnya tanpa mengorbankan hak-hak dasar pengguna.

DAFTAR PUSTAKA

A. Buku

———. *Code and Other Laws of Cyberspace*. New York: Basic Book, 2009.

———. *Cyber Law dan Tantangan Penegakannya*. Bandung: Logoz Publishing, 2021.

———. *Hukum Perdata Internasional*. Jakarta: Raja Grafindo Persada, 2018.

———. *Penemuan Hukum*. Yogyakarta: Liberty, 2016.

———. *Pengantar Hukum Telematika*. Jakarta: Raja Grafindo Persada, 2019.

Andriyani, Widyastuti, Rian Sacipto, Deny Susanto, Cory Vidiati, Lathifaturahmah, Reza Kurniawan, and Rr. Aline Gratika Nugrahani. *Technology, Law And Society*. Makassar: Tohar Media, 2023.

Arief, Barda Nawawi. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana, 2019.

Arifudin, Nur, Jufrin Jufrin, Arini Asriyani, Theresia N.A Narwadan, Djulya Eka Pusvita, Muhammad Ardhi Razaq Abqa, Hairul Saleh Satrul, et al. *Pengantar Ilmu Hukum*. Padang: CV. Gita Lentera, 2024.

Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.

Ayres, Ian, dan John Braithwaite. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press, 1992.

Bainbridge, D. I. (2015). *Information technology law* (8th ed.). Pearson.

Barkatullah, Abdul Halim. *Hukum Transaksi Elektronik*. Bandung: Nusa Media, 2017.

Beck, U. (1992). *Risk society*. SAGE.

Born, Gary. *International Commercial Arbitration*. Alphen aan den Rijn: Kluwer Law International, 2014.

Brenner, S. (2010). *Cybercrime*. Praeger.

Broadhurst, K., & Gray, N. (2022). Understanding resilient places: Multi-level governance in times of crisis. *Local Economy*, *37*(1-2), 84-103

Brownsword, R., Scotford, E., & Yeung, K. (Eds.). (2017). *Law, regulation and technology*.Oxford University Press.

Buchanan, B. (2016). *The cybersecurity dilemma*. Oxford University Press.

Budhijanto, Danrivanto. *Cyber Law: Sistem dan Permasalahan Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2020.

Budiyanto. *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*. Banten: PT Sada Kurnia Pustaka, 2025.

Casey, E. (2019). *Digital evidence and computer crime* (4th ed.). Academic Press.

Cortés, Pablo. *Online Dispute Resolution for Consumers in the European Union*. London: Routledge, 2011.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Fiss, O. (2003). *The law as it could be*. NYU Press.

Goldsmith, J., & Wu, T. (2006). *Who controls the internet?* Oxford University Press.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?* Oxford: Oxford University Press, 2008.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Anchor.

Goodpaster, Gary. *Negotiation and Dispute Resolution*. New York: Aspen Publishers, 2001.

Hamzah, A. (2017). *Hukum Pidana Indonesia*. Sinar Grafika.

Hastri, Evi Dwi, Miftakhul Huda, Elfitri Yuza, Jana Milia, Endah Rantau Itasari, Muhammad Ryan Ramadhani Miano, M. Haafidh Zufar Purwanto, et al. *Hukum Internasional Era Society 5.0*. Sumedang: CV. Mega Press Nusantara, 2025.

Hollis, D. B. (Ed.). (2021). *The Oxford handbook of cybersecurity*. Oxford University Press.

Imelda, Chitra, Putri Maha Dewi, Eren Arif Budiman, Lola Yustrisia, Khristyawan Wisnu Wardana, Achmad Hariri, Rini Apriyani, et al. *Transformasi Hukum*. Padang: CV. Gita Lentera, 2025.

Indarta, Yose. *Cyber Law: Dimensi Hukum Dalam Era Digital*. Padang: Pustaka Galeri Mandiri, 2025.

Isaacson, Walter. *The Innovators: Kisah Para Peretas, Genius, Dan Maniak Yang Melahirkan Revolusi Digital*. Yogyakarta: Bentang Pustaka, 2016.

Juwana, Hikmahanto. *Hukum Perdata Internasional*. Jakarta: Raja Grafindo Persada, 2018.

Katharina, Riris. *Pelayanan Publik & Pemerintahan Digital Indonesia*. Jakarta: Yayasan Pustaka Obor Indonesia, 2020.

Katsh, Ethan, and Orna Rabinovich-Einy. *Digital Justice: Technology and the Internet of Disputes*. Oxford: Oxford University Press, 2017.

Kello, L. (2017). Cyber security: gridlock and innovation.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Lessig, Lawrence. *Code: Version 2.0*. New York: Basic Book, 2006.

Makarim, Edmon. *Hukum Pembuktian Elektronik*. Jakarta: Raja Grafindo Persada, 2020.

Marpi, Yapiter. *Perlindungan Hukum Terhadap Konsumen Atas Keabsahan Kontrak Elektronik Dalam Transaksi E-Commerce*. Tasikmalaya: PT. Zona Media Mandiri, 2020.

Maskun. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana, 2022.

Mertokusumo, Sudikno. *Hukum Acara Perdata Indonesia*. Yogyakarta: Liberty, 2015.

Nawawi Arief, Barda. *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara.* Semarang: Badan Penerbit Universitas Diponegoro, 2010.

Nugroho, Catur. *Cyber Society: Teknologi, Media Baru, Dan Disrupsi Informasi*. Jakarta: Kencana, 2020.

Pakarti, Muhammad Husni Abdulah, Didik Suhariyanto, Hanuring Ayu, Taqyuddin Kadir, Andrian Sah, Lilik Prihatin, Sri Ayu Astuti, Dedy Muharman, Arief Fahmi Lubis, and Pajar Pahrudin. *Hukum Siber: Menyikapi Tantangan Hukum Di Era Digital*. Jambi: PT Nawala Gama Education, 2025.

Putra, Tomi Wicaksono, Hamidah Abdurrachman, and Hamzani Achmad Irwan. *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*. Pekalongan: NEM, 2023.

Rahardjo, S. (2006). *Membedah hukum progresif*. Penerbit Buku Kompas.

Rahmadi, Takdir. *Mediasi: Penyelesaian Sengketa Melalui Pendekatan Mufakat*. Jakarta: Raja Grafindo Persada, 2017.

Ramadhani, Syarifah Fitrah. *Singularity: Interaksi Manusia Dan Mesin Dalam Teknologi Informasi*. Padang: Takaza Innovatix Labs, 2024.

Ramli, Ahmad M. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia.* Bandung: Refika Aditama, 2004.

Reed, C. (2004). *Internet law*. Cambridge University Press.

Rosadi, Sinta Dewi. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional.* Bandung: Refika Aditama, 2015.

Rule, Colin. *Online Dispute Resolution for Business*. San Francisco: Jossey-Bass, 2022.

Salim, M., Sulistiawati Ahmad, Hariati Husain, Syaifuddin Syaifuddin, Mursyid Ardiansyah, Alex Copernikus Andaria, Hastuti Dalai, Hamka Witri Kamase, Safaruddin Safaruddin, and Muh. Saleh. *Pengantar Forensik Digital*. Agam: Yayasan Tri Edukasi Ilmiah, 2025.

Sanusi, Mustakim La Dee, Tiyas Vika Widyastuti, and Arief Fahmi Lubis. *Hukum Implikasi Teknologi Dalam Perubahan Hukum*. Malang: Literasi Nusantara Abadi Group, 2023.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0*. Cambridge University Press.

Setiawan, Dodi, Asri Kunda, Giandari Maulani, Leon A. Abdillah, FA. Bambang Sukoco, Tri Yusnanto, Vivi Monita, et al. *Blockchain*. Sumedang: Mega Press Nusantara, 2025.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar*. Oxford University Press.

Ulrich, B. (1999). *World risk society*. Polity Press.

Soeprapto, M. F. I. (2018). *Ilmu Perundang-undangan 2: Proses dan Teknik Penyusunan*. PT Kanisius.

Studiawan, Hudan, and I. Kadek Agus Ariesta Putra. *Forensik Digital: Analisis Dan Investigasi Pada Sistem Android*. Yogyakarta: Andi, 2025.

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press.

United Nations Office on Drugs and Crime. *Comprehensive Study on Cybercrime.* New York: United Nations, 2013.

Varma, Anton D. *Kecerdasan Buatan (AI) Dan Hukum Di Masa Depan: Sebuah Pengantar*. Yogyakarta: Deepublish, 2024.

Viddy, Arkas, Erick Karunia, and Rafiqoh. *Crypto & Blockchain: Masa Depan Keuangan Global*. Padang: Takaza Innovatix Labs, 2025.

Wibowo, Kurniawan Tri. *Aspek Hukum Dalam Dunia Digital*. Banten: Sada Kurnia Pustaka, 2025.

B. Jurnal

Adrian Sutedi. *Hukum Informasi Dan Transaksi Elektronik*. Jakarta: Sinar Grafika, 2020.

Ahdiat, Adi. "Pemerintahan, Sektor Paling Rentan Insiden Siber," 2024. https://databoks.katadata.co.id/infografik/2024/07/02/pemerintahan-sektor-paling-rentan-insiden-siber.

Ajamalus, H.dan Agung Cucu Purnawirawan. “Perkembangan Hukum Cyber Di Indonesia: Tantangan Dan Peluang.” *Bulletin of Community Engagement*, 2024.

Aprilia, G. P., & Zulkarnain, Z. (2024). Tinjauan Hukum Pidana Islam dan Hukum Informasi dan Transaksi Elektronik terhadap Kejahatan Penagihan Pinjaman Online. *Jurnal Mediasas: Media Ilmu Syari'ah dan Ahwal Al-Syakhsiyyah*, *7*(2), 483-494.

Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media manipulation. *The computational propaganda project*, *1*, 1-26.

Braithwaite, John. "The essence of responsive regulation." *UBC Law Review* 44, no. 3 (2011): 475-520.

Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. UPNE.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

Budi Rahardjo. *Eamanan Sistem Informasi Berbasis Internet*. Bandung: PT. Insan Indonesia, 2005.

Budin, Abd. Rofik. “Indonesia Alami Lonjakan 13,6 Juta Serangan Siber,” 2024. https://event.cloudcomputing.id/berita/lonjakan-serangan-siber-indonesia.

Canton, H. (2021). Organisation for economic co-operation and development—OECD. In *The Europa Directory of international organizations 2021* (pp. 677-687). Routledge.

Citaristi, I. (2022). United Nations Office on Drugs and Crime—UNODC. In *The Europa Directory of International Organizations 2022* (pp. 248-252). Routledge.

Cortés, Pablo. “Developing Online Dispute Resolution for Consumers.” *International Journal of Law and Information Technology* 19, no. 1 (2011): 1–24.

Duggan, A. J. (2010). Roman, canon and common law in twelfth-century England: the council of Northampton (1164) re-examined. *Historical Research*, *83*(221), 379-408.

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, *27*(1), 1-3.

Greenleaf, G. (2014). *Asian data privacy laws: trade & human rights perspectives*. Oup Oxford.

Handrini Ardiyanti. "Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 5, no. 1 (2016).

Hikmawati, Puteri. "Penerapan Hukum Pidana dalam Penanganan Kasus Pinjaman Online Ilegal." *Info Singkat: Kajian Singkat Terhadap Isu Aktual dan Strategis* XIII, no. 17 (September 2021): 1-6.

JHIS, "Peran dan Tanggung Jawab Platform Digital dalam Pajak Era Society 5.0" (2024).ejurnal.politeknikpratama

JIMIK, "Pelanggaran Batas Privasi Anak dalam Praktik Sharenting di Indonesia" (2024).journal.stmiki

Jurnal Ilmu Hukum Unissula, "Pertanggungjawaban Platform Digital dalam Mengatasi Konten Ilegal" (2022).repository.unissula

Jurnal Privat Law, "Pertanggungjawaban Hukum Penyedia Platform." Vol. VIII No. 1 (2020).jurnal.uns

Juwana, Hikmahanto. "Harmonisasi Hukum Nasional di Era Digital." *Jurnal Hukum Dan Pembangunan* 50, no. 3 (2020): 398–407.

Kerr, L. (2017). The Legitimate Scope of Criminal Law: A Question for Legal History?. *Critical Analysis L.*, *4*, 11.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Columbia Law Review, 105*(1), 279–318.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Colum. L. Rev.*, *105*, 279.

Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

Koops, B. J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. *International Review of Law, Computers & Technology*, *28*(2), 159-171.

Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). The EU general data protection regulation: a commentary. *Updat. Sel. Artic.(May 4, 2021)*.

Law Justice Journal, "Kasus Kebocoran Data Pengguna Layanan E-Commerce" (2024).journal.pubmedia

Lessig, L. (1996). Reading the constitution in cyberspace. *Emory Lj*, *45*, 869.

Maharani, M. A., & Atman, W. (2025). Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik*, *2*(3), 344-354.

Makarim, Edmon. "Pembuktian Elektronik dalam Sistem Peradilan Indonesia." *Jurnal Hukum IUS QUIA IUSTUM* 25, no. 2 (2018): 225–33.

Menon, Sundaresh. "Technology and the Changing Face of Justice." *Singapore Academy of Law Journal* 28, no. 1 (2016): 1–18.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.

Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In *The ethics of information technologies* (pp. 141-178). Routledge.

O'hara, K., & Hall, W. (2018). Four internets: The geopolitics of digital governance.

Rachlinski, J. J. (2010). Evidence-based law. *Cornell L. Rev.*, *96*, 901.

Rahmayanti, Herni. "Peran Hukum Dalam Mengatakan Serangan Cyber Yang Mengancam Keamanan Nasional." *Jurnal Hukum Dan HAM Wara Sains* 2, no. 9 (2023): 907.

Reidenberg, J. R. (2005). Technology and internet jurisdiction. *University of Pennsylvania law review*, *153*(6), 1951-1974.

Risma Siti Maesaroh. "Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital." *STAATSRECHT* 4, no. 2 (2024): 258.

Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE dalam Perspektif Perkembangan teknologi informasi dan komunikasi. *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam*, *7*(2), 309-339.

Rudi Nasution. "Tantangan Implementasi UU Perlindungan Data Pribadi Di Indonesia." *Jurnal Hukum Dan Informasi* 9, no. 2 (2023).

Sabila, Syifa Nurul, dan Wira Atman. "Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia." *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik* 2, no. 3 (2025): 142-154.

Sanskara Hukum dan HAM. "Tinjauan Yuridis terhadap Tanggung Jawab Platform Digital atas Konten Ilegal di Indonesia." Vol. 4 No. 01 (2025): 276–286.eastasouth-institute

Scherer, Matthew U. "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies." *Harvard Journal of Law & Technology* 29, no. 2 (2016): 354-400.

Solum, L. B. (2019). Artificially intelligent law. *BioLaw Journal-Rivista di BioDiritto*, (1), 53-62.

Sunstein, C. (2008). Democracy and the Internet. *Information technology and moral philosophy*, *93*.

Svantesson, D. J. B. (2018). Enter the quagmire–the complicated relationship between data protection law and consumer protection law. *Computer law & security review*, *34*(1), 25-36.

Tufekci, Z. (2018). It's the (democracy-poisoning) golden age of free speech. *Wired*, *16*(01), 2018.

Wall*, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1-2), 45-63.

Yeboah-Ofori, A., Yeboah-Boateng, E., & Yankson, H. G. (2019, May). Relativism digital forensics investigations model: a case for the emerging economies. In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)* (pp. 93-100). IEEE.

Zenz, A., & Powles, J. (2024). Resisting technological inevitability: Google Wing's delivery drones and the fight for our skies. *Philosophical Transactions A*, *382*(2285), 20240107.

C. Perundang-Undangan

———. *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik.* PP No. 71 Tahun 2019, LN No. 185 Tahun 2019, TLN No. 6400.

———. *Peraturan Presiden tentang Pelindungan Infrastruktur Informasi Vital.* Perpres No. 82 Tahun 2022.

———. *Peraturan Presiden tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.* Perpres No. 133 Tahun 2017.

———. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.*

———. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (2022).

———. Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa (1999).

———. *Undang-Undang tentang Bantuan Hukum Timbal Balik dalam Masalah Pidana.* UU No. 1 Tahun 2006, LN No. 18 Tahun 2006, TLN No. 4607.

———. *Undang-Undang tentang Hak Cipta.* UU No. 28 Tahun 2014, LN No. 266 Tahun 2014, TLN No. 5599.

———. *Undang-Undang tentang Intelijen Negara.* UU No. 17 Tahun 2011, LN No. 52 Tahun 2011, TLN No. 5218.

———. *Undang-Undang tentang Otoritas Jasa Keuangan.* UU No. 21 Tahun 2011, LN No. 111 Tahun 2011, TLN No. 5253.

———. *Undang-Undang tentang Pelindungan Data Pribadi.* UU No. 27 Tahun 2022, LN No. 163 Tahun 2022, TLN No. 6833.

———. *Undang-Undang tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.* UU No. 8 Tahun 2010, LN No. 122 Tahun 2010, TLN No. 5164.

———. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* UU No. 19 Tahun 2016, LN No. 251 Tahun 2016, TLN No. 5952.

———. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.* UU No. 31 Tahun 2014, LN No. 293 Tahun 2014, TLN No. 5602.

———. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme.* UU No. 5 Tahun 2018, LN No. 92 Tahun 2018, TLN No. 6216.

———. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak.* UU No. 35 Tahun 2014, LN No. 297 Tahun 2014, TLN No. 5606.

———. *Undang-Undang tentang Pornografi.* UU No. 44 Tahun 2008, LN No. 181 Tahun 2008, TLN No. 4928.

ASEAN. *ASEAN Cybersecurity Cooperation Strategy.* Jakarta: ASEAN Secretariat, 2021.

Badan Standardisasi Nasional. *Standar Nasional Indonesia tentang Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Persyaratan, SNI ISO/IEC 27001:2013.* Jakarta: BSN, 2013.

Bareskrim Polri. *Laporan Tahunan Direktorat Tindak Pidana Siber Tahun 2022.* Jakarta: Kepolisian Negara Republik Indonesia, 2023.

BSSN. (2024). *Peraturan BSSN 5/2024 tentang RAN Keamanan Siber*.

Council of Europe. *Convention on Cybercrime.* ETS No. 185. Budapest: Council of Europe, 2001.

European Commission, Regulation (EU) No 524/2013 on Online Dispute Resolution for Consumer Disputes (2013).

European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing*

Directive 95/46/EC (General Data Protection Regulation). OJ L 119 (2016).

European Parliament and Council of the European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act)*. OJ L (2024).

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).* 27 April 2016.

G20 Indonesia. *G20 Digital Economy Ministers' Meeting: Chair's Summary.* Bali: G20 Indonesia Presidency, 2022.

Indonesia. *Kitab Undang-Undang Hukum Pidana [Wetboek van Strafrecht]*. Diterjemahkan oleh Moeljatno. Jakarta: Bumi Aksara, 2008.

Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (2008).

Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Kejaksaan Republik Indonesia. *Peraturan Jaksa Agung tentang Tata Cara Penanganan Perkara Pidana Siber.* Perja No. 15 Tahun 2020.

Kementerian Komunikasi dan Informatika Republik Indonesia. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. 19 Desember 2023.

Kepolisian Negara Republik Indonesia. *Peraturan Kapolri tentang Tata Cara Penanganan Barang Bukti Digital.* Perkap No. 10 Tahun 2021.

Kominfo. (2020). *Permenkominfo 5/2020 tentang PSE Privat*.

Kominfo. (2021). *Permenkominfo 10/2021*.

Mahkamah Agung Republik Indonesia. *Cetak Biru Pembaruan Peradilan 2010–2035*. Jakarta: MA RI, 2020.

Mahkamah Agung Republik Indonesia. Peraturan Mahkamah Agung Nomor 1 Tahun 2019 (2019).

Makarim, Edmon. "Implikasi Ratifikasi Konvensi Budapest terhadap Kedaulatan Digital Indonesia." *Jurnal Hukum dan Pembangunan* 49, no. 3 (2019): 567-589.

Otoritas Jasa Keuangan. *Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.* POJK No. 11/POJK.03/2022.

Peraturan Menteri Kominfo No. 5 Tahun 2020.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Presiden RI. (2017). *Perpres 53/2017 tentang BSSN*.

Presiden RI. (2021). *Perpres 28/2021 tentang BSSN*.

Presiden RI. (2023). *Perpres 47/2023 tentang SKSN*.

Republik Indonesia. (1945). *UUD 1945*.

Republik Indonesia. (2008). *UU 11/2008 tentang ITE*.

Republik Indonesia. (2016). *UU 19/2016 tentang Perubahan ITE*.

Republik Indonesia. (2019). *PP 71/2019 tentang PSTE*.

Republik Indonesia. (2022). *UU 27/2022 tentang PDP*.

Republik Indonesia. (2024). *UU 1/2024 tentang Perubahan Kedua UU ITE*.

Republik Indonesia. PP Nomor 5 Tahun 2021 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko.

Republik Indonesia. PP Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE.

Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE.

Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP).

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 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

United Nations Commission on International Trade Law (UNCITRAL). *Technical Notes on Online Dispute Resolution*. New York: United Nations, 2017.

D.INTERNET

DPMPTSP Babel, “OSS-RBA Stimulus Pelaku Usaha untuk Berinvestasi di Indonesia,” (2023).dpmptsp.babelprov

Dunia Dosen. "7 Contoh Kasus Penyalahgunaan AI di Bidang Pendidikan." 19 Oktober 2024. https://duniadosen.com/penyalahgunaan-ai/.

http://repository.unissula.ac.id/38087/1/Ilmu%20Hukum_30302100452_fullpdf.pdf

http://www.detikmahasiswahukum.id/2024/01/mengenal-safe-harbor-prinsip-pembatasan.html

https://balmonsemarang.postel.go.id/blog/artikel/sah!-ini-dia-perubahan-kedua-atas-uu-ite

https://business-law.binus.ac.id/2017/04/30/mengenal-safe-harbor-dalam-hukum-siber-indonesia/
https://business-law.binus.ac.id/2017/04/30/mengenal-safe-harbor-dalam-hukum-siber-indonesia/
https://dpmptsp.babelprov.go.id/content/oss-rba-stimulus-pelaku-usaha-untuk-berinvestasi-di-indonesia
https://ejournal3.undip.ac.id/index.php/interaksi-online/article/download/41300/29916
https://ejurnal.politeknikpratama.ac.id/index.php/jhpis/article/view/4670
https://ejurnal.undipa.ac.id/index.php/sisiti/article/view/1674
https://ejurnal.undipa.ac.id/index.php/sisiti/article/view/1674/1233
https://id.kaspersky.com/resource-center/threats/children-photos-and-online-safety
https://jdih.komdigi.go.id/produk_hukum/view/id/884/t/undangundang+nomor+1+tahun+2024
https://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara
https://journal.appihi.or.id/index.php/Amandemen/article/download/472/710/2554
https://journal.pubmedia.id/index.php/lawjustice/article/download/3601/3444/7929
https://journal.stmiki.ac.id/index.php/jimik/article/download/598/478
https://jurnal.uns.ac.id/privatlaw/article/download/40358/26537
https://jurnal.uns.ac.id/privatlaw/article/view/54793
https://ojs.rewangrencang.com/index.php/JHLG/article/download/1437/762/6425
https://peraturan.bpk.go.id/Download/332870/UU%20Nomor%201%20Tahun%202024.pdf
https://prokom.kukarkab.go.id/index.php/berita/info-nasional/revisi-uu-ite-akan-kembangkan-dunia-ti-indonesia
https://putusan3.mahkamahagung.go.id/direktori/download_file/6502605f12269306aeb2d73071ed0c56/zip/zaee30313fa3f75698c7313330343137

https://putusan3.mahkamahagung.go.id/search.html/?q=%22Gugatan+pembagian+harta+warisan%22

https://putusan3.mahkamahagung.go.id/search.html/?q=%22Pemohon+sebagai++wali+dari+anak%22

https://putusan3.mahkamahagung.go.id/search.html/?q=%22Penetapan+ahli+waris+dan+perwalian+anak%22

https://putusan3.mahkamahagung.go.id/search.html/?q=%22Penetapan+ahli+waris+dan+perwalian%22

https://putusan3.mahkamahagung.go.id/search.html/?q=%22Penetapan+ahli+waris%22

https://putusan3.mahkamahagung.go.id/search.html/?q=%22Permohonan+penetapan+perwalian+anak%22

https://putusan3.mahkamahagung.go.id/search.html?q=%22Perwalian+anak+dibawah+umur%22

https://repository.ub.ac.id/186760/

https://sj.eastasouth-institute.com/index.php/shh/article/view/609

https://www.hukumonline.com/berita/a/evolusi-hak-asuh-anak-dalam-putusan-putusan-hakim-lt65846d0fb2985/?page=all

https://www.mediajustitia.com/edukasi-hukum/perlindungan-data-pribadi-dalam-era-digital/

https://www.voaindonesia.com/a/awas-bahaya-sharenting-/7927317.html

https://xynexis.com/uu-pdp-langkah-awal-melindungi-data-pribadi/

https://yurijaya.unmerpas.ac.id/index.php/fakultas_hukum/article/download/160/87

Kaspersky, “Sharenting: Apa yang harus dipertimbangkan orang tua...,” 8 Mei 2025.kaspersky

Koalisi Masyarakat Sipil untuk Advokasi UU ITE. "Revisi Kedua UU ITE: Masih Mempertahankan Pasal-Pasal Karet yang Lama, Menambah Pasal Baru." *Aliansi Jurnalis Independen*. Diakses 15 September 2025. https://aji.or.id/informasi/revisi-kedua-uu-ite-masih-mempertahankan-pasal-pasal-karet-yang-lama-menambah-pasal-baru.

Mahkamah Agung Republik Indonesia, Direktori Putusan, “Penetapan ahli waris dan perwalian anak”.

Media Justitia, “Perlindungan Data Pribadi dalam Era Digital,” 8 Januari 2025.mediajustitia

Rewangrencang, “Kekosongan hukum dan ketidakjelasan tanggung jawab platform e-commerce” (2024).ojs.rewangrencang

Rosenberg, Matthew, Nicholas Confessore, dan Carole Cadwalladr. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*, 17 Maret 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

BIODATA PENULIS

Sumardi Efendi, S.H.I., M.Ag. Putra pertama Bapak Suwirman dan Ibu Maizatun lahir di Indra Damai Aceh Selatan Provinsi Aceh pada 24 Mei 1990. Pendidikan S-1 Program Studi Syariah Jinayah Siyasah di Fakultas Syariah dan Ekonomi Islam IAIN Ar-Raniry Banda Aceh tahun 2009 s/d 2013. Pendidikan S-2 di Pascasarjana UIN Ar-Raniry Banda Aceh dengan Program Studi Ilmu Agama Islam dan Konsentrasi Fiqh Modern/Hukum Islam tahun 2014 s/d 2016, saat ini sebagai Dosen Tetap dan Sekretaris Program Studi Hukum Pidana Islam, Jurusan Syariah dan Ekonomi Islam STAIN Teungku Dirundeng Meulaboh, penulis aktif sebagai Editor, Reviwer dan Penulis Jurnal baik nasional maupun internasional, penulis telah menulis dan menerbitkan beberapa Buku kolaborasi bersama Adikara Cipta Aksa sejak tahun 2025 diantaranya sebagai berikut: "*Pengantar Hukum Pidana*", " *Tindak Pidana Korupsi Di Indonesia*", "*Kriminologi (Suatu Pengantar)*". Email: sumardi.efendi@staindirundeng.ac.id

Dr. Andi Zulfa Majida, M.H. merupakan dosen tetap pada Fakultas Hukum Universitas Pancasakti (UPS) Tegal. Penulis lahir di Kabupaten Semarang pada tanggal 28 Oktober 1986. Latar belakang akademiknya ditempuh secara berkesinambungan di bidang ilmu hukum, yang membentuk keahlian dan fokus kajiannya hingga saat ini. Pendidikan sarjana (S1) diselesaikan pada Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang pada tahun 2008. Selanjutnya, penulis melanjutkan pendidikan magister (S2) pada program Magister Ilmu Hukum di universitas yang sama dan berhasil diselesaikan pada tahun 2010. Komitmen terhadap pengembangan keilmuan hukum kemudian dilanjutkan melalui pendidikan doktoral (S3) pada Program Doktor Ilmu Hukum Universitas Islam Sultan Agung Semarang, yang diselesaikan pada tahun 2023. Dalam bidang akademik dan keilmuan, penulis memiliki fokus utama pada hukum pidana, khususnya hukum pidana anak. Kajian yang dikembangkan tidak hanya menitikberatkan pada aspek normatif dan dogmatik hukum pidana, tetapi juga pada pendekatan perlindungan anak, kepentingan terbaik bagi anak (*the best interests of the child*), serta kebijakan pemidanaan yang berorientasi pada keadilan substantif. Selain itu, penulis juga memiliki perhatian dan konsentrasi khusus pada pengembangan dan penerapan konsep *restorative justice* dalam sistem peradilan pidana, terutama dalam konteks penyelesaian perkara pidana anak dan tindak pidana tertentu yang menuntut pendekatan pemulihan bagi korban, pelaku, dan masyarakat. Sebagai dosen dan peneliti, penulis aktif dalam kegiatan pendidikan, penelitian, dan pengabdian kepada masyarakat di bidang hukum, serta terlibat dalam penulisan karya ilmiah, artikel jurnal, dan kajian hukum yang relevan dengan isu-isu aktual dalam hukum pidana, perlindungan anak, dan pembaruan hukum pidana di Indonesia. Biodata ini mencerminkan komitmen penulis dalam mengembangkan ilmu hukum yang berorientasi pada keadilan, kemanusiaan, dan perlindungan terhadap kelompok rentan, khususnya anak.

Dr. Joice Soraya, S.H., M.Hum. Penulis lahir di Malang pada tanggal 24 April 1973. Penulis adalah dosen tetap pada Program Studi D-3 TEKNIK INFORMASI (PSDKU LUMAJANG), Politeknik Negeri Malang. Menyelesaikan pendidikan Program Sarjana Hukum (S. H.) pada tahun 1997 di Fakultas Hukum Universitas Brawijaya Malang, dan melanjutkan Program Pascasarjana Magister Hukum (M. Hum.) pada tahun 2002 di Fakultas Hukum Universitas Brawijaya, Malang. Kemudian melanjutkan Program Doktor (Dr.) pada tahun 2016 di Fakultas Hukum Universitas Brawijaya Malang. Saat ini Penulis mengajar pada perguruan tinggi, antara lain Fakultas Hukum Universitas Kanjuruhan (2003-2022) Malang, Fakultas Hukum Wisnuwardhana (2022-2024) Malang, Politeknik Negeri Malang (sekarang). Selain itu Penulis juga aktif sebagai Wakil Ketua II Jawa Timur pada Masyarakat Hukum Pidana dan Kriminilogi Indonesia, Anggota pada Perkumpulan Pengajar dan Praktisi Hukum Ketenagakerjaan Indonesia, Anggota pada Asosiasi Pengajar Viktimologi Indonesia, dan Asosiasi Pengajar Hukum Adat. Corresponding Email: joicewijayas99@gmail.com, No. HP: 081332667336

Prof. Dr. Hamidah Abdurrachman, S.H., M.Hum. kelahiran Tanjung Pinang, menyelesaikan Sekolah Dasar, Sekolah Menengah Pertama dan Sekolah Menengah Atas di Kota Tanjung Pinang (*teriring doa untuk para guru, "Ya Allah, ampunilah guru-guru kami dan orang yang telah mengajar kami. Sayangilah mereka, muliakanlah mereka dengan keridhaan-Mu yang Agung, di tempat yang disenangi di sisi-Mu, wahai yang Maha Penyayang di antara penyayang*). Dosen Fakultas Hukum ini, melanjutkan kuliah Program Sarjana di Fakultas Hukum Universitas Kristen Satya Wacana. Tak berhenti di situ, penulis juga memperoleh kesempatan untuk mengikuti Program Magister Hukum Universitas

Diponegoro dan Program Doktor Universitas Pajajaran Bandung, lulus tahun 2010 dengan predikat *cumlaude* di bawah bimbingan Promotor Prof. Romli Atmasasmita, Prof. Komariah E. Sapardjaja dan Prof. Nyoman Serikat Putra Jaya. Tahun 2023 mendapat gelar Profesor dalam bidang Ilmu Hukum pada Fakultas Hukum Universitas Pancasakti Tegal. Penulis mengajar pada Program Magister Ilmu Hukum Universitas Pancasakti, Tegal. Penulis mengajar juga di Program Magister Ilmu Hukum Universitas Bung Hatta Padang (2023-sekarang), Sekolah Pascasarjana UGJ Cirebon (2024), STIH Manokwari Papua Barat. Mei 2025 menjadi Dosen di Prodi S3 Universitas 17 Agustus 1945 Jakarta (UTA45) (2024). Pengalaman profesi antara lain sebagai Pengawas Notaris Wilayah Tegal, Kabupaten Tegal dan Kabupaten Brebes (2006-2023). Tahun 2012-2016 menjadi Anggota Komisi Kepolisian Nasional. Ketua Tim Penyusunan Naskah Akademik di DPRD Kabupaten Tegal (2020-2023) dan Ketua Tim Penyusunan Nasakah Akademik di DPRD Kota Tegal (2024-2025) serta Saksi ahli PIdana di Polres dan Pengadilan Negeri dan PN Tipikor di Semarang. Penulis juga menjadi narasumber di Elsinta talk n news serta RRI dan TVRI Jawa Tengah.

Dr. Suci Lestari Halam, S.H., M.H. Lahir di Jakarta, 27 Januari 1978. Penulis menyelesaikan pendidikan Sarjana Hukum di Fakultas Hukum Universitas Trisakti, Jakarta, lulus tahun 2000. Kemudian, penulis menyelesaikan pendidikan Magister Hukum di Program Pascasarjana Universitas Indonesia, Hukum Ekonomi lulus Tahun 2008. Dan penulis menyelesaikan Pendidikan Program Doktor Ilmu Hukum (PDIH) FH Universitas Trisakti, Jakarta, lulus tahun 2022. Penulis juga menyelesaikan TAPLAI (Pemantapan Nilai-Nilai Kebangsaan) Lemhannas RI Angkatan III tahun 2020. Penulis saat ini adalah Dosen Tetap di Program Sarjana Ilmu Hukum Fakultas Hukum Universitas Trisakti, Jakarta. Penulis juga merupakan anggota PERADI Jakarta Barat dan mediator non hakim tersertifikasi PERPAHI. Penulis berkonsentrasi di Hukum Bisnis, khususnya Hukum Lembaga Keuangan. Penulis juga aktif dalam berbagai organisasi.

Amirah Dwi Subarkah, S.H., M.H. lahir di Kotabumi, Lampung Utara, pada tanggal 3 November 1996. Penulis merupakan dosen pada Fakultas Hukum Universitas 17 Agustus 1945 Semarang. Pendidikan Sarjana (S1) Ilmu Hukum ditempuh di Universitas Bandar Lampung dengan peminatan Hukum Keperdataan. Penulis menyelesaikan pendidikan Magister Hukum (S2) pada Fakultas Hukum Universitas Sebelas Maret (UNS) dengan konsentrasi Hukum Bisnis pada tahun 2023. Dalam kegiatan akademik, penulis mengampu mata kuliah Hak Kekayaan Intelektual dan Hukum Adat, serta aktif menulis karya ilmiah dan publikasi jurnal di bidang hukum.

Dessy Puspita Tjahjadi. Penulis lahir di Bandung pada tanggal 2 Februari. Penulis merupakan akademisi di Fakultas Hukum, Universitas Esa Unggul Jakarta. Penulis juga merupakan praktisi kewirausahaan diantaranya di bidang tehnologi informatika. Sebagai praktisi di dunia usaha dan sebagai akademisi, ia harus memahami berbagai bentuk praktik legalitas, perizinan, dan prosedural terkait management perusahaan dan platform digital. Dalam penulisan buku ini, Penulis menggabungkan perspektif akademik dan pengalaman praktisnya untuk memberikan wawasan yang sistematis dan aplikatif bagi para pembaca, terutama mahasiswa hukum dan praktisi yang ingin mendalami aspek legalitas dan regulasi hukum cyber di Indonesia.

Dr. Ani Purwati, S.H., M.H. Lahir di Surabaya 19 Desember 1982. Memperoleh Sarjana Hukum tahun 2005 dari Fakultas Hukum Universitas Hangtuah Surabaya, Tahun 2008 Magister Hukum Fakultas Hukum Universitas Airlangga Surabaya, Tahun 2015 Doktor di bidang Progam Doktor Ilmu Hukum Fakultas Hukum Universitas Airlangga Surabaya, Tahun 2025 Doktor Ilmu Hukum Kosentrasi Hukum Kesehatan di Universitas 17 Agustus 1945 Semarang, Seorang Advokat, Konsultan Hukum, Dosen Pasca Sarjana Universitas Sahid, Keterangan Ahli Pidana. Beberapa sertifikasi ahli yang diperoleh: *Contract Management Specialist* (CCMs)/BNSP)), Sertifikasi Assesor Pengadaan Barang dan Jasa (BNSP), *certified procurement specialist* (CPSp), C*ertified Legal Auditor* (CLA (BNSP), *Certified Tax Lawyer* (CTL), *Certified Liquidator* Indonesia (CLI), *Certified Mediator* (CMe), *Certified Custom Lawyer* (CCL), Manrisk (QRMO), Kurator Himpunan Kurator Pengurus Indonesia, Pengalaman organisasi. Tahun 2016 Sekretaris LAPPHI (Lembaga Advokasi Penyelesaian Perselisihan Hubungan Industrial), Sekretaris Div. Litbang DPC Peradi Surabaya, Wakil Direktur LPHMI (Lembaga Pendidikan Hukum & Mediator Indonesia) 2019 sampai sekarang, Direktur Kantor Hukum Ani Purwati Wijaya & Rekan. Tergabung Asosiasi Ikatan Ahli Pengadaan Indonesia (IAPI), Asosiasi Auditor Hukum Indonesia (ASAHI), Perkumpulan Pengacara Pajak dan Kuasa Hukum Pengadilan Pajak Indonesia (PKPPI), Masyarakat Mediator Indonesia (MMI) dan Pusat Mediasi Indonesia (PMI), Perkumpulan Profesi Liquidator Indonesia (PPLI), Keanggotaan Himpunan Kurator Pengurus Indonesia (HKPI). Pengembangan riset trafiking 2005 TKW Plan Internasional Ponorogo, Riset Anak Berkonflik LBH Anak SCCC (*Surabaya Children Crisis Centre*) bersama Plan Internasional. Perwakilan Indonesia NGO (*Asia Pasific Forum on Women, Law, Development*) tahun 2014. Tahun 2019 sampai 2022 (Kepala Departemen BUMN PT PAL INDONESIA), 2025 Ketua Bidang Hukum, Ham, Antar Lembaga (Forum Pemberdayaan Perempuan Indonesia), Tahun 2022 sampai Sekarang menjadi Direktur Legal PT Antakesuma Inti Raharja dan PT Putindo Trada Wisesa.

Muhammad Arif Rahman, S.H Penulis adalah seorang sarjana hukum dari Universitas Lambung Mangkurat asal Kabupaten Balangan Provinsi Kalimantan Selatan yang tertarik pada penelaahan isu-isu hukum di bidang teknologi dan informasi digital. Penulis pernah bekerja sebagai Legal Officer di Yayasan Hasnur Centre dan PT. Cipta Daya Inovasi (Hasnur Group). Dengan latar belakang sebagai Calon Ahli Pertama Jaksa, penulis memiliki minat mendalam pada persinggungan antara inovasi teknologi, penegakan hukum pidana, dan perlindungan hak-hak fundamental warga negara di era digital. Penulis senang mengkaji tentang tantangan regulasi yang ditimbulkan oleh perkembangan pesat *Artificial Intelligence* dan *Big Data*, serta terkait rumusan solusi-solusi kebijakan yang berbasis bukti dan berorientasi pada keadilan.

Dr. Subaidah Ratna Juita, S.H., M.H. ., menyelesaikan pendidikan S1 pada Program Studi S1 Ilmu Hukum FH-UII Yogyakarta pada tahun 2002, selanjutnya menyelesaikan studi S2 pada Program Magister Ilmu Hukum, FH-UII Yogyakarta pada tahun 2005. Selanjutnya pada tahun 2022, penulis menyelesaikan Program Doktor Ilmu Hukum pada Universitas Islam Sultan Agung (UNISSULA) Semarang. Penulis memiliki kepakaran di bidang Ilmu Hukum Pidana. Dan untuk mewujudkan karir sebagai dosen profesional, penulis pun aktif sebagai peneliti. Beberapa penelitian yang telah dilakukan didanai oleh internal perguruan tinggi dan juga Kemenristek DIKTI. Selain meneliti, penulis juga aktif menulis buku diantaranya, Asas-asas Hukum Pidana dan Hukum Pidana Anak, serta berbagai artikel ilmiah yang merupakan hasil penelitian/hasil pemikiran yang dipublikasikan pada Jurnal Internasional, Jurnal Nasional, Prosiding, dan *Book Chapter* yang berkaitan dengan bidang kepakaran penulis, dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara ini. Selain itu, Penulis juga dalam beberapa perkara pidana diminta untuk memberikan keterang sebagai

ahli, dintaranya perkara terkait ketentuan dalam Pasal 78 KUHP tentang Daluwarsa, Pasal 81 KUHP Jo. PERMA No. 1 Tahun 1956 Jo. SEMA No. 4 Tahun 1980 tentang *Prejudicieel Geschil*, Perkara Tindak Pidana Penggelapan, Perkara Tindak Pidana Korupsi berupa Penyalahgunaan Wewenang dalam Jabatan, perkara Tindak Pidana Pencabulan terhadap Anak, dan memberikan keterangan sebagai ahi berkaitan dengan alat bukti digital.

Bagus Hermanto, S.H., M.H. (lahir di Denpasar, 14 Juni 1997) adalah dosen tetap PNS dan peneliti independen di Fakultas Hukum Universitas Udayana dengan fokus pada legislasi, hukum tata negara, hukum kebijakan publik, HAM, dan perancangan peraturan perundang-undangan. Ia juga mengajar di Universitas Bali Dwipa pada bidang metodologi penelitian dan berbagai cabang ilmu hukum.

Sejak Agustus 2023, ia menjabat sebagai Wakil Ketua Pembina DPD Bali PETKI, menjadi kontributor aktif di Penerbit Uwais Inspirasi Indonesia, serta terlibat dalam berbagai kegiatan pengabdian masyarakat. Ia juga aktif sebagai guest editor, editor, dan peer reviewer di sejumlah jurnal nasional dan internasional bereputasi, termasuk yang terindeks Scopus dan Web of Science.

Bagus menyelesaikan S1 Hukum di Universitas Udayana (2018), mengikuti short course di Yamaguchi University, Jepang (2018), dan meraih gelar Magister Hukum dari Universitas Udayana (2021). Hingga Februari 2025, ia telah menghasilkan 121 karya ilmiah, termasuk artikel internasional bereputasi dan buku seperti *Kapita Selekta dan Filsafat Ilmu Hukum Kenotariatan Kontemporer Indonesia* (2024) dan *Teori Hukum Pancasila* (2024).

HUKUM CYBER

TANTANGAN DAN SOLUSI DI ERA DIGITAL

Perkembangan teknologi digital telah mengubah cara manusia berinteraksi, bertransaksi, dan membangun kehidupan sosial. Namun di balik kemajuan tersebut, muncul tantangan hukum yang semakin kompleks—mulai dari kejahatan siber, perlindungan data pribadi, keamanan transaksi digital, hingga regulasi kecerdasan buatan dan big data. *Buku Hukum Cyber: Tantangan dan Solusi di Era Digital* mengulas secara komprehensif prinsip, asas, dan dinamika regulasi hukum siber di Indonesia serta perspektif internasional. Buku ini membahas UU ITE, UU Perlindungan Data Pribadi, tanggung jawab platform digital, penyelesaian sengketa daring, hingga masa depan hukum di tengah transformasi teknologi. Disusun secara sistematis dan analitis, buku ini menjadi referensi penting bagi mahasiswa, akademisi, praktisi hukum, pembuat kebijakan, dan pelaku industri digital dalam memahami serta membangun sistem hukum yang adaptif, adil, dan relevan di era digital.

AKASA
ADIKARA CIPTA AKSA

Ruko Mahkota Mas Blok C, Jl. MH
Thamrin, Cikokol, Kecamatan Tanerang
Kota, Kota Tangerang Banten, 15117
Telepon: (+62) 821 669 576 72 (Lim)
E-mail: adikaraciptaaksa@gmail.com
www.adikaraciptaaksa.co.id

PT. ADIKARA CIPTA AKSA
DIVISI PERCETAKAN

ISBN 978-634-05-2349-2 (PDF)
9 786340 523492

HUKUM CYBER

TANTANGAN DAN SOLUSI DI ERA DIGITAL

Perkembangan teknologi digital telah mengubah cara manusia berinteraksi, bertransaksi, dan membangun kehidupan sosial. Namun di balik kemajuan tersebut, muncul tantangan hukum yang semakin kompleks mulai dari kejahatan siber, perlindungan data pribadi, keamanan transaksi digital, hingga regulasi kecerdasan buatan dan big data. Buku Hukum Cyber: Tantangan dan Solusi di Era Digital mengulas secara komprehensif prinsip, asas, dan dinamika regulasi hukum siber di Indonesia serta perspektif internasional. Buku ini membahas UU ITE, UU Perlindungan Data Pribadi, tanggung jawab platform digital, penyelesaian sengketa daring, hingga masa depan hukum di tengah transformasi teknologi. Disusun secara sistematis dan analitis, buku ini menjadi referensi penting bagi mahasiswa, akademisi, praktisi hukum, pembuat kebijakan, dan pelaku industri digital dalam memahami serta membangun sistem hukum yang adaptif, adil, dan relevan di era digital.

AKASA
PT. ADIKARA CIPTA AKSA

Ruko Mahkota Mas Blok C, Jl MH Thamrin, Cikokol, Kec Tangerang, Kota, Kota Tangerang, Banten 15117
Telp. +6282166957672
Email: adikaraciptaaksa@gmail.com
Website: adikaraciptaaksa.co.id

ISBN 978-634-05-2349-2 (PDF)
9 786340 523492