HUKUM SIBER:
FONDASI, TANTANGAN, DAN MASA DEPAN
REGULASI DI ERA DIGITAL

Buku ini membahas hukum siber secara bertahap, mulai dari fondasi konseptual dan perkembangan hukum siber, karakteristik ruang siber, sumber dan prinsip hukum yang relevan, hingga berbagai bentuk kejahatan dan pelanggaran hukum di ruang digital. Pembahasan juga diarahkan pada persoalan pembuktian elektronik, yurisdiksi dan penegakan hukum siber, perlindungan data pribadi, keamanan informasi, tanggung jawab penyelenggara sistem elektronik, serta hubungan antara perkembangan teknologi dengan kebutuhan pembaruan regulasi.

Buku ini diharapkan dapat menjadi referensi bagi mahasiswa, akademisi, praktisi hukum, aparat penegak hukum, pembentuk kebijakan, pelaku usaha digital, serta masyarakat yang ingin memahami perkembangan hukum dalam ekosistem digital. Penulis menyadari bahwa perkembangan teknologi digital berlangsung demikian dinamis sehingga pembahasan mengenai hukum siber tidak akan pernah berhenti pada satu titik. Oleh karena itu, buku ini tidak dimaksudkan sebagai jawaban final, melainkan sebagai bagian dari upaya untuk membangun pemahaman, membuka ruang diskusi, dan mendorong kajian lebih lanjut mengenai arah perkembangan hukum di era digital.

ISBN 978-634-05-7654-2 (PDF)
9 786340 576542

PT Andalas Global Research Center

Penerbit:
PT Andalas Global Research Center
Jl. Mulia 2, No. 52A, Sariharjo, Ngaglik, Sleman,
DI Yogyakarta 55581
Telp : +62 811 7488 066
Email : globalpublisherofficial@gmail.com
Website : www.andalaspress.com

HUKUM SIBER: FONDASI, TANTANGAN, DAN MASA DEPAN
REGULASI DI ERA DIGITAL

Andalas Global Research Center

HUKUM SIBER:
FONDASI, TANTANGAN, DAN MASA DEPAN
REGULASI DI ERA DIGITAL

Penulis:
Dr. Cut Fadhlan Akhyar, S.H., M.M., M.H.
Andi Mohammad Galib, S.H., M.H.
Prof. Dr. Henny Saida Flora., S.H. M.Hum. M.Kn. M.H.Kes.
Dr. Hanuring Ayu, S.H., M.H.
Yuda Mustajab, S.H.
Rini Indhyra Khumaerah, S.H., M.H.
Dr. Rabith Madah Khulaili Harsya, S.H.I., S.H., M.H.I., M.H.
Dr. Basarudin, S.H.I., M.Pd., M.H.
Olivia Putri Madani, S.I.Kom.
Rahmat, S.H,M.H.



PT Andalas Global Research Center

HUKUM SIBER: FONDASI, TANTANGAN, DAN MASA DEPAN REGULASI DI ERA DIGITAL

Dr. Cut Fadhlan Akhyar, S.H., M.M., M.H.
Andi Mohammad Galib, S.H., M.H.
Prof. Dr. Henny Saida Flora., S.H. M.Hum. M.Kn. M.H.Kes.
Dr. Hanuring Ayu, S.H., M.H.
Yuda Mustajab, S.H.
Rini Indhyra Khumaerah, S.H., M.H.
Dr. Rabith Madah Khulaili Harsya, S.H.I., S.H., M.H.I., M.H.
Dr. Basarudin, S.H.I., M.Pd., M.H.
Olivia Putri Madani, S.I.Kom.
Rahmat, S.H,M.H.
Editor : Fitri Arianti Saputri, S.H

PT. Andalas Global Research Center

Penerbit PT. Andalas Global Research Center

Judul : **Hukum Siber: Fondasi, Tantangan, Dan Masa Depan Regulasi di Era Digital**
Penulis : Cut F. A., Andi M. G., Henny S. F., Hanuring A., Yuda M., Rini I. K., Rabith M. K. H., Basarudin, Olivia P. M. Rahmat.
Editor : Fitri Arianti Saputri, S.H
Design Cover : Rahmat Purnomo, S.Kom
Penerbit : **PT Andalas Global Research Center**
Jl. Mulia 2, No. 52A, Sariharjo, Ngaglik, Sleman, DI Yogyakarta 55581
Telp : +62 811 7488 066
Email : globalpublisherofficial@gmail.com
Website : www.andalaspress.com
ISBN : 978-634-05-7654-2

Anggota Ikatan Penerbit Indonesia (IKAPI)

Hak Cipta Dilindungi Undang-Undang

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini dalam bentuk apapun tanpa izin tertulis dari penerbit.

Diterbitkan oleh PT. Andalas Global Research Center
Yogyakarta, 2026

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga buku yang berjudul **"Hukum Siber: Fondasi, Tantangan, Dan Masa Depan Regulasi di Era Digital"** ini dapat diselesaikan dengan baik. Buku ini disusun sebagai bagian dari upaya untuk memberikan pemahaman yang komprehensif mengenai perkembangan hukum siber serta berbagai persoalan hukum yang muncul seiring dengan semakin luasnya pemanfaatan teknologi informasi dan komunikasi dalam kehidupan masyarakat.

Buku ini membahas hukum siber secara bertahap, mulai dari fondasi konseptual dan perkembangan hukum siber, karakteristik ruang siber, sumber dan prinsip hukum yang relevan, hingga berbagai bentuk kejahatan dan pelanggaran hukum di ruang digital. Pembahasan juga diarahkan pada persoalan pembuktian elektronik, yurisdiksi dan penegakan hukum siber, perlindungan data pribadi, keamanan informasi, tanggung jawab penyelenggara sistem elektronik, serta hubungan antara perkembangan teknologi dengan kebutuhan pembaruan regulasi.

Buku ini diharapkan dapat menjadi referensi bagi mahasiswa, akademisi, praktisi hukum, aparat penegak hukum, pembentuk kebijakan, pelaku usaha digital, serta masyarakat yang ingin memahami perkembangan hukum dalam ekosistem digital. Bagi mahasiswa dan akademisi, buku ini diharapkan dapat menjadi bahan

untuk memahami konsep dan problematika hukum siber secara lebih sistematis. Bagi praktisi dan pembentuk kebijakan, pembahasan dalam buku ini diharapkan dapat memberikan perspektif mengenai tantangan penerapan hukum dalam menghadapi perkembangan teknologi yang berlangsung secara cepat.

Penulis menyadari bahwa perkembangan teknologi digital berlangsung demikian dinamis sehingga pembahasan mengenai hukum siber tidak akan pernah berhenti pada satu titik. Regulasi yang relevan pada suatu masa dapat menghadapi tantangan baru ketika teknologi mengalami perkembangan. Oleh karena itu, buku ini tidak dimaksudkan sebagai jawaban final atas seluruh persoalan hukum siber, melainkan sebagai bagian dari upaya untuk membangun pemahaman, membuka ruang diskusi, serta mendorong kajian lebih lanjut mengenai arah perkembangan hukum di era digital.

Akhir kata, penulis menyampaikan terima kasih kepada seluruh pihak yang telah memberikan dukungan, pemikiran, dan kontribusi dalam proses penyusunan buku ini.

Penulis

DAFTAR ISI

KATA PENGANTAR..... **iii**
DAFTAR ISI..... **v**
BAB I REVOLUSI DIGITAL DAN LAHIRNYA HUKUM SIBER (Dr. Cut Fadhlan Akhyar, S.H., M.M., M.H.)..... **1**
1. Revolusi Digital dan Transformasi Kehidupan Masyarakat..... 4
2. Perkembangan Teknologi Informasi dan Munculnya Ruang Siber..... 9
3. Konsep, Karakteristik, dan Ruang Lingkup Hukum Siber..... 13
4. Faktor Pendorong Lahirnya dan Perkembangan Hukum Siber..... 16
5. Urgensi Hukum Siber dalam Mewujudkan Tata Kelola Digital..... 20

BAB II LANDASAN FILOSOFIS DAN TEORI HUKUM DI RUANG SIBER (Andi Mohammad Galib, S.H., M.H.)... **27**
1. Landasan Filosofis Hukum Siber: Keadilan, Kepastian Hukum, dan Kemanfaatan 30
2. Teori Hukum dan Adaptasi Norma dalam Perkembangan Teknologi Digital 34
3. Hak Asasi Manusia, Privasi, dan Perlindungan Hak Digital 38
4. Teori Kedaulatan, Yurisdiksi, dan Tanggung Jawab Hukum di Ruang Siber..... 43

BAB III YURISDIKSI TANPA BATAS: PROBLEMATIKA HUKUM LINTAS NEGARA DI DUNIA DIGITAL (Prof. Dr. Henny Saida Flora., S.H.

M.Hum. M.Kn. M.H.Kes) **48**
1. Transformasi Konsep Yurisdiksi dalam Ruang Siber 48
2. Konflik Yurisdiksi dan Hukum yang Berlaku dalam Transaksi serta Aktivitas Digital Lintas Negara 55
3. Kejahatan Siber Lintas Negara dan Problematika Penegakan Hukum..... 60
4. Kedaulatan Digital, Perlindungan Data, dan Tanggung Jawab Negara di Ruang Siber..... 66
5. Harmonisasi Hukum dan Masa Depan Tata Kelola Yurisdiksi Siber Internasional 71

BAB IV KEJAHATAN SIBER: KLASIFIKASI, MODUS, DAN RESPONS HUKUM (Dr. Hanuring Ayu, S.H., M.H.) **77**
1. Klasifikasi dan Karakteristik Kejahatan Siber Dalam Ekosistem Digital..... 80
2. Modus Operandi dan Evolusi Kejahatan Siber di Era Teknologi Cerdas..... 86
3. Pertanggungjawaban Pidana dan Problematika Pembuktian Dalam Kejahatan Siber..... 93
4. Respons Hukum dan Strategi Penanggulangan Kejahatan Siber..... 99

BAB V PERLINDUNGAN DATA PRIBADI SEBAGAI HAK FUNDAMENTAL DI ERA DIGITAL (Yuda Mustajab, S.H.) **110**
1. Data Pribadi Sebagai Hak Fundamental dan Bagian Dari Perlindungan Privasi 112
2. Prinsip-Prinsip Perlindungan Data Pribadi Dalam Pemrosesan Data Digital 119
3. Hak Subjek Data dan Mekanisme Pengendalian Atas Data Pribadi 125
4. Tanggung Jawab Pengendali, Prosesor Data, dan Penyelenggara Sistem Digital 131

5. Pribadi di Era Kecerdasan Artifisial 138
BAB VI TRANSAKSI ELEKTRONIK, KONTRAK DIGITAL, DAN KEABSAHAN HUKUMNYA (Rini Indhyra Khumaerah, S.H., M.H). **150**
1. Transformasi Transaksi Konvensional Dalam Ekosistem Digital 152
2. Kontrak Digital dan Mekanisme Pembentukan Kesepakatan..... 159
3. Keabsahan Kontrak Elektronik Dalam Perspektif Hukum Perdata dan Hukum Siber..... 166
4. Alat Bukti Elektronik dan Kekuatan Pembuktian Dalam Sengketa Transaksi Digital..... 172
5. Wanprestasi, Perlindungan Para Pihak, dan Penyelesaian Sengketa Transaksi Elektronik 178
BAB VII KEBEBASAN BEREKSPRESI, KONTEN ILEGAL, DAN SENSOR DI RUANG SIBER (Dr. Rabith Madah Khulaili Harsya, S.H.I., S.H., M.H.I., M.H.) **189**
1. Kebebasan Berekspresi Sebagai Hak Fundamental di Ruang Siber..... 191
2. Batasan Kebebasan Berekspresi dan Pertanggungjawaban Hukum di Ruang Siber .196
3. Konten Ilegal dan Problematika Penentuan Batas Antara Konten Terlarang dan Konten yang Dilindungi..... 201
4. Sensor, Moderasi Konten, dan Tanggung Jawab Platform Digital 207
5. Menyeimbangkan Kebebasan Berekspresi, Perlindungan Publik, dan Tata Kelola Ruang Siber 213
BAB VIII KEAMANAN SIBER NASIONAL: ANTARA KEDAULATAN DIGITAL DAN ANCAMAN GLOBAL (Dr. Basarudin, S.H.I., M.Pd., M.H.) **221**
1. Konsep dan Dimensi Keamanan Siber Nasional dalam Negara Digital 221

2. Ancaman Siber Global dan Kerentanan Infrastruktur Digital Strategis..... 229
3. Kedaulatan Digital, Ketergantungan Teknologi, dan Penguasaan Data Strategis..... 236
4. Strategi Ketahanan Siber dan Tata Kelola Keamanan Siber Nasional..... 244

BAB IX KECEERDASAN BUATAN, *BLOCKCHAIN,* DAN TANTANGAN REGULASI TEKNOLOGI BARU (Olivia Putri Madani, S.I.Kom.)..... **255**

1. Kecerdasan Buatan dan Transformasi Hubungan Hukum di Era Digital..... 255
2. Pertanggungjawaban Hukum dan Risiko Algoritmik dalam Penggunaan Kecerdasan Buatan..... 263
3. *Blockchain*, *Smart Contract*, dan Rekonstruksi Keabsahan Hukum Transaksi Digital..... 270
4. Regulasi Teknologi Baru: Antara Inovasi, Kepastian Hukum, dan Perlindungan Masyarakat 277
5. Masa Depan Hukum di Tengah Konvergensi AI, Blockchain, dan Teknologi Otonom..... 284

BAB X MENUJU ARSITEKTUR HUKUM SIBER YANG ADAFTIF: REKOMENDASI DAN PROSPEK (Rahmat, S.H,M.H.)..... **294**

1. Rekonstruksi dan Harmonisasi Kerangka Hukum Siber Nasional..... 297
2. Penguatan Kelembagaan, Penegakan Hukum, dan Kapasitas Digital Negara..... 303
3. Model Regulasi Adaptif dan Tata Kelola Teknologi yang Berorientasi pada Hak..... 309
4. Prospek Arsitektur Hukum Siber Indonesia dalam Ekosistem Digital Global..... 315

DAFTAR PUSTAKA..... **327**

BAB I
REVOLUSI DIGITAL DAN LAHIRNYA HUKUM SIBER

Perkembangan teknologi digital telah membawa perubahan mendasar terhadap kehidupan manusia. Perubahan tersebut tidak hanya terlihat dari semakin luasnya penggunaan komputer, internet, dan perangkat pintar, tetapi juga dari bergesernya cara manusia berkomunikasi, bekerja, melakukan transaksi, memperoleh informasi, serta berhubungan dengan pemerintah dan berbagai institusi. Teknologi digital secara perlahan telah menjadi bagian dari kehidupan sehari-hari sehingga batas antara ruang fisik dan ruang digital semakin sulit dipisahkan. Transformasi tersebut pada akhirnya melahirkan lingkungan sosial baru yang memiliki karakter, risiko, dan kebutuhan hukum yang berbeda dari kehidupan masyarakat sebelumnya.

Revolusi digital juga menghasilkan perubahan terhadap struktur kegiatan ekonomi dan sosial. Pelaku usaha dapat menjangkau konsumen tanpa harus memiliki toko fisik, masyarakat dapat memperoleh layanan melalui aplikasi, dan informasi dapat disebarluaskan dalam hitungan detik. Perubahan tersebut menunjukkan bahwa teknologi bukan lagi sekadar instrumen pendukung kegiatan manusia, melainkan telah menjadi bagian dari infrastruktur

kehidupan modern. Transformasi digital mengubah bisnis, masyarakat, perilaku konsumen, serta berbagai sektor kehidupan secara luas dan saling berkaitan (Paul dkk., 2024; Van Veldhoven & Vanthienen, 2021).

Perubahan tersebut menciptakan bentuk hubungan baru yang sebelumnya tidak ditemukan dalam skala yang sama. Hubungan antara penjual dan pembeli dapat berlangsung sepenuhnya secara elektronik, komunikasi antara individu dapat dilakukan melalui platform digital, sedangkan pelayanan publik dapat diselenggarakan melalui sistem elektronik. Setiap aktivitas tersebut menghasilkan konsekuensi hukum. Kesepakatan elektronik, data pribadi, identitas digital, bukti transaksi, keamanan sistem, serta tanggung jawab penyelenggara layanan merupakan contoh persoalan yang muncul sebagai konsekuensi dari digitalisasi kehidupan.

Kondisi tersebut menunjukkan bahwa perkembangan teknologi selalu memiliki dimensi hukum. Ketika teknologi digunakan dalam kehidupan masyarakat, hukum harus menentukan batas antara penggunaan yang sah dan penggunaan yang melanggar hak atau kepentingan pihak lain. Hukum juga perlu memberikan kepastian mengenai hak dan kewajiban para pihak dalam hubungan digital. Digitalisasi hukum karena itu tidak sekadar berarti memindahkan prosedur konvensional ke media elektronik, tetapi juga berkaitan dengan pembentukan konsep dan norma hukum yang mampu berfungsi dalam lingkungan digital (Ennan, 2024).

Kebutuhan tersebut semakin besar karena ruang digital memiliki karakter lintas batas. Pelaku, korban, sistem, dan data yang berkaitan dengan suatu peristiwa dapat berada di negara yang berbeda. Seseorang dapat melakukan serangan terhadap sistem yang berada di Indonesia dari negara lain dengan menggunakan infrastruktur digital yang terdapat di negara ketiga. Kondisi tersebut menciptakan persoalan yurisdiksi dan penegakan hukum yang tidak mudah diselesaikan melalui pendekatan hukum konvensional (Lukmana, 2025; Noor, 2025).

Hukum siber kemudian berkembang sebagai salah satu respons terhadap perubahan tersebut. Bidang hukum ini tidak hanya berfungsi untuk menangani kejahatan yang dilakukan melalui komputer atau internet, tetapi juga mengatur hubungan hukum yang lahir dari penggunaan teknologi digital. Ruang lingkupnya meliputi transaksi elektronik, perlindungan data pribadi, keamanan siber, kejahatan siber, hak digital, kekayaan intelektual, dan berbagai bentuk hubungan hukum lainnya (Alifah, 2024; Bhange, 2025).

Dengan demikian, pembahasan mengenai hukum siber perlu diawali dengan pemahaman terhadap revolusi digital itu sendiri. Hukum siber tidak muncul dalam ruang kosong. Kelahirannya merupakan konsekuensi dari perubahan teknologi yang kemudian mengubah struktur hubungan sosial, ekonomi, dan kelembagaan. Pemahaman tersebut menjadi dasar untuk melihat mengapa hukum harus beradaptasi dan bagaimana hukum siber dapat ditempatkan sebagai fondasi bagi tata kelola ruang digital.

1. Revolusi Digital dan Transformasi Kehidupan Masyarakat

Revolusi digital merupakan salah satu perubahan paling penting dalam perkembangan masyarakat modern. Perubahan ini ditandai oleh meningkatnya penggunaan teknologi digital dalam hampir seluruh aspek kehidupan, mulai dari komunikasi, pendidikan, perdagangan, keuangan, kesehatan, pemerintahan, hingga hiburan. Perkembangan teknologi tersebut menghasilkan perubahan tidak hanya pada alat yang digunakan manusia, tetapi juga pada cara manusia melakukan aktivitas dan membangun hubungan. Transformasi digital dalam satu dekade terakhir bahkan telah menjangkau hampir seluruh sektor kehidupan dan mengubah cara organisasi serta masyarakat menjalankan aktivitasnya (Paul dkk., 2024; Van Veldhoven & Vanthienen, 2021).

Perubahan paling mudah terlihat dalam pola komunikasi. Komunikasi yang sebelumnya bergantung pada pertemuan langsung atau media komunikasi konvensional kini banyak berlangsung melalui aplikasi pesan instan, media sosial, surat elektronik, dan konferensi video. Kecepatan komunikasi meningkat secara signifikan karena informasi dapat dikirim dan diterima tanpa dibatasi oleh jarak. Seseorang yang berada di Indonesia dapat berkomunikasi dengan orang lain di negara berbeda dalam waktu yang hampir bersamaan. Kondisi tersebut memperluas jaringan sosial sekaligus mengubah karakter hubungan antarmanusia.

Teknologi telah memengaruhi struktur sosial, pola konektivitas, komunikasi, dan pembentukan jejaring sosial dalam masyarakat modern (Hanandini, 2024).

Perubahan pola komunikasi tersebut memberikan manfaat yang besar. Teknologi memungkinkan individu mempertahankan hubungan meskipun terpisah oleh jarak geografis. Informasi dapat diperoleh dengan lebih cepat, sementara berbagai komunitas dapat terbentuk berdasarkan kesamaan kepentingan tanpa harus berada dalam wilayah yang sama. Kondisi ini memperluas ruang partisipasi masyarakat dan memungkinkan pertukaran gagasan dalam skala yang jauh lebih besar. Namun, perubahan tersebut juga menghadirkan persoalan baru, terutama ketika interaksi sosial semakin bergantung pada teknologi. Ketergantungan tersebut dapat menyebabkan interaksi menjadi lebih impersonal dan meningkatkan ketergantungan masyarakat terhadap data serta sistem digital (Hanandini, 2024).

Transformasi digital juga mengubah aktivitas ekonomi. Perdagangan elektronik memungkinkan transaksi dilakukan tanpa pertemuan langsung antara penjual dan pembeli. Konsumen dapat mencari produk, membandingkan harga, membaca ulasan, melakukan pembayaran, dan menerima barang melalui suatu rangkaian proses yang berlangsung secara digital. Pelaku usaha memperoleh kesempatan untuk menjangkau pasar yang lebih luas dengan biaya tertentu yang lebih efisien. Perkembangan digitalisasi menjadi salah satu

faktor yang mendorong pertumbuhan *E-commerce* dan sekaligus menimbulkan kebutuhan baru terhadap regulasi transaksi elektronik (Homonai, 2024).

Perubahan dalam aktivitas ekonomi tidak berhenti pada perdagangan. Sistem pembayaran elektronik, layanan perbankan digital, *financial technology*, platform jasa, dan berbagai model bisnis berbasis aplikasi menciptakan hubungan ekonomi yang semakin bergantung pada teknologi. Data konsumen menjadi bagian penting dari proses tersebut karena digunakan untuk memberikan layanan, melakukan analisis, menyusun strategi pemasaran, dan meningkatkan pengalaman pengguna. Situasi ini menunjukkan bahwa transformasi digital tidak hanya mengubah cara transaksi dilakukan, tetapi juga mengubah sumber daya yang digunakan dalam kegiatan ekonomi.

Digitalisasi juga memperluas akses masyarakat terhadap informasi dan layanan. Pendidikan dapat dilakukan melalui platform pembelajaran daring, layanan publik dapat diakses melalui sistem elektronik, dan berbagai informasi pemerintah dapat disampaikan secara digital. Teknologi digital dapat memperluas akses terhadap informasi, pendidikan, layanan penting, serta pasar global. Penggunaan teknologi juga dapat meningkatkan partisipasi warga dan mendukung transparansi pemerintahan apabila disertai tata kelola yang memadai (Widayanti dkk., 2025).

Perubahan tersebut menghasilkan konsekuensi terhadap hubungan antara masyarakat dan pemerintah. Pemerintah tidak lagi hanya berfungsi sebagai penyedia layanan melalui kantor fisik, tetapi juga sebagai penyelenggara layanan digital. Masyarakat dapat berinteraksi dengan institusi publik melalui platform elektronik, mengajukan permohonan, memperoleh informasi, dan melakukan berbagai proses administratif secara daring. Perubahan ini meningkatkan efisiensi, tetapi juga menimbulkan kebutuhan terhadap keamanan sistem, perlindungan data, transparansi, serta akuntabilitas dalam pengelolaan teknologi.

Perkembangan teknologi juga menyebabkan data menjadi semakin penting dalam kehidupan masyarakat. Setiap aktivitas digital dapat menghasilkan data yang menggambarkan perilaku, preferensi, transaksi, komunikasi, dan berbagai aspek kehidupan seseorang. Data tersebut memiliki nilai ekonomi dan strategis karena dapat digunakan untuk mengambil keputusan atau mengembangkan layanan. Ketergantungan terhadap data sekaligus meningkatkan risiko penyalahgunaan informasi. Kondisi ini menjadikan perlindungan data sebagai salah satu persoalan utama dalam transformasi digital.

Dari perspektif hukum, perubahan tersebut memiliki konsekuensi yang sangat luas. Hubungan hukum yang sebelumnya terjadi melalui dokumen fisik dapat berlangsung melalui sistem elektronik. Persetujuan dapat diberikan secara digital,

komunikasi dapat menjadi bagian dari bukti transaksi, dan dokumen dapat disimpan dalam bentuk elektronik. Digitalisasi dengan demikian mengubah bentuk hubungan hukum tanpa menghilangkan kebutuhan terhadap prinsip dasar seperti kepastian, keadilan, perlindungan, dan tanggung jawab.

Transformasi digital menciptakan masyarakat yang semakin bergantung pada sistem teknologi. Ketergantungan tersebut membawa manfaat dalam bentuk efisiensi dan aksesibilitas, tetapi juga menciptakan kerentanan. Gangguan terhadap sistem digital dapat menghambat aktivitas ekonomi, pelayanan publik, komunikasi, bahkan kehidupan sehari-hari. Oleh sebab itu, perkembangan teknologi harus diikuti dengan perkembangan kerangka hukum yang mampu mengantisipasi risiko dan memberikan perlindungan terhadap masyarakat.

Revolusi digital dengan demikian tidak dapat dipahami hanya sebagai revolusi teknologi. Ia merupakan perubahan sosial yang memengaruhi cara manusia berinteraksi, cara ekonomi bekerja, cara pemerintah memberikan pelayanan, serta cara hak dan kewajiban terbentuk. Perubahan multidimensional tersebut menjadi dasar munculnya kebutuhan terhadap hukum yang mampu memahami lingkungan digital dan memberikan aturan yang sesuai dengan karakteristiknya (Paul dkk., 2024; Van Veldhoven & Vanthienen, 2021).

2. Perkembangan Teknologi Informasi dan Munculnya Ruang Siber

Perkembangan ruang siber merupakan konsekuensi dari perkembangan teknologi informasi dan komunikasi. Komputer yang pada awalnya digunakan untuk pengolahan data secara terbatas berkembang menjadi perangkat yang saling terhubung melalui jaringan. Internet kemudian memperluas konektivitas tersebut hingga membentuk jaringan global. Perkembangan perangkat bergerak membuat akses terhadap jaringan tidak lagi bergantung pada lokasi tertentu. Masyarakat dapat terhubung melalui telepon pintar, tablet, komputer, dan berbagai perangkat lainnya.

Perkembangan tersebut semakin kompleks dengan hadirnya *cloud computing*, *Internet of Things* (IoT), kecerdasan artifisial, dan *big data*. Teknologi tersebut memungkinkan data dikumpulkan dalam jumlah besar, diproses secara cepat, serta digunakan untuk berbagai tujuan. Hubungan antara manusia dan sistem digital menjadi semakin intens karena berbagai aktivitas sehari-hari mulai bergantung pada teknologi. Perkembangan internet, *cloud computing*, IoT, AI, dan *big data* telah memperluas ruang siber sebagai lingkungan interaksi yang semakin kompleks (Ababneh dkk., 2026; Alifah, 2024; Noor, 2025).

Ruang siber pada dasarnya merupakan lingkungan yang terbentuk dari interaksi manusia dengan jaringan, perangkat, aplikasi, sistem informasi, dan data. Ruang tersebut tidak memiliki batas fisik sebagaimana ruang konvensional.

Aktivitas di dalamnya dapat berlangsung secara simultan di berbagai lokasi. Percakapan, transaksi, penyimpanan data, pelayanan publik, pembelajaran, dan berbagai kegiatan lainnya dapat terjadi dalam ruang yang sama meskipun para pihak berada di wilayah yang berbeda.

Karakter lintas batas menjadi salah satu ciri paling penting ruang siber. Sebuah transaksi dapat melibatkan konsumen di Indonesia, perusahaan yang berkedudukan di Amerika Serikat, sistem pembayaran di negara lain, dan pusat data yang berada di wilayah berbeda. Situasi serupa dapat ditemukan dalam kejahatan siber. Pelaku dapat berada di satu negara, korban berada di negara kedua, sementara server atau infrastruktur yang digunakan untuk melakukan kejahatan berada di negara ketiga. Kondisi semacam ini menantang konsep yurisdiksi tradisional (Lukmana, 2025; Noor, 2025).

Ruang siber juga memiliki karakter kecepatan yang tinggi. Informasi dapat diproduksi, disalin, dimodifikasi, dan disebarluaskan dalam waktu sangat singkat. Suatu informasi dapat menyebar kepada masyarakat dalam hitungan detik tanpa memerlukan jaringan distribusi fisik. Kecepatan tersebut memberikan manfaat besar dalam komunikasi dan perdagangan, tetapi sekaligus meningkatkan dampak dari tindakan yang melanggar hukum. Konten yang merugikan, informasi palsu, penipuan, atau data yang disebarkan tanpa hak dapat

menyebar jauh sebelum mekanisme hukum mampu merespons.

Karakter lainnya adalah ketergantungan terhadap infrastruktur. Ruang siber tidak dapat berfungsi tanpa jaringan komunikasi, pusat data, perangkat keras, perangkat lunak, sistem keamanan, dan berbagai penyedia layanan. Ketergantungan tersebut membuat gangguan terhadap satu bagian sistem dapat memengaruhi aktivitas yang lebih luas. Serangan terhadap infrastruktur digital tertentu bahkan dapat menimbulkan dampak ekonomi dan sosial yang signifikan. Keamanan siber karena itu tidak hanya menjadi persoalan teknis, tetapi juga menjadi persoalan hukum dan kebijakan publik.

Perkembangan ruang siber kemudian menciptakan berbagai aktivitas hukum baru. Transaksi elektronik menjadi salah satu bentuk paling jelas. Kontrak dapat dibuat tanpa pertemuan fisik, pembayaran dapat dilakukan secara elektronik, dan dokumen dapat ditandatangani secara digital. Kondisi tersebut menuntut kepastian mengenai validitas tindakan elektronik, identitas para pihak, pembentukan kontrak, serta kekuatan pembuktian data elektronik. Perkembangan perdagangan digital menunjukkan pentingnya regulasi yang mampu menjamin keamanan dan kepastian transaksi elektronik (Homonai, 2024; Kashyap & Chaudhary, 2023).

Selain transaksi, ruang siber juga menjadi tempat berkembangnya berbagai bentuk pelanggaran hukum. Akses tanpa hak, pencurian

data, penipuan elektronik, serangan terhadap sistem, penyebaran perangkat berbahaya, dan *ransomware* merupakan contoh tindakan yang memanfaatkan teknologi sebagai sarana maupun sasaran. Perkembangan *cybercrime* menjadi salah satu alasan utama mengapa hukum harus mengembangkan instrumen yang mampu memberikan perlindungan terhadap sistem dan pengguna digital (Noor, 2025).

Perbedaan antara ruang fisik dan ruang siber juga terlihat dari karakter bukti. Dalam ruang konvensional, bukti sering kali berbentuk dokumen, benda, atau kesaksian yang dapat diamati secara langsung. Dalam ruang siber, bukti dapat berupa log sistem, rekaman komunikasi, metadata, alamat IP, data transaksi, atau informasi yang tersimpan dalam server. Kondisi tersebut menuntut kemampuan hukum dan aparat penegak hukum untuk memahami karakter bukti elektronik.

Ruang siber pada akhirnya menjadi lingkungan sosial dan ekonomi yang nyata dalam kehidupan masyarakat. Meskipun tidak memiliki batas fisik, konsekuensi yang terjadi di dalamnya dapat berdampak nyata terhadap seseorang, perusahaan, maupun negara. Karena itu, anggapan bahwa ruang digital merupakan wilayah yang bebas dari hukum tidak lagi dapat dipertahankan. Justru karena karakter ruang siber berbeda dari ruang fisik, diperlukan pendekatan hukum yang secara khusus mampu mengaturnya.

3. Konsep, Karakteristik, dan Ruang Lingkup Hukum Siber

Hukum siber berkembang sebagai respons terhadap kebutuhan untuk mengatur aktivitas manusia dalam lingkungan digital. Secara umum, hukum siber dapat dipahami sebagai seperangkat prinsip dan aturan yang mengatur penggunaan internet, teknologi informasi, komunikasi elektronik, serta aktivitas yang berlangsung dalam ruang siber (Alifah, 2024; Bhange, 2025; Muharman, 2025). Pengertian tersebut memperlihatkan bahwa hukum siber tidak hanya berhubungan dengan tindakan kriminal, tetapi mencakup hubungan hukum yang lebih luas.

Karakter utama hukum siber adalah sifatnya yang multidisipliner. Aktivitas digital dapat menimbulkan persoalan hukum pidana, perdata, administrasi, perlindungan konsumen, hak asasi manusia, hingga hukum internasional. Satu peristiwa digital bahkan dapat memiliki beberapa dimensi hukum sekaligus. Sebuah serangan terhadap sistem perusahaan, misalnya, dapat berkaitan dengan kejahatan siber, kerugian perdata, perlindungan data, tanggung jawab perusahaan, dan kewajiban pelaporan insiden.

Ruang lingkup hukum siber pertama dapat dilihat melalui transaksi elektronik. Transaksi yang dilakukan melalui sistem elektronik membutuhkan aturan mengenai identitas, persetujuan, kontrak, pembayaran, bukti, dan tanggung jawab. *E-commerce* menjadi contoh penting karena hubungan hukum

antara penjual dan pembeli dapat terbentuk tanpa adanya pertemuan fisik. Perkembangan *E-commerce* mendorong kebutuhan terhadap regulasi yang memberikan kepastian dan perlindungan terhadap seluruh pihak dalam transaksi digital (Homonai, 2024; Kashyap & Chaudhary, 2023).

Perlindungan data pribadi merupakan ruang lingkup yang semakin penting. Data digital dapat mengandung informasi yang sangat berkaitan dengan identitas dan kehidupan seseorang. Ketika data dikumpulkan dan diproses dalam jumlah besar, risiko penyalahgunaan juga meningkat. Hukum diperlukan untuk mengatur bagaimana data dapat dikumpulkan, digunakan, disimpan, dibagikan, dan dilindungi. Perlindungan privasi dan data menjadi salah satu pusat perkembangan hukum siber modern karena digitalisasi meningkatkan intensitas pemrosesan informasi pribadi (Alifah, 2024; Muharman, 2025).

Keamanan siber merupakan bagian yang tidak terpisahkan dari hukum siber. Sistem elektronik harus dilindungi dari akses tanpa hak, manipulasi, gangguan, pencurian, dan penghancuran. Keamanan tersebut bukan hanya kepentingan penyelenggara sistem, tetapi juga kepentingan pengguna dan masyarakat. Risiko keamanan dapat berkembang menjadi persoalan sosial apabila sistem yang terganggu berkaitan dengan layanan penting atau infrastruktur kritis. Oleh sebab itu, keamanan siber membutuhkan standar dan tanggung jawab

hukum yang jelas (Ababneh dkk., 2026; Khanna, 2024).

Kejahatan siber merupakan ruang lingkup yang secara historis paling banyak dikaitkan dengan hukum siber. Teknologi dapat digunakan untuk melakukan penipuan, pencurian identitas, pencurian data, serangan terhadap sistem, *ransomware*, dan berbagai tindakan lainnya. Karakter kejahatan tersebut berbeda dari kejahatan konvensional karena pelaku dapat menyembunyikan identitas dan beroperasi dari lokasi yang jauh. Penegakan hukum menjadi lebih kompleks karena bukti berada dalam sistem elektronik dan aktivitas dapat melintasi batas negara (Gussman & Jannah, 2026; Noor, 2025).

Hak digital juga menjadi bagian penting dalam perkembangan hukum siber. Ketika kehidupan manusia semakin bergantung pada teknologi, hak atas privasi, kebebasan berekspresi, akses informasi, dan perlindungan terhadap data memperoleh dimensi digital. Hukum tidak hanya diperlukan untuk menghukum pelanggaran, tetapi juga untuk memastikan bahwa teknologi digunakan dengan menghormati hak individu. Keamanan siber pada akhirnya memiliki hubungan erat dengan perlindungan hak digital dan pembentukan kepercayaan dalam ruang digital (Touria, 2025).

Kekayaan intelektual juga memiliki hubungan erat dengan hukum siber. Konten digital dapat disalin dan disebarkan dengan mudah tanpa menghilangkan bentuk aslinya. Kemudahan tersebut meningkatkan peluang pemanfaatan karya secara tidak sah. Hukum

perlu memberikan perlindungan terhadap pencipta dan pemilik hak sekaligus mempertimbangkan karakter distribusi informasi dalam lingkungan digital. Perkembangan teknologi membuat perlindungan kekayaan intelektual tidak lagi dapat hanya bergantung pada mekanisme konvensional.

Hukum siber juga memiliki dimensi internasional. Transaksi dan aktivitas digital dapat melibatkan beberapa yurisdiksi secara bersamaan. Perbedaan aturan antarnegara dapat menimbulkan persoalan ketika suatu tindakan dianggap sah di satu negara tetapi melanggar hukum di negara lain. Harmonisasi dan kerja sama menjadi penting untuk memastikan bahwa ruang siber tidak menjadi tempat berlindung bagi pelaku pelanggaran hukum.

Dengan ruang lingkup tersebut, hukum siber tidak dapat diposisikan sebagai cabang hukum yang sepenuhnya terpisah dari sistem hukum yang sudah ada. Hukum siber justru berinteraksi dengan berbagai bidang hukum dan mengadaptasikan prinsip-prinsip yang sudah ada ke dalam lingkungan digital. Sifat multidisipliner tersebut menjadi karakter fundamental hukum siber sekaligus menjelaskan mengapa pengembangannya membutuhkan perspektif yang luas (Bhange, 2025; Ennan, 2024).

4. Faktor Pendorong Lahirnya dan Perkembangan Hukum Siber

Kelahiran hukum siber tidak dapat dipisahkan dari perkembangan teknologi dan perubahan perilaku masyarakat. Ketika teknologi

mulai digunakan secara luas, berbagai aktivitas yang sebelumnya berlangsung dalam ruang fisik berpindah ke ruang digital. Perubahan tersebut menciptakan kebutuhan terhadap aturan baru karena hukum konvensional tidak selalu mampu memberikan jawaban terhadap persoalan yang memiliki karakter digital.

Meningkatnya kejahatan siber menjadi salah satu faktor utama perkembangan hukum siber. Semakin luas penggunaan teknologi, semakin besar pula potensi teknologi digunakan untuk melakukan tindakan yang merugikan. Pencurian data, penipuan daring, *ransomware*, serangan terhadap sistem, dan berbagai bentuk *cybercrime* menunjukkan bahwa ruang digital memiliki risiko yang membutuhkan perlindungan hukum. Perkembangan ancaman siber juga berlangsung secara dinamis sehingga hukum harus terus menyesuaikan diri (Ababneh dkk., 2026; Noor, 2025).

Kebutuhan perlindungan pengguna menjadi faktor berikutnya. Pengguna sering kali tidak mengetahui secara rinci bagaimana data mereka dikumpulkan dan diproses oleh suatu platform. Pengguna juga dapat menghadapi ketidakseimbangan posisi ketika berhadapan dengan perusahaan teknologi yang memiliki sumber daya, informasi, dan kemampuan teknis lebih besar. Hukum diperlukan untuk memastikan bahwa penggunaan teknologi tidak menghasilkan praktik yang merugikan pengguna atau mengurangi hak mereka secara tidak proporsional.

Pertumbuhan ekonomi digital turut mempercepat perkembangan hukum siber. Perdagangan elektronik, pembayaran digital, layanan berbasis aplikasi, dan berbagai model bisnis digital menciptakan transaksi dalam jumlah besar. Aktivitas tersebut membutuhkan kepastian mengenai kontrak, pembayaran, identitas, perlindungan konsumen, keamanan, dan penyelesaian sengketa. Digitalisasi perdagangan secara langsung meningkatkan kebutuhan terhadap kerangka hukum yang mampu memberikan kepastian bagi pelaku usaha maupun konsumen (Homonai, 2024; Kashyap & Chaudhary, 2023).

Transaksi lintas batas juga menjadi faktor penting. Internet memungkinkan pelaku usaha menjangkau konsumen di berbagai negara tanpa harus memiliki kehadiran fisik di setiap wilayah. Kemudahan tersebut memberikan peluang ekonomi, tetapi sekaligus menimbulkan persoalan hukum mengenai yurisdiksi dan hukum yang berlaku. Persoalan yang sama terjadi dalam *cybercrime* ketika pelaku dan korban berada dalam yurisdiksi berbeda. Kondisi tersebut membuat kerja sama internasional menjadi bagian penting dalam perkembangan hukum siber (Fahey, 2024; Noor, 2025).

Perkembangan teknologi yang sangat cepat juga menciptakan tekanan terhadap hukum. Regulasi umumnya membutuhkan proses pembentukan yang lebih lama daripada perkembangan teknologi. Teknologi baru dapat muncul sebelum regulasi sebelumnya mampu memberikan jawaban yang

memadai. Kecerdasan artifisial, IoT, *blockchain*, dan teknologi digital lainnya memperlihatkan bahwa hukum harus memiliki kemampuan adaptasi agar tidak selalu tertinggal dari perubahan teknologi (Octaviandini & Listyani, 2025).

Fragmentasi regulasi juga menjadi tantangan. Pengaturan mengenai teknologi digital dapat tersebar dalam berbagai peraturan dan berada di bawah kewenangan lembaga yang berbeda. Kondisi tersebut dapat menyebabkan tumpang tindih kewenangan atau perbedaan interpretasi. Reformasi hukum siber karena itu tidak hanya berkaitan dengan pembentukan aturan baru, tetapi juga harmonisasi berbagai aturan yang sudah ada.

Tuntutan terhadap kepastian hukum menjadi faktor yang semakin penting bagi perkembangan ekonomi digital. Pelaku usaha membutuhkan kepastian mengenai batas tindakan yang diperbolehkan, sementara masyarakat membutuhkan kepastian bahwa hak mereka mendapatkan perlindungan. Tanpa kepastian hukum, perkembangan teknologi dapat menghasilkan risiko yang menghambat inovasi dan mengurangi kepercayaan masyarakat terhadap layanan digital.

Kebutuhan terhadap penegakan hukum yang efektif juga mendorong perkembangan hukum siber. Keberadaan aturan tidak akan memberikan manfaat apabila tidak disertai kemampuan untuk melakukan investigasi, memperoleh bukti elektronik, mengidentifikasi pelaku, dan melakukan koordinasi lintas yurisdiksi. Penegakan hukum siber

menghadapi berbagai hambatan, termasuk anonimitas pelaku, kompleksitas teknologi, keterbatasan kapasitas aparat, serta persoalan yurisdiksi (Gussman & Jannah, 2026).

Perkembangan kebijakan keamanan siber di berbagai negara menunjukkan bahwa hukum siber juga dipengaruhi oleh kebutuhan harmonisasi. Negara-negara menghadapi ancaman digital yang serupa meskipun memiliki sistem hukum berbeda. Kerja sama internasional dan konvergensi kebijakan menjadi semakin penting untuk menghadapi ancaman yang tidak mengenal batas negara (Fahey, 2024).

Dengan demikian, hukum siber lahir dari kombinasi berbagai kebutuhan. Kejahatan digital menciptakan kebutuhan perlindungan, ekonomi digital menciptakan kebutuhan kepastian transaksi, perkembangan teknologi menciptakan kebutuhan adaptasi, sedangkan sifat lintas batas menciptakan kebutuhan kerja sama internasional. Seluruh faktor tersebut saling berkaitan dan membentuk alasan kuat bagi perkembangan hukum siber sebagai bidang hukum yang terus mengalami perubahan.

5. Urgensi Hukum Siber dalam Mewujudkan Tata Kelola Digital

Hukum siber memiliki posisi strategis dalam membangun tata kelola digital. Tata kelola digital tidak hanya berkaitan dengan kemampuan suatu negara atau organisasi menggunakan teknologi, tetapi juga berkaitan dengan bagaimana teknologi diarahkan agar digunakan secara aman, bertanggung

jawab, transparan, dan dapat dipertanggungjawabkan. Hukum memberikan dasar bagi penentuan hak, kewajiban, larangan, standar, dan mekanisme pertanggungjawaban dalam lingkungan digital (Bhange, 2025; Muharman, 2025).

Keamanan merupakan salah satu tujuan utama tata kelola digital. Masyarakat tidak akan memiliki kepercayaan terhadap sistem digital apabila data mudah dicuri, transaksi mudah dimanipulasi, atau layanan mudah terganggu. Keamanan karena itu harus menjadi bagian dari desain tata kelola sejak awal. Regulasi dapat menetapkan standar keamanan, tanggung jawab penyelenggara sistem, kewajiban pelaporan insiden, dan mekanisme penanganan ketika terjadi serangan (Ababneh dkk., 2026).

Kepastian hukum juga merupakan fondasi penting. Pelaku usaha membutuhkan aturan yang jelas untuk mengembangkan produk dan layanan digital. Masyarakat membutuhkan kepastian bahwa transaksi dan data mereka dilindungi. Pemerintah membutuhkan dasar kewenangan yang jelas untuk melakukan pengawasan. Regulasi yang tidak jelas atau saling bertentangan dapat menghasilkan ketidakpastian dan mengurangi kepercayaan terhadap ekosistem digital.

Perlindungan hak merupakan dimensi lain yang tidak dapat dipisahkan dari tata kelola digital. Teknologi dapat digunakan untuk meningkatkan pelayanan dan akses informasi, tetapi juga dapat digunakan untuk melakukan pengawasan, mengumpulkan data, atau membatasi hak individu.

Hukum perlu memastikan bahwa kepentingan keamanan tidak digunakan secara berlebihan untuk mengurangi privasi dan kebebasan masyarakat. Keamanan siber karena itu perlu berjalan seimbang dengan perlindungan hak digital (Touria, 2025).

Akuntabilitas menjadi penting karena lingkungan digital melibatkan banyak aktor. Suatu layanan dapat melibatkan pengembang perangkat lunak, penyedia platform, penyedia infrastruktur, pengelola data, dan pengguna. Ketika terjadi pelanggaran atau kerugian, harus dapat ditentukan pihak yang memiliki tanggung jawab. Tata kelola digital yang baik membutuhkan mekanisme pertanggungjawaban yang jelas sehingga tidak terjadi keadaan ketika setiap pihak melepaskan tanggung jawab kepada pihak lainnya.

Harmonisasi regulasi juga diperlukan karena ruang digital bersifat lintas batas. Negara tidak dapat sepenuhnya menyelesaikan persoalan siber melalui hukum nasional apabila tindakan tersebut melibatkan sistem, pelaku, atau data di negara lain. Kerja sama internasional diperlukan dalam pertukaran informasi, penyidikan, penegakan hukum, dan penyelarasan kebijakan. Perkembangan hukum dan kebijakan keamanan siber menunjukkan semakin pentingnya konvergensi antarnegara dalam menghadapi ancaman digital (Fahey, 2024).

Tata kelola digital juga membutuhkan kolaborasi antara pemerintah, sektor swasta, akademisi, dan masyarakat. Pemerintah memiliki kewenangan regulasi, perusahaan memiliki

penguasaan terhadap banyak infrastruktur dan teknologi, akademisi berperan dalam pengembangan pengetahuan, sedangkan masyarakat merupakan pengguna sekaligus pihak yang terdampak oleh kebijakan digital. Pendekatan multidisipliner diperlukan karena persoalan siber tidak hanya berkaitan dengan hukum, tetapi juga teknologi, ekonomi, sosial, dan etika (Sari & Herman, 2025).

Kebutuhan terhadap pendekatan adaptif semakin penting dengan munculnya teknologi baru. Kecerdasan artifisial dapat mengambil keputusan atau menghasilkan konten secara otomatis, IoT menghubungkan berbagai perangkat, dan *blockchain* menawarkan mekanisme pencatatan transaksi yang berbeda dari sistem konvensional. Setiap teknologi tersebut membawa manfaat sekaligus risiko. Hukum perlu mampu mengantisipasi risiko tanpa menghambat inovasi. Reformasi hukum siber di Indonesia karena itu perlu mempertimbangkan dinamika teknologi dan arah kebijakan yang adaptif (Octaviandini & Listyani, 2025).

Tata kelola digital juga berkaitan dengan pembangunan kepercayaan. Masyarakat akan lebih bersedia menggunakan layanan digital apabila mereka percaya bahwa data mereka aman, transaksi mereka terlindungi, dan terdapat mekanisme yang dapat digunakan ketika terjadi pelanggaran. Kepercayaan tersebut menjadi salah satu fondasi penting perkembangan ekonomi dan masyarakat digital. Keamanan siber, perlindungan hak, akuntabilitas, dan kepastian hukum saling berkaitan

dalam membangun kepercayaan tersebut (Touria, 2025).

Hukum siber karena itu tidak seharusnya dipandang semata-mata sebagai instrumen represif. Hukum siber juga memiliki fungsi preventif melalui penetapan standar dan larangan, fungsi protektif melalui perlindungan hak, fungsi korektif melalui penegakan dan penyelesaian sengketa, serta fungsi fasilitatif melalui penciptaan kepastian bagi inovasi. Perspektif tersebut menempatkan hukum siber sebagai bagian dari arsitektur tata kelola digital.

Urgensi tersebut semakin jelas ketika mempertimbangkan hubungan antara keamanan digital dan pertumbuhan ekonomi. Ekonomi digital membutuhkan lingkungan yang aman dan dapat dipercaya. Apabila masyarakat khawatir terhadap pencurian data atau penipuan, tingkat penggunaan layanan digital dapat menurun. Sebaliknya, regulasi yang terlalu berat dan tidak proporsional juga dapat membatasi inovasi. Karena itu, regulasi perlu mencari keseimbangan antara perlindungan dan perkembangan ekonomi digital (Widayanti dkk., 2025).

Hukum siber merupakan salah satu fondasi penting bagi terciptanya ruang digital yang aman, tertib, dan bertanggung jawab. Revolusi digital telah mengubah struktur kehidupan masyarakat, sedangkan ruang siber telah menjadi tempat berlangsungnya berbagai aktivitas sosial dan ekonomi. Perubahan tersebut menciptakan hubungan hukum dan risiko hukum yang tidak dapat

sepenuhnya dijawab melalui pendekatan konvensional.

Hukum siber hadir untuk menjawab kebutuhan tersebut. Perannya tidak terbatas pada penanganan kejahatan digital, tetapi mencakup transaksi elektronik, perlindungan data, keamanan sistem, hak digital, perlindungan konsumen, serta tata kelola teknologi. Sifat multidisipliner tersebut membuat hukum siber menjadi bidang yang terus berkembang mengikuti perubahan teknologi (Bhange, 2025; Ennan, 2024).

Tantangan ke depan terletak pada kemampuan hukum untuk tetap memberikan kepastian tanpa kehilangan fleksibilitas. Teknologi akan terus berkembang, sementara bentuk risiko baru akan muncul. Regulasi yang terlalu kaku berpotensi menghambat inovasi, sedangkan regulasi yang terlalu longgar dapat meningkatkan risiko terhadap masyarakat. Karena itu, hukum siber membutuhkan pendekatan yang adaptif, harmonis, berbasis hak, dan mampu merespons perubahan teknologi secara berkelanjutan (Octaviandini & Listyani, 2025; Sari & Herman, 2025).

Dengan kerangka tersebut, hukum siber dapat ditempatkan sebagai instrumen untuk membangun ekosistem digital yang tidak hanya maju secara teknologi, tetapi juga memiliki kepastian hukum, keamanan, perlindungan hak, dan akuntabilitas. Tata kelola digital yang baik pada akhirnya bukan hanya persoalan bagaimana teknologi digunakan, tetapi bagaimana teknologi

ditempatkan dalam kerangka hukum yang mampu menjaga kepentingan masyarakat sekaligus memberikan ruang bagi inovasi.

BAB II
LANDASAN FILOSOFIS DAN TEORI HUKUM DI RUANG SIBER

Perkembangan teknologi digital tidak hanya menghasilkan perubahan terhadap cara manusia berkomunikasi dan melakukan kegiatan ekonomi, tetapi juga mengubah cara hukum bekerja. Ruang siber menghadirkan bentuk hubungan sosial yang berlangsung melalui jaringan, sistem elektronik, algoritme, dan data. Perubahan tersebut menimbulkan pertanyaan mendasar mengenai bagaimana hukum seharusnya hadir dalam lingkungan yang bergerak cepat, lintas batas, dan terus mengalami perkembangan teknologi. Hukum siber karena itu tidak cukup dibangun hanya berdasarkan kebutuhan praktis untuk mengatur teknologi, tetapi juga membutuhkan dasar filosofis yang menjelaskan nilai apa yang harus dilindungi dan tujuan apa yang hendak dicapai.

Landasan filosofis menjadi penting karena hukum pada hakikatnya tidak hanya terdiri atas aturan yang bersifat teknis. Di balik setiap larangan, kewajiban, hak, dan sanksi terdapat pilihan nilai yang menentukan arah pengaturan. Dalam ruang siber, pilihan nilai tersebut menjadi semakin kompleks karena teknologi dapat memberikan manfaat sekaligus menciptakan risiko. Teknologi dapat memperluas akses informasi, meningkatkan efisiensi, dan membuka kesempatan

ekonomi, tetapi juga dapat digunakan untuk melakukan pengawasan, manipulasi, diskriminasi, atau pelanggaran privasi.

Persoalan hukum siber pada akhirnya mempertemukan tiga kepentingan utama. Kepentingan pertama adalah kebutuhan terhadap kepastian hukum agar masyarakat mengetahui batas tindakan yang diperbolehkan. Kepentingan kedua adalah kebutuhan terhadap keadilan agar perkembangan teknologi tidak menghasilkan distribusi manfaat dan risiko yang timpang. Kepentingan ketiga adalah kebutuhan terhadap kemanfaatan agar hukum mampu menciptakan lingkungan digital yang aman dan produktif. Ketiga nilai tersebut perlu ditempatkan secara seimbang dalam pembentukan dan penerapan hukum siber (Arafat dkk., 2025; Rohmy dkk., 2021).

Permasalahan menjadi semakin kompleks ketika teknologi berkembang lebih cepat daripada regulasi. Hukum yang terlalu kaku dapat kehilangan relevansi, sedangkan hukum yang terlalu fleksibel dapat mengurangi kepastian. Ketegangan tersebut mendorong perkembangan teori hukum yang lebih adaptif terhadap perubahan teknologi. Hukum responsif dan hukum progresif memberikan perspektif bahwa hukum tidak seharusnya hanya mempertahankan kepatuhan formal, tetapi juga harus mampu memberikan perlindungan terhadap kepentingan manusia dalam menghadapi perubahan sosial dan teknologi (Antony dkk., 2025; Firdaus dkk., 2025; Gulyaeva dkk., 2025).

Ruang siber juga membawa dimensi hak asasi manusia yang semakin kuat. Privasi, kebebasan

berekspresi, akses informasi, dan perlindungan data pribadi harus tetap mendapatkan perlindungan ketika aktivitas manusia berpindah ke lingkungan digital. Hak yang berlaku dalam kehidupan nyata tidak kehilangan relevansinya ketika seseorang menggunakan internet. Sebaliknya, hak tersebut membutuhkan bentuk perlindungan baru karena teknologi dapat memperluas kemampuan untuk mengumpulkan, memproses, menyebarkan, dan memengaruhi informasi mengenai individu (AlDesouki, 2024; Allahrakha, 2025; Okonkwo, 2025).

Persoalan lain muncul karena ruang siber tidak berhenti pada batas negara. Aktivitas digital dapat melibatkan pelaku, korban, server, platform, dan data yang berada di yurisdiksi berbeda. Kondisi ini menguji konsep kedaulatan dan yurisdiksi yang selama ini banyak dibangun berdasarkan wilayah teritorial. Hukum internasional menghadapi kebutuhan untuk menyesuaikan konsep kedaulatan, non-intervention, *due diligence*, atribusi, serta pertanggungjawaban dengan karakter aktivitas siber (Çora & Mikail, 2026; Lazari, 2025).

Atas dasar tersebut, pembahasan Bab II diarahkan pada empat persoalan utama. Pertama, landasan filosofis hukum siber melalui keadilan, kepastian hukum, dan kemanfaatan. Kedua, teori hukum yang dapat digunakan untuk menjelaskan kebutuhan adaptasi norma terhadap perkembangan teknologi. Ketiga, hubungan antara hak asasi manusia dan perlindungan hak digital. Keempat, persoalan kedaulatan, yurisdiksi, dan tanggung jawab hukum dalam

aktivitas siber lintas batas. Keempatnya membentuk fondasi untuk memahami bagaimana hukum seharusnya dibangun dan diterapkan dalam ruang digital.

1. **Landasan Filosofis Hukum Siber: Keadilan, Kepastian Hukum, dan Kemanfaatan**

   Landasan filosofis hukum siber berangkat dari pertanyaan mengenai tujuan keberadaan hukum dalam kehidupan digital. Teknologi pada dasarnya merupakan sarana yang digunakan manusia untuk mencapai tujuan tertentu. Karena itu, hukum tidak seharusnya hanya berorientasi pada teknologi sebagai objek pengaturan, tetapi harus mempertimbangkan manusia sebagai subjek utama yang harus dilindungi. Keadilan, kepastian hukum, dan kemanfaatan menjadi tiga nilai yang penting untuk memastikan bahwa perkembangan teknologi tetap berada dalam kerangka kehidupan yang tertib dan manusiawi.

   Keadilan dalam ruang siber memiliki makna yang lebih luas daripada sekadar memberikan perlakuan yang sama kepada setiap orang. Keadilan juga berkaitan dengan bagaimana manfaat teknologi dan risiko yang ditimbulkannya didistribusikan. Akses terhadap teknologi, kemampuan memahami teknologi, kemampuan melindungi data, serta kemampuan memperoleh pemulihan ketika terjadi pelanggaran tidak selalu dimiliki setiap orang secara sama. Keadilan digital karena itu perlu memperhatikan kesenjangan akses, ketimpangan kemampuan, serta distribusi manfaat dan risiko

teknologi secara proporsional (Firdaus dkk., 2025; Humin, 2026).

Persoalan keadilan juga dapat muncul melalui sistem algoritmik. Algoritme dapat digunakan untuk menentukan rekomendasi, menilai risiko, menyaring informasi, bahkan membantu mengambil keputusan yang berdampak terhadap individu. Apabila data atau desain algoritme mengandung bias, keputusan yang dihasilkan dapat memberikan dampak yang tidak adil kepada kelompok tertentu. Kondisi tersebut menunjukkan bahwa keadilan dalam hukum siber tidak cukup diwujudkan melalui larangan terhadap tindakan diskriminatif secara konvensional, tetapi juga membutuhkan perhatian terhadap proses teknologi yang menghasilkan keputusan.

Keadilan juga harus diterapkan dalam hubungan antara penyelenggara teknologi dan pengguna. Perusahaan teknologi umumnya memiliki sumber daya teknis dan informasi yang lebih besar daripada pengguna. Pengguna sering kali hanya dapat menerima syarat dan ketentuan yang telah disusun oleh penyelenggara. Kondisi tersebut dapat menghasilkan ketidakseimbangan apabila tidak terdapat mekanisme perlindungan yang memadai. Hukum perlu memastikan bahwa hubungan digital tidak menghasilkan keadaan ketika pihak yang lebih kuat dapat menentukan seluruh aturan tanpa mempertimbangkan kepentingan pihak yang lebih lemah.

Nilai kedua adalah kepastian hukum. Kepastian menjadi penting karena masyarakat membutuhkan aturan yang dapat dipahami dan diprediksi. Dalam ruang digital, ketidakjelasan norma dapat menghasilkan konsekuensi yang lebih besar karena aktivitas berlangsung cepat dan melibatkan banyak pihak. Norma yang kabur, tumpang tindih, atau memiliki banyak interpretasi dapat melemahkan perlindungan hak dan mengurangi efektivitas penegakan hukum (Tan dkk., 2026).

Kepastian hukum juga berkaitan dengan kemampuan negara merumuskan batas perilaku secara jelas. Dalam konteks kejahatan siber, misalnya, masyarakat perlu mengetahui tindakan apa yang dikategorikan sebagai pelanggaran, unsur apa yang harus dibuktikan, dan sanksi apa yang dapat dikenakan. Prinsip legalitas tetap memiliki arti penting karena seseorang tidak seharusnya dikenai sanksi berdasarkan norma yang tidak jelas. Positivisme hukum memberikan kontribusi penting dalam hal ini karena menekankan pentingnya norma yang dirumuskan secara jelas dan dapat diterapkan secara terukur (Sukirno dkk., 2021; Tan dkk., 2026).

Kepastian juga diperlukan dalam transaksi elektronik. Para pihak perlu mengetahui kapan suatu kontrak dianggap terbentuk, bagaimana persetujuan diberikan, bagaimana identitas diverifikasi, serta bagaimana bukti elektronik dapat digunakan ketika terjadi sengketa. Tanpa kepastian tersebut, transaksi digital dapat meningkatkan risiko bagi pelaku usaha

dan konsumen. Hukum karena itu harus mampu memberikan struktur yang dapat diprediksi tanpa menghilangkan fleksibilitas yang dibutuhkan oleh perkembangan teknologi.

Nilai ketiga adalah kemanfaatan. Hukum siber harus menghasilkan manfaat yang dapat dirasakan oleh masyarakat. Kemanfaatan tersebut tidak hanya berupa efisiensi ekonomi, tetapi juga keamanan, perlindungan hak, akses terhadap layanan, serta terciptanya lingkungan digital yang sehat. Hukum yang hanya berorientasi pada kontrol dapat menghambat inovasi, sementara hukum yang terlalu berorientasi pada inovasi tanpa perlindungan dapat meningkatkan risiko terhadap masyarakat. Kemanfaatan harus dipahami sebagai kemampuan hukum menciptakan keseimbangan antara perkembangan teknologi dan kepentingan manusia (Arafat dkk., 2025; Humin, 2026).

Ketiga nilai tersebut tidak dapat dipisahkan. Kepastian tanpa keadilan dapat menghasilkan aturan yang formal tetapi tidak mampu melindungi pihak yang rentan. Keadilan tanpa kepastian dapat menimbulkan ketidakprediktifan dalam penerapan hukum. Kemanfaatan tanpa keduanya dapat mengarah pada kebijakan yang hanya mengejar efisiensi tanpa memperhatikan hak. Dalam konteks hukum siber, ketiga nilai tersebut harus dipertemukan melalui regulasi yang memiliki dasar filosofis, yuridis, dan sosiologis yang kuat (Rohmy dkk., 2021).

Penerapan ketiga nilai tersebut menjadi semakin penting ketika hukum menghadapi teknologi baru. Pengaturan kecerdasan artifisial, misalnya, harus memberikan ruang bagi inovasi sekaligus memastikan bahwa penggunaan AI tidak menghasilkan diskriminasi atau pelanggaran hak. Pengaturan data harus memungkinkan pemanfaatan data untuk kepentingan ekonomi dan pelayanan publik sekaligus menjaga privasi individu. Setiap regulasi digital karena itu perlu mempertimbangkan keseimbangan antara manfaat teknologi dan risiko yang mungkin ditimbulkannya.

Landasan filosofis hukum siber menentukan arah regulasi. Hukum tidak seharusnya dibentuk hanya karena teknologi menimbulkan masalah baru, tetapi karena terdapat kebutuhan untuk memastikan bahwa perubahan teknologi tetap berjalan sesuai nilai yang dianggap penting dalam kehidupan bermasyarakat. Keadilan, kepastian hukum, dan kemanfaatan menjadi dasar untuk menilai apakah suatu regulasi digital benar-benar memberikan perlindungan dan manfaat bagi masyarakat.

2. Teori Hukum dan Adaptasi Norma dalam Perkembangan Teknologi Digital

Perkembangan teknologi menempatkan hukum pada situasi yang berbeda dari kondisi ketika banyak doktrin hukum konvensional dibentuk. Perubahan teknologi dapat berlangsung dalam waktu singkat, sedangkan perubahan peraturan membutuhkan proses yang lebih panjang. Akibatnya, hukum sering kali berhadapan dengan situasi ketika

teknologi baru telah digunakan secara luas sebelum tersedia aturan yang secara khusus mengaturnya. Kondisi tersebut menimbulkan kebutuhan untuk memikirkan kembali bagaimana teori hukum digunakan dalam menghadapi perubahan teknologi.

Positivisme hukum tetap memiliki arti penting dalam ruang siber. Hukum membutuhkan norma yang jelas, dapat diketahui, dan memiliki mekanisme penegakan. Dalam menghadapi *cybercrime* , misalnya, aparat tidak dapat bertindak hanya berdasarkan penilaian moral tanpa dasar hukum yang jelas. Kepastian mengenai unsur tindak pidana, kewenangan aparat, dan jenis sanksi menjadi bagian penting dari perlindungan hukum. Prinsip tersebut menjadi semakin penting dalam lingkungan digital karena tindakan negara juga berpotensi memengaruhi hak individu secara luas (Sukirno dkk., 2021; Tan dkk., 2026). Namun, pendekatan positivistik menghadapi tantangan ketika teknologi berubah lebih cepat daripada pembentukan norma. Aturan yang terlalu spesifik dapat segera kehilangan relevansi ketika teknologi mengalami perubahan. Jika setiap inovasi membutuhkan aturan baru yang sangat rinci, sistem hukum akan selalu berada dalam posisi mengejar perkembangan teknologi. Karena itu, kebutuhan terhadap kepastian harus dipadukan dengan kemampuan hukum untuk beradaptasi.

Hukum responsif menawarkan perspektif yang lebih terbuka terhadap perubahan sosial. Hukum tidak hanya dipahami sebagai sistem aturan yang harus ditaati, tetapi juga sebagai instrumen

untuk merespons kebutuhan masyarakat. Dalam konteks digital, pendekatan responsif menuntut keterbukaan terhadap perkembangan teknologi, partisipasi publik, harmonisasi regulasi, dan evaluasi terhadap efektivitas aturan yang telah berlaku (Antony dkk., 2025).

Responsivitas menjadi penting karena regulasi digital dapat memiliki dampak yang luas terhadap masyarakat. Peraturan mengenai moderasi konten, perlindungan data, pengawasan digital, atau kecerdasan artifisial dapat memengaruhi jutaan pengguna. Pembentukan regulasi karena itu tidak seharusnya hanya dilakukan dari perspektif pemerintah atau industri teknologi. Perspektif masyarakat, akademisi, kelompok pengguna, dan pihak lain yang terdampak perlu dipertimbangkan.

Hukum progresif memberikan dimensi lain terhadap adaptasi hukum. Hukum progresif menempatkan manusia sebagai orientasi utama hukum. Dalam lingkungan digital, prinsip tersebut berarti hukum harus aktif melindungi manusia ketika teknologi menghasilkan risiko terhadap martabat, kebebasan, privasi, atau keadilan. Hukum tidak seharusnya berhenti pada kepatuhan formal apabila penerapan aturan justru menghasilkan ketidakadilan substantif (Firdaus dkk., 2025; Nur dkk., 2026).

Adaptasi hukum juga membutuhkan pendekatan interdisipliner. Hukum tidak dapat memahami persoalan kecerdasan artifisial, keamanan siber, algoritme, atau blockchain hanya dengan membaca norma hukum. Pemahaman

tersebut membutuhkan komunikasi antara ahli hukum, teknologi, ekonomi, sosial, dan etika. Perkembangan teknologi telah mengubah doktrin, struktur kelembagaan, dan cara bernalar hukum sehingga teori hukum perlu berkembang bersama perubahan tersebut (Gulyaeva dkk., 2025).

Adaptasi juga tidak berarti bahwa semua teknologi harus diatur dengan cara yang sama. Setiap teknologi memiliki tingkat risiko, manfaat, dan karakter yang berbeda. Pendekatan berbasis risiko dapat digunakan untuk menentukan intensitas pengaturan. Teknologi yang berpotensi memberikan dampak besar terhadap hak dan keselamatan masyarakat membutuhkan pengawasan yang lebih ketat dibandingkan teknologi yang memiliki risiko rendah.

Salah satu instrumen yang dapat digunakan adalah *regulatory sandbox*. Mekanisme ini memungkinkan teknologi atau model bisnis baru diuji dalam lingkungan yang terkontrol sebelum diterapkan secara lebih luas. Pendekatan tersebut memberikan ruang bagi regulator untuk memahami teknologi sekaligus memberikan kesempatan kepada inovator untuk mengembangkan produk. Teori adaptasi hukum mendorong penggunaan pendekatan seperti *sandbox, Soft law*, dan kerja interdisipliner agar hukum tidak tertinggal dari inovasi (Firdaus dkk., 2025).

Soft law juga dapat digunakan untuk merespons bidang teknologi yang masih berkembang. Pedoman, standar, kode etik, atau

prinsip tata kelola dapat memberikan arahan sebelum norma yang lebih mengikat dibentuk. Pendekatan tersebut dapat mempercepat respons regulasi, tetapi tetap membutuhkan batas yang jelas agar tidak menggantikan kebutuhan terhadap perlindungan hukum yang mengikat ketika hak masyarakat berada dalam risiko.

Adaptasi hukum juga membutuhkan evaluasi berkelanjutan. Regulasi digital tidak seharusnya dianggap selesai setelah diberlakukan. Efektivitasnya perlu dievaluasi berdasarkan perubahan teknologi, pengalaman masyarakat, perkembangan risiko, serta hasil penegakan hukum. Dengan cara demikian, regulasi dapat diperbaiki sebelum kesenjangan antara hukum dan teknologi menjadi terlalu besar.

Teori hukum dalam ruang siber tidak harus memilih antara kepastian dan fleksibilitas. Keduanya dapat ditempatkan dalam hubungan yang saling melengkapi. Positivisme memberikan fondasi kepastian norma, hukum responsif memberikan kemampuan merespons kebutuhan masyarakat, sedangkan hukum progresif memberikan orientasi pada perlindungan manusia. Ketiganya dapat menjadi perspektif yang saling melengkapi dalam membangun hukum siber yang adaptif (Antony dkk., 2025; Firdaus dkk., 2025; Gulyaeva dkk., 2025).

3. Hak Asasi Manusia, Privasi, dan Perlindungan Hak Digital

Perkembangan ruang digital tidak menghapus keberadaan hak asasi manusia. Hak yang dimiliki seseorang dalam kehidupan nyata tetap

memiliki relevansi ketika orang tersebut menggunakan internet, media sosial, layanan digital, atau sistem elektronik. Perubahan yang terjadi adalah cara hak tersebut diwujudkan dan cara pelanggaran terhadapnya dapat terjadi. Hak atas privasi, kebebasan berekspresi, akses informasi, dan perlindungan terhadap data pribadi kini memiliki dimensi digital yang semakin kuat (AlDesouki, 2024; Okonkwo, 2025).

Privasi menjadi salah satu persoalan utama. Teknologi memungkinkan pengumpulan informasi mengenai seseorang dalam jumlah yang jauh lebih besar dibandingkan sebelumnya. Data dapat dikumpulkan dari aktivitas transaksi, penggunaan aplikasi, interaksi media sosial, lokasi, dan berbagai sumber lainnya. Kemampuan tersebut memberikan manfaat bagi layanan digital, tetapi juga meningkatkan risiko apabila data digunakan tanpa dasar yang sah atau tanpa perlindungan yang memadai.

Hak atas privasi tidak berarti bahwa seluruh informasi mengenai seseorang harus selalu dirahasiakan. Dalam masyarakat digital, terdapat kebutuhan tertentu untuk mengumpulkan dan memproses data. Persoalannya terletak pada bagaimana menentukan batas yang sah antara kepentingan penggunaan data dan hak individu. Prinsip kebutuhan, proporsionalitas, transparansi, serta akuntabilitas menjadi penting dalam menentukan batas tersebut (Allahrakha, 2025; Tan dkk., 2026).

Kebebasan berekspresi juga mengalami perubahan dalam ruang digital. Media sosial memungkinkan seseorang menyampaikan pendapat kepada publik tanpa harus memiliki akses terhadap media konvensional. Kondisi tersebut memperluas partisipasi publik, tetapi juga menimbulkan persoalan mengenai konten yang merugikan, ujaran kebencian, disinformasi, dan pelanggaran privasi. Pembatasan terhadap ekspresi harus dilakukan secara hati-hati agar tidak berubah menjadi pembatasan yang berlebihan terhadap kebebasan masyarakat.

Hubungan antara kebebasan berekspresi dan privasi sering kali tidak sederhana. Informasi yang benar mengenai seseorang belum tentu selalu dapat disebarluaskan tanpa batas. Sebaliknya, hak atas privasi tidak selalu dapat digunakan untuk menghapus informasi yang memiliki kepentingan publik. Konflik tersebut menunjukkan bahwa perlindungan hak digital membutuhkan mekanisme penyeimbangan yang mempertimbangkan konteks dan proporsionalitas (C'orac, 2025; Okonkwo, 2025).

Persoalan tersebut dapat dilihat dalam perkembangan konsep hak untuk dilupakan. Informasi digital memiliki karakter persisten karena dapat disalin, disimpan, dan disebarluaskan kembali. Kesalahan atau informasi lama yang dahulu mudah hilang dapat tetap muncul melalui mesin pencari atau platform digital. Hak untuk dilupakan kemudian menjadi salah satu bentuk upaya menyeimbangkan perlindungan privasi dengan kepentingan publik

terhadap informasi. Perkembangan yurisprudensi Eropa memperlihatkan bahwa keseimbangan tersebut terus mengalami perkembangan (C' orac, 2025).

Hak digital juga berkaitan dengan akses terhadap informasi. Internet telah menjadi salah satu sarana penting untuk memperoleh pengetahuan, pendidikan, layanan, dan berpartisipasi dalam kehidupan publik. Pembatasan akses terhadap internet atau informasi tertentu dapat memiliki konsekuensi terhadap hak masyarakat. Namun, akses tersebut juga perlu ditempatkan dalam kerangka keamanan dan perlindungan terhadap hak pihak lain.

Tantangan baru muncul melalui penggunaan algoritme. Keputusan yang berdampak terhadap individu dapat dibuat atau dipengaruhi oleh sistem otomatis. Algoritme dapat digunakan untuk menentukan iklan yang ditampilkan, menilai kelayakan seseorang, menyaring konten, atau memberikan rekomendasi. Ketika keputusan tersebut mengandung bias, individu dapat mengalami perlakuan yang tidak adil tanpa memahami bagaimana keputusan tersebut dibuat. Perlindungan hak digital karena itu perlu mencakup akuntabilitas terhadap sistem teknologi yang digunakan.

Persoalan diskriminasi algoritmik menunjukkan bahwa perlindungan hak tidak cukup bergantung pada persetujuan formal. Seseorang mungkin telah menyetujui penggunaan layanan digital, tetapi persetujuan tersebut tidak selalu

berarti bahwa seluruh proses pengolahan data atau keputusan algoritmik dapat dibenarkan. Perlindungan yang efektif membutuhkan transparansi, mekanisme pengawasan, dan kemampuan untuk meminta pertanggungjawaban ketika teknologi menghasilkan kerugian (Campione, 2025; Firdaus dkk., 2025; Gulyaeva dkk., 2025).

Institusi pengawas memiliki peran penting dalam memastikan perlindungan hak digital. Pengawasan perlu dilakukan secara independen, transparan, dan berdasarkan prinsip kebutuhan serta proporsionalitas. Mekanisme pengaduan dan pemulihan juga harus tersedia bagi individu yang haknya dilanggar. Perlindungan hak digital tidak akan efektif apabila masyarakat tidak memiliki cara untuk memperoleh pemulihan ketika terjadi pelanggaran (Nur dkk., 2026; Tan dkk., 2026).

Keamanan digital juga harus ditempatkan sebagai bagian dari perlindungan hak. Kebocoran data, pencurian identitas, atau akses ilegal terhadap informasi dapat mengganggu kehidupan individu secara nyata. Karena itu, keamanan dan kebebasan tidak selalu berada dalam posisi yang berlawanan. Keduanya perlu ditempatkan dalam hubungan yang seimbang. Keamanan diperlukan untuk melindungi hak, tetapi tindakan keamanan juga harus dibatasi agar tidak menghasilkan pengawasan atau pembatasan yang tidak proporsional (Allahrakha, 2025).

Dengan demikian, hak asasi manusia dalam ruang digital membutuhkan pendekatan yang lebih

substantif. Perlindungan tidak cukup dilakukan melalui pengakuan formal terhadap hak, tetapi harus memastikan adanya mekanisme nyata untuk menjaga hak tersebut. Privasi, kebebasan berekspresi, akses informasi, keamanan, dan perlindungan data merupakan bagian dari ekosistem hak digital yang saling berhubungan (AlDesouki, 2024; Okonkwo, 2025).

4. **Teori Kedaulatan, Yurisdiksi, dan Tanggung Jawab Hukum di Ruang Siber**

Ruang siber menantang konsep kedaulatan negara karena aktivitas digital tidak selalu mengikuti batas wilayah. Dalam sistem konvensional, negara memiliki kewenangan yang relatif jelas terhadap wilayah, penduduk, dan aktivitas yang berlangsung di dalam wilayahnya. Dalam ruang digital, batas tersebut menjadi lebih kompleks karena sistem dan data dapat tersebar di berbagai negara. Kondisi tersebut menyebabkan penerapan hukum nasional terhadap aktivitas digital sering kali membutuhkan pertimbangan lintas yurisdiksi (Allahrakha, 2025; Asyari, 2023; Hefjullah, 2025).

Kedaulatan dalam ruang siber karena itu tidak lagi dapat dipahami semata-mata sebagai penguasaan teritorial. Negara tetap memiliki kepentingan untuk melindungi sistem, data, masyarakat, dan infrastruktur yang berada dalam wilayahnya. Namun, pelaksanaan kepentingan tersebut harus berhadapan dengan kenyataan bahwa teknologi bekerja melalui jaringan global. Kedaulatan siber kemudian berkembang menjadi konsep yang

lebih kompleks dan berlapis (Hefjullah, 2025; Lazari, 2025).

Persoalan yurisdiksi muncul ketika suatu peristiwa memiliki hubungan dengan lebih dari satu negara. Misalnya, seorang pelaku berada di negara A, korban berada di negara B, server berada di negara C, sedangkan penyedia platform berkedudukan di negara D. Negara mana yang berwenang menyelidiki? Hukum negara mana yang berlaku? Bagaimana bukti diperoleh dari negara lain? Pertanyaan tersebut menunjukkan bahwa yurisdiksi siber tidak dapat ditentukan hanya berdasarkan lokasi pelaku.

Persoalan semakin kompleks ketika hukum negara-negara yang terlibat memiliki ketentuan berbeda. Suatu tindakan dapat dianggap sah di satu negara tetapi melanggar hukum di negara lain. Perbedaan tersebut dapat menciptakan konflik norma dan menghambat penegakan hukum. Fragmentasi interpretasi juga dapat mengurangi prediktabilitas hukum internasional dalam menghadapi operasi siber (Çora & Mikail, 2026).

Hukum internasional karena itu menghadapi kebutuhan untuk memberikan kerangka yang dapat menjelaskan tindakan negara di ruang siber. Perdebatan tidak lagi berhenti pada pertanyaan apakah hukum internasional berlaku di ruang siber, tetapi beralih pada bagaimana konsep kedaulatan, non-intervention, *due diligence*, atribusi, dan ambang serangan siber diterapkan dalam konteks digital (Çora & Mikail, 2026; Lazari, 2025).

Atribusi menjadi salah satu persoalan yang sangat penting. Dalam serangan siber, identitas pelaku tidak selalu mudah diketahui. Pelaku dapat menggunakan perangkat yang telah dikompromikan, jaringan anonim, atau infrastruktur yang berada di negara lain. Negara yang menjadi korban kemudian menghadapi kesulitan untuk menentukan siapa yang sebenarnya bertanggung jawab. Kesalahan atribusi dapat menimbulkan konsekuensi hukum dan politik yang serius.

Konsep *due diligence* juga menjadi penting. Negara memiliki kepentingan untuk memastikan bahwa wilayah atau infrastrukturnya tidak digunakan untuk melakukan tindakan yang merugikan negara lain. Namun, menentukan batas kewajiban tersebut dalam lingkungan digital tidak mudah. Negara mungkin tidak mengetahui seluruh aktivitas yang dilakukan melalui sistem yang berada dalam wilayahnya. Karena itu, standar kewajiban negara dalam mencegah atau merespons aktivitas siber lintas batas membutuhkan interpretasi yang hati-hati.

Persoalan yurisdiksi juga berkaitan dengan bukti elektronik. Bukti dapat tersimpan pada server yang berada di luar negara tempat penyidikan dilakukan. Aparat membutuhkan mekanisme hukum untuk memperoleh data tersebut tanpa melanggar kedaulatan negara lain. Prosedur bantuan hukum timbal balik dan kerja sama antarotoritas menjadi penting dalam kondisi semacam ini.

Tanggung jawab hukum juga harus ditentukan berdasarkan peran masing-masing aktor. Pelaku serangan tentu dapat memiliki tanggung jawab atas tindakannya. Namun, dalam ekosistem digital terdapat pula penyedia platform, penyedia infrastruktur, pengelola data, dan pihak ketiga lainnya. Tidak setiap kerugian dapat secara otomatis dibebankan kepada semua pihak. Hukum perlu menentukan hubungan antara tindakan, kewajiban, kelalaian, dan akibat yang ditimbulkan.

Kedaulatan digital karena itu membutuhkan pendekatan kooperatif. Negara tetap mempertahankan kewenangan hukumnya, tetapi pelaksanaan kewenangan tersebut harus mempertimbangkan kebutuhan kerja sama. Pertukaran informasi, penyelarasan aturan, kerja sama penyidikan, serta mekanisme penyelesaian sengketa dapat menjadi instrumen untuk mengurangi konflik yurisdiksi (Hefjullah, 2025; Lazari, 2025; Zhuang, 2026).

Harmonisasi hukum menjadi semakin penting karena ancaman digital tidak mengenal batas negara. Jika setiap negara menerapkan standar yang sepenuhnya berbeda, pelaku dapat memanfaatkan perbedaan tersebut untuk menghindari pertanggungjawaban. Harmonisasi tidak selalu berarti semua negara harus memiliki hukum yang identik. Harmonisasi dapat dilakukan melalui kesamaan prinsip, prosedur kerja sama, standar pembuktian, dan mekanisme penegakan tertentu.

Kerja sama internasional juga harus mempertimbangkan perlindungan hak. Upaya memperoleh data atau melakukan tindakan penegakan hukum lintas batas tidak boleh mengabaikan privasi dan hak individu. Kebutuhan penegakan hukum harus diseimbangkan dengan prinsip proporsionalitas dan perlindungan hak. Dengan demikian, kerja sama siber tidak hanya menjadi persoalan efektivitas penegakan, tetapi juga legitimasi tindakan negara.

Persoalan kedaulatan, yurisdiksi, dan tanggung jawab di ruang siber memperlihatkan keterbatasan pendekatan hukum yang hanya berorientasi teritorial. Ruang digital membutuhkan model hukum yang menggabungkan kewenangan nasional dengan kerja sama internasional. Kedaulatan tetap penting, tetapi penerapannya perlu disesuaikan dengan karakter jaringan digital yang saling terhubung (Asyari, 2023; Hefjullah, 2025).

Hukum siber masa depan dengan demikian perlu dibangun melalui kombinasi antara kepastian hukum nasional dan koordinasi internasional. Negara perlu memiliki aturan yang jelas mengenai kewenangan, pertanggungjawaban, dan perlindungan masyarakat, sementara pada saat yang sama harus membangun mekanisme kerja sama dengan negara lain. Pendekatan tersebut memungkinkan hukum tetap memiliki kekuatan dalam wilayah nasional sekaligus mampu menghadapi aktivitas digital yang bersifat transnasional.

BAB III
YURISDIKSI TANPA BATAS: PROBLEMATIKA HUKUM LINTAS NEGARA DI DUNIA DIGITAL

1. Transformasi Konsep Yurisdiksi dalam Ruang Siber

Yurisdiksi pada dasarnya merupakan kewenangan negara untuk mengatur suatu perbuatan, menentukan hukum yang berlaku, mengadili sengketa atau tindak pidana, serta menjalankan keputusan hukum terhadap pihak yang berada dalam lingkup kewenangannya. Dalam konstruksi hukum konvensional, kewenangan tersebut sangat erat dengan wilayah. Negara memiliki kemampuan untuk mengatur karena negara memiliki kedaulatan atas wilayah tertentu, sedangkan individu dan badan hukum pada umumnya dapat ditempatkan secara geografis. Hubungan antara kewenangan dan wilayah tersebut menjadikan prinsip teritorialitas sebagai salah satu fondasi utama yurisdiksi. Ruang siber mengubah situasi tersebut tanpa benar-benar menghilangkan prinsip teritorialitas. Aktivitas digital dapat berlangsung melalui jaringan yang melewati beberapa negara, menggunakan infrastruktur yang tersebar, melibatkan pihak yang berada di lokasi

berbeda, serta menimbulkan akibat hukum di tempat yang tidak sama dengan lokasi pelaku. Karakter ruang siber yang demikian membuat prinsip teritorialitas tetap diperlukan, tetapi tidak lagi cukup untuk menjelaskan seluruh hubungan hukum yang terbentuk (Allahrakha, 2024; Situmeang dkk., 2026; Tebenkova, 2024).

Bayangkan seseorang yang berada di suatu negara mengakses sistem komputer milik perusahaan yang berada di negara lain. Serangan tersebut menggunakan perangkat yang telah dikendalikan dari negara ketiga dan memanfaatkan layanan *Cloud computing* yang dikelola perusahaan teknologi global. Data yang dicuri kemudian digunakan untuk menimbulkan kerugian terhadap konsumen di negara keempat. Dalam peristiwa seperti itu, sulit menunjuk satu tempat sebagai lokasi tunggal terjadinya perbuatan. Pelaku berada di satu wilayah, sistem yang menjadi sasaran berada di wilayah lain, infrastruktur perantara berada di tempat berbeda, sedangkan kerugian muncul pada wilayah korban. Peristiwa tersebut menunjukkan bahwa ruang digital menciptakan hubungan hukum yang bersifat multilokasi. Negara tidak lagi berhadapan dengan tindakan yang secara sederhana dapat ditempatkan pada satu titik geografis, tetapi dengan rangkaian tindakan yang tersebar di beberapa yurisdiksi.

Karakter multilokasi tersebut menjadikan persoalan *locus delicti* semakin kompleks. Dalam kejahatan konvensional, tempat terjadinya perbuatan

dan tempat timbulnya akibat sering kali dapat ditemukan secara fisik. Kejahatan siber tidak selalu memiliki karakter yang sama. Lokasi pelaku, lokasi perangkat yang digunakan, lokasi server yang ditembus, lokasi korban, lokasi penyedia platform, dan lokasi munculnya kerugian dapat berbeda. Bahkan, beberapa unsur tersebut dapat berpindah atau berubah selama proses berlangsung. Karena itu, *locus delicti* dalam kejahatan siber tidak selalu dapat dipahami sebagai satu lokasi fisik. Ia dapat memiliki beberapa titik relevansi hukum yang masing-masing memberikan dasar bagi klaim yurisdiksi (Islami, 2025; Tobing & Fitria, 2025).

Persoalan menjadi lebih rumit ketika data berada dalam sistem *cloud*. Pengguna dapat mengunggah data melalui perangkat yang berada di Indonesia, tetapi data tersebut mungkin diproses melalui beberapa pusat data yang terletak di negara berbeda. Penyedia layanan bahkan dapat mengubah lokasi pemrosesan secara otomatis berdasarkan kebutuhan teknis. Akibatnya, lokasi fisik data tidak selalu diketahui oleh pengguna dan tidak selalu dapat ditentukan secara cepat oleh aparat penegak hukum. Kondisi ini menunjukkan bahwa hubungan antara data dan wilayah semakin berbeda dari hubungan antara benda fisik dan lokasi. Data dapat berpindah tanpa perpindahan fisik manusia dan dapat digunakan secara simultan dari berbagai tempat. Persoalan *Cloud computing* karena itu menjadi salah satu contoh paling jelas mengenai keterbatasan

konsep yurisdiksi yang hanya bertumpu pada lokasi geografis (Glasze dkk., 2022).

Meskipun demikian, munculnya ruang siber tidak berarti bahwa negara kehilangan kewenangan teritorialnya. Prinsip teritorialitas tetap menjadi dasar penting karena negara memiliki tanggung jawab untuk melindungi masyarakat, infrastruktur, dan kepentingan hukumnya. Apabila sistem pemerintahan suatu negara diserang, negara tersebut memiliki kepentingan yang kuat untuk melakukan penyelidikan dan penegakan hukum, meskipun pelaku berada di luar wilayahnya. Demikian pula apabila konsumen di suatu negara mengalami kerugian dari transaksi digital yang dilakukan dengan perusahaan asing. Hubungan antara aktivitas digital dan wilayah negara masih dapat menjadi dasar yurisdiksi. Yang berubah adalah cara menentukan apakah hubungan tersebut cukup kuat untuk memberikan kewenangan kepada negara tertentu (Situmeang dkk., 2026; Tebenkova, 2024).

Dalam konteks tersebut, yurisdiksi tidak lagi hanya berbicara mengenai pertanyaan "di mana tindakan dilakukan", tetapi juga mengenai "dengan negara mana tindakan tersebut memiliki hubungan hukum yang substansial". Pertanyaan kedua menjadi semakin penting dalam ruang digital. Lokasi pelaku tetap relevan, tetapi bukan satu-satunya faktor. Lokasi korban, tempat timbulnya kerugian, tujuan aktivitas, pasar yang dituju, kewarganegaraan para pihak, lokasi infrastruktur, dan hubungan ekonomi dapat menjadi dasar pertimbangan. Pergeseran ini

menunjukkan bahwa penerapan yurisdiksi dalam ruang siber membutuhkan pendekatan yang lebih fungsional. Negara perlu melihat keseluruhan hubungan hukum yang terbentuk daripada hanya mencari satu lokasi fisik.

Dari sini muncul konsep yurisdiksi konkuren. Beberapa negara dapat memiliki dasar yang sama-sama kuat untuk menyatakan dirinya berwenang. Dalam sebuah serangan siber, negara tempat pelaku berada dapat mengklaim yurisdiksi berdasarkan teritorialitas. Negara korban dapat mengklaim kewenangan karena sistem atau masyarakatnya menjadi sasaran. Negara tempat server berada dapat memiliki hubungan dengan infrastruktur yang digunakan. Apabila perusahaan teknologi yang menyediakan layanan berada di negara lain, negara tersebut juga dapat memiliki dasar kewenangan tertentu. Situasi seperti ini tidak otomatis berarti bahwa salah satu negara telah melakukan pelanggaran. Persoalan sebenarnya adalah bagaimana menentukan penggunaan kewenangan tersebut secara proporsional dan bagaimana mencegah konflik antarnegara (Allahrakha, 2024; Situmeang dkk., 2026).

Yurisdiksi konkuren bahkan dapat memberikan manfaat apabila dikelola dengan baik. Keberadaan lebih dari satu dasar yurisdiksi dapat memperluas kemungkinan korban memperoleh perlindungan hukum. Namun, tanpa koordinasi, kondisi tersebut dapat berubah menjadi sumber ketidakpastian. Dua negara dapat melakukan

penyidikan terhadap perkara yang sama, dua pengadilan dapat memeriksa sengketa yang sama, atau dua sistem hukum dapat menghasilkan konsekuensi yang berbeda. Pelaku juga dapat memanfaatkan perbedaan tersebut untuk mencari yurisdiksi yang dianggap paling menguntungkan. Karena itu, persoalan yurisdiksi digital bukan hanya persoalan memperluas kewenangan, tetapi juga membangun mekanisme untuk mengelola kewenangan yang saling bertumpang tindih.

Pembatasan menjadi penting karena kemampuan teknologi untuk menjangkau suatu wilayah tidak seharusnya secara otomatis menghasilkan yurisdiksi tanpa batas. Hampir setiap situs internet dapat diakses dari berbagai negara. Jika akses saja sudah cukup untuk menciptakan yurisdiksi, pelaku usaha digital akan menghadapi kemungkinan tunduk pada hukum hampir semua negara di dunia. Situasi tersebut akan menciptakan ketidakpastian dan dapat menghambat aktivitas ekonomi digital. Karena itu, perlu dibedakan antara sekadar dapat diakses dan aktivitas yang memang diarahkan kepada masyarakat atau pasar suatu negara. Perbedaan tersebut kemudian menjadi dasar penting dalam menentukan hubungan hukum yang relevan dalam aktivitas digital lintas negara.

Transformasi konsep yurisdiksi juga memperlihatkan bahwa hukum harus membedakan antara kewenangan untuk membuat aturan, kewenangan untuk mengadili, dan kewenangan untuk menegakkan hukum. Ketiganya dapat memiliki

persoalan yang berbeda. Negara mungkin memiliki dasar untuk mengatur suatu aktivitas, tetapi belum tentu dapat mengambil tindakan penegakan secara langsung di wilayah negara lain. Aparat penegak hukum suatu negara tidak dapat begitu saja memasuki sistem komputer yang berada di wilayah negara lain tanpa memperhatikan hukum internasional dan kedaulatan negara tersebut. Pemisahan antara *prescriptive jurisdiction*, *adjudicative jurisdiction*, dan *enforcement jurisdiction* menjadi penting untuk mencegah perluasan kewenangan yang tidak terkendali.

Persoalan tersebut memperlihatkan bahwa ruang siber bukan ruang tanpa hukum. Sebaliknya, semakin luas aktivitas digital, semakin besar kebutuhan terhadap aturan yang menentukan kapan suatu negara berwenang. Hukum internasional tetap mengakui teritorialitas sebagai dasar utama, tetapi aktivitas siber menunjukkan keterbatasan teritorialitas ketika lokasi tindakan tidak mudah ditentukan. Karena itu, transformasi yurisdiksi seharusnya tidak dipahami sebagai penghapusan batas negara, melainkan sebagai proses menyesuaikan cara hukum memahami hubungan antara tindakan digital dan kewenangan negara.

Persoalan yurisdiksi siber terletak pada ketegangan antara teknologi yang bersifat global dan hukum yang masih banyak disusun berdasarkan batas wilayah. Negara tetap menjadi aktor utama dalam hukum, tetapi aktivitas digital membuat hubungan hukum semakin tersebar. Model yurisdiksi

yang mampu menjawab keadaan tersebut harus mempertahankan prinsip teritorialitas sekaligus membuka ruang bagi pendekatan berbasis akibat, kewarganegaraan, kepentingan negara, dan hubungan substantif dengan aktivitas digital. Arah tersebut akan menjadi dasar untuk memahami persoalan berikutnya, yaitu ketika beberapa negara tidak hanya sama-sama mengklaim kewenangan, tetapi juga menerapkan hukum yang berbeda terhadap aktivitas digital yang sama.

2. Konflik Yurisdiksi dan Hukum yang Berlaku dalam Transaksi serta Aktivitas Digital Lintas Negara

Sebuah transaksi digital dapat berlangsung tanpa mempertemukan para pihak secara fisik. Konsumen dapat berada di Indonesia, perusahaan berada di Singapura, pembayaran diproses melalui perusahaan di Amerika Serikat, dan data transaksi dikelola melalui infrastruktur *cloud* di negara lain. Dari sudut pandang teknologi, rangkaian tersebut dapat berlangsung dalam hitungan detik. Dari sudut pandang hukum, rangkaian yang sama menciptakan sejumlah pertanyaan: negara mana yang memiliki kewenangan, hukum mana yang berlaku, dan pengadilan mana yang harus menyelesaikan sengketa? Pertanyaan tersebut menunjukkan bahwa persoalan yurisdiksi tidak dapat dipisahkan dari persoalan *conflict of laws*. Satu aktivitas digital dapat memiliki hubungan dengan beberapa sistem hukum sekaligus (Allahrakha, 2024; Taufiqurokhman dkk., 2025; Wu, 2025).

Dalam perdagangan elektronik, persoalan tersebut menjadi semakin nyata karena sebuah perusahaan dapat menawarkan produk kepada konsumen di berbagai negara tanpa membangun kehadiran fisik di masing-masing negara. Situs atau aplikasi dapat diakses dari hampir seluruh dunia. Namun, kemampuan untuk mengakses suatu situs tidak selalu berarti bahwa perusahaan tersebut menargetkan pasar di negara tertentu. Jika akses semata-mata dijadikan dasar yurisdiksi, perusahaan digital akan menghadapi kemungkinan tunduk pada hukum setiap negara tempat situsnya dapat dibuka. Karena itu, hukum membutuhkan kriteria yang lebih substantif untuk menentukan hubungan antara perusahaan dan pasar tertentu.

Pendekatan *directed activity* atau *targeting* menjadi penting dalam keadaan tersebut. Pertanyaan yang perlu diajukan bukan hanya apakah konsumen dapat mengakses situs, tetapi apakah pelaku usaha memang mengarahkan aktivitasnya kepada konsumen di negara tersebut. Penggunaan mata uang lokal, bahasa tertentu, metode pembayaran lokal, layanan pengiriman ke wilayah tertentu, iklan yang secara khusus diarahkan kepada pengguna suatu negara, serta penawaran produk yang disesuaikan dengan pasar tertentu dapat menunjukkan adanya hubungan yang lebih kuat. Pendekatan semacam ini memberikan batas yang lebih rasional antara akses global dan aktivitas ekonomi yang sengaja diarahkan kepada yurisdiksi tertentu (Taufiqurokhman dkk., 2025; Wu, 2025).

Konflik yurisdiksi menjadi semakin sulit ketika transaksi tersebut menghasilkan sengketa konsumen. Konsumen pada umumnya tidak memiliki kekuatan negosiasi yang sama dengan perusahaan digital. Syarat dan ketentuan biasanya disusun oleh pelaku usaha dan ditampilkan dalam bentuk kontrak elektronik yang harus diterima sebelum transaksi berlangsung. Di dalamnya dapat terdapat klausul yang menentukan hukum negara tertentu dan pengadilan tertentu sebagai forum penyelesaian sengketa. Secara formal, konsumen telah menyetujui klausul tersebut. Namun, persetujuan formal tidak selalu berarti bahwa konsumen benar-benar memiliki kebebasan untuk memilih. Dalam keadaan tertentu, klausul *choice of law* dan *jurisdiction clause* justru dapat digunakan untuk menjauhkan konsumen dari perlindungan hukum di negara tempat ia tinggal (Christopher & Fitria, 2026).

Di sinilah prinsip *party autonomy* perlu ditempatkan secara proporsional. Kebebasan para pihak untuk memilih hukum dan forum merupakan bagian penting dari kepastian kontraktual, terutama dalam hubungan bisnis internasional. Pelaku usaha membutuhkan kepastian mengenai hukum yang akan digunakan, sedangkan para pihak perlu mengetahui forum yang tersedia apabila terjadi sengketa. Namun, kebebasan tersebut tidak dapat digunakan untuk menghilangkan norma perlindungan yang bersifat wajib. Dalam kontrak konsumen, hukum perlu mempertimbangkan ketimpangan posisi para pihak. Perlindungan konsumen dapat menjadi batas

terhadap kebebasan kontraktual apabila pilihan hukum atau forum digunakan untuk menghindari kewajiban yang seharusnya tetap berlaku (Christopher & Fitria, 2026; Taufiqurokhman dkk., 2025; Wu, 2025).

Masalah yang serupa muncul pada layanan *cloud computing*. Data perusahaan atau konsumen dapat disimpan melalui sistem yang tersebar di berbagai negara. Apabila terjadi kebocoran data, kehilangan data, atau pelanggaran keamanan, pihak yang dirugikan mungkin tidak mengetahui di mana data sebenarnya diproses. Kontrak layanan dapat menunjuk hukum negara penyedia layanan, sedangkan hukum perlindungan data di negara pengguna dapat menetapkan kewajiban berbeda. Persoalan tersebut memperlihatkan bahwa lokasi server tidak selalu menjadi jawaban atas pertanyaan hukum. Hubungan kontraktual, lokasi pengguna, lokasi perusahaan, jenis data, dan akibat yang timbul harus dianalisis secara bersama-sama (Glasze dkk., 2022).

Perbedaan hukum nasional juga dapat menciptakan keadaan ketika suatu tindakan diwajibkan oleh satu negara tetapi dibatasi oleh negara lain. Misalnya, suatu negara dapat mengharuskan perusahaan menyerahkan data kepada aparat penegak hukum, sementara negara tempat perusahaan menyimpan data memiliki aturan perlindungan privasi yang membatasi pengungkapan data tersebut. Perusahaan kemudian berada di antara dua kewajiban hukum. Jika mematuhi negara

pertama, perusahaan dapat melanggar hukum negara kedua. Jika mematuhi negara kedua, perusahaan dapat dianggap tidak memenuhi perintah hukum negara pertama. Situasi semacam ini memperlihatkan bahwa konflik yurisdiksi dapat berkembang menjadi konflik kewajiban hukum yang nyata.

Teknologi penyelesaian sengketa daring menawarkan kemungkinan untuk mengurangi persoalan tersebut. *Online dispute resolution* dapat menyediakan mekanisme penyelesaian yang tidak bergantung sepenuhnya pada keberadaan fisik para pihak. Bagi transaksi bernilai kecil, mekanisme tersebut dapat menjadi lebih rasional daripada membawa sengketa ke pengadilan asing. Kontrak digital juga dapat dirancang dengan klausul yang lebih transparan mengenai hukum dan forum. Dalam perkembangan tertentu, *hybrid forums* dan teknologi seperti *blockchain* dapat digunakan untuk mendukung kepastian proses. Namun, teknologi tidak menggantikan kebutuhan akan aturan mengenai pengakuan dan pelaksanaan hasil penyelesaian sengketa lintas negara (Kirani & Lie, 2026; Wu, 2025).

Oleh karena itu, konflik hukum dalam aktivitas digital membutuhkan keseimbangan antara kebebasan para pihak dan kepentingan publik. Hukum tidak dapat memaksa seluruh transaksi digital tunduk pada satu sistem hukum global karena perbedaan kepentingan negara masih nyata. Namun, membiarkan setiap negara menerapkan aturan

sendiri tanpa mekanisme koordinasi juga akan menghasilkan fragmentasi. Harmonisasi tidak harus menghilangkan seluruh perbedaan hukum, tetapi perlu memastikan bahwa perbedaan tersebut tidak menghalangi pengakuan kewenangan, perlindungan konsumen, dan pelaksanaan putusan.

Konflik yurisdiksi bukan sekadar persoalan teknis mengenai forum pengadilan. Ia menyentuh pertanyaan yang lebih mendasar tentang siapa yang berhak mengatur hubungan digital dan bagaimana kepentingan berbagai negara harus diseimbangkan. Jika negara terlalu mudah mengklaim yurisdiksi, aktivitas digital menjadi penuh ketidakpastian. Jika negara terlalu berhati-hati, korban dapat kehilangan perlindungan ketika pelaku berada di luar negeri. Jalan tengahnya terletak pada penentuan hubungan hukum yang nyata, pembatasan kewenangan yang proporsional, dan kerja sama antarnegara.

3. Kejahatan Siber Lintas Negara dan Problematika Penegakan Hukum

Kejahatan siber memperlihatkan secara nyata bahwa kemampuan teknologi dapat bergerak jauh lebih cepat daripada kemampuan hukum untuk merespons. Pelaku tidak perlu hadir di negara korban untuk melakukan serangan. Sebuah komputer dapat digunakan dari satu negara untuk mengendalikan perangkat di negara kedua, menerobos sistem di negara ketiga, dan mencuri data korban yang berada di negara keempat. Dalam beberapa kasus, pelaku bahkan dapat menyembunyikan jejaknya dengan menggunakan perangkat atau server milik pihak lain.

Kejahatan akhirnya tidak memiliki satu lokasi yang mudah ditunjuk. Karakter transnasional tersebut membuat penegakan hukum membutuhkan kerja sama lintas negara sejak tahap penyelidikan sampai pelaksanaan putusan (Praja, 2026; Situmeang dkk., 2026).

Hambatan pertama muncul ketika aparat harus menentukan siapa sebenarnya pelaku. Identitas digital tidak selalu identik dengan identitas fisik. Alamat *Internet Protocol* (IP) atau *Internet Protocol Address*, akun, perangkat, atau server yang digunakan dalam suatu serangan belum tentu secara langsung menunjukkan orang yang mengendalikan aktivitas tersebut. Pelaku dapat menggunakan jaringan yang telah diretas, identitas palsu, layanan anonim, atau infrastruktur yang berada di negara lain. Karena itu, atribusi membutuhkan rangkaian bukti yang mampu menghubungkan tindakan digital dengan individu atau kelompok tertentu. Kesalahan atribusi dapat mengakibatkan penegakan hukum diarahkan kepada pihak yang sebenarnya tidak bertanggung jawab.

Setelah identitas pelaku mulai diketahui, persoalan berikutnya adalah keberadaan bukti. Bukti elektronik dapat tersimpan pada komputer korban, perangkat pelaku, server perusahaan, layanan *cloud*, platform media sosial, atau penyedia jasa internet. Masing-masing pihak dapat berada dalam yurisdiksi yang berbeda. Penyidik tidak dapat secara bebas mengambil data yang berada di negara lain tanpa memperhatikan hukum negara tempat data tersebut

berada. Prinsip kedaulatan menjadi batas penting bagi tindakan penegakan hukum lintas negara. Aparat suatu negara tidak dapat memperlakukan wilayah digital negara lain seolah-olah merupakan bagian dari wilayah hukumnya sendiri.

Karakter data digital juga menimbulkan persoalan tersendiri. Data dapat diubah, dipindahkan, dihapus, atau ditimpa dalam waktu singkat. Sistem tertentu juga menggunakan kebijakan retensi data yang berbeda. Data yang dibutuhkan penyidik mungkin tidak lagi tersedia ketika permintaan resmi telah sampai kepada penyedia layanan. Pada saat yang sama, negara tempat data berada dapat mensyaratkan prosedur tertentu sebelum data dapat diberikan kepada aparat negara asing. Perbedaan mengenai retensi, autentikasi, privasi, *chain of custody*, dan *admissibility* dapat menentukan apakah bukti tersebut akhirnya dapat digunakan di pengadilan (Chaudhary & Asghar, 2026; Solodovnik, 2026).

Masalah pembuktian tersebut memperlihatkan bahwa hukum acara memiliki kedudukan yang sangat penting dalam penanganan kejahatan siber. Memiliki aturan pidana yang melarang suatu perbuatan tidak cukup apabila aparat tidak memiliki kemampuan memperoleh bukti yang dibutuhkan. Penegakan hukum digital membutuhkan prosedur yang dapat bergerak cukup cepat mengikuti karakter bukti elektronik. Pada saat yang sama, kecepatan tersebut tidak boleh menghilangkan perlindungan terhadap privasi dan hak tersangka.

Tantangannya adalah menemukan prosedur yang memungkinkan data diperoleh secara efektif, tetapi tetap dapat dipertanggungjawabkan secara hukum.

Dalam penegakan hukum terhadap kejahatan siber lintas negara, persoalan yurisdiksi menjadi semakin kompleks ketika bukti elektronik, data, atau infrastruktur yang dibutuhkan berada di wilayah negara lain. Kondisi tersebut membuat negara tidak selalu dapat memperoleh bukti atau melakukan tindakan hukum secara langsung berdasarkan kewenangan nasionalnya. Oleh karena itu, diperlukan mekanisme kerja sama antarnegara yang mampu menghubungkan kebutuhan penyidikan dengan penghormatan terhadap kedaulatan masing-masing negara. Salah satu mekanisme yang memiliki fungsi tersebut adalah *Mutual Legal Assistance* (MLA), yang memungkinkan permintaan bantuan hukum dilakukan melalui otoritas negara terkait.

MLA menjadi salah satu instrumen penting untuk menjembatani persoalan tersebut. Melalui MLA, negara dapat meminta bantuan negara lain untuk memperoleh bukti, melakukan tindakan penyidikan tertentu, atau membantu proses penegakan hukum. Mekanisme ini menghormati kedaulatan negara karena tindakan dilakukan melalui otoritas negara yang memiliki kewenangan atas wilayahnya. Namun, prosedur MLA dapat memerlukan waktu yang panjang. Dalam perkara digital, keterlambatan beberapa hari bahkan dapat menentukan apakah suatu bukti masih tersedia atau sudah hilang. Karena itu, mekanisme kerja sama

perlu terus disesuaikan dengan kebutuhan penyidikan digital (Abdelkarim, 2025; Solodovnik, 2026).

Ekstradisi juga tidak selalu dapat menjadi solusi. Pelaku dapat berada di negara yang tidak memiliki perjanjian ekstradisi dengan negara korban. Perbedaan definisi tindak pidana dapat menimbulkan persoalan *dual criminality*. Negara tempat pelaku berada juga dapat memiliki aturan yang membatasi penyerahan warga negaranya. Pertimbangan mengenai hak asasi manusia dapat menjadi faktor tambahan. Karena itu, penanganan kejahatan siber transnasional membutuhkan kombinasi mekanisme, termasuk ekstradisi, MLA, transfer penuntutan, pertukaran informasi, dan kerja sama antarlembaga (Klevtsov, 2022; Situmeang dkk., 2026).

Pertanyaan mengenai *universal jurisdiction* juga perlu ditempatkan secara hati-hati. Tidak setiap kejahatan siber secara otomatis dapat menjadi dasar bagi semua negara untuk melakukan penuntutan. Penggunaan konsep tersebut tanpa dasar hukum internasional yang jelas dapat memperluas kewenangan secara berlebihan. Bahkan, literatur mengenai yurisdiksi kejahatan siber menunjukkan adanya perdebatan mengenai apakah pendekatan universal tepat diterapkan atau justru berpotensi menimbulkan persoalan kedaulatan dan konflik hukum (Abdelkarim, 2025; Situmeang dkk., 2026).

Perluasan yurisdiksi ekstrateritorial juga memiliki dua sisi. Di satu sisi, pendekatan tersebut

dapat membantu negara melindungi masyarakat ketika pelaku berada di luar negeri. Pendekatan berbasis akibat atau *effects-based jurisdiction* dapat memberikan dasar bagi negara korban untuk bertindak ketika serangan dari luar negeri menghasilkan dampak serius di wilayahnya. Di sisi lain, penggunaan yurisdiksi ekstrateritorial yang terlalu luas dapat menghasilkan tumpang tindih kewenangan dan konflik dengan negara tempat pelaku berada. Risiko tersebut bahkan dapat berkembang menjadi bentuk *legal imperialism* ketika negara dengan kapasitas ekonomi dan teknologi yang lebih besar memaksakan hukum dan standar penegakannya kepada negara lain (Allahrakha, 2024; Arnell & Faturoti, 2023; Praja, 2026).

Oleh karena itu, penegakan hukum terhadap kejahatan siber membutuhkan prinsip *reasonableness*. Negara harus memiliki alasan yang cukup untuk menggunakan yurisdiksinya dan mempertimbangkan kepentingan negara lain. Tindakan penegakan juga harus dilakukan melalui saluran yang sesuai dengan hukum internasional. Pendekatan ini tidak berarti negara harus pasif ketika menghadapi serangan siber, tetapi memastikan bahwa responsnya tidak menciptakan persoalan hukum yang lebih besar.

Persoalan penegakan hukum siber menunjukkan bahwa keberhasilan pemberantasan kejahatan digital tidak ditentukan hanya oleh kekuatan hukum pidana nasional. Kemampuan untuk bekerja sama, memperoleh bukti, menentukan

atribusi, mengeksekusi permintaan hukum, dan menjaga hak para pihak sama pentingnya. Dunia digital membuat pelaku dapat bergerak lintas negara dengan mudah, sehingga negara juga perlu membangun kemampuan hukum untuk bekerja lintas batas secara sah dan terkoordinasi.

4. **Kedaulatan Digital, Perlindungan Data, dan Tanggung Jawab Negara di Ruang Siber**

Kedaulatan pada mulanya dibangun berdasarkan penguasaan negara terhadap wilayah tertentu. Negara mengetahui batas wilayahnya, mengendalikan institusi di dalamnya, dan menetapkan aturan yang berlaku bagi masyarakat yang berada dalam wilayah tersebut. Digitalisasi mengubah sebagian asumsi tersebut. Infrastruktur yang digunakan masyarakat suatu negara dapat dimiliki perusahaan asing. Data warga negara dapat disimpan di pusat data negara lain. Platform yang digunakan untuk berkomunikasi dapat tunduk pada hukum negara berbeda. Bahkan, layanan digital yang sangat penting bagi kehidupan masyarakat dapat bergantung pada perusahaan yang secara geografis berada di luar jangkauan langsung negara. Keadaan tersebut melahirkan kebutuhan untuk memikirkan kembali bentuk kedaulatan dalam lingkungan digital (Farrand & Carrapico, 2022; Hutchinson dkk., 2024; Pohle dkk., 2025).

Kedaulatan digital tidak berarti bahwa negara memiliki "wilayah internet" yang dapat dipagari seperti wilayah daratan. Yang menjadi persoalan adalah kemampuan negara mempertahankan kendali

hukum terhadap kepentingan digital yang strategis. Data merupakan salah satu kepentingan tersebut. Data pribadi menggambarkan identitas dan perilaku individu. Data perusahaan berkaitan dengan kepentingan ekonomi. Data pemerintah dapat berkaitan dengan keamanan nasional. Semakin besar nilai data, semakin besar pula kepentingan negara untuk memastikan bahwa data tersebut tidak digunakan secara sewenang-wenang. Kedaulatan data kemudian berkembang sebagai konsep mengenai kemampuan mengendalikan bagaimana data dikumpulkan, diproses, disimpan, dipindahkan, dan digunakan (Hummel dkk., 2021; Hutchinson dkk., 2024).

Kendati demikian, data memiliki karakter yang berbeda dari benda fisik. Data dapat bergerak melintasi batas negara tanpa harus memindahkan objek secara fisik. Sebuah perusahaan dapat memproses data pengguna dari beberapa negara melalui satu sistem yang terintegrasi. Jika setiap negara mewajibkan seluruh data warga negaranya disimpan secara fisik di dalam negeri, biaya operasional dapat meningkat dan struktur ekonomi digital menjadi lebih terfragmentasi. Di sisi lain, arus data tanpa perlindungan dapat menciptakan risiko terhadap privasi, keamanan, dan kepentingan nasional. Kedaulatan data karena itu harus dipahami secara lebih kompleks daripada sekadar lokasi penyimpanan.

Persoalan tersebut melahirkan ketegangan antara kedaulatan dan globalisasi digital. Negara

membutuhkan kemampuan untuk melindungi masyarakatnya, tetapi ekonomi digital membutuhkan arus data lintas batas. Perusahaan global membutuhkan interoperabilitas, sedangkan negara membutuhkan kepastian bahwa data yang keluar dari wilayahnya tetap mendapatkan perlindungan. Fragmentasi aturan nasional dapat membebani perusahaan dan menghambat pertukaran informasi. Namun, harmonisasi yang terlalu lemah juga dapat membuat perlindungan data menjadi tidak efektif. Persoalannya bukan memilih antara kedaulatan atau globalisasi, melainkan menemukan bentuk kedaulatan yang dapat bekerja di dalam sistem global (Hutchinson dkk., 2024).

Kedaulatan digital juga berhubungan dengan keamanan nasional. Negara memiliki kepentingan untuk memastikan bahwa infrastruktur penting seperti sistem energi, keuangan, kesehatan, komunikasi, dan pemerintahan terlindungi dari serangan. Serangan terhadap infrastruktur tersebut dapat menimbulkan akibat yang jauh lebih besar daripada kerugian individual. Namun, menentukan siapa yang bertanggung jawab tidak selalu mudah. Serangan dapat berasal dari wilayah negara lain dan dilakukan oleh aktor nonnegara. Dalam kondisi tertentu, terdapat pula persoalan apakah suatu serangan dapat dikaitkan dengan negara tempat pelaku berada. Pertanyaan mengenai atribusi kemudian menjadi penting dalam menentukan tanggung jawab.

Tanggung jawab negara di ruang siber tidak dapat dilepaskan dari kewajiban menghormati kedaulatan negara lain. Sebuah negara tidak dapat menggunakan alasan keamanan nasional untuk melakukan tindakan yang secara tidak sah memasuki sistem digital negara lain. Pada saat yang sama, negara juga memiliki kepentingan untuk mencegah wilayahnya digunakan sebagai basis aktivitas yang merugikan negara lain. Prinsip *due diligence* menjadi relevan dalam membangun keseimbangan tersebut. Negara perlu mengambil langkah yang wajar untuk menangani ancaman yang berasal dari wilayah atau infrastrukturnya, tanpa berarti setiap tindakan individu otomatis menjadi tanggung jawab negara.

Kedaulatan juga berhadapan dengan perusahaan teknologi global. Sebuah platform dapat memiliki jutaan pengguna di Indonesia tanpa memiliki struktur perusahaan yang sepenuhnya berada di Indonesia. Pemerintah tetap memiliki kepentingan untuk memastikan bahwa platform tersebut menghormati hukum nasional, termasuk kewajiban perlindungan data dan keamanan digital. Namun, penerapan hukum terhadap perusahaan asing dapat menimbulkan konflik apabila hukum negara tempat perusahaan berkedudukan memberikan kewajiban yang berbeda. Persoalan tersebut menunjukkan bahwa kedaulatan digital juga membutuhkan mekanisme koordinasi antarnegara.

Perlindungan data tidak boleh dijadikan alasan untuk membangun sistem pengawasan tanpa batas. Negara memiliki kemampuan teknologi yang

semakin besar untuk mengakses, mengolah, dan menghubungkan data masyarakat. Kemampuan tersebut dapat membantu penegakan hukum dan keamanan, tetapi juga berpotensi mengancam privasi jika tidak dibatasi. Kedaulatan digital karena itu harus berjalan bersama prinsip negara hukum. Penggunaan data harus memiliki dasar hukum, tujuan yang jelas, mekanisme pengawasan, dan batas yang proporsional. Keamanan tidak boleh menghapus hak individu.

Pada sisi lain, perlindungan data juga tidak dapat hanya menjadi tanggung jawab negara. Perusahaan teknologi menguasai sebagian besar infrastruktur dan data yang digunakan masyarakat. Karena itu, tata kelola digital membutuhkan pembagian tanggung jawab antara negara, perusahaan, dan pengguna. Negara membentuk kerangka hukum dan melakukan pengawasan, perusahaan menerapkan standar keamanan dan perlindungan, sedangkan pengguna perlu memahami hak dan kewajibannya dalam menggunakan layanan digital.

Kedaulatan digital pada akhirnya harus dipahami sebagai kemampuan untuk mengatur dan melindungi kepentingan digital tanpa memutus hubungan dengan sistem global. Negara yang terlalu menutup diri akan menghadapi persoalan efisiensi dan interoperabilitas. Sebaliknya, negara yang menyerahkan seluruh kendali kepada aktor global akan menghadapi risiko ketergantungan. Jalan tengahnya adalah membangun kapasitas regulasi

nasional yang kuat sekaligus mengembangkan kerja sama internasional. Pendekatan tersebut memungkinkan kedaulatan tetap berfungsi dalam lingkungan digital yang saling terhubung.

5. Harmonisasi Hukum dan Masa Depan Tata Kelola Yurisdiksi Siber Internasional

Jika aktivitas digital dapat melewati batas negara dalam hitungan detik, hukum yang mengaturnya tidak dapat sepenuhnya berhenti pada batas negara. Negara tetap memiliki kewenangan untuk membuat hukum nasional, tetapi efektivitas hukum tersebut sering kali bergantung pada negara lain. Pelaku dapat berada di luar negeri, bukti dapat berada di server asing, korban dapat berada di negara berbeda, dan perusahaan penyedia layanan dapat tunduk pada hukum yurisdiksi lain. Kondisi tersebut membuat kerja sama internasional bukan lagi pilihan tambahan, melainkan bagian penting dari tata kelola hukum siber. Harmonisasi, *mutual recognition*, standardisasi bukti elektronik, dan kerja sama investigasi menjadi instrumen untuk mengurangi benturan antarhukum (Chaudhary & Asghar, 2026; Hutchinson dkk., 2024; Tobing & Fitria, 2025).

Harmonisasi tidak harus berarti setiap negara memiliki undang-undang yang sama. Perbedaan sistem hukum merupakan kenyataan yang tidak dapat dihapus begitu saja. Yang diperlukan adalah titik temu pada persoalan-persoalan yang memang membutuhkan kerja sama. Negara dapat memiliki definisi tertentu mengenai perlindungan data, tetapi perlu memiliki mekanisme yang

memungkinkan permintaan data lintas negara diproses secara sah. Negara dapat memiliki prosedur pidana yang berbeda, tetapi perlu memiliki cara untuk mengakui bukti elektronik yang diperoleh melalui proses hukum negara lain. Dengan demikian, harmonisasi lebih tepat dipahami sebagai pembangunan kompatibilitas antarhukum daripada penyeragaman total.

Bukti elektronik merupakan bidang yang membutuhkan harmonisasi paling mendesak. Penyidik membutuhkan kepastian mengenai cara meminta data, otoritas yang berwenang, jangka waktu penyimpanan, autentikasi, dan perlindungan terhadap integritas bukti. Tanpa standar yang cukup seragam, bukti yang diperoleh di satu negara dapat menghadapi persoalan ketika diajukan di pengadilan negara lain. Perbedaan *chain of custody*, standar autentikasi, retensi data, dan *admissibility* dapat memperlemah proses penuntutan (Chaudhary & Asghar, 2026; Solodovnik, 2026).

MLA menjadi bagian penting dari proses tersebut. Negara dapat meminta bantuan negara lain untuk memperoleh bukti atau melakukan tindakan hukum tertentu. Mekanisme ini menjaga prinsip kedaulatan karena tindakan penegakan dilakukan melalui otoritas negara yang bersangkutan. Namun, prosesnya harus cukup cepat untuk menghadapi karakter bukti digital. Jika prosedur terlalu lambat, data dapat hilang sebelum permintaan selesai diproses. Karena itu, perkembangan kerja sama internasional perlu memperhatikan kebutuhan

terhadap mekanisme yang lebih responsif (Abdelkarim, 2025; Solodovnik, 2026).

Kerja sama juga dapat dilakukan melalui mekanisme ekstradisi dan transfer penuntutan. Ekstradisi memungkinkan tersangka diserahkan kepada negara yang memiliki kewenangan untuk mengadili. Transfer penuntutan memungkinkan negara tempat tersangka berada melakukan proses hukum apabila terdapat dasar yang memadai. Masing-masing mekanisme memiliki kelebihan dan keterbatasan. Pilihan yang tepat bergantung pada hubungan yurisdiksi, hukum nasional, perjanjian internasional, dan perlindungan hak tersangka. Karena itu, tidak ada satu mekanisme yang dapat digunakan untuk seluruh jenis perkara siber (Klevtsov, 2022; Situmeang dkk., 2026).

Harmonisasi juga harus memperhatikan hak asasi manusia. Kemudahan pertukaran data dapat mempercepat penegakan hukum, tetapi dapat pula memperbesar risiko penyalahgunaan informasi pribadi. Negara yang menerima data harus memiliki jaminan bahwa data digunakan untuk tujuan yang sah dan tidak dialihkan secara sembarangan. Permintaan data lintas negara karena itu harus memiliki dasar hukum dan memenuhi prinsip kebutuhan serta proporsionalitas. Kerja sama yang efektif justru membutuhkan kepercayaan, dan kepercayaan hanya dapat dibangun apabila setiap negara mengetahui bahwa mekanisme kerja sama memiliki batas hukum yang jelas.

Dalam transaksi digital, harmonisasi dapat diarahkan pada penguatan ODR. Mekanisme penyelesaian sengketa daring dapat mengurangi biaya dan waktu, khususnya bagi sengketa konsumen. Namun, hasil ODR harus dapat diakui dan dilaksanakan di yurisdiksi lain. Klausul *choice of law* dan *choice of forum* juga perlu dirancang secara transparan. Penggunaan teknologi seperti *blockchain* dapat membantu menciptakan catatan transaksi yang lebih dapat diverifikasi, tetapi teknologi tersebut tidak dapat menggantikan kebutuhan terhadap dasar hukum yang menentukan kewenangan dan pelaksanaan putusan (Kirani & Lie, 2026; Wu, 2025).

Masa depan tata kelola yurisdiksi siber juga membutuhkan prinsip *due diligence*. Negara perlu memiliki kemampuan untuk mencegah wilayah atau infrastrukturnya digunakan sebagai tempat berlangsungnya aktivitas yang merugikan negara lain. Prinsip tersebut tidak berarti negara bertanggung jawab atas seluruh aktivitas digital yang berasal dari wilayahnya. Yang dibutuhkan adalah tindakan yang wajar sesuai dengan kemampuan dan kewajiban hukumnya. Pendekatan tersebut dapat menjadi jembatan antara kepentingan kedaulatan dan kebutuhan keamanan kolektif.

Perluasan yurisdiksi ekstrateritorial harus tetap dibatasi. Ketika negara menghadapi serangan dari luar wilayahnya, terdapat dorongan untuk memperluas kewenangan. Namun, tindakan unilateral yang memasuki wilayah hukum negara lain

dapat menimbulkan persoalan kedaulatan. Perdebatan mengenai yurisdiksi transnasional menunjukkan bahwa perluasan kewenangan perlu mempertimbangkan *reasonableness*, kepentingan negara lain, dan prinsip hukum internasional. Pendekatan yang tidak terkendali dapat menciptakan konflik dan bahkan risiko *legal imperialism* (Allahrakha, 2024; Arnell & Faturoti, 2023; Praja, 2026).

Masa depan hukum siber karena itu bukan terletak pada penciptaan satu "hukum internet dunia" yang menggantikan seluruh hukum nasional. Yang lebih realistis adalah membangun jaringan aturan yang saling terhubung. Hukum nasional tetap menjadi fondasi, sedangkan hukum internasional menyediakan prinsip dan mekanisme kerja sama. Negara mempertahankan kedaulatan, tetapi bersedia bekerja sama ketika suatu perkara melampaui batas wilayahnya. Perusahaan digital menjalankan kewajiban hukum, tetapi juga membutuhkan kepastian mengenai aturan yang berlaku. Masyarakat memperoleh perlindungan, tetapi tetap dapat menikmati manfaat arus informasi global.

Dengan demikian, harmonisasi hukum siber harus diarahkan pada tiga tujuan sekaligus. Pertama, menciptakan kepastian hukum sehingga pelaku usaha, pengguna, dan aparat mengetahui batas kewenangan masing-masing. Kedua, menciptakan efektivitas penegakan hukum sehingga pelaku tidak dapat berlindung hanya karena berada di negara lain. Ketiga, menciptakan perlindungan hak sehingga

kerja sama lintas negara tidak menjadi alasan untuk memperluas kewenangan secara tidak proporsional. Ketiga tujuan tersebut harus berjalan secara bersamaan.

Problematika yurisdiksi siber bukanlah ketiadaan hukum, melainkan benturan antara struktur hukum yang berbasis wilayah dengan teknologi yang bekerja melampaui wilayah. Pelaku, korban, server, platform, data, dan akibat hukum dapat tersebar di berbagai negara. Kondisi tersebut menuntut perubahan cara berpikir mengenai yurisdiksi. Teritorialitas tetap menjadi fondasi, tetapi harus dilengkapi dengan pendekatan yang mempertimbangkan hubungan substantif, akibat, kepentingan, dan kerja sama antarnegara. Masa depan tata kelola siber dengan demikian bergantung pada kemampuan negara membangun sistem yang tidak menghapus batas negara, tetapi mampu bekerja secara efektif ketika aktivitas hukum melampaui batas tersebut.

BAB IV
KEJAHATAN SIBER: KLASIFIKASI, MODUS, DAN RESPONS HUKUM

Perkembangan teknologi digital telah mengubah cara manusia berkomunikasi, bekerja, bertransaksi, menyimpan informasi, dan menjalankan aktivitas ekonomi. Perubahan tersebut membawa manfaat yang sangat besar, tetapi pada saat yang sama menciptakan ruang baru bagi terjadinya tindak pidana. Kejahatan tidak lagi selalu membutuhkan pertemuan fisik antara pelaku dan korban. Seseorang dapat kehilangan uang tanpa pernah bertemu dengan pelaku, suatu perusahaan dapat mengalami gangguan operasional karena sistemnya diserang dari negara lain, dan data pribadi dapat dicuri melalui perangkat yang berada ribuan kilometer dari tempat korban berada. Keadaan tersebut memperlihatkan bahwa teknologi digital bukan sekadar alat tambahan dalam melakukan kejahatan, melainkan dalam beberapa keadaan telah menjadi lingkungan tempat kejahatan itu sendiri berlangsung.

Persoalan hukum yang muncul kemudian bukan hanya bagaimana menghukum pelaku setelah kejahatan terjadi, tetapi juga bagaimana memahami bentuk kejahatan yang terus mengalami perubahan. Istilah *cybercrime* sendiri tidak memiliki satu definisi dan satu sistem klasifikasi yang sepenuhnya diterima secara universal. Perbedaan definisi tersebut berpengaruh

terhadap cara kejahatan diukur, dilaporkan, dikriminalisasi, dan ditangani oleh aparat penegak hukum. Karena itu, pembahasan kejahatan siber tidak dapat berhenti pada daftar jenis serangan atau nama teknologi yang digunakan pelaku. Dibutuhkan kerangka yang mampu menjelaskan hubungan antara teknologi, pelaku, korban, objek serangan, kerugian, dan respons hukum (Dupont & Whelan, 2021; Phillips dkk., 2022).

Karakter kejahatan siber juga memperlihatkan pergeseran dari kejahatan yang dilakukan secara individual menuju bentuk kejahatan yang lebih terorganisasi, terhubung, otomatis, dan dapat dilakukan dalam skala besar. Pelaku dapat membeli perangkat lunak berbahaya, memperoleh data korban dari pasar gelap, menggunakan layanan komputasi, memanfaatkan akun palsu, atau mengotomatisasi komunikasi dengan ribuan korban sekaligus. Perkembangan kecerdasan artifisial semakin memperluas kemungkinan tersebut karena teknologi dapat digunakan untuk menghasilkan pesan yang lebih meyakinkan, melakukan personalisasi serangan, membuat konten palsu, dan mempercepat proses yang sebelumnya membutuhkan keterlibatan manusia secara langsung (Jadala, 2026; Schmitt & Flechais, 2023).

Persoalan berikutnya terletak pada pembuktian. Lingkungan digital menghasilkan bukti yang berbeda dari bukti konvensional. Informasi dapat tersimpan dalam perangkat korban, server penyedia layanan, pusat data berbasis *cloud*, akun media sosial, aplikasi pesan, atau sistem pihak ketiga. Bukti tersebut dapat berubah, terhapus, terenkripsi, atau berada di negara lain. Oleh

sebab itu, keberhasilan penegakan hukum sangat bergantung pada kemampuan mengidentifikasi, mengamankan, memperoleh, memeriksa, dan menghadirkan bukti elektronik dengan tetap menjaga keaslian serta integritasnya (Luhina & Paliukh, 2025; Moussa, 2021; Shyshenko, 2025).

Kondisi tersebut membuat respons terhadap kejahatan siber tidak dapat hanya mengandalkan pendekatan pemidanaan. Hukum pidana tetap penting untuk memberikan batas terhadap perbuatan yang dilarang dan menentukan konsekuensi bagi pelaku. Namun, pendekatan tersebut perlu dilengkapi dengan pencegahan, peningkatan keamanan sistem, literasi digital, perlindungan korban, kerja sama antara pemerintah dan sektor swasta, serta kerja sama internasional. Hubungan antara keamanan siber dan pemberantasan kejahatan siber bahkan semakin erat karena pencegahan kerentanan sistem dapat mengurangi ruang yang tersedia bagi pelaku untuk melakukan serangan (Bartoli, 2025).

Atas dasar itu, Bab IV ini membahas kejahatan siber melalui empat persoalan utama. Pembahasan pertama diarahkan pada klasifikasi dan karakteristik kejahatan siber. Pembahasan kedua melihat perubahan modus operandi dan munculnya teknologi cerdas sebagai sarana baru kejahatan. Pembahasan ketiga mengkaji pertanggungjawaban pidana dan problematika pembuktian digital. Pembahasan keempat membahas respons hukum yang tidak hanya represif, tetapi juga preventif, kolaboratif, dan adaptif.

1. Klasifikasi dan Karakteristik Kejahatan Siber Dalam Ekosistem Digital

Membicarakan kejahatan siber pertama-tama membutuhkan kejelasan mengenai apa yang dimaksud dengan kejahatan tersebut. Kesulitan muncul karena teknologi dapat memiliki posisi yang berbeda dalam suatu tindak pidana. Dalam satu kasus, komputer atau jaringan menjadi sasaran serangan. Dalam kasus lain, komputer hanya digunakan sebagai sarana untuk melakukan penipuan yang pada dasarnya telah dikenal sebelum munculnya internet. Perbedaan posisi teknologi tersebut penting karena menentukan bagaimana suatu perbuatan dipahami, dikategorikan, dan ditangani. Karena itu, *cybercrime* sebaiknya tidak dipahami semata-mata sebagai "kejahatan yang menggunakan internet", melainkan sebagai spektrum tindak pidana yang hubungan antara kejahatan dan teknologi digitalnya memiliki tingkat ketergantungan yang berbeda (Lusthaus, 2024; Phillips dkk., 2022).

Salah satu pembedaan yang paling berguna adalah antara *cyber-dependent crime* dan *cyber-enabled crime*. *Cyber-dependent crime* merujuk pada tindak pidana yang keberadaannya bergantung pada teknologi informasi. Tanpa sistem komputer, jaringan, atau infrastruktur digital, jenis kejahatan tersebut pada dasarnya tidak dapat dilakukan dalam bentuk yang sama. Serangan *hacking*, penyebaran *malware*, dan *denial-of-service attack* merupakan contoh yang menunjukkan ketergantungan tersebut. Teknologi bukan hanya alat yang membantu pelaku,

tetapi merupakan objek sekaligus lingkungan utama tempat tindak pidana berlangsung (Dupont & Whelan, 2021; Whitty & Young, 2025).

Berbeda dengan itu, *cyber-enabled crime* merupakan kejahatan yang secara konseptual dapat dilakukan tanpa teknologi digital, tetapi teknologi memperluas jangkauan, kecepatan, skala, atau efektivitasnya. Penipuan, pencurian identitas, pemerasan, eksploitasi seksual, dan berbagai bentuk kejahatan ekonomi dapat masuk dalam kategori ini ketika teknologi digital digunakan sebagai sarana. Penipuan yang dahulu mungkin membutuhkan komunikasi langsung atau surat fisik dapat dilakukan melalui ribuan pesan elektronik secara bersamaan. Pencurian identitas juga dapat berlangsung dengan memanfaatkan kumpulan data pribadi yang diperoleh dari berbagai sumber digital. Teknologi dengan demikian memperbesar kapasitas pelaku tanpa selalu mengubah karakter dasar perbuatan pidananya (Dupont & Whelan, 2021; Kang, 2025; Lusthaus, 2024).

Pembedaan tersebut menjadi penting ketika melihat objek dan sasaran kejahatan. Kejahatan siber dapat diarahkan terhadap sistem komputer, data, individu, kepentingan ekonomi, maupun infrastruktur yang memiliki fungsi penting bagi masyarakat. Serangan terhadap sistem bertujuan mengakses, mengubah, merusak, atau mengganggu fungsi suatu sistem. Kejahatan berbasis data berfokus pada pengambilan, penyalahgunaan, perubahan, atau penyebaran informasi. Kejahatan terhadap individu

dapat berupa pencurian identitas, penipuan, pelecehan, ancaman, dan eksploitasi. Kejahatan ekonomi digital menyasar uang, rekening, transaksi, aset digital, atau aktivitas bisnis. Sementara itu, serangan terhadap infrastruktur kritis dapat menimbulkan dampak yang jauh lebih luas karena gangguan terhadap sistem digital dapat memengaruhi layanan publik dan aktivitas masyarakat.

Klasifikasi berdasarkan sasaran tersebut memperlihatkan bahwa dampak kejahatan siber tidak selalu berbentuk kerugian finansial. Kerugian dapat berupa kehilangan privasi, rusaknya reputasi, terganggunya pelayanan, hilangnya kepercayaan, kerusakan sistem, terhentinya kegiatan usaha, bahkan ancaman terhadap keselamatan masyarakat apabila serangan diarahkan pada infrastruktur yang memiliki fungsi vital. Karena itu, pengukuran *harm* dalam kejahatan siber perlu memperhatikan bukan hanya nilai uang yang hilang, tetapi juga dampak terhadap korban, organisasi, dan masyarakat. Kerangka klasifikasi yang lebih rinci dapat membantu menghubungkan jenis kejahatan dengan bentuk kerugian serta kebutuhan pencegahan yang sesuai (Phillips dkk., 2022; Whitty & Young, 2025).

Persoalan menjadi semakin kompleks karena satu serangan dapat menghasilkan beberapa bentuk kejahatan sekaligus. Sebuah serangan terhadap sistem perusahaan, misalnya, dapat dimulai dengan pencurian kredensial, dilanjutkan dengan akses tidak sah, pengambilan data, pemerasan, dan penyebaran

informasi. Apabila data pelanggan kemudian digunakan untuk melakukan penipuan, maka satu peristiwa digital telah menghasilkan lebih dari satu jenis kerugian. Situasi semacam ini menunjukkan bahwa klasifikasi tidak boleh digunakan secara kaku. Klasifikasi seharusnya menjadi alat analisis untuk memahami rangkaian perbuatan, hubungan antarpelaku, sasaran, dan akibat yang ditimbulkan.

Perkembangan berikutnya memperlihatkan perlunya melihat kejahatan siber sebagai fenomena yang bersifat relasional. Kejahatan dapat terjadi melalui hubungan antara pelaku, korban, perangkat, platform, penyedia layanan, dan infrastruktur digital. Kerangka yang lebih granular bahkan mengusulkan pengelompokan seperti *crimes against the machine*, *crimes using the machine*, kejahatan terorganisasi berbasis *cybercrime -as-a-service*, serta kejahatan yang memanipulasi informasi dan perilaku manusia. Pendekatan tersebut membantu menjelaskan mengapa batas antara kejahatan terhadap sistem dan kejahatan terhadap manusia sering kali tidak lagi tegas (Whitty & Young, 2025).

Dari perspektif hukum, klasifikasi memiliki konsekuensi yang lebih jauh daripada sekadar persoalan terminologi. Klasifikasi dapat membantu menentukan norma yang digunakan, kewenangan aparat, teknik penyidikan, kebutuhan ahli, bentuk kerugian yang harus dibuktikan, dan strategi perlindungan korban. Kesalahan dalam mengklasifikasikan suatu perbuatan dapat membuat respons hukum menjadi tidak tepat sasaran.

Kejahatan yang membutuhkan pemeriksaan forensik sistem, misalnya, tidak dapat ditangani dengan pendekatan yang sama seperti penipuan sederhana yang hanya menggunakan media digital sebagai alat komunikasi.

Karakteristik lain yang membedakan kejahatan siber adalah kemampuan teknologi menghilangkan batas geografis dalam pelaksanaan kejahatan. Pelaku dapat berada di satu negara, korban berada di negara lain, server berada di negara ketiga, sedangkan penyedia layanan berada di yurisdiksi keempat. Kondisi ini menyebabkan satu perbuatan dapat memiliki dimensi hukum yang melampaui batas negara. Kejahatan siber dengan demikian tidak hanya menghadirkan masalah kriminalitas, tetapi juga persoalan yurisdiksi, akses terhadap bukti, kerja sama antarnegara, dan perbedaan sistem hukum.

Karakter anonimitas juga memiliki posisi penting. Pelaku dapat menggunakan identitas palsu, jaringan perantara, akun yang dibuat khusus, perangkat yang telah dikompromikan, atau berbagai lapisan layanan digital untuk menyembunyikan identitasnya. Anonimitas tidak selalu berarti pelaku tidak dapat ditemukan, tetapi meningkatkan biaya dan waktu yang diperlukan untuk melakukan *attribution*. Dalam konteks penegakan hukum, persoalannya bukan hanya membuktikan bahwa suatu serangan terjadi, tetapi juga menghubungkan serangan tersebut dengan orang tertentu secara meyakinkan.

Kejahatan siber juga memiliki karakter skalabilitas. Sebuah pesan penipuan dapat dikirim kepada satu orang, tetapi dengan otomatisasi dapat dikirim kepada ribuan atau jutaan target. Demikian pula sebuah perangkat lunak berbahaya dapat menyerang satu sistem, tetapi dapat diperluas untuk menyerang banyak sistem. Skala tersebut mengubah hubungan antara usaha pelaku dan jumlah korban yang mungkin ditimbulkan. Teknologi memungkinkan pelaku memperoleh jangkauan yang sebelumnya sulit dicapai dengan metode konvensional.

Karakter skalabilitas tersebut menjelaskan mengapa klasifikasi kejahatan siber perlu terus diperbarui. Kategori yang terlalu umum akan kehilangan kemampuan untuk membedakan pola kejahatan yang berbeda. Sebaliknya, kategori yang terlalu sempit dapat cepat kehilangan relevansi ketika teknologi berubah. Literatur mengenai konseptualisasi *cybercrime* menunjukkan bahwa ketidakseragaman definisi dan taksonomi merupakan persoalan yang masih berlangsung dan berpengaruh terhadap penelitian serta penegakan hukum (Phillips dkk., 2022).

Klasifikasi yang baik bukanlah klasifikasi yang menghasilkan sebanyak mungkin istilah, melainkan klasifikasi yang membantu hukum memahami persoalan secara lebih akurat. Pendekatan tersebut perlu mempertimbangkan setidaknya empat unsur: teknologi yang digunakan, objek atau sasaran kejahatan, hubungan pelaku

dengan korban, serta akibat yang ditimbulkan. Dengan kerangka tersebut, hukum dapat bergerak dari sekadar mengenali "kejahatan berbasis internet" menuju pemahaman yang lebih spesifik mengenai bagaimana teknologi mengubah struktur kejahatan.

Dengan demikian, karakteristik kejahatan siber memperlihatkan adanya pergeseran dari kejahatan yang bersifat lokal menuju kejahatan yang dapat berlangsung secara simultan pada berbagai tempat. Teknologi membuat pelaku mampu bergerak lebih cepat, menyembunyikan identitas, memperluas jumlah korban, dan memanfaatkan infrastruktur yang berada di luar kendalinya. Kondisi ini menuntut sistem hukum untuk memiliki kategori yang cukup jelas, tetapi tetap fleksibel. Klasifikasi harus menjadi dasar untuk memahami masalah dan menentukan respons, bukan menjadi batas yang menghambat kemampuan hukum mengikuti perubahan bentuk kriminalitas digital.

2. Modus Operandi dan Evolusi Kejahatan Siber di Era Teknologi Cerdas

Perubahan kejahatan siber dapat dilihat paling jelas dari cara pelaku menjalankan aksinya. Kejahatan digital tidak lagi selalu berbentuk serangan teknis yang rumit dan membutuhkan kemampuan pemrograman tinggi. Banyak serangan justru memanfaatkan kelemahan manusia, seperti rasa percaya, ketakutan, rasa ingin tahu, kebutuhan mendesak, atau kebiasaan menggunakan layanan digital. Kondisi ini menjadikan manusia sebagai bagian penting dari permukaan serangan. Teknologi

dapat memperkuat manipulasi psikologis tersebut sehingga batas antara serangan teknis dan manipulasi sosial semakin kabur (Aslan dkk., 2023; Ghazi-Tehrani & Pontell, 2021).

Phishing merupakan contoh paling jelas. Pelaku biasanya membangun komunikasi yang tampak berasal dari pihak yang dipercaya korban, kemudian mendorong korban untuk melakukan tindakan tertentu, seperti membuka tautan, memasukkan kredensial, mengirim kode autentikasi, atau melakukan pembayaran. Perkembangan *phishing* menunjukkan bahwa modus ini tidak hilang meskipun kesadaran keamanan digital semakin meningkat. Sebaliknya, bentuknya berubah dan menjadi semakin terarah. *Spear phishing*, misalnya, menargetkan individu tertentu dengan pesan yang dibuat lebih relevan terhadap posisi, pekerjaan, hubungan sosial, atau aktivitas korban (Alkhalil dkk., 2021; Ghazi-Tehrani & Pontell, 2021).

Persoalan hukum dari *phishing* tidak terletak semata-mata pada adanya pesan palsu. Yang lebih penting adalah bagaimana rangkaian tindakan tersebut menghasilkan kerugian dan bagaimana setiap tindakan dapat dikaitkan dengan pelaku. Dalam suatu kasus, pelaku dapat memperoleh data melalui pesan palsu, menggunakan data tersebut untuk mengambil alih akun, lalu mengakses rekening korban dan memindahkan dana. Rangkaian tersebut memperlihatkan bahwa satu modus operandi dapat terdiri atas beberapa tindakan yang secara hukum mempunyai karakter berbeda.

Social engineering memperlihatkan perkembangan yang serupa. Pelaku tidak selalu berusaha menembus sistem melalui kerentanan teknis. Mereka dapat mencoba meyakinkan korban bahwa mereka adalah petugas bank, teman, atasan, rekan kerja, atau pihak resmi lainnya. Keberhasilan serangan kemudian bergantung pada kemampuan pelaku membaca situasi dan menciptakan kepercayaan. Teknologi digital memperluas ruang manipulasi karena identitas, suara, gambar, dan komunikasi dapat direkayasa dengan relatif mudah.

Munculnya kecerdasan artifisial generatif semakin memperbesar kemampuan tersebut. Sistem AI dapat membantu menghasilkan teks yang lebih natural, menyesuaikan pesan berdasarkan informasi target, menerjemahkan komunikasi ke berbagai bahasa, dan mempercepat produksi konten dalam jumlah besar. Teknologi tersebut tidak dengan sendirinya merupakan tindak pidana, tetapi dapat digunakan untuk meningkatkan efektivitas tindakan yang melanggar hukum. Penggunaan *generative AI* dalam *social engineering* dan *phishing* menunjukkan bahwa kemampuan teknologi untuk menghasilkan konten yang meyakinkan dapat memperbesar risiko penipuan digital (Schmitt & Flechais, 2023).

Perubahan tersebut menjadi lebih serius ketika AI dikombinasikan dengan *deepfake*. Pelaku dapat menciptakan gambar, video, atau suara yang menyerupai seseorang. Dalam konteks penipuan, suara yang menyerupai anggota keluarga dapat digunakan untuk menciptakan situasi darurat palsu.

Dalam konteks bisnis, identitas pimpinan dapat ditiru untuk meminta transfer dana. Perkembangan semacam ini meningkatkan persoalan pembuktian karena korban tidak lagi dapat mengandalkan persepsi visual atau audio sebagai indikator sederhana mengenai keaslian komunikasi. Ancaman *AI-enabled phishing*, *deepfake*, dan *social engineering* menjadi bagian dari perkembangan baru yang perlu diantisipasi oleh sistem hukum (Jadala, 2026).

Malware merupakan bentuk lain yang memperlihatkan hubungan antara teknologi dan kejahatan. Program berbahaya dapat digunakan untuk memperoleh akses, mencuri informasi, mengganggu sistem, atau membuka jalan bagi tindakan kriminal berikutnya. Dalam perkembangan tertentu, malware tidak hanya digunakan untuk merusak sistem, tetapi menjadi bagian dari ekosistem kriminal yang lebih luas. Pelaku yang satu dapat menyediakan perangkat lunak, sementara pelaku lain bertugas mendistribusikan, mengoperasikan, atau memanfaatkan hasil serangan (Aslan dkk., 2023; Dupont & Whelan, 2021).

Ransomware memperlihatkan bagaimana serangan teknis dapat berubah menjadi model pemerasan. Data atau sistem korban dikunci sehingga korban menghadapi gangguan operasional. Pelaku kemudian meminta pembayaran sebagai syarat untuk memberikan akses kembali atau mengancam menyebarkan data yang telah diambil. Dalam model seperti ini, teknologi menjadi sarana untuk menghasilkan tekanan ekonomi dan

psikologis. Korban dapat berupa individu, perusahaan, lembaga publik, bahkan organisasi yang menyediakan layanan penting (Aslan dkk., 2023; Mujianto, 2025).

Account takeover menunjukkan bahwa akun digital telah menjadi aset yang memiliki nilai ekonomi dan sosial. Akun dapat digunakan untuk mengakses uang, informasi, jaringan pertemanan, atau layanan tertentu. Ketika akun diambil alih, pelaku dapat menggunakan identitas pemilik untuk melakukan tindakan berikutnya. Korban bukan hanya kehilangan akses, tetapi juga dapat mengalami kerugian reputasi apabila akun tersebut digunakan untuk menipu orang lain. Karena itu, pencurian kredensial sering menjadi pintu masuk bagi tindak pidana lain (Alkhalil dkk., 2021; Kang, 2025).

Data breach juga perlu dipahami sebagai proses, bukan hanya peristiwa kebocoran. Data yang berhasil diperoleh dapat dijual, dipakai untuk penipuan, digunakan untuk pemerasan, atau dikombinasikan dengan informasi lain untuk membuat serangan yang lebih personal. Semakin lengkap data yang diperoleh, semakin besar kemungkinan pelaku membangun profil korban. Kejahatan berbasis data dengan demikian memperlihatkan bahwa informasi pribadi dapat berubah menjadi komoditas dalam ekosistem kriminal digital (Noor, 2025; Phillips dkk., 2022).

Perkembangan tersebut menunjukkan adanya pergeseran dari kejahatan individual menuju kejahatan yang terorganisasi. Pelaku tidak harus

menguasai seluruh kemampuan teknis. Ekosistem digital memungkinkan pembagian kerja antara pembuat perangkat lunak, penyedia data, operator serangan, pencuci hasil kejahatan, dan pihak yang menjual akses. Model *cybercrime -as-a-service* memperlihatkan bagaimana kemampuan melakukan kejahatan dapat "dipaketkan" menjadi layanan sehingga hambatan teknis bagi pelaku baru menjadi lebih rendah (Lusthaus, 2024; Whitty & Young, 2025).

Organisasi kejahatan siber juga tidak selalu berbentuk struktur hierarkis seperti organisasi kriminal tradisional. Jaringan dapat bersifat longgar, fleksibel, dan berbasis hubungan sementara. Seorang pelaku dapat bekerja dengan pihak tertentu untuk satu operasi kemudian berpindah ke jaringan lain. Forum daring dan pasar digital dapat menjadi ruang untuk mempertemukan orang yang memiliki kemampuan teknis dengan orang yang memiliki akses terhadap korban atau data. Fenomena tersebut membuat penegakan hukum harus mampu membaca hubungan jaringan, bukan hanya mencari satu individu sebagai pelaku tunggal (Lusthaus, 2024).

Perubahan modus operandi juga menunjukkan bahwa keamanan tidak dapat hanya diletakkan pada teknologi. Sistem yang sangat kuat secara teknis tetap dapat diserang apabila pengguna mudah dimanipulasi. Sebaliknya, pengguna yang memiliki kesadaran tinggi dapat tetap menjadi korban apabila sistem yang digunakan memiliki kerentanan. Karena itu, penanggulangan kejahatan

siber harus memperhatikan hubungan antara manusia, teknologi, organisasi, dan lingkungan hukum. Kajian mengenai kerentanan, ancaman, dan serangan siber menunjukkan bahwa keamanan merupakan persoalan multidimensi yang membutuhkan kombinasi solusi teknis dan kelembagaan (Aslan dkk., 2023).

Perkembangan modus tersebut membawa konsekuensi terhadap hukum pidana. Norma hukum yang hanya menyebut bentuk teknologi tertentu akan menghadapi risiko cepat usang. Pelaku dapat mengganti aplikasi, perangkat, teknik komunikasi, atau infrastruktur tanpa mengubah tujuan kriminalnya. Hukum perlu dirumuskan berdasarkan perilaku yang dilarang dan akibat yang ditimbulkan, bukan semata-mata berdasarkan nama teknologi yang sedang digunakan.

Dengan demikian, evolusi modus operandi menunjukkan bahwa kejahatan siber semakin personal sekaligus semakin otomatis. Teknologi memungkinkan pelaku mengenali korban secara lebih spesifik, menghasilkan komunikasi yang lebih meyakinkan, melakukan serangan dalam skala lebih besar, dan memanfaatkan jaringan pelaku yang tersebar. Tantangan hukum bukan hanya mengejar teknologi baru, tetapi memahami pola kejahatan di balik teknologi tersebut. Pendekatan yang demikian memungkinkan hukum tetap relevan meskipun perangkat dan metode yang digunakan pelaku terus berubah.

3. Pertanggungjawaban Pidana dan Problematika Pembuktian Dalam Kejahatan Siber

Suatu kejahatan tidak berhenti pada pertanyaan apakah serangan telah terjadi. Dalam proses hukum, pertanyaan yang jauh lebih menentukan adalah siapa yang bertanggung jawab, tindakan apa yang dilakukan, bagaimana kesalahan dibuktikan, dan apakah bukti yang diperoleh dapat diterima di pengadilan. Persoalan tersebut menjadi lebih kompleks dalam kejahatan siber karena pelaku dapat menggunakan identitas palsu, perangkat orang lain, jaringan pihak ketiga, layanan *cloud*, atau sistem yang berada di luar yurisdiksi negara tempat perkara diperiksa.

Pembuktian dalam lingkungan digital memiliki karakter khusus karena informasi elektronik dapat hadir dalam berbagai bentuk. Data dapat berupa *log*, metadata, alamat IP, pesan elektronik, percakapan, rekaman transaksi, file, gambar, video, data lokasi, atau informasi yang tersimpan dalam aplikasi. Tidak semua data tersebut secara otomatis membuktikan siapa pelakunya. Bukti digital harus ditempatkan dalam rangkaian fakta yang memungkinkan penyidik dan pengadilan menghubungkan suatu aktivitas digital dengan orang tertentu. Persoalan keaslian dan dapat diterimanya bukti menjadi bagian penting dari proses tersebut (Moussa, 2021; Shyshenko, 2025).

Contoh sederhana dapat memperlihatkan persoalan tersebut. Sebuah alamat IP mungkin menunjukkan bahwa aktivitas tertentu berasal dari

suatu koneksi internet. Namun, alamat IP tidak selalu identik dengan orang yang melakukan tindakan. Komputer dapat digunakan bersama, koneksi dapat digunakan oleh banyak perangkat, atau perangkat tersebut sendiri dapat telah dikompromikan oleh pihak lain. Oleh sebab itu, *attribution* membutuhkan korelasi dengan bukti lain. Penegakan hukum perlu membangun hubungan antara perangkat, akun, aktivitas, waktu, lokasi, komunikasi, transaksi, dan tindakan manusia yang berada di baliknya.

Persoalan semakin rumit ketika pelaku menggunakan perangkat yang bukan miliknya. Komputer yang digunakan untuk menyerang sistem dapat merupakan perangkat korban yang telah diretas. Server pihak ketiga dapat digunakan sebagai perantara. Akun dapat dibeli atau dicuri. Layanan *cloud* dapat dimanfaatkan untuk menyimpan atau memproses data. Situasi tersebut membuat penyidik menghadapi kemungkinan bahwa objek digital yang ditemukan dalam penyidikan bukan secara langsung milik atau dikendalikan oleh pelaku. Penentuan tanggung jawab karena itu membutuhkan analisis terhadap penguasaan, penggunaan, pengetahuan, dan hubungan pelaku dengan sistem.

Unsur kesalahan tetap menjadi bagian penting dalam pertanggungjawaban pidana. Tidak setiap orang yang perangkatnya digunakan untuk melakukan kejahatan otomatis dapat dianggap sebagai pelaku. Demikian pula penyedia teknologi tidak serta-merta bertanggung jawab atas seluruh perbuatan yang dilakukan oleh penggunanya. Hukum

harus membedakan antara tindakan yang dilakukan dengan sengaja, tindakan yang dilakukan karena kelalaian, penggunaan sistem tanpa sepengetahuan pemilik, serta keadaan ketika pihak tertentu secara sadar membantu terjadinya tindak pidana.

Pembedaan peran menjadi semakin penting ketika kejahatan dilakukan melalui jaringan. Pelaku utama mungkin tidak pernah berkomunikasi dengan korban. Ada pihak yang memperoleh data, pihak yang menyediakan perangkat serangan, pihak yang menjalankan operasi, dan pihak yang menikmati hasil. Pembuktian perlu menunjukkan kontribusi masing-masing pihak. Dengan pendekatan tersebut, pertanggungjawaban tidak dibangun berdasarkan asumsi bahwa setiap anggota jaringan mempunyai tingkat kesalahan yang sama.

Pertanggungjawaban korporasi menghadirkan persoalan tersendiri. Organisasi dapat menjadi korban kejahatan siber, tetapi dalam keadaan tertentu organisasi juga dapat menjadi pihak yang memperoleh manfaat dari tindakan melawan hukum yang dilakukan melalui sistemnya. Pertanyaan hukum kemudian berkaitan dengan hubungan antara tindakan individu dan entitas, kewenangan pengambil keputusan, kebijakan internal, manfaat yang diperoleh, serta kegagalan organisasi memenuhi kewajiban tertentu. Perkembangan teknologi membuat persoalan tersebut semakin penting karena sistem digital biasanya dikelola oleh banyak unit dan pihak.

Posisi penyedia platform dan penyelenggara sistem elektronik juga harus ditempatkan secara hati-hati. Platform dapat menjadi tempat berlangsungnya komunikasi, transaksi, penyimpanan data, atau distribusi konten. Namun, keberadaan suatu kejahatan di dalam platform tidak otomatis berarti platform tersebut merupakan pelaku. Pertanggungjawaban harus ditentukan berdasarkan norma yang berlaku, tingkat pengetahuan, kewajiban hukum, tindakan atau kelalaian, serta hubungan sebab akibat dengan kerugian. Pendekatan yang terlalu luas dapat menghambat inovasi dan aktivitas digital, sedangkan pendekatan yang terlalu sempit dapat menciptakan ruang impunitas.

Persoalan berikutnya adalah autentikasi. Pengadilan harus memiliki dasar untuk mempercayai bahwa suatu data benar berasal dari sumber yang diklaim dan tidak mengalami perubahan yang merusak maknanya. Bukti elektronik memiliki sifat yang berbeda dari benda fisik karena data dapat disalin tanpa menghilangkan salinan asli, dapat berubah karena proses otomatis, dan dapat diakses melalui berbagai perangkat. Karena itu, autentikasi membutuhkan prosedur dan penjelasan teknis yang memadai (Moussa, 2021; Shyshenko, 2025).

Integritas bukti juga menjadi perhatian utama. Penyidik perlu dapat menunjukkan bahwa data yang dihadirkan masih memiliki hubungan yang dapat dipercaya dengan data yang diperoleh pada saat pengumpulan. Setiap tindakan terhadap bukti perlu dicatat secara sistematis. Prinsip tersebut

berkaitan erat dengan *chain of custody*, yaitu dokumentasi mengenai siapa yang memperoleh, menangani, memindahkan, menyimpan, memeriksa, dan menyerahkan bukti. Ketidakjelasan dalam rantai penguasaan dapat menimbulkan keraguan terhadap keutuhan bukti (Gafarova & Jabbarova, 2025).

Masalah tersebut menjadi lebih sulit ketika bukti berada dalam *cloud computing*. Data tidak selalu berada pada perangkat yang digunakan korban atau penyidik. Data dapat diproses dan disimpan melalui infrastruktur yang dikelola penyedia layanan. Lokasi fisik data bahkan dapat berubah atau tersebar pada beberapa pusat data. Penyidik karena itu tidak cukup hanya mengetahui bahwa data "ada di internet". Mereka perlu mengetahui siapa yang menguasai data, bagaimana data dapat diperoleh secara sah, prosedur apa yang digunakan, dan bagaimana integritasnya dipertahankan (Luhina & Paliukh, 2025).

Enkripsi juga menciptakan dilema. Dari sisi keamanan, enkripsi merupakan mekanisme penting untuk melindungi komunikasi dan data. Dari sisi penyidikan, enkripsi dapat menghambat akses terhadap informasi yang relevan dengan tindak pidana. Persoalan tersebut menjadi semakin kompleks pada platform komunikasi yang menggunakan enkripsi kuat. Penegakan hukum harus mencari keseimbangan antara kebutuhan memperoleh bukti dengan perlindungan terhadap keamanan dan hak pengguna. Tantangan tersebut menunjukkan bahwa akses terhadap bukti tidak

dapat dipisahkan dari persoalan privasi dan keamanan digital (Gajic´, 2026).

Admissibility atau dapat diterimanya bukti menjadi tahap penting setelah bukti diperoleh. Bukti yang secara teknis tersedia belum tentu secara otomatis dapat digunakan dalam proses peradilan apabila proses memperoleh atau mengelolanya melanggar ketentuan hukum acara. Kesalahan prosedural dapat menimbulkan persoalan mengenai keabsahan atau bobot pembuktian. Karena itu, penyidikan digital harus memperhatikan hukum acara sejak tahap awal, bukan baru memikirkan kelayakan bukti ketika perkara telah masuk persidangan (Miller, 2022; Shyshenko, 2025).

Peran penyidik, jaksa, ahli forensik, dan hakim menjadi semakin penting dalam kondisi tersebut. Pengetahuan hukum tanpa pemahaman teknis dapat menghasilkan penilaian yang tidak tepat terhadap bukti digital. Sebaliknya, kemampuan teknis tanpa pemahaman hukum acara dapat menghasilkan bukti yang diperoleh dengan prosedur yang bermasalah. Kebutuhan terhadap kombinasi kompetensi tersebut membuat peningkatan kapasitas aparat menjadi bagian dari sistem pembuktian, bukan sekadar persoalan pelatihan tambahan. Pengalaman penyidik dan penuntut dalam menggunakan bukti digital juga menunjukkan pentingnya kompetensi dan prosedur yang konsisten dalam menangani perkara siber (Miller, 2022).

Kondisi tersebut menghasilkan satu kesimpulan penting: dalam kejahatan siber,

pembuktian tidak dapat hanya berorientasi pada "menemukan data". Tujuan akhirnya adalah membangun rangkaian pembuktian yang mampu menjelaskan apa yang terjadi, kapan terjadi, bagaimana terjadi, siapa yang terlibat, serta bagaimana keterlibatan tersebut dapat dibuktikan secara sah. Bukti digital harus ditempatkan dalam konteks keseluruhan perkara. Satu bukti mungkin lemah apabila berdiri sendiri, tetapi dapat menjadi kuat apabila dikaitkan dengan bukti lain yang saling menguatkan.

Oleh karena itu, sistem hukum membutuhkan pendekatan pembuktian yang mampu menggabungkan kemampuan forensik digital dengan prinsip hukum pidana dan hukum acara. Prosedur pengumpulan, autentikasi, penyimpanan, analisis, dan penyajian bukti harus dibangun sedemikian rupa sehingga mampu menjaga keandalan informasi sekaligus menjamin hak pihak yang diperiksa. Tantangan kejahatan siber bukan hanya bagaimana memperoleh bukti sebanyak-banyaknya, tetapi bagaimana memperoleh bukti yang dapat dipercaya dan dipertanggungjawabkan secara hukum.

4. Respons Hukum dan Strategi Penanggulangan Kejahatan Siber

Respons hukum terhadap kejahatan siber tidak dapat dirancang dengan asumsi bahwa teknologi akan berhenti berkembang. Setiap kali hukum berhasil mengidentifikasi satu pola kejahatan, pelaku dapat menemukan teknik baru untuk menghindari deteksi. Karena itu, ukuran

keberhasilan sistem hukum tidak hanya terletak pada banyaknya perkara yang berhasil diproses, tetapi juga pada kemampuan sistem tersebut beradaptasi terhadap perubahan teknologi dan pola kriminalitas. Respons hukum perlu dibangun sebagai sistem yang terus belajar.

Pendekatan pertama adalah kriminalisasi. Hukum pidana harus memberikan batas yang jelas mengenai perbuatan digital yang dilarang. Kejelasan tersebut diperlukan agar masyarakat mengetahui perilaku yang memiliki konsekuensi hukum dan agar aparat mempunyai dasar yang sah untuk melakukan penindakan. Namun, kriminalisasi tidak boleh dilakukan hanya dengan menambahkan setiap teknologi baru ke dalam daftar tindak pidana. Hukum perlu merumuskan perilaku, unsur kesalahan, objek perlindungan, dan akibat secara cukup jelas agar norma tidak cepat kehilangan relevansi.

Pendekatan pidana juga harus diikuti dengan kapasitas penyidikan yang sesuai. Penyidik kejahatan siber membutuhkan kemampuan memahami sistem jaringan, perangkat digital, *malware*, transaksi elektronik, komunikasi digital, *cloud*, dan teknik forensik. Kebutuhan tersebut tidak berarti seluruh aparat harus menjadi ahli teknologi. Sistem penegakan hukum dapat dibangun melalui kerja sama antara penyidik, ahli forensik, jaksa, analis keamanan, dan pihak lain yang memiliki kompetensi khusus. Pengalaman penggunaan bukti digital menunjukkan pentingnya keterampilan teknis

sekaligus pemahaman mengenai kebutuhan pembuktian di pengadilan (Miller, 2022).

Penuntutan juga menghadapi tantangan yang berbeda. Jaksa perlu mengubah data teknis menjadi konstruksi hukum yang dapat dipahami oleh pengadilan. Informasi seperti *log*, metadata, alamat IP, atau jejak transaksi perlu dijelaskan hubungannya dengan unsur tindak pidana. Karena itu, keberhasilan penuntutan tidak hanya bergantung pada kemampuan memperoleh bukti, tetapi juga kemampuan menerjemahkan bukti tersebut menjadi argumentasi hukum yang koheren.

Pemidanaan harus mempertimbangkan karakter dan tingkat bahaya perbuatan. Serangan terhadap individu dengan kerugian terbatas tentu memiliki konsekuensi yang berbeda dari serangan terhadap sistem yang menyebabkan gangguan luas. Demikian pula pelaku utama, pihak yang membantu, dan pihak yang hanya memiliki hubungan tidak langsung dengan peristiwa harus diperlakukan berdasarkan tingkat kesalahan dan kontribusinya. Prinsip proporsionalitas tetap relevan dalam kejahatan siber meskipun medianya berbeda dari kejahatan konvensional.

Respons hukum juga harus memperhatikan korban. Korban kejahatan siber dapat mengalami kerugian finansial, kehilangan data, rusaknya reputasi, tekanan psikologis, dan hilangnya rasa aman. Dalam beberapa kasus, korban bahkan tidak segera menyadari bahwa dirinya telah menjadi sasaran. Perlindungan hukum karena itu perlu

mencakup mekanisme pelaporan, bantuan, pemulihan akses, perlindungan data, dan apabila memungkinkan pemulihan kerugian. Perlindungan korban merupakan bagian penting dari kebijakan penanggulangan kejahatan siber, bukan sekadar konsekuensi tambahan setelah pelaku dihukum (Mujianto, 2025).

Pendekatan penal juga memiliki keterbatasan. Aparat penegak hukum pada umumnya baru bergerak setelah terdapat indikasi tindak pidana. Sementara itu, serangan digital dapat berlangsung dalam hitungan detik. Kerugian bahkan dapat terjadi sebelum korban mengetahui bahwa sistemnya sedang diserang. Karena itu, penanggulangan membutuhkan pendekatan non-penal yang dapat mengurangi peluang terjadinya kejahatan sejak awal.

Pencegahan dapat dimulai dari peningkatan keamanan sistem. Organisasi perlu mengidentifikasi kerentanan, memperbarui perangkat lunak, menerapkan autentikasi yang kuat, mengelola hak akses, melakukan pencadangan, serta memiliki prosedur respons insiden. Langkah tersebut bukan hanya persoalan teknis. Dalam lingkungan hukum modern, keamanan sistem juga berkaitan dengan tata kelola dan tanggung jawab organisasi dalam mengelola risiko digital.

Literasi keamanan digital merupakan unsur lain yang tidak dapat diabaikan. Banyak serangan memanfaatkan keputusan manusia, terutama ketika korban menerima pesan yang tampak meyakinkan.

Masyarakat perlu memahami cara mengenali komunikasi mencurigakan, menjaga kredensial, menggunakan autentikasi berlapis, serta melaporkan insiden. Namun, tanggung jawab pencegahan tidak boleh sepenuhnya dibebankan kepada korban. Penyedia layanan dan organisasi juga memiliki peran untuk merancang sistem yang mengurangi kemungkinan pengguna menjadi korban.

Kerja sama pemerintah dan sektor swasta menjadi semakin penting karena sebagian besar infrastruktur digital dikelola oleh perusahaan. Data yang dibutuhkan dalam penyidikan dapat berada pada platform, penyedia *cloud*, penyedia komunikasi, bank, perusahaan teknologi, atau penyedia layanan lainnya. Pemerintah memiliki kewenangan hukum, sedangkan perusahaan sering memiliki akses teknis terhadap data dan infrastruktur. Hubungan keduanya perlu dibangun melalui prosedur yang jelas agar permintaan data, pelaporan insiden, dan respons terhadap serangan dapat dilakukan secara cepat dan tetap menghormati hukum.

Pelaporan insiden merupakan salah satu instrumen penting dalam strategi penanggulangan. Insiden yang tidak dilaporkan akan sulit dipetakan. Tanpa data yang memadai, negara dan organisasi akan kesulitan mengetahui pola serangan, sektor yang paling rentan, serta modus yang sedang berkembang. Karena itu, mekanisme pelaporan harus dirancang agar mudah digunakan, memberikan perlindungan yang memadai kepada pelapor, dan

menghasilkan informasi yang dapat digunakan untuk memperbaiki sistem keamanan.

Kerja sama internasional menjadi kebutuhan yang tidak dapat dihindari. Kejahatan siber dapat melibatkan pelaku, korban, server, penyedia layanan, dan bukti yang berada di berbagai negara. Penegakan hukum nasional karena itu sering membutuhkan akses terhadap data atau bantuan dari yurisdiksi lain. Perkembangan kerja sama internasional dalam kerangka *Budapest Convention on Cybercrime* dan *Protocol* II menunjukkan pentingnya mekanisme yang memungkinkan akses terhadap bukti elektronik serta kerja sama antaraparat penegak hukum (Spiezia, 2022).

Kerja sama tersebut tidak cukup hanya dengan kesepakatan formal. Prosedur harus mampu menjawab kebutuhan praktis penyidikan. Data digital dapat hilang atau berubah dengan cepat sehingga mekanisme yang terlalu lambat dapat mengurangi nilai bukti. Karena itu, kerja sama internasional perlu diarahkan pada mekanisme yang memungkinkan pengamanan data secara cepat, pertukaran informasi, serta permintaan bantuan hukum yang lebih efektif. Tantangan tersebut menjadi semakin penting karena perbedaan aturan nasional mengenai bukti elektronik, privasi, dan prosedur penyidikan dapat memengaruhi kemampuan suatu negara menggunakan bukti yang diperoleh dari negara lain (Gafarova & Jabbarova, 2025; Satbayeva dkk., 2024).

Respons hukum juga perlu memperhatikan perkembangan *Artificial Intelligence* (AI). Regulasi

yang hanya berfokus pada teknologi tertentu dapat cepat tertinggal karena kemampuan AI berkembang melalui berbagai aplikasi dan model. Yang perlu menjadi perhatian adalah penggunaan teknologi untuk menghasilkan akibat yang melanggar hukum. Apabila AI digunakan untuk memperkuat penipuan, membuat identitas palsu, mengotomatisasi serangan, atau menghasilkan konten yang digunakan untuk merugikan korban, hukum harus memiliki dasar yang cukup untuk menilai perbuatan tersebut tanpa harus menunggu munculnya nama teknologi baru.

Pada titik ini, pendekatan adaptif menjadi penting. Adaptivitas bukan berarti hukum harus selalu berubah setiap kali teknologi baru muncul. Adaptivitas justru berarti norma memiliki kemampuan untuk diterapkan terhadap bentuk perilaku baru tanpa kehilangan kepastian hukum. Hal tersebut dapat dicapai melalui kombinasi norma yang berbasis prinsip, regulasi teknis yang dapat diperbarui, pedoman penegakan, serta mekanisme evaluasi berkala.

Hubungan antara keamanan siber dan pemberantasan kejahatan siber juga perlu dipandang sebagai satu kesatuan. Keamanan yang baik dapat mencegah kejahatan, tetapi keamanan tidak boleh dijadikan alasan untuk mengabaikan hak. Sebaliknya, perlindungan hak tidak seharusnya menghilangkan kemampuan negara dan masyarakat untuk melindungi sistem digital. Hubungan tersebut membutuhkan keseimbangan antara keamanan,

efektivitas penegakan hukum, privasi, kebebasan, dan kepastian hukum (Bartoli, 2025).

Strategi penanggulangan juga membutuhkan pendekatan berbasis risiko. Tidak semua sistem memiliki tingkat ancaman dan dampak yang sama. Sistem yang mengelola layanan publik, keuangan, kesehatan, energi, komunikasi, atau infrastruktur strategis dapat memerlukan perlindungan lebih tinggi dibandingkan sistem dengan dampak terbatas. Penentuan prioritas berdasarkan risiko membantu negara dan organisasi menggunakan sumber daya secara lebih efektif.

Pendidikan aparat menjadi bagian yang tidak terpisahkan dari strategi tersebut. Teknologi berubah lebih cepat daripada kurikulum pelatihan konvensional. Aparat perlu mendapatkan pembaruan secara berkala mengenai teknik serangan, metode forensik, perkembangan AI, bukti elektronik, enkripsi, serta bentuk kerja sama internasional. Tanpa pembaruan kompetensi, hukum mungkin memiliki norma yang memadai tetapi tidak memiliki kapasitas untuk menerapkannya secara efektif.

Respons terhadap kejahatan siber pada akhirnya perlu mengintegrasikan pendekatan penal dan non-penal. Pendekatan penal memberikan kepastian bahwa tindakan yang merugikan akan memperoleh konsekuensi hukum. Pendekatan non-penal mengurangi peluang terjadinya kejahatan melalui keamanan, pendidikan, tata kelola, dan kerja sama. Keduanya tidak seharusnya diposisikan sebagai pilihan yang saling menggantikan. Keduanya

merupakan bagian dari satu kebijakan penanggulangan yang saling melengkapi (Bartoli, 2025; Dupont & Whelan, 2021).

Kerja sama internasional, penguatan kapasitas, perlindungan korban, dan pengembangan sistem keamanan juga perlu berjalan secara simultan. Pengalaman internasional menunjukkan bahwa kejahatan siber tidak dapat diatasi oleh satu lembaga atau satu negara saja. Perbedaan hukum, teknologi, dan kapasitas dapat dimanfaatkan oleh pelaku untuk mencari titik terlemah dalam sistem. Karena itu, koordinasi menjadi faktor penting dalam membangun respons yang efektif (Satbayeva dkk., 2024).

Hukum siber menghadapi tantangan yang berbeda dari hukum pidana konvensional karena objek, alat, pelaku, korban, dan bukti dapat tersebar pada ruang yang berbeda. Respons hukum yang efektif harus mampu bergerak cepat tanpa mengorbankan prosedur, bekerja lintas lembaga tanpa menghilangkan batas kewenangan, dan menggunakan teknologi tanpa mengabaikan hak. Pendekatan semacam itu membutuhkan desain kelembagaan yang mampu menggabungkan hukum, teknologi, keamanan, dan perlindungan masyarakat.

Perubahan modus operandi menunjukkan bahwa ancaman semakin personal, otomatis, terorganisasi, dan berskala besar. *Phishing*, *social engineering*, *malware*, *ransomware*, *account takeover*, *data breach*, *deepfake*, dan serangan berbasis AI bukan sekadar daftar teknik kejahatan, tetapi bagian

dari transformasi ekosistem kriminal digital. Teknologi dapat digunakan untuk meningkatkan kemampuan pelaku dalam memperoleh korban, menyembunyikan identitas, mengotomatisasi serangan, dan memanfaatkan jaringan pelaku yang lebih luas (Ghazi-Tehrani & Pontell, 2021; Jadala, 2026; Schmitt & Flechais, 2023).

Pertanggungjawaban pidana menghadapi tantangan karena hubungan antara tindakan digital dan individu tidak selalu mudah dibuktikan. *Attribution*, autentikasi, integritas, *chain of custody*, enkripsi, *cloud computing*, serta penggunaan infrastruktur pihak ketiga menjadikan pembuktian digital sebagai salah satu persoalan utama. Bukti harus tidak hanya ditemukan, tetapi juga harus diperoleh, dipelihara, dianalisis, dan disajikan dengan cara yang dapat dipertanggungjawabkan secara hukum (Luhina & Paliukh, 2025; Moussa, 2021; Shyshenko, 2025).

Respons hukum karena itu harus bersifat adaptif. Kriminalisasi, penyidikan, penuntutan, dan pemidanaan tetap menjadi bagian penting, tetapi harus dilengkapi dengan pencegahan, keamanan sistem, literasi digital, perlindungan korban, pelaporan insiden, kerja sama pemerintah-swasta, dan kerja sama internasional. Kerangka kerja sama internasional seperti *Budapest Convention* dan *Protocol* II memperlihatkan bahwa akses terhadap bukti elektronik dan koordinasi lintas negara semakin penting dalam menghadapi kejahatan yang tidak mengenal batas geografis (Spiezia, 2022).

Dengan demikian, arah perkembangan hukum siber seharusnya tidak semata-mata mengejar teknologi setelah digunakan untuk melakukan kejahatan. Hukum perlu membangun kemampuan untuk mengantisipasi pola risiko, memahami perubahan modus, memperkuat pembuktian, dan melindungi korban. Kejahatan siber menuntut hukum yang mampu beradaptasi tanpa kehilangan prinsip kepastian, keadilan, dan perlindungan hak. Tantangan tersebut menjadikan hukum siber bukan hanya bidang hukum yang merespons kejahatan digital, tetapi juga instrumen untuk membangun tata kelola ruang digital yang aman, bertanggung jawab, dan berkelanjutan.

BAB V
PERLINDUNGAN DATA PRIBADI SEBAGAI HAK FUNDAMENTAL DI ERA DIGITAL

Perkembangan teknologi digital telah mengubah cara data pribadi diproduksi, dikumpulkan, dipertukarkan, dianalisis, dan digunakan. Dalam kehidupan sehari-hari, seseorang dapat meninggalkan ratusan bahkan ribuan jejak informasi tanpa secara aktif menyadari bahwa dirinya sedang menghasilkan data. Ketika seseorang menggunakan mesin pencari, melakukan pembelian melalui *E-commerce*, mengakses media sosial, menggunakan aplikasi transportasi, melakukan pembayaran digital, mengunggah foto, atau menggunakan layanan berbasis lokasi, berbagai informasi mengenai dirinya dapat tercatat dalam sistem. Data tersebut dapat menunjukkan identitas, kebiasaan, preferensi, hubungan sosial, lokasi, pola konsumsi, kondisi ekonomi, dan berbagai karakteristik lain yang sebelumnya berada dalam ruang privat.

Perubahan tersebut menyebabkan konsep privasi mengalami transformasi. Privasi tidak lagi cukup dipahami sebagai hak untuk terbebas dari gangguan pihak lain terhadap kehidupan pribadi. Dalam lingkungan digital, persoalan yang lebih mendasar adalah kemampuan seseorang untuk mengetahui bagaimana

informasi mengenai dirinya dikumpulkan dan digunakan, kepada siapa informasi tersebut diberikan, untuk tujuan apa informasi diproses, serta sejauh mana dirinya dapat mengendalikan pemrosesan tersebut. Perlindungan data pribadi karena itu berkembang menjadi instrumen yang memberikan bentuk operasional terhadap perlindungan privasi dalam lingkungan teknologi informasi. Perkembangan literatur menunjukkan bahwa perlindungan data pribadi semakin dipahami sebagai hak yang memiliki kedudukan mandiri, meskipun tetap mempunyai hubungan erat dengan hak atas privasi dan hak asasi manusia (Khan, 2025; Kovalenko, 2022; Rahmadani & Prastyanti, 2025).

Persoalan perlindungan data menjadi semakin penting karena data telah berubah menjadi salah satu sumber daya utama dalam ekonomi digital. Perusahaan menggunakan data untuk memahami konsumen, mengembangkan produk, melakukan pemasaran, memprediksi perilaku, menentukan risiko, dan mengotomatisasi keputusan. Pemerintah memanfaatkan data untuk memberikan pelayanan publik, melakukan perencanaan, mengidentifikasi risiko, dan menjalankan kebijakan. Di sisi lain, pelaku kejahatan juga melihat data sebagai aset yang dapat dicuri, dijual, dimanipulasi, atau digunakan untuk melakukan penipuan. Kondisi tersebut menunjukkan bahwa nilai data tidak hanya terletak pada informasi yang dikandungnya, tetapi juga pada kemampuan data untuk menghasilkan pengetahuan dan keputusan.

Dalam keadaan demikian, perlindungan data pribadi tidak dapat ditempatkan sebagai hambatan

terhadap digitalisasi. Perlindungan justru menjadi salah satu syarat agar digitalisasi dapat berlangsung secara berkelanjutan. Masyarakat akan sulit mempercayai layanan digital apabila mereka merasa data pribadi dapat digunakan tanpa batas. Dunia usaha juga akan menghadapi risiko hukum dan reputasi apabila tidak mampu menjaga informasi pelanggan. Negara membutuhkan kerangka hukum yang mampu memberikan ruang bagi inovasi sekaligus menetapkan batas terhadap pemrosesan data yang dapat merugikan individu.

Bab ini membahas perlindungan data pribadi melalui lima dimensi yang saling berhubungan. Pembahasan pertama melihat kedudukan data pribadi sebagai hak fundamental dan bagian dari perlindungan privasi. Pembahasan kedua menguraikan prinsip-prinsip yang harus menjadi dasar pemrosesan data. Pembahasan ketiga menempatkan individu sebagai subjek data yang memiliki hak untuk mengendalikan informasi mengenai dirinya. Pembahasan keempat membahas tanggung jawab pengendali, prosesor, platform, dan penyelenggara sistem digital. Pembahasan terakhir mengkaji tantangan yang muncul dari *big data, cloud computing, Internet of Things, profiling, automated decision-making*, dan kecerdasan artifisial atau *Artificial Intelligence* (AI).

1. Data Pribadi Sebagai Hak Fundamental dan Bagian Dari Perlindungan Privasi

Pada masa ketika sebagian besar aktivitas manusia berlangsung secara fisik, privasi relatif mudah dibayangkan sebagai ruang yang tidak boleh dimasuki pihak lain tanpa izin. Rumah, surat pribadi,

percakapan, dan kehidupan keluarga merupakan contoh ruang yang secara intuitif dianggap berada dalam lingkup privat. Digitalisasi mengubah batas tersebut. Informasi yang dahulu hanya diketahui oleh lingkungan terdekat kini dapat direkam dan dianalisis oleh sistem yang bahkan tidak terlihat oleh individu. Seseorang dapat berada di ruang privat secara fisik, tetapi aktivitas digitalnya tetap menghasilkan data yang diproses oleh banyak pihak.

Perubahan tersebut memperluas makna privasi. Privasi digital tidak hanya berkaitan dengan larangan memasuki ruang pribadi, tetapi juga berkaitan dengan kemampuan seseorang mengendalikan informasi tentang dirinya. Individu perlu mengetahui informasi apa yang dikumpulkan, bagaimana informasi tersebut digunakan, dan kepada siapa informasi dapat diberikan. Dengan demikian, kendali terhadap informasi menjadi bagian penting dari privasi dalam masyarakat digital (Khan, 2025; Nafi'ah & Prastyanti, 2025; Shehu & Shehu, 2023).

Hubungan antara privasi dan perlindungan data pribadi perlu dipahami secara hati-hati. Keduanya berhubungan erat, tetapi tidak sepenuhnya identik. Privasi memberikan perlindungan terhadap kehidupan pribadi seseorang, sedangkan hukum perlindungan data memberikan seperangkat prinsip dan hak yang mengatur bagaimana informasi mengenai seseorang dapat diproses. Perbedaan tersebut penting karena suatu pemrosesan data dapat menimbulkan persoalan perlindungan data

meskipun tidak selalu terlihat sebagai bentuk campur tangan langsung terhadap kehidupan pribadi. Data mengenai aktivitas konsumsi, misalnya, dapat digunakan untuk membuat profil perilaku tanpa adanya akses langsung terhadap ruang privat seseorang.

Kedudukan perlindungan data pribadi sebagai hak fundamental memiliki dasar yang kuat dalam perkembangan hukum hak asasi manusia. Hak atas privasi telah memperoleh pengakuan dalam berbagai instrumen internasional, termasuk *Universal Declaration of Human Rights* (UDHR), *International Covenant on Civil and Political Rights* (ICCPR), *European Convention on Human Rights* (ECHR), serta Piagam Hak Fundamental Uni Eropa. Instrumen tersebut menjadi dasar normatif bagi berkembangnya perlindungan terhadap informasi pribadi dalam masyarakat digital (Christodoulou & Limniotis, 2024; Khan, 2025; Rahmadani & Prastyanti, 2025).

Kedudukan tersebut menjadi semakin relevan karena data pribadi dapat menggambarkan seseorang secara lebih mendalam dibandingkan informasi konvensional. Data lokasi dapat menunjukkan pola pergerakan. Riwayat pencarian dapat menggambarkan minat. Data transaksi dapat menunjukkan kemampuan dan kebiasaan ekonomi. Interaksi media sosial dapat memperlihatkan hubungan sosial. Data digital tertentu bahkan dapat digunakan untuk menyimpulkan pandangan, preferensi, atau karakteristik individu. Semakin

banyak data yang dikumpulkan, semakin besar pula kemungkinan terbentuknya gambaran yang sangat rinci mengenai kehidupan seseorang (Adytia dkk., 2024; Nafi'ah & Prastyanti, 2025; Shehu & Shehu, 2023).

Risiko tersebut tidak hanya muncul ketika data dicuri. Pemrosesan yang sah secara formal pun dapat menghasilkan persoalan apabila dilakukan secara berlebihan, tidak transparan, atau digunakan untuk tujuan yang tidak dipahami individu. Seseorang mungkin memberikan data untuk memperoleh suatu layanan, tetapi kemudian data tersebut digunakan untuk tujuan lain. Persoalan tersebut menunjukkan bahwa perlindungan data tidak cukup dilakukan dengan mencegah kebocoran. Perlindungan juga harus mengatur perilaku pihak yang secara sah memperoleh data.

Nilai fundamental perlindungan data terletak pada pengakuan bahwa individu bukan sekadar sumber data. Dalam ekonomi digital, terdapat kecenderungan melihat data sebagai komoditas yang dapat dikumpulkan dan dimonetisasi. Perspektif hak fundamental memberikan batas terhadap kecenderungan tersebut. Individu tetap menjadi pemilik kepentingan hukum yang harus dihormati meskipun datanya diproses oleh perusahaan, pemerintah, atau organisasi lain.

Konsepsi tersebut juga menjelaskan mengapa persetujuan semata tidak selalu dapat menyelesaikan persoalan perlindungan data. Dalam hubungan digital, pengguna sering dihadapkan pada pilihan

untuk menerima syarat layanan yang panjang atau kehilangan akses terhadap layanan. Persetujuan dalam keadaan semacam itu dapat bersifat formal tetapi belum tentu mencerminkan kontrol yang benar-benar bermakna. Perlindungan data karena itu membutuhkan prinsip dan hak yang tetap berlaku meskipun individu telah memberikan persetujuan terhadap pemrosesan tertentu (Lalova-Spinks dkk., 2024).

Kebutuhan perlindungan juga meningkat karena pemrosesan data berlangsung dalam jaringan yang saling terhubung. Data yang dikumpulkan oleh satu layanan dapat diteruskan kepada pihak lain, dianalisis dengan sumber data tambahan, disimpan pada sistem cloud, atau dipindahkan ke negara lain. Individu sering tidak mengetahui keseluruhan rantai pemrosesan tersebut. Kondisi tersebut membuat model perlindungan yang hanya mengandalkan hubungan langsung antara individu dan pengumpul data menjadi tidak memadai.

Masalah menjadi semakin kompleks ketika data pribadi digunakan untuk membuat prediksi. Sistem dapat menggunakan data historis untuk memperkirakan preferensi atau perilaku seseorang. Informasi yang dihasilkan bahkan mungkin belum pernah secara eksplisit diberikan oleh individu. Dalam kondisi tersebut, persoalan hukum bukan hanya mengenai siapa yang memiliki data, tetapi juga bagaimana informasi yang "disimpulkan" mengenai seseorang dapat memengaruhi dirinya. Perkembangan *inferred* data menunjukkan bahwa

hak atas data menghadapi persoalan baru ketika informasi yang diproses merupakan hasil prediksi, bukan fakta yang secara langsung diberikan oleh subjek data (Häuselmann & Custers, 2025).

Perlindungan data juga memiliki hubungan dengan kebebasan individu. Ketika seseorang mengetahui bahwa setiap aktivitas dapat dipantau dan dianalisis, terdapat kemungkinan munculnya perilaku menahan diri. Individu mungkin enggan mencari informasi tertentu, mengemukakan pendapat, atau menggunakan layanan tertentu karena khawatir aktivitasnya tercatat. Dengan demikian, perlindungan data tidak hanya berkaitan dengan kerahasiaan informasi, tetapi juga menciptakan kondisi yang memungkinkan individu menjalani kehidupan digital tanpa pengawasan yang tidak proporsional.

Kedudukan data pribadi sebagai hak fundamental juga membawa konsekuensi terhadap negara. Negara tidak hanya mempunyai kewenangan untuk mengatur pengumpulan data, tetapi memiliki kewajiban membangun sistem perlindungan yang efektif. Pengakuan hak tanpa mekanisme pengaduan, pengawasan, penegakan, dan pemulihan akan menghasilkan perlindungan yang bersifat deklaratif. Hak harus dapat digunakan ketika individu menghadapi pelanggaran.

Dunia usaha juga perlu melihat perlindungan data sebagai bagian dari tata kelola. Keamanan dan privasi tidak lagi dapat diposisikan hanya sebagai persoalan departemen teknologi informasi.

Keputusan bisnis mengenai desain produk, pemasaran, pengembangan AI, penggunaan pihak ketiga, dan penyimpanan data memiliki konsekuensi terhadap hak individu. Perlindungan data perlu masuk ke dalam proses pengambilan keputusan sejak awal.

Perkembangan tersebut memperlihatkan bahwa perlindungan data pribadi merupakan bentuk konkret dari penyesuaian hukum terhadap perubahan cara manusia hidup. Ketika informasi pribadi menjadi bagian dari hampir seluruh aktivitas digital, perlindungan terhadap informasi tersebut menjadi bagian dari perlindungan terhadap individu itu sendiri. Karena itu, data pribadi tidak dapat hanya dipandang sebagai aset ekonomi atau objek administratif, melainkan sebagai bagian dari kepentingan fundamental manusia dalam masyarakat digital.

Dengan demikian, perubahan konsep privasi menuju perlindungan data menunjukkan adanya pergeseran dari paradigma "hak untuk dibiarkan sendiri" menuju paradigma "hak untuk memiliki kendali yang bermakna atas informasi mengenai diri sendiri". Perlindungan data menjadi semakin mandiri sebagai rezim hukum, tetapi tetap memiliki akar kuat dalam hak privasi dan hak asasi manusia (Khan, 2025; Kovalenko, 2022). Pergeseran tersebut menjadi dasar bagi pembentukan prinsip pemrosesan data dan hak subjek data yang dibahas pada bagian berikutnya.

2. Prinsip-Prinsip Perlindungan Data Pribadi Dalam Pemrosesan Data Digital

Perlindungan data pribadi tidak akan berjalan apabila hanya didasarkan pada larangan umum untuk "menyalahgunakan data". Pemrosesan data berlangsung dalam banyak tahap dan melibatkan berbagai aktor. Data dapat dikumpulkan, dicatat, dianalisis, disimpan, dipindahkan, digabungkan, dan dihapus. Setiap tahap tersebut memiliki risiko sendiri. Karena itu, hukum membutuhkan prinsip yang dapat menjadi pedoman sejak data pertama kali diperoleh hingga data tidak lagi diperlukan.

Prinsip pertama adalah lawfulness, fairness, dan transparency. Pemrosesan harus memiliki dasar hukum yang sah, dilakukan secara adil, dan dapat dijelaskan kepada subjek data. Prinsip ini mencegah pemrosesan yang dilakukan secara tersembunyi atau dengan cara yang menempatkan individu pada posisi yang tidak wajar. Transparansi juga tidak berarti sekadar menyediakan dokumen kebijakan privasi. Informasi harus disampaikan dengan cara yang memungkinkan individu memahami apa yang terjadi terhadap datanya (Borgesius, 2025; Zisu, 2025).

Transparansi menjadi semakin penting karena pemrosesan data sering berlangsung di balik antarmuka yang sederhana. Pengguna hanya melihat tombol "setuju", sementara di belakangnya terdapat jaringan perusahaan, penyedia layanan, sistem analitik, dan pihak ketiga yang mungkin menerima data. Apabila informasi mengenai rantai pemrosesan

tersebut tidak jelas, individu sulit menggunakan haknya. Transparansi karena itu harus dipahami sebagai kemampuan memahami proses, bukan sekadar formalitas administratif.

Prinsip berikutnya adalah purpose limitation. Data dikumpulkan untuk tujuan tertentu yang sah dan tidak semestinya digunakan secara bebas untuk tujuan yang sama sekali berbeda. Prinsip ini penting karena nilai data membuat organisasi memiliki insentif untuk mempertahankan dan menggunakan kembali informasi yang telah diperoleh. Tanpa pembatasan tujuan, pengumpulan data untuk satu layanan dapat berubah menjadi dasar bagi berbagai bentuk pemrosesan lain yang tidak pernah dibayangkan oleh subjek data (Borgesius, 2025; Shehu & Shehu, 2023).

Data *minimisation* melengkapi pembatasan tujuan tersebut. Organisasi seharusnya tidak mengumpulkan lebih banyak data daripada yang diperlukan untuk mencapai tujuan yang sah. Pengumpulan berlebihan memperbesar risiko kebocoran dan penyalahgunaan. Semakin banyak data yang disimpan, semakin besar pula dampak apabila sistem mengalami serangan. Minimalisasi data karena itu bukan hanya prinsip privasi, tetapi juga merupakan strategi pengurangan risiko keamanan.

Prinsip akurasi menuntut agar data yang digunakan tetap benar dan relevan. Data yang tidak akurat dapat menghasilkan keputusan yang salah. Dalam konteks layanan digital, kesalahan data dapat

menyebabkan seseorang menerima perlakuan yang berbeda, kehilangan akses, atau memperoleh penilaian yang tidak sesuai. Persoalan akurasi menjadi semakin sulit ketika data berasal dari berbagai sumber atau ketika sistem menggunakan prediksi dan inferensi.

Pembatasan penyimpanan atau storage limitation memberikan batas terhadap lamanya data disimpan. Data tidak seharusnya disimpan selamanya hanya karena secara teknis memungkinkan. Penyimpanan harus memiliki alasan yang jelas dan jangka waktu yang dapat dipertanggungjawabkan. Prinsip tersebut juga memaksa organisasi untuk menentukan kapan data harus dihapus, dianonimkan, atau dipisahkan dari identitas individu (Borgesius, 2025).

Keamanan menjadi prinsip yang tidak dapat dipisahkan dari seluruh proses pemrosesan. Data yang sah dikumpulkan sekalipun tetap dapat menimbulkan pelanggaran apabila tidak dilindungi secara memadai. Keamanan mencakup perlindungan terhadap akses tanpa izin, kehilangan, perubahan, penghancuran, dan bentuk pemrosesan yang tidak sah. Karena ancaman digital terus berubah, standar keamanan juga harus mengikuti perkembangan risiko.

Prinsip *accountability* menempatkan tanggung jawab pada organisasi yang menentukan tujuan dan cara pemrosesan. Organisasi tidak cukup mengatakan bahwa mereka telah memiliki kebijakan privasi. Mereka harus mampu menunjukkan bahwa

prinsip perlindungan benar-benar diterapkan. Akuntabilitas dengan demikian mengubah pendekatan dari sekadar "mematuhi aturan" menjadi "mampu membuktikan kepatuhan" (Borgesius, 2025; Christodoulou & Limniotis, 2024).

Prinsip *privacy by design* memperluas perlindungan ke tahap sebelum pemrosesan berlangsung. Perlindungan privasi seharusnya tidak menjadi tambahan setelah suatu aplikasi selesai dibangun. Sistem harus dirancang sejak awal dengan mempertimbangkan minimalisasi data, kontrol akses, keamanan, pengaturan privasi, dan kemampuan pengguna menggunakan haknya. Pendekatan tersebut penting karena keputusan teknis pada tahap desain sering menentukan bagaimana data akan diproses dalam jangka panjang (Christodoulou & Limniotis, 2024; Nafi'ah & Prastyanti, 2025).

Pendekatan *privacy by design* juga mengubah posisi perlindungan data dalam organisasi. Tim hukum, teknologi, keamanan, produk, dan bisnis perlu bekerja bersama. Ketika perlindungan baru diperiksa setelah sistem selesai dibangun, perubahan dapat menjadi mahal dan tidak efektif. Sebaliknya, apabila perlindungan dimasukkan sejak tahap perencanaan, risiko dapat dikurangi sebelum sistem digunakan oleh masyarakat.

Prinsip-prinsip tersebut pada dasarnya membentuk satu rangkaian. Lawfulness memastikan adanya dasar yang sah. Fairness memastikan pemrosesan tidak dilakukan secara tidak wajar.

Transparansi memastikan individu mengetahui apa yang terjadi. Purpose limitation menentukan tujuan. Data minimisation membatasi jumlah data. Akurasi menjaga kualitas informasi. Storage limitation menentukan masa penyimpanan. Keamanan melindungi data. Akuntabilitas memastikan seluruh prinsip tersebut dapat dipertanggungjawabkan.

Hubungan antarp prinsip menjadi penting ketika terjadi konflik kepentingan. Dunia usaha mungkin menginginkan sebanyak mungkin data untuk meningkatkan akurasi sistem. Prinsip minimalisasi mengingatkan bahwa lebih banyak data bukan selalu lebih baik. Organisasi mungkin ingin menyimpan data selama mungkin karena data memiliki nilai ekonomi. Storage limitation memberikan batas. Pengguna mungkin menginginkan layanan yang sangat personal, tetapi personalisasi yang berlebihan dapat menciptakan risiko profiling. Di sinilah prinsip perlindungan berfungsi sebagai mekanisme keseimbangan.

Dalam pemrosesan berbasis AI, prinsip-prinsip tersebut menjadi semakin relevan. Sistem AI membutuhkan data dalam jumlah besar, tetapi kebutuhan teknis tersebut tidak otomatis menjadi dasar hukum untuk mengumpulkan semua data yang tersedia. Penggunaan data harus tetap memiliki tujuan dan dasar yang jelas. Data yang digunakan untuk melatih atau menjalankan sistem juga perlu dinilai dari sisi kualitas, relevansi, keamanan, dan potensi dampaknya terhadap individu.

Prinsip perlindungan juga perlu diterapkan pada penghapusan data. Penghapusan bukan sekadar tindakan teknis menghapus file. Dalam ekosistem digital, salinan dapat berada pada sistem cadangan, perangkat pihak ketiga, atau sistem analitik. Karena itu, organisasi harus memahami siklus hidup data secara keseluruhan. Perlindungan yang efektif membutuhkan kemampuan untuk mengetahui di mana data berada dan bagaimana data berpindah dalam organisasi.

Prinsip perlindungan data berfungsi sebagai "arsitektur hukum" yang membatasi kekuasaan atas informasi. Tanpa prinsip tersebut, organisasi yang menguasai data akan memiliki ruang yang sangat luas untuk menentukan apa yang dapat dilakukan terhadap informasi individu. Prinsip-prinsip tersebut memastikan bahwa kekuasaan tersebut tetap dibatasi oleh tujuan, kebutuhan, transparansi, keamanan, dan akuntabilitas.

Prinsip pemrosesan juga menjadi jembatan antara pengakuan data pribadi sebagai hak fundamental dengan praktik sehari-hari. Hak fundamental akan sulit dirasakan manfaatnya apabila tidak diterjemahkan menjadi kewajiban konkret bagi pengendali data. Karena itu, prinsip lawfulness, transparansi, minimalisasi, keamanan, akuntabilitas, dan *privacy by design* merupakan instrumen yang membuat perlindungan data dapat bekerja dalam praktik (Borgesius, 2025; Zisu, 2025).

3. Hak Subjek Data dan Mekanisme Pengendalian Atas Data Pribadi

Apabila data pribadi dipandang sebagai bagian dari hak fundamental, individu tidak dapat ditempatkan hanya sebagai objek pemrosesan. Individu harus memiliki posisi hukum yang memungkinkan dirinya mengetahui, mempertanyakan, dan dalam batas tertentu mengendalikan penggunaan data mengenai dirinya. Posisi tersebut diwujudkan melalui hak subjek data. Hak tersebut merupakan mekanisme yang mengubah perlindungan data dari konsep abstrak menjadi kemampuan yang dapat digunakan dalam kehidupan sehari-hari.

Hak untuk memperoleh informasi merupakan titik awal. Individu perlu mengetahui siapa yang memproses datanya, untuk tujuan apa, jenis data apa yang digunakan, serta bagaimana data tersebut diperlakukan. Informasi menjadi dasar bagi penggunaan hak-hak lain. Seseorang tidak mungkin mengajukan keberatan atau meminta penghapusan apabila dirinya tidak mengetahui bahwa data tersebut sedang diproses.

Hak akses memberikan kemampuan kepada individu untuk mengetahui data apa yang dimiliki atau diproses mengenai dirinya. Hak tersebut penting karena terdapat kemungkinan bahwa individu tidak mengetahui keseluruhan data yang berada dalam sistem organisasi. Akses memungkinkan individu memeriksa apakah data yang digunakan benar, apakah terdapat data yang tidak seharusnya

diproses, dan apakah informasi tersebut digunakan untuk tujuan yang sesuai.

Hak perbaikan atau *rectification* melengkapi hak akses. Data yang salah dapat menghasilkan konsekuensi yang nyata. Kesalahan identitas, alamat, riwayat transaksi, atau informasi lain dapat memengaruhi pelayanan dan keputusan. Karena itu, individu harus memiliki kesempatan untuk meminta perbaikan. Tantangan baru muncul ketika sistem menggunakan inferred data, karena informasi tersebut merupakan hasil prediksi dan tidak selalu dapat diverifikasi seperti data faktual. Persoalan hak perbaikan terhadap data yang diinferensikan menunjukkan batas baru dalam perlindungan data digital (Häuselmann & Custers, 2025).

Hak penghapusan memberikan mekanisme bagi individu untuk meminta data dihapus dalam keadaan tertentu. Hak ini tidak berarti bahwa setiap data harus dapat dihapus kapan saja tanpa pengecualian. Kepentingan hukum lain, kewajiban penyimpanan, kepentingan publik, atau kebutuhan pembuktian dapat menjadi pertimbangan. Namun, prinsip dasarnya adalah bahwa organisasi tidak boleh menganggap data sebagai aset yang dapat disimpan selamanya tanpa alasan.

Hak pembatasan pemrosesan memberikan alternatif ketika penghapusan belum tepat dilakukan. Dalam kondisi tertentu, individu mungkin tidak menuntut data segera dihapus, tetapi ingin penggunaan data dihentikan sementara atau dibatasi. Mekanisme tersebut penting dalam

sengketa mengenai akurasi, dasar pemrosesan, atau keberatan terhadap penggunaan tertentu.

Hak untuk mengajukan keberatan memberikan ruang bagi individu untuk mempertanyakan pemrosesan tertentu. Hak ini menjadi semakin penting dalam konteks profiling dan pemasaran berbasis perilaku. Individu dapat merasa bahwa pola aktivitasnya digunakan untuk membuat prediksi atau penawaran yang tidak diinginkan. Hak keberatan memberikan mekanisme untuk menguji kembali legitimasi pemrosesan tersebut.

Portabilitas data merupakan perkembangan lain yang memperkuat posisi individu. Hak tersebut memungkinkan data tertentu dipindahkan dari satu penyedia layanan kepada penyedia lain dalam kondisi tertentu. Secara konseptual, portabilitas mengurangi ketergantungan individu terhadap satu platform. Data tidak semestinya menjadi mekanisme yang membuat seseorang tidak dapat berpindah layanan karena seluruh informasi mengenai dirinya terkunci dalam sistem tertentu (Drechsler, 2023; Vrabec, 2021).

Penarikan persetujuan juga merupakan bagian penting dari kontrol individu. Apabila pemrosesan didasarkan pada persetujuan, individu pada prinsipnya perlu memiliki kemampuan untuk menarik persetujuan tersebut. Namun, penarikan persetujuan harus dibedakan dari penghapusan seluruh kewajiban hukum pengendali. Apabila

terdapat dasar pemrosesan lain yang sah, konsekuensi hukumnya dapat berbeda.

Persoalan *consent* menjadi kompleks karena hubungan digital sering tidak sepenuhnya seimbang. Pengguna dapat berhadapan dengan perusahaan yang memiliki kekuatan teknologi, informasi, dan ekonomi yang jauh lebih besar. Pilihan "setuju atau tidak menggunakan layanan" tidak selalu merupakan pilihan yang benar-benar bebas. Penelitian mengenai kontrol individu atas data menunjukkan bahwa persetujuan penting, tetapi tidak selalu cukup ketika pilihan nyata bagi subjek data terbatas (Lalova-Spinks dkk., 2024).

Kondisi tersebut menunjukkan bahwa perlindungan data tidak boleh seluruhnya diserahkan kepada kemampuan individu membaca kebijakan privasi. Dokumen yang sangat panjang dan teknis dapat membuat pengguna menyetujui sesuatu tanpa benar-benar memahami implikasinya. Karena itu, hukum perlu mengombinasikan persetujuan dengan prinsip pemrosesan, pembatasan tujuan, minimalisasi, keamanan, dan akuntabilitas. Kontrol individu harus didukung oleh struktur hukum yang memaksa organisasi bertindak secara bertanggung jawab.

Hak subjek data juga memiliki dimensi kolektif. Pelanggaran terhadap data pribadi seseorang dapat memengaruhi kelompok yang lebih luas. Kebocoran data pelanggan, misalnya, dapat menimpa ribuan atau jutaan orang. Penggunaan algoritma yang diskriminatif juga dapat

menghasilkan pola perlakuan yang memengaruhi kelompok tertentu. Dengan demikian, mekanisme perlindungan tidak hanya perlu memberi ruang bagi pengaduan individual, tetapi juga membutuhkan pengawasan kelembagaan.

Dalam transfer data lintas negara, perlindungan hak subjek data menghadapi tantangan tambahan. Data dapat berpindah dari satu pengendali ke pengendali lain yang berada dalam yurisdiksi berbeda. Perbedaan hukum dapat menyebabkan hak individu yang kuat di satu negara menjadi lebih lemah ketika data dipindahkan. Karena itu, mekanisme transfer perlu mempertahankan tingkat perlindungan yang memadai dan memberikan informasi yang jelas kepada subjek data (Drechsler, 2023; Fachran dkk., 2026).

Hak subjek data pada akhirnya harus memiliki mekanisme pemulihan. Apabila seseorang menemukan bahwa datanya disalahgunakan, hak tersebut tidak cukup apabila hanya memungkinkan dirinya mengajukan permintaan administratif. Harus tersedia jalur pengaduan, pemeriksaan, penyelesaian sengketa, dan apabila memenuhi syarat, kompensasi atau bentuk pemulihan lainnya. Hak tanpa mekanisme penegakan berisiko menjadi hak yang bersifat simbolik.

Kewajiban organisasi terhadap hak subjek data juga harus didukung oleh sistem internal. Permintaan akses, koreksi, penghapusan, atau keberatan perlu dapat diproses dalam jangka waktu yang wajar. Organisasi harus mengetahui data apa

yang dimiliki, di mana data berada, siapa yang mengaksesnya, dan bagaimana perubahan dapat diterapkan. Hal ini menunjukkan bahwa pemenuhan hak subjek data sekaligus merupakan persoalan tata kelola informasi.

Dalam praktiknya, pengendalian individu tidak berarti individu dapat mengendalikan setiap aspek data secara absolut. Sistem digital memiliki kebutuhan operasional, kewajiban hukum, kepentingan publik, dan kebutuhan keamanan. Yang lebih penting adalah menciptakan keseimbangan agar individu tidak kehilangan seluruh kemampuan untuk menentukan bagaimana informasi mengenai dirinya digunakan. Kontrol harus dipahami sebagai kemampuan yang nyata dan proporsional, bukan sebagai kekuasaan mutlak atas setiap bentuk pemrosesan.

Perkembangan hak subjek data menunjukkan adanya perubahan hubungan antara individu dan organisasi. Pada model lama, organisasi cenderung menjadi pihak yang menguasai informasi, sedangkan individu hanya menjadi sumber informasi. Model perlindungan modern mencoba membalik hubungan tersebut dengan menempatkan individu sebagai pemegang hak dan organisasi sebagai pihak yang memikul kewajiban. Hak akses, perbaikan, penghapusan, pembatasan, keberatan, portabilitas, dan penarikan persetujuan merupakan instrumen yang mewujudkan perubahan tersebut (Nafi'ah & Prastyanti, 2025; Vrabec, 2021).

Dengan demikian, hak subjek data merupakan inti operasional perlindungan data pribadi. Prinsip hukum menetapkan bagaimana data boleh diproses, sedangkan hak subjek memberikan kemampuan kepada individu untuk mengawasi dan mempertanyakan pemrosesan tersebut. Keduanya tidak dapat dipisahkan. Ketika hak tersebut berjalan bersama prinsip pemrosesan dan mekanisme penegakan, perlindungan data berubah dari sekadar kewajiban organisasi menjadi sistem yang benar-benar memberikan posisi hukum kepada individu.

4. Tanggung Jawab Pengendali, Prosesor Data, dan Penyelenggara Sistem Digital

Pemrosesan data pribadi hampir tidak pernah dilakukan oleh satu pihak saja. Sebuah aplikasi dapat dikembangkan oleh satu perusahaan, menggunakan layanan cloud dari perusahaan lain, memanfaatkan sistem pembayaran pihak ketiga, menggunakan layanan analitik, dan terhubung dengan berbagai penyedia teknologi. Data pengguna dapat bergerak di antara banyak sistem tanpa terlihat oleh pengguna. Kondisi tersebut menimbulkan pertanyaan mengenai siapa yang bertanggung jawab ketika terjadi kesalahan atau pelanggaran.

Dalam kerangka perlindungan data, penting membedakan pihak yang menentukan tujuan dan cara pemrosesan dengan pihak yang memproses data berdasarkan instruksi. Pembedaan antara *data controller* dan *data processor* membantu menentukan pembagian tanggung jawab. Pengendali pada dasarnya memiliki tanggung jawab utama untuk

memastikan bahwa pemrosesan dilakukan sesuai prinsip dan dasar hukum yang berlaku, sedangkan prosesor menjalankan pemrosesan sesuai hubungan dan instruksi yang sah.

Pembedaan tersebut tidak berarti prosesor bebas dari tanggung jawab. Prosesor memiliki kewajiban tertentu dalam menjaga keamanan dan menjalankan pemrosesan sesuai ketentuan. Perkembangan regulasi juga menunjukkan bahwa otoritas dapat menegakkan kewajiban tertentu secara langsung terhadap prosesor (Borgesius, 2025). Pembagian peran karena itu harus diterjemahkan ke dalam kontrak, prosedur keamanan, pembatasan akses, dan mekanisme pengawasan.

Tanggung jawab pengendali tidak berhenti ketika data diberikan kepada pihak ketiga. Organisasi perlu mengetahui siapa yang memproses data atas namanya, untuk tujuan apa, dan dengan standar perlindungan seperti apa. Penggunaan pihak ketiga tidak semestinya menjadi cara untuk mengalihkan tanggung jawab. Akuntabilitas tetap harus melekat pada pihak yang menentukan tujuan dan struktur pemrosesan.

Keamanan data menjadi salah satu tanggung jawab utama. Organisasi perlu melakukan pengendalian akses, pengamanan sistem, pemantauan, pencadangan, pengujian, serta tindakan lain sesuai tingkat risiko. Keamanan harus dilihat sebagai proses yang berkelanjutan karena ancaman berubah. Sistem yang aman ketika dirancang dapat

menjadi rentan ketika teknologi dan modus serangan berkembang.

Pencegahan kebocoran menjadi semakin penting karena dampak data breach dapat berlangsung panjang. Data yang sekali tersebar sulit dikembalikan ke kondisi semula. Nomor identitas, informasi kontak, kredensial, atau informasi lain dapat digunakan kembali untuk penipuan dan kejahatan lain. Karena itu, pencegahan memiliki nilai yang jauh lebih tinggi daripada sekadar mengandalkan pemulihan setelah kebocoran terjadi.

Ketika terjadi pelanggaran data, organisasi juga perlu memiliki mekanisme respons insiden dan data breach notification. Tujuannya bukan hanya memenuhi kewajiban administratif, tetapi memungkinkan risiko ditangani dengan cepat. Korban dapat mengambil langkah perlindungan apabila mengetahui bahwa datanya telah terkompromi. Keterlambatan informasi dapat memperbesar kerugian karena korban tidak memiliki kesempatan untuk mengubah kredensial, memblokir akses, atau melakukan tindakan pencegahan lain.

Akuntabilitas korporasi juga berkaitan dengan dokumentasi. Organisasi perlu mampu menunjukkan kebijakan, prosedur, penilaian risiko, kontrak dengan pihak ketiga, pelatihan, pengujian keamanan, dan langkah mitigasi yang dilakukan. Akuntabilitas tidak dapat dibuktikan hanya dengan pernyataan bahwa perusahaan "menghargai privasi".

Harus terdapat bukti bahwa prinsip perlindungan benar-benar diterapkan.

Data Protection Impact Assessment (DPIA) menjadi instrumen penting ketika suatu pemrosesan berpotensi menghasilkan risiko tinggi terhadap individu. Penilaian tersebut memungkinkan organisasi mengidentifikasi risiko sebelum sistem digunakan secara luas. Risiko terhadap privasi, keamanan, diskriminasi, pengawasan, dan hak individu dapat dianalisis sejak awal. Pendekatan ini sejalan dengan gagasan *privacy by design*, yaitu memasukkan perlindungan ke dalam arsitektur sistem sejak tahap perancangan (Christodoulou & Limniotis, 2024; Zisu, 2025).

DPIA sangat relevan dalam penggunaan teknologi baru. Sistem pengenalan wajah, profiling, AI, analisis perilaku, dan pemrosesan data dalam jumlah besar dapat menghasilkan risiko yang tidak mudah terlihat. Penilaian dampak membantu organisasi menjawab pertanyaan mendasar: data apa yang diproses, mengapa diperlukan, siapa yang terdampak, risiko apa yang muncul, dan bagaimana risiko tersebut dikurangi.

Persoalan tanggung jawab semakin rumit ketika data dipindahkan ke luar negeri. Data dapat diproses oleh penyedia layanan yang memiliki infrastruktur di negara lain. Transfer tersebut memberikan manfaat ekonomi dan teknis, tetapi sekaligus membawa data ke lingkungan hukum yang berbeda. Karena itu, organisasi perlu memastikan adanya mekanisme perlindungan yang memadai

ketika data berpindah yurisdiksi (Coetzee, 2024; Fachran dkk., 2026).

Transfer lintas batas juga membutuhkan transparansi. Individu perlu mengetahui apabila datanya dikirim atau diproses di negara lain dan memahami konsekuensi yang mungkin timbul. Penelitian mengenai aplikasi digital menunjukkan bahwa informasi mengenai transfer lintas batas kadang disampaikan secara ambigu sehingga menyulitkan pengguna memahami bagaimana data mereka diproses (Guama´n dkk., 2021). Ketidakjelasan tersebut dapat melemahkan transparansi sekaligus menimbulkan persoalan kepastian hukum.

Kontrak antarpihak menjadi instrumen penting dalam hubungan pemrosesan data. Pengendali dan prosesor perlu menentukan tujuan pemrosesan, jenis data, jangka waktu, standar keamanan, akses, penggunaan pihak lain, serta tindakan ketika kontrak berakhir. Kontrak juga perlu mengatur apa yang terjadi terhadap data apabila terjadi insiden. Dengan demikian, hubungan hukum tidak hanya mengatur layanan, tetapi juga mengatur perlindungan terhadap hak individu.

Tanggung jawab tidak berhenti pada hubungan kontraktual. Organisasi perlu memastikan bahwa standar perlindungan tetap berjalan ketika data berpindah dari satu pihak ke pihak lain. Apabila pihak ketiga memiliki standar keamanan yang jauh lebih rendah, keseluruhan sistem menjadi rentan. Karena itu, akuntabilitas perlu dipahami sebagai

tanggung jawab terhadap keseluruhan rantai pemrosesan, bukan hanya terhadap sistem internal.

Perusahaan teknologi dan platform digital juga memiliki posisi strategis karena mereka sering mengendalikan infrastruktur tempat data dikumpulkan dan diproses. Platform memiliki kemampuan teknis untuk mendeteksi pola akses, mengendalikan sistem, dan menerapkan pengamanan. Namun, tanggung jawab tersebut harus dibedakan berdasarkan peran hukum masing-masing. Tidak semua pihak yang menyediakan teknologi otomatis menjadi pengendali atas seluruh data yang berada dalam sistemnya.

Tantangan tersebut menunjukkan pentingnya pembagian tanggung jawab yang jelas. Individu harus mengetahui kepada siapa permintaan hak dapat diajukan. Pengendali harus mengetahui kewajiban yang harus dipenuhi. Prosesor harus memahami batas instruksi dan tanggung jawab keamanan. Pihak ketiga harus memahami kewajiban kontraktual dan hukum. Ketidakjelasan pembagian peran dapat menciptakan ruang saling melempar tanggung jawab ketika terjadi pelanggaran.

Akuntabilitas korporasi juga harus bersifat substantif. Kepatuhan formal melalui dokumen kebijakan tidak cukup apabila praktik sehari-hari tidak sesuai. Organisasi perlu membangun budaya perlindungan data melalui pelatihan, pengawasan, evaluasi, dan kepemimpinan. Perlindungan data pada akhirnya merupakan persoalan tata kelola organisasi.

Hal tersebut menjadi semakin penting dalam ekonomi digital karena data sering menjadi bagian dari model bisnis. Semakin besar nilai ekonomi data, semakin besar pula insentif untuk mengumpulkan dan menggunakan data. Hukum harus memastikan bahwa nilai ekonomi tersebut tidak menghilangkan kepentingan individu. Perlindungan data dan keamanan data perlu berjalan bersama agar pasar digital dapat berkembang tanpa mengorbankan hak pengguna (Ke & Sudhir, 2022).

Tanggung jawab terhadap data juga harus mencakup kemampuan menghadapi perubahan. Organisasi tidak dapat menganggap bahwa kepatuhan pada saat sistem diluncurkan akan tetap memadai selamanya. Teknologi, ancaman, model bisnis, dan pola pemrosesan berubah. Evaluasi risiko karena itu harus dilakukan secara berkala. Akuntabilitas merupakan proses berkelanjutan, bukan satu kali pemeriksaan.

Dengan demikian, struktur tanggung jawab dalam perlindungan data harus dibangun berdasarkan rantai pemrosesan. Pengendali memiliki tanggung jawab atas tujuan dan tata kelola, prosesor memiliki kewajiban dalam pemrosesan yang dipercayakan kepadanya, pihak ketiga harus tunduk pada standar yang jelas, dan penyelenggara sistem harus menerapkan keamanan sesuai perannya. Kerangka tersebut memungkinkan perlindungan data tetap efektif meskipun data bergerak melalui banyak sistem.

5. Tantangan dan Masa Depan Perlindungan Data Pribadi di Era Kecerdasan Artifisial

Perkembangan *big data* mengubah skala pemrosesan data secara fundamental. Data tidak lagi dikumpulkan hanya untuk kebutuhan administratif tertentu, tetapi dapat dikombinasikan dari berbagai sumber untuk menemukan pola. Nilai utama *big data* justru muncul ketika informasi yang sebelumnya terpisah dapat dianalisis secara bersamaan. Kondisi tersebut memberikan manfaat besar bagi penelitian, bisnis, pelayanan publik, dan inovasi, tetapi juga meningkatkan risiko terhadap kendali individu atas informasi pribadinya.

Cloud computing memperluas persoalan tersebut karena data tidak selalu tersimpan dalam perangkat atau lokasi yang mudah diketahui. Data dapat diproses melalui infrastruktur yang dikelola oleh pihak lain dan tersebar di berbagai wilayah. Bagi organisasi, kondisi ini memberikan efisiensi dan fleksibilitas. Bagi hukum, kondisi tersebut menimbulkan pertanyaan mengenai lokasi data, kewenangan, akses, keamanan, dan yurisdiksi yang berlaku.

Internet of Things menghadirkan persoalan lain. Perangkat yang sebelumnya tidak dianggap sebagai alat pengumpulan informasi kini dapat menghasilkan data secara terus-menerus. Jam tangan pintar, kamera, kendaraan, perangkat rumah, dan berbagai sensor dapat mencatat perilaku dan lingkungan pengguna. Ketika jumlah perangkat meningkat, jumlah data yang dihasilkan juga

meningkat. Batas antara ruang fisik dan ruang digital semakin sulit dipisahkan.

Teknologi facial recognition menunjukkan bagaimana data biometrik dapat digunakan untuk mengidentifikasi individu. Berbeda dari kata sandi yang dapat diganti ketika bocor, karakteristik biometrik melekat pada tubuh seseorang. Risiko karena itu memiliki sifat yang berbeda. Penggunaan teknologi pengenalan wajah juga menimbulkan pertanyaan mengenai proporsionalitas, tujuan, persetujuan, pengawasan, dan kemungkinan penggunaan tanpa sepengetahuan individu.

Profiling menjadi tantangan lain karena sistem dapat menyusun gambaran mengenai seseorang berdasarkan berbagai data. Profil tersebut dapat digunakan untuk pemasaran, penilaian risiko, rekomendasi, atau keputusan lainnya. Masalah muncul ketika individu tidak mengetahui bagaimana profil dibuat atau ketika profil tersebut menghasilkan konsekuensi yang merugikan. Semakin kompleks sistem analitik, semakin sulit pula bagi individu memahami alasan di balik suatu keputusan.

Persoalan tersebut mencapai tingkat baru dengan *automated decision-making*. Sistem dapat menghasilkan keputusan atau rekomendasi berdasarkan pemrosesan data tanpa intervensi manusia yang berarti. Dalam konteks tertentu, keputusan otomatis dapat memengaruhi kesempatan seseorang memperoleh layanan, pekerjaan, fasilitas, atau perlakuan tertentu. Karena itu, keputusan otomatis dengan dampak signifikan membutuhkan

batas hukum dan pengawasan yang memadai (Borgesius, 2025; Christodoulou & Limniotis, 2024).

Masalah utama AI terletak pada sifat sistem yang sering sulit dijelaskan. Data masuk ke sistem, diproses melalui model, kemudian menghasilkan keluaran. Namun, hubungan antara data dan hasil tidak selalu mudah dipahami manusia. Ketika individu mempertanyakan suatu keputusan, muncul pertanyaan mengenai seberapa jauh organisasi harus menjelaskan proses algoritmik tersebut. Transparansi algoritmik menjadi bagian dari perkembangan perlindungan data.

AI juga dapat menggunakan data untuk menghasilkan informasi yang sebelumnya tidak secara eksplisit diberikan oleh individu. Sistem dapat memperkirakan minat, risiko, perilaku, atau karakteristik berdasarkan pola data. Informasi tersebut disebut sebagai inferred data. Hak tradisional seperti hak perbaikan menjadi lebih sulit diterapkan karena seseorang dapat membantah suatu prediksi, tetapi tidak selalu dapat membuktikan bahwa prediksi tersebut "salah" dengan cara yang sama seperti kesalahan alamat atau nama (Häuselmann & Custers, 2025).

Risiko diskriminasi algoritmik juga menjadi perhatian. Apabila data yang digunakan mencerminkan bias historis, sistem dapat mengulang atau memperkuat bias tersebut. Bahkan ketika sistem tidak secara eksplisit menggunakan atribut tertentu, kombinasi data lain dapat menghasilkan korelasi yang berfungsi sebagai proksi. Karena itu,

perlindungan data tidak hanya perlu memikirkan kerahasiaan informasi, tetapi juga dampak keputusan yang dihasilkan dari pemrosesan data (Borgesius, 2025; Zisu, 2025).

Pengawasan digital menjadi tantangan lain. Data dapat digunakan untuk memantau pergerakan, perilaku, komunikasi, dan aktivitas masyarakat. Dalam konteks tertentu, pengawasan dapat memiliki tujuan keamanan atau pelayanan publik. Namun, penggunaan pengawasan yang berlebihan dapat memengaruhi kebebasan dan privasi. Karena itu, penggunaan teknologi pengawasan membutuhkan dasar hukum, tujuan yang jelas, proporsionalitas, serta mekanisme pengawasan.

Penggunaan data sensitif juga membutuhkan perhatian khusus. Data yang berkaitan dengan karakteristik tertentu dapat menghasilkan dampak yang lebih serius apabila disalahgunakan. Ketika data sensitif digunakan oleh sistem AI, risiko tidak hanya berasal dari kebocoran, tetapi juga dari kemampuan sistem menarik kesimpulan mengenai individu. Perlindungan harus mencakup bagaimana data diperoleh, untuk apa digunakan, bagaimana dianalisis, dan bagaimana hasilnya memengaruhi individu.

Persoalan lain adalah penggunaan data pribadi untuk melatih AI. Model AI membutuhkan data dalam jumlah besar. Pertanyaan hukum muncul mengenai sumber data, dasar pemrosesan, tujuan penggunaan, hak individu, serta kemungkinan penggunaan kembali data untuk tujuan yang

berbeda. Tidak semua data yang tersedia secara publik otomatis berarti bebas digunakan untuk semua tujuan. Konsep keterbukaan informasi perlu dibedakan dari kebebasan tanpa batas untuk mengambil dan memproses data.

AI juga memperbesar persoalan purpose limitation. Data yang awalnya dikumpulkan untuk satu layanan dapat menjadi bahan bagi sistem analitik atau pelatihan model yang berbeda. Penggunaan sekunder semacam itu perlu dinilai berdasarkan tujuan awal, dasar hukum, risiko, dan ekspektasi subjek data. Tanpa batas yang jelas, ekonomi AI dapat menciptakan dorongan untuk mengumpulkan sebanyak mungkin data dengan alasan bahwa data tersebut mungkin berguna di masa depan.

Privacy by design menjadi semakin penting dalam kondisi tersebut. Sistem AI perlu dirancang dengan mekanisme pembatasan akses, minimalisasi data, pseudonymisation, keamanan, dokumentasi, dan pengawasan manusia. Perlindungan tidak dapat ditempelkan setelah model selesai dibangun. Risiko harus dianalisis sejak tahap pengumpulan data dan desain sistem (Christodoulou & Limniotis, 2024; Zisu, 2025).

Human oversight juga memiliki posisi penting. Pengawasan manusia dapat menjadi mekanisme untuk memeriksa keputusan otomatis yang berpotensi menimbulkan dampak besar. Namun, pengawasan manusia tidak boleh sekadar formal. Manusia yang melakukan pengawasan harus

memiliki kemampuan memahami hasil sistem, memiliki kewenangan untuk menolak hasil yang bermasalah, dan tidak sekadar menerima rekomendasi algoritma tanpa pemeriksaan.

Transfer data lintas negara menjadi tantangan yang semakin besar dalam ekonomi digital. Data dapat diproses oleh perusahaan global, disimpan dalam cloud internasional, dan dianalisis oleh sistem yang berada di negara berbeda. Perbedaan regulasi dapat menciptakan ketidakpastian mengenai standar perlindungan. Karena itu, diperlukan mekanisme yang memungkinkan arus data tetap berjalan tanpa menurunkan tingkat perlindungan terhadap individu (Coche dkk., 2023; Coetzee, 2024).

Dalam transfer internasional, hak subjek data harus tetap diperhatikan. Perpindahan data tidak boleh menyebabkan individu kehilangan hak hanya karena informasi berpindah negara. Kerangka transfer karena itu perlu memperhatikan standar perlindungan, transparansi, kontrak, serta mekanisme pemulihan. Perlindungan yang efektif harus mengikuti data sepanjang siklus pemrosesannya, bukan berhenti di batas wilayah negara (Drechsler, 2023; Fachran dkk., 2026).

Persoalan lintas batas juga menunjukkan keterbatasan pendekatan hukum yang hanya berorientasi nasional. Perusahaan digital dapat beroperasi di banyak negara sekaligus. Satu layanan dapat digunakan oleh jutaan orang dari yurisdiksi berbeda. Harmonisasi prinsip, kerja sama regulator,

dan mekanisme saling pengakuan menjadi semakin penting agar organisasi tidak menghadapi fragmentasi aturan yang ekstrem sekaligus agar individu tidak kehilangan perlindungan ketika datanya bergerak lintas negara (Coche dkk., 2023; Khan, 2025).

Masa depan perlindungan data karena itu tidak dapat hanya dibangun melalui larangan. Regulasi perlu memberikan kepastian bagi inovasi sekaligus menetapkan batas yang jelas. Terlalu sedikit regulasi dapat meningkatkan risiko terhadap individu. Sebaliknya, regulasi yang terlalu kaku dapat menghambat penelitian, teknologi, dan ekonomi digital. Keseimbangan tersebut membutuhkan pendekatan berbasis risiko dan prinsip yang mampu diterapkan pada berbagai teknologi.

Regulasi juga perlu bersifat adaptif. Perubahan teknologi dapat berlangsung lebih cepat daripada proses legislasi. Apabila setiap teknologi baru membutuhkan undang-undang baru, hukum akan selalu berada dalam posisi mengejar perkembangan teknologi. Prinsip yang kuat perlu dikombinasikan dengan aturan teknis, pedoman, standar, pengawasan, dan evaluasi berkala. Dengan pendekatan tersebut, hukum dapat merespons teknologi baru tanpa kehilangan kepastian.

Masa depan perlindungan data juga membutuhkan kerja sama antara regulator, industri, akademisi, masyarakat sipil, dan komunitas teknologi. Tidak ada satu pihak yang memiliki seluruh pengetahuan mengenai risiko digital.

Regulator memahami norma dan kepentingan publik, perusahaan memahami sistem dan model bisnis, akademisi mengembangkan pengetahuan, sedangkan masyarakat mengalami langsung dampak pemrosesan data. Kerja sama tersebut penting untuk menghasilkan kebijakan yang tidak hanya ideal secara normatif, tetapi juga dapat diterapkan.

Perlindungan data pada akhirnya harus mampu menjawab pertanyaan yang lebih mendasar: seberapa jauh teknologi boleh mengetahui tentang seseorang dan seberapa jauh informasi tersebut boleh digunakan untuk menentukan kehidupan orang tersebut? Pertanyaan ini tidak dapat diselesaikan hanya dengan teknologi. Ia merupakan persoalan hukum, etika, ekonomi, dan hak asasi manusia. AI dapat meningkatkan kemampuan manusia memproses informasi, tetapi kemampuan tersebut harus tetap berada dalam batas yang menghormati martabat dan otonomi individu.

Masa depan hukum perlindungan data juga perlu mempertimbangkan bahwa individu tidak selalu mampu memahami seluruh proses yang terjadi terhadap datanya. Sistem semakin kompleks, pemrosesan semakin otomatis, dan jaringan pemrosesan semakin panjang. Karena itu, hukum perlu membangun perlindungan yang tidak seluruhnya bergantung pada kewaspadaan pengguna. Prinsip perlindungan harus bekerja bahkan ketika individu tidak memiliki kemampuan teknis untuk memahami keseluruhan sistem.

Kondisi tersebut mengarah pada kebutuhan untuk mengembangkan model perlindungan yang bersifat preventif. *Privacy by design*, DPIA, pseudonymisation, keamanan, human oversight, dan pengujian risiko dapat digunakan sebelum suatu sistem menimbulkan kerugian. Pendekatan tersebut lebih efektif dibandingkan hanya menunggu pelanggaran kemudian menjatuhkan sanksi (Christodoulou & Limniotis, 2024; Zisu, 2025).

Perlindungan data pribadi di era AI harus menjaga keseimbangan antara empat kepentingan besar. Pertama, kepentingan individu untuk mempertahankan privasi dan kendali atas informasi mengenai dirinya. Kedua, kepentingan dunia usaha untuk mengembangkan inovasi dan menciptakan nilai ekonomi. Ketiga, kepentingan negara dalam menjalankan pelayanan publik dan menjaga keamanan. Keempat, kepentingan masyarakat untuk memperoleh manfaat dari perkembangan teknologi. Tidak satu pun kepentingan tersebut dapat dihapus, tetapi semuanya harus ditempatkan dalam kerangka hukum yang adil.

Masa depan regulasi juga membutuhkan koordinasi lintas negara. Arus data global tidak dapat dipisahkan dari perdagangan digital, layanan cloud, AI, dan ekonomi berbasis platform. Perbedaan standar perlindungan yang terlalu ekstrem dapat menghambat arus data, sedangkan standar yang terlalu rendah dapat mengorbankan hak individu. Kerja sama internasional karena itu menjadi salah satu syarat penting untuk membangun tata kelola

data yang mampu menyeimbangkan hak, inovasi, keamanan, dan kepentingan ekonomi (Coche dkk., 2023; Nafi'ah & Prastyanti, 2025).

Perlindungan data pribadi pada akhirnya harus dipahami sebagai sistem yang hidup. Hak fundamental menjadi dasar normatifnya. Prinsip pemrosesan menjadi pedoman perilakunya. Hak subjek data menjadi mekanisme kontrolnya. Akuntabilitas pengendali menjadi mekanisme pertanggungjawabannya. Teknologi dan regulasi yang adaptif menjadi sarana untuk mempertahankan relevansinya. Seluruh unsur tersebut harus berjalan bersama agar perlindungan data tidak berhenti sebagai deklarasi hukum.

Dengan demikian, tantangan masa depan bukan hanya bagaimana mencegah data dicuri, tetapi bagaimana memastikan bahwa data tidak digunakan dengan cara yang menghilangkan otonomi manusia. Risiko terbesar dalam ekonomi data bukan semata-mata kehilangan kerahasiaan, melainkan hilangnya kemampuan individu untuk mengetahui dan memengaruhi bagaimana informasi mengenai dirinya digunakan. *AI, big data, profiling, automated decision-making, cloud computing*, dan *Internet of Things* membuat persoalan tersebut semakin nyata (Lee, 2024; Saura dkk., 2022; Zisu, 2025).

Perlindungan data pribadi karena itu perlu bergerak dari paradigma reaktif menuju paradigma preventif dan adaptif. Hukum tidak seharusnya menunggu kebocoran data atau diskriminasi algoritmik terjadi sebelum bertindak. Risiko perlu

diidentifikasi sejak desain sistem, hak individu perlu diperkuat sejak awal, dan organisasi perlu mampu menunjukkan akuntabilitas sepanjang siklus hidup data. Pendekatan tersebut memungkinkan hukum mengikuti perkembangan teknologi tanpa kehilangan tujuan utamanya.

Hak subjek data memberikan dimensi operasional terhadap perlindungan tersebut melalui hak akses, perbaikan, penghapusan, pembatasan, keberatan, portabilitas, dan penarikan persetujuan. Sementara itu, pengendali, prosesor, platform, dan penyelenggara sistem digital memikul tanggung jawab untuk memastikan bahwa pemrosesan berlangsung secara aman, transparan, dan dapat dipertanggungjawabkan. Perlindungan tersebut harus tetap tersedia ketika data bergerak lintas sistem dan lintas negara (Drechsler, 2023; Fachran dkk., 2026).

Tantangan terbesar berada pada kemampuan hukum merespons teknologi yang semakin mampu mengolah dan menyimpulkan informasi tentang manusia. AI tidak hanya memproses data yang diberikan, tetapi dapat menghasilkan prediksi dan keputusan yang memengaruhi individu. Karena itu, perlindungan data masa depan harus memperhatikan *profiling, inferred data*, diskriminasi algoritmik, pengawasan, *automated decision-making*, dan penggunaan data untuk pengembangan AI (Häuselmann & Custers, 2025; Zisu, 2025).

Tujuan perlindungan data bukan untuk menghentikan penggunaan teknologi, melainkan

memastikan bahwa perkembangan teknologi tetap berada dalam kerangka penghormatan terhadap manusia. Inovasi digital hanya dapat berkembang secara berkelanjutan apabila masyarakat memiliki kepercayaan bahwa data mereka diperlakukan secara bertanggung jawab. Perlindungan data dengan demikian bukan lawan dari inovasi, melainkan salah satu fondasi agar inovasi digital dapat diterima, dipercaya, dan berkembang secara berkelanjutan.

BAB VI
TRANSAKSI ELEKTRONIK, KONTRAK DIGITAL, DAN KEABSAHAN HUKUMNYA

Perkembangan teknologi digital telah mengubah cara manusia melakukan transaksi. Hubungan jual beli yang dahulu berlangsung melalui pertemuan langsung antara penjual dan pembeli kini dapat terbentuk melalui layar telepon pintar, aplikasi, *marketplace*, surat elektronik, atau sistem perdagangan digital lainnya. Perubahan tersebut bukan sekadar perubahan media transaksi. Perubahan tersebut menyentuh cara para pihak mengenali lawan transaksinya, menyatakan kehendak, melakukan pembayaran, menerima barang atau jasa, menyimpan bukti, serta menyelesaikan sengketa apabila kewajiban tidak dilaksanakan. Transaksi elektronik pada akhirnya membentuk lingkungan hukum yang berbeda secara faktual, meskipun sebagian besar prinsip dasar hubungan perjanjiannya tetap berakar pada hukum perdata. Literatur menunjukkan bahwa transaksi elektronik telah menjadi instrumen penting dalam *E-commerce*, layanan digital, dan pembayaran lintas negara, tetapi kepastian hukumnya sangat bergantung pada kualitas persetujuan, keandalan sistem elektronik, serta kemampuan hukum mengantisipasi hubungan yang melibatkan lebih dari

satu yurisdiksi (Khaled, 2026; Kitov & Kartsev, 2025; Nabila, 2025; Syahmi dkk., 2026).

Perubahan tersebut menimbulkan pertanyaan mendasar: kapan suatu tindakan digital dapat dianggap sebagai tindakan hukum, kapan suatu transaksi dianggap telah terjadi, dan bagaimana hukum memastikan bahwa tindakan yang dilakukan melalui sistem elektronik benar-benar berasal dari pihak yang bersangkutan. Pertanyaan tersebut menjadi semakin penting karena transaksi digital sering berlangsung dalam hitungan detik, sementara proses pembuktiannya dapat dilakukan jauh setelah transaksi selesai. Dengan demikian, hukum tidak cukup hanya menjawab apakah transaksi elektronik diperbolehkan. Hukum juga harus menjelaskan bagaimana transaksi tersebut dibentuk, bagaimana kesepakatan dibuktikan, siapa yang bertanggung jawab ketika terjadi kegagalan sistem, dan bagaimana pihak yang dirugikan memperoleh pemulihan.

Dalam kerangka tersebut, transaksi elektronik perlu dipahami sebagai bagian dari perkembangan hukum perdata yang berhadapan dengan teknologi, bukan sebagai wilayah hukum yang sepenuhnya terpisah dari hukum perdata. Asas kesepakatan, kebebasan berkontrak, itikad baik, kepastian hukum, serta kekuatan mengikat perjanjian tetap memiliki arti penting. Perbedaannya terletak pada medium yang digunakan untuk mewujudkan kehendak para pihak. Jika dalam transaksi konvensional kehendak dapat ditunjukkan melalui pertemuan fisik, tanda tangan di atas kertas, penyerahan barang, atau pembayaran secara langsung,

dalam transaksi elektronik kehendak tersebut diwujudkan melalui data, klik, autentikasi, tanda tangan elektronik, komunikasi digital, dan proses otomatis dalam sistem.

1. **Transformasi Transaksi Konvensional Dalam Ekosistem Digital**

   Perubahan paling mendasar dalam transaksi digital dapat dilihat dari hilangnya kebutuhan untuk mempertemukan para pihak secara fisik. Seorang konsumen dapat membeli barang dari penjual yang berada di kota lain tanpa pernah mengetahui lokasi fisik toko penjual. Perusahaan dapat membuat kontrak dengan mitra bisnis di negara berbeda melalui surat elektronik dan tanda tangan elektronik. Pembayaran dapat dilakukan melalui *payment gateway*, dompet elektronik, transfer bank, kartu pembayaran, atau mekanisme pembayaran digital lainnya. Hubungan hukum dengan demikian terbentuk melalui serangkaian tindakan yang berlangsung dalam sistem elektronik. Transaksi telah bergeser dari model tatap muka menuju model yang bergantung pada infrastruktur digital dan memungkinkan pembentukan hubungan hukum tanpa kehadiran fisik para pihak (Mahfud dkk., 2026; Syahmi dkk., 2026; Syahmi & Subekti, 2026).

   Transformasi tersebut tidak menghilangkan struktur dasar transaksi. Dalam transaksi jual beli tetap terdapat pihak yang menawarkan barang atau jasa, pihak yang menerima penawaran, objek transaksi, harga atau imbalan, serta kewajiban untuk memenuhi prestasi. Yang berubah adalah cara unsur-

unsur tersebut disampaikan dan didokumentasikan. Informasi mengenai barang dapat ditampilkan dalam bentuk katalog digital, harga dapat muncul secara otomatis, persetujuan dapat diberikan dengan menekan tombol tertentu, dan pembayaran dapat diproses oleh sistem pihak ketiga. Proses yang sebelumnya dilakukan melalui beberapa tahapan manual dapat berlangsung secara otomatis dalam satu rangkaian sistem. *E-commerce* modern mencakup hubungan B2B, B2C, C2C, dan berbagai transaksi yang melibatkan pemerintah, dengan karakteristik kecepatan, fleksibilitas, transparansi, dan dematerialisasi proses bisnis (Ansari dkk., 2024; Khaled, 2026).

Dalam transaksi B2B (*business to business*), digitalisasi memungkinkan perusahaan mengadakan hubungan kontraktual tanpa harus berada pada tempat yang sama. Pemesanan bahan baku, pengadaan barang, penyediaan jasa teknologi informasi, pembayaran, pengiriman dokumen, dan konfirmasi penerimaan dapat dilakukan secara elektronik. Kondisi tersebut memberikan efisiensi yang besar, tetapi sekaligus menuntut ketelitian yang lebih tinggi dalam menentukan kapan suatu pesanan menjadi perjanjian yang mengikat. Sistem perusahaan dapat secara otomatis mengirimkan konfirmasi pesanan, tetapi konfirmasi tersebut belum tentu selalu memiliki makna yang sama dengan penerimaan penawaran. Penentuan kedudukan hukum setiap pesan elektronik menjadi

penting agar para pihak tidak keliru membedakan antara informasi administratif dan tindakan hukum.

Pada transaksi B2C (*business to consumer*), persoalan hukum menjadi lebih kompleks karena terdapat kemungkinan ketidakseimbangan posisi antara pelaku usaha dan konsumen. Konsumen biasanya berhadapan dengan kontrak yang telah dirancang sebelumnya dan hanya diberi pilihan untuk menerima atau tidak menggunakan layanan. Situasi tersebut membuat prinsip kebebasan berkontrak harus dibaca bersama dengan prinsip perlindungan konsumen. Persoalan tidak hanya terletak pada apakah konsumen menekan tombol "setuju", tetapi juga apakah konsumen memperoleh informasi yang cukup mengenai isi kontrak, biaya, risiko, pembatasan tanggung jawab, mekanisme pengembalian dana, serta forum penyelesaian sengketa. Undang-Undang Perlindungan Konsumen tetap berlaku sebagai salah satu dasar penting perlindungan dalam hubungan tersebut, termasuk terhadap klausula baku yang dilarang dan klausula yang merugikan konsumen.

Sementara itu, transaksi C2C (*consumer to consumer*) memperlihatkan bentuk hubungan yang berbeda. Platform digital dapat mempertemukan individu yang bertindak sebagai penjual dengan individu lain sebagai pembeli. Platform tersebut mungkin tidak menjadi pemilik barang, tetapi memiliki fungsi penting dalam mempertemukan para pihak, menyediakan sistem komunikasi, memfasilitasi pembayaran, memberikan sistem

penilaian, serta menyediakan mekanisme pengaduan. Karena itu, hubungan hukum dalam transaksi digital tidak selalu hanya terdiri atas penjual dan pembeli. Dalam satu transaksi dapat terdapat penjual, pembeli, penyedia platform, penyedia pembayaran, penyedia logistik, penyedia layanan autentikasi, dan pihak lain yang memberikan infrastruktur digital. Kompleksitas tersebut menyebabkan pembagian tanggung jawab tidak dapat ditentukan hanya berdasarkan siapa yang menerima pembayaran.

Peran *marketplace* menjadi semakin penting karena platform tidak sekadar menjadi ruang pertemuan antara penjual dan pembeli. Platform dapat menentukan format penawaran, sistem pembayaran, mekanisme pengiriman, kebijakan pengembalian barang, sistem ulasan, hingga prosedur penyelesaian komplain. Dalam kondisi demikian, platform memiliki pengaruh terhadap struktur transaksi meskipun tidak selalu menjadi pihak utama dalam kontrak jual beli. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik mengatur perdagangan melalui sistem elektronik dan menempatkan kegiatan perdagangan digital dalam kerangka kewajiban perdagangan yang tetap menuntut legalitas, informasi yang jelas, dan perlindungan konsumen. Regulasi tersebut masih berstatus berlaku.

Perubahan berikutnya berkaitan dengan pembayaran. Dalam transaksi konvensional,

pembayaran sering menjadi tindakan yang dapat diamati secara langsung. Dalam transaksi digital, pembayaran dapat melibatkan beberapa sistem yang bekerja secara berurutan. Konsumen memberikan instruksi pembayaran, sistem pembayaran melakukan autentikasi, bank atau penyedia pembayaran memproses transaksi, kemudian platform menerima informasi keberhasilan pembayaran. Mekanisme seperti kartu internasional, transfer bank, dompet elektronik, *payment gateway*, dan QR lintas negara membuat transaksi menjadi semakin mudah, tetapi juga menambah lapisan hubungan hukum dan risiko operasional (Ansari dkk., 2024).

Persoalan menjadi lebih kompleks ketika transaksi berlangsung lintas batas negara. Pembeli dapat berada di Indonesia, penjual berada di Singapura, server platform berada di Amerika Serikat, sistem pembayaran diproses melalui perusahaan di negara lain, sedangkan barang dikirim dari pusat distribusi di negara keempat. Dalam satu transaksi terdapat beberapa titik hubungan yang memiliki kemungkinan relevansi hukum. *E-commerce*, pembayaran digital, *cloud computing*, dan teknologi berbasis *blockchain* memperluas perdagangan lintas negara, tetapi sekaligus meningkatkan beban kepatuhan terhadap berbagai yurisdiksi (Ansari dkk., 2024; Kitov & Kartsev, 2025).

Kondisi tersebut mengubah cara hukum memahami waktu transaksi. Dalam transaksi konvensional, waktu pembentukan kesepakatan

sering relatif mudah diidentifikasi karena terdapat pertemuan langsung atau pertukaran dokumen. Dalam transaksi elektronik, pesan dapat dikirim dari satu wilayah waktu dan diterima pada wilayah waktu berbeda. Sistem dapat mencatat waktu server, waktu perangkat, atau waktu layanan pihak ketiga. Kontrak dapat terbentuk dalam hitungan detik melintasi batas geografis, sehingga konsep waktu transaksi menjadi lebih cair (Nabila, 2025; Syahmi dkk., 2026).

Persoalan tempat juga mengalami perubahan. Dalam transaksi digital, tidak selalu terdapat satu tempat yang secara sederhana dapat disebut sebagai tempat transaksi. Tempat tinggal penjual, domisili pembeli, lokasi server, lokasi penyedia pembayaran, serta lokasi barang dapat berada di wilayah yang berbeda. Kondisi tersebut tidak berarti konsep tempat kehilangan makna. Sebaliknya, tempat menjadi faktor yang harus dianalisis secara lebih hati-hati untuk menentukan hukum yang berlaku, kewenangan pengadilan, kewajiban pajak, perlindungan konsumen, serta tanggung jawab para pihak. Karena itu, transformasi digital tidak menghapus konsep waktu dan tempat, tetapi membuat kedua konsep tersebut harus dibaca melalui karakteristik teknologi.

Identitas para pihak juga mengalami transformasi. Dalam transaksi tatap muka, identitas dapat diverifikasi melalui kehadiran fisik, dokumen identitas, atau tanda tangan. Dalam transaksi elektronik, identitas dapat direpresentasikan melalui akun, alamat surat elektronik, nomor telepon,

kredensial, sertifikat elektronik, *one-time password*, biometrik, atau mekanisme autentikasi lainnya. Ketergantungan pada data elektronik membuat identitas semakin terkait dengan sistem autentikasi dan infrastruktur platform (Awwad & Abdelsattar, 2025; Syahmi dkk., 2026).

Masalah muncul ketika identitas digital digunakan oleh orang lain. Seseorang dapat kehilangan kendali atas akun, kredensial dapat dicuri, atau perangkat dapat digunakan tanpa persetujuan pemilik. Dalam kondisi demikian, pertanyaan hukum bukan hanya apakah sistem mencatat suatu tindakan, tetapi apakah tindakan tersebut benar-benar dapat diatribusikan kepada pihak yang namanya tercantum dalam sistem. Hal ini menunjukkan bahwa keberadaan catatan digital tidak selalu identik dengan keberadaan kehendak hukum. Catatan tersebut harus ditempatkan dalam rangkaian bukti yang menunjukkan identitas, proses autentikasi, integritas sistem, dan hubungan antara tindakan elektronik dengan pihak yang bersangkutan.

Transformasi transaksi juga mengubah bentuk hubungan hukum dari hubungan yang bersifat sederhana menjadi hubungan yang bersifat ekosistem. Dalam transaksi konvensional, hubungan jual beli dapat digambarkan secara langsung antara penjual dan pembeli. Dalam ekosistem digital, transaksi dapat menghasilkan jaringan hubungan yang melibatkan platform, penyedia pembayaran, perusahaan logistik, penyedia *cloud*, penyedia autentikasi, dan penyedia teknologi lainnya. Masing-

masing pihak dapat memiliki fungsi dan tingkat tanggung jawab yang berbeda. Penentuan tanggung jawab karena itu harus mempertimbangkan fungsi aktual masing-masing pihak, bukan sekadar posisi formalnya.

Pada akhirnya, digitalisasi transaksi tidak seharusnya dipahami sebagai penggantian kertas dengan layar. Perubahan yang terjadi jauh lebih dalam karena teknologi memengaruhi proses pembentukan kehendak, identifikasi para pihak, pembayaran, penyimpanan bukti, serta pelaksanaan prestasi. Kerangka hukum perdagangan elektronik sendiri menegaskan bahwa kegiatan perdagangan melalui sistem elektronik tetap harus memenuhi aspek legalitas dan kejelasan informasi sebelum, selama, dan setelah transaksi berlangsung. Dengan demikian, tantangan hukum transaksi digital bukan sekadar mengakui transaksi elektronik, melainkan memastikan bahwa efisiensi teknologi tidak mengurangi kepastian hukum dan perlindungan pihak yang terlibat.

2. Kontrak Digital dan Mekanisme Pembentukan Kesepakatan

Jika transaksi elektronik menjelaskan keseluruhan proses hubungan perdagangan melalui sistem elektronik, kontrak digital berfokus pada titik ketika kehendak para pihak bertemu dan menghasilkan hubungan hukum. Kontrak digital pada dasarnya bukan jenis perjanjian yang sepenuhnya baru. Perbedaannya terutama terletak pada cara kehendak para pihak dinyatakan,

dikomunikasikan, direkam, dan diverifikasi. Prinsip dasar kontrak tetap relevan, terutama kesepakatan, kecakapan, objek tertentu, dan sebab yang halal (Asan & Azis, 2026; Mahfud dkk., 2026; Ningsih dkk., 2026; Syahmi & Subekti, 2026).

Dalam praktik digital, kesepakatan dapat terbentuk tanpa adanya dokumen yang secara eksplisit ditandatangani oleh kedua pihak. Konsumen mungkin memilih barang, memasukkan barang ke keranjang, melakukan pembayaran, kemudian menerima konfirmasi dari sistem. Dalam situasi lain, perusahaan mengirimkan penawaran melalui surat elektronik dan pihak penerima membalas dengan persetujuan. Pada aplikasi tertentu, pengguna cukup menekan tombol "*I agree*" sebelum dapat menggunakan layanan. Berbagai tindakan tersebut menimbulkan pertanyaan apakah klik, balasan elektronik, atau tindakan penggunaan sistem dapat dianggap sebagai manifestasi kehendak yang memenuhi unsur kesepakatan.

Konsep *offer* dan *acceptance* tetap dapat digunakan untuk menganalisis transaksi semacam itu. Penawaran dapat berupa informasi barang atau jasa yang disampaikan dengan maksud tertentu untuk mengikat, sedangkan penerimaan dapat dilakukan melalui pernyataan maupun tindakan yang menunjukkan persetujuan. Hukum tidak seharusnya terjebak pada bentuk fisik dokumen. Yang lebih penting adalah apakah terdapat hubungan antara penawaran, tindakan penerimaan, dan kehendak untuk terikat. Tindakan elektronik seperti "I agree"

dapat menjadi bentuk persetujuan yang mengikat apabila prosesnya mampu menunjukkan bahwa pengguna mengetahui dan menerima syarat yang ditawarkan (Mahfud dkk., 2026; Sunardi dkk., 2026).

Salah satu bentuk yang paling dikenal adalah *click-wrap agreement*. Pengguna biasanya dihadapkan pada syarat dan ketentuan kemudian diminta memberikan persetujuan dengan menekan kotak atau tombol tertentu. Mekanisme ini relatif lebih kuat karena terdapat tindakan afirmatif yang dapat dicatat oleh sistem. Sistem dapat menyimpan waktu persetujuan, akun pengguna, alamat IP, versi persyaratan, dan informasi teknis lainnya. *Click-wrap* karena itu cenderung lebih mudah digunakan untuk menunjukkan adanya tindakan persetujuan dibandingkan mekanisme yang hanya mengandalkan penggunaan layanan (Mahfud dkk., 2026; Rawat dkk., 2026; Syahmi & Subekti, 2026).

Berbeda dengan *click-wrap*, *browse-wrap agreement* biasanya menganggap bahwa pengguna menyetujui syarat dan ketentuan hanya dengan menggunakan suatu situs atau layanan. Pengguna mungkin tidak diminta menekan tombol persetujuan secara khusus. Mekanisme semacam itu menimbulkan persoalan karena tindakan penggunaan situs belum tentu menunjukkan bahwa pengguna mengetahui keberadaan kontrak dan bermaksud terikat olehnya. Karena itu, kekuatan *browse-wrap* cenderung lebih lemah dan sangat bergantung pada cara syarat tersebut ditampilkan, keterlihatan informasi, serta konteks penggunaan

layanan (Mahfud dkk., 2026; Rawat dkk., 2026; Syahmi & Subekti, 2026).

Perkembangan berikutnya adalah *sign-in-wrap agreement*. Dalam mekanisme ini, persetujuan terhadap syarat layanan dikaitkan dengan proses pembuatan akun atau masuk ke dalam suatu sistem. Persetujuan dapat dinyatakan melalui tindakan seperti menekan tombol "*Create Account", "Sign Up*", atau "*Continue*", dengan pemberitahuan bahwa tindakan tersebut berarti pengguna menyetujui syarat tertentu. Mekanisme ini berada di antara *click-wrap* dan bentuk persetujuan yang lebih implisit. Kekuatan hukumnya sangat bergantung pada apakah pengguna memperoleh pemberitahuan yang cukup jelas mengenai hubungan antara tindakannya dengan persetujuan terhadap kontrak.

Kontrak melalui aplikasi juga memperlihatkan bagaimana proses kontraktual semakin terintegrasi dengan desain sistem. Ketika pengguna melakukan pemesanan melalui aplikasi, sistem dapat secara otomatis menentukan harga, menghitung biaya pengiriman, memproses pembayaran, mengirim notifikasi, dan membuat catatan transaksi. Dari perspektif hukum, otomatisasi tersebut tidak menghapus keberadaan kehendak manusia. Sistem bertindak sebagai sarana yang menerjemahkan tindakan manusia menjadi data dan kemudian menjalankan fungsi tertentu. Persoalan hukumnya terletak pada bagaimana memastikan bahwa sistem bekerja sesuai dengan konfigurasi yang

telah ditetapkan dan bahwa tindakan pengguna dapat dihubungkan dengan kehendaknya.

Surat elektronik juga dapat menjadi media pembentukan kontrak. Penawaran dapat dikirim melalui *email*, kemudian diterima atau ditolak melalui balasan elektronik. Dalam transaksi B2B, pertukaran *email* bahkan dapat berlangsung selama berhari-hari dan menghasilkan serangkaian perubahan terhadap harga, spesifikasi, jadwal, serta syarat pembayaran. Dalam kondisi tersebut, tidak selalu terdapat satu dokumen kontrak tunggal. Hubungan hukum justru dapat dibentuk oleh rangkaian komunikasi. Karena itu, penentuan isi kontrak membutuhkan pembacaan terhadap keseluruhan komunikasi dan tindakan para pihak.

Marketplace menghadirkan persoalan lain karena syarat kontrak dapat berasal dari beberapa sumber sekaligus. Penjual mempunyai deskripsi produk dan kebijakan penjualan, platform mempunyai syarat penggunaan, penyedia pembayaran mempunyai ketentuan layanan, sedangkan konsumen mempunyai hak berdasarkan peraturan perlindungan konsumen. Apabila terjadi sengketa, pertanyaan penting adalah ketentuan mana yang menjadi bagian dari kontrak antara penjual dan pembeli. Masalah tersebut memperlihatkan bahwa kontrak digital tidak selalu berupa satu dokumen, melainkan dapat menjadi kumpulan ketentuan yang tersebar di dalam ekosistem digital.

Di sinilah asas kebebasan berkontrak perlu ditempatkan secara proporsional. Kebebasan

berkontrak memberikan ruang bagi para pihak untuk menentukan isi, bentuk, serta mekanisme hubungan kontraktual. Namun, kebebasan tersebut bukan kebebasan tanpa batas. Dalam transaksi digital, khususnya transaksi konsumen, kontrak sering kali dirancang sepihak oleh pelaku usaha. Konsumen hanya mempunyai pilihan menerima keseluruhan syarat atau meninggalkan layanan. Klausula mengenai pembatasan tanggung jawab, forum sengketa, arbitrase wajib, perubahan sepihak terhadap layanan, dan penggunaan data dapat menimbulkan persoalan fairness kontraktual (Admiral dkk., 2025; Sunardi dkk., 2026).

Persoalan menjadi lebih serius ketika desain antarmuka digunakan untuk memengaruhi keputusan pengguna. *Dark patterns*, misalnya, dapat membuat tombol persetujuan terlihat jauh lebih jelas dibandingkan pilihan untuk menolak, menyembunyikan informasi penting, atau membuat pengguna merasa bahwa persetujuan merupakan satu-satunya pilihan yang tersedia. Dalam keadaan tersebut, secara formal mungkin terdapat klik persetujuan, tetapi secara substantif muncul pertanyaan apakah kehendak pengguna benar-benar terbentuk secara bebas dan terinformasi. Literatur menunjukkan bahwa kontrak digital standar dapat memenuhi konsensualisme secara formal-prosedural, tetapi belum tentu mencerminkan kehendak bebas dan terinformasi ketika terdapat asimetri informasi dan desain manipulatif (Admiral dkk., 2025; Tito dkk., 2026).

Asas itikad baik menjadi penting untuk mengatasi persoalan tersebut. Itikad baik tidak hanya diperlukan pada saat kontrak dilaksanakan, tetapi juga relevan dalam proses pembentukan hubungan kontraktual. Pelaku usaha seharusnya tidak menyusun mekanisme persetujuan dengan tujuan menyembunyikan kewajiban atau mempersulit konsumen memahami konsekuensi kontrak. Sebaliknya, konsumen juga harus menggunakan sistem secara jujur dan tidak melakukan manipulasi terhadap mekanisme transaksi. Dengan demikian, digitalisasi tidak mengubah prinsip itikad baik, tetapi memperluas ruang tempat prinsip tersebut harus diterapkan.

Kontrak digital juga berkembang menuju bentuk yang lebih otomatis melalui *Smart Contract*. Dalam bentuk tertentu, ketentuan kontrak diterjemahkan ke dalam kode yang secara otomatis menjalankan tindakan apabila kondisi yang ditentukan terpenuhi. Misalnya, pembayaran dapat diteruskan ketika sistem mencatat bahwa suatu kondisi telah terjadi. Keunggulan mekanisme tersebut adalah efisiensi dan pengurangan kebutuhan intervensi manusia. Namun, otomatisasi juga menimbulkan persoalan ketika kode tidak mampu mengantisipasi keadaan yang tidak direncanakan oleh pembuatnya. Literatur mengakui potensi *Smart Contract* sebagai inovasi kontraktual, tetapi masih menemukan persoalan mengenai kekosongan norma dan kesesuaian mekanisme

otomatis dengan syarat sah perjanjian (Asan & Azis, 2026; Kitov & Kartsev, 2025).

Perbandingan tersebut memperlihatkan bahwa pertanyaan utama dalam kontrak digital bukan apakah teknologi dapat menghasilkan kontrak, tetapi apakah teknologi mampu menunjukkan kehendak para pihak secara cukup jelas. Semakin kuat hubungan antara tindakan pengguna, informasi yang diberikan, mekanisme autentikasi, dan catatan sistem, semakin mudah tindakan tersebut dipertanggungjawabkan secara hukum. Sebaliknya, semakin implisit mekanisme persetujuan dan semakin kabur informasi kontraktual, semakin besar risiko sengketa mengenai keberadaan maupun isi kesepakatan.

3. Keabsahan Kontrak Elektronik Dalam Perspektif Hukum Perdata dan Hukum Siber

Keberadaan kontrak elektronik tidak berarti hukum perdata harus menciptakan seluruh aturan kontrak dari awal. Prinsip dasar keabsahan perjanjian tetap menjadi titik tolak. Dalam hukum perdata Indonesia, keabsahan perjanjian secara umum bertumpu pada kesepakatan para pihak, kecakapan, adanya objek tertentu, dan sebab yang halal. Kontrak elektronik menghadirkan persoalan bukan karena unsur-unsur tersebut menjadi tidak berlaku, tetapi karena cara membuktikan pemenuhannya berubah. Literatur mengenai kontrak digital di Indonesia juga menempatkan kesepakatan, kecakapan, objek tertentu, dan sebab yang halal sebagai dasar untuk menilai keabsahan kontrak yang

dibuat melalui media elektronik (Asan & Azis, 2026; Mahfud dkk., 2026; Ningsih dkk., 2026; Syahmi & Subekti, 2026).

Unsur kesepakatan merupakan persoalan yang paling sering muncul. Dalam transaksi fisik, kesepakatan dapat terlihat dari pernyataan langsung, tanda tangan, atau tindakan menyerahkan dan menerima barang. Dalam transaksi elektronik, kesepakatan dapat diwujudkan melalui klik, balasan *email*, konfirmasi pembayaran, penggunaan aplikasi, atau tindakan lain yang secara objektif menunjukkan penerimaan. Persoalan hukumnya adalah menentukan apakah tindakan tersebut memang merupakan manifestasi kehendak atau hanya konsekuensi teknis dari penggunaan sistem.

Kehadiran fisik para pihak tidak menjadi syarat mutlak untuk lahirnya kesepakatan. Hubungan kontraktual dapat terbentuk melalui media komunikasi yang memungkinkan pertukaran kehendak. Karena itu, ketiadaan pertemuan fisik tidak dengan sendirinya menghilangkan keabsahan kontrak. Yang harus diperiksa adalah apakah terdapat proses yang cukup untuk menunjukkan bahwa para pihak mengetahui objek transaksi, syarat yang berlaku, serta konsekuensi hukum dari tindakannya. Dalam konteks tersebut, *digital consent* menjadi pusat analisis keabsahan kontrak elektronik (Mahfud dkk., 2026).

Kecakapan para pihak juga tetap menjadi persyaratan penting. Sistem digital pada dasarnya tidak selalu mampu mengetahui apakah seseorang

yang menggunakan akun benar-benar memiliki kapasitas hukum untuk melakukan tindakan tertentu. Seseorang dapat membuat akun menggunakan data tertentu, tetapi sistem belum tentu mengetahui usia, kondisi hukum, atau kewenangan orang tersebut. Dalam transaksi konsumen, persoalan dapat muncul ketika anak atau pihak yang tidak berwenang melakukan transaksi melalui perangkat yang tersedia. Karena itu, teknologi autentikasi identitas perlu ditempatkan bersama mekanisme verifikasi kecakapan, terutama untuk transaksi bernilai tinggi atau transaksi yang menimbulkan konsekuensi hukum signifikan.

Objek tertentu dalam kontrak digital juga harus dapat diidentifikasi. Deskripsi barang dalam *marketplace*, misalnya, harus cukup jelas untuk menentukan barang apa yang dibeli. Dalam kontrak jasa digital, objeknya dapat berupa akses perangkat lunak, layanan penyimpanan, layanan konsultasi, atau hak menggunakan suatu platform. Ketidakjelasan objek dapat menimbulkan kesulitan ketika terjadi sengketa karena para pihak tidak mempunyai dasar yang sama mengenai apa yang sebenarnya diperjanjikan. Digitalisasi tidak mengurangi kebutuhan akan kejelasan objek; justru karena informasi tersebar dalam banyak layar dan dokumen digital, kejelasan tersebut semakin penting.

Sebab yang halal menempatkan kontrak elektronik dalam batas-batas hukum yang sama dengan kontrak konvensional. Fakta bahwa suatu tindakan dilakukan melalui sistem digital tidak

membuat tindakan yang dilarang menjadi sah. Transaksi yang objek atau tujuannya bertentangan dengan hukum tetap bermasalah sekalipun sistem telah mencatat transaksi tersebut secara sempurna. Dengan demikian, keandalan teknologi tidak dapat menggantikan penilaian mengenai legalitas substansi kontrak.

Persoalan berikutnya adalah identitas digital. Identitas digital berfungsi sebagai jembatan antara orang atau badan hukum dengan tindakan yang dilakukan melalui sistem elektronik. Dalam praktiknya, identitas dapat diverifikasi melalui kombinasi *username*, kata sandi, *one-time password*, biometrik, sertifikat elektronik, perangkat tertentu, atau metode lain. Ketergantungan pada identitas digital menuntut sistem yang mampu menghubungkan tindakan tertentu dengan pihak yang tepat. Identitas yang hanya berbentuk akun tidak selalu cukup apabila terdapat risiko pengambilalihan akun atau penggunaan oleh pihak lain.

Tanda tangan elektronik menjadi salah satu mekanisme penting dalam menghubungkan identitas dengan persetujuan. Tanda tangan elektronik dapat berfungsi untuk mengidentifikasi penanda tangan, menunjukkan persetujuan terhadap dokumen, menjaga integritas dokumen, dan mendukung prinsip *non-repudiation*. Namun, tanda tangan elektronik bukan sekadar gambar tanda tangan yang ditempelkan pada dokumen. Keandalan tanda tangan bergantung pada mekanisme autentikasi, keamanan

kunci, sertifikat, serta infrastruktur yang mendukungnya. Literatur menunjukkan bahwa tanda tangan elektronik mempunyai peran sentral dalam memastikan identitas dan integritas, tetapi juga menghadapi risiko pencurian identitas, penyalahgunaan *private key*, dan serangan terhadap infrastruktur sertifikasi (Bendjerad, 2026; Faizin dkk., 2025).

Persoalan menjadi semakin menarik ketika salah satu pihak menyangkal pernah memberikan persetujuan. Misalnya, seseorang menyatakan tidak pernah menekan tombol persetujuan, tidak pernah menandatangani dokumen, atau tidak pernah melakukan transaksi. Dalam kondisi tersebut, sistem elektronik mungkin menunjukkan bahwa transaksi memang terjadi. Akan tetapi, catatan tersebut belum otomatis menyelesaikan persoalan. Harus ditentukan apakah akun tersebut benar-benar berada dalam penguasaan pihak yang bersangkutan, apakah autentikasi dilakukan dengan prosedur yang layak, apakah dokumen telah berubah, dan apakah sistem memiliki catatan yang dapat dipercaya.

Penolakan terhadap persetujuan atau *repudiation* menunjukkan mengapa validitas kontrak dan pembuktian kontrak harus dibedakan. Sebuah kontrak dapat secara normatif sah, tetapi pihak yang mengklaim dirugikan masih harus membuktikan keberadaan kontrak tersebut apabila terjadi sengketa. Sebaliknya, sebuah sistem dapat menghasilkan bukti transaksi yang sangat rinci, tetapi apabila sejak awal tidak terdapat kesepakatan

yang sah, bukti teknis tersebut tidak otomatis menjadikan kontrak sah. Hubungan antara keabsahan dan pembuktian karena itu bersifat saling melengkapi, tetapi tidak dapat disamakan.

Kualitas persetujuan menjadi semakin penting dalam kontrak digital standar. Kontrak yang panjang, menggunakan istilah teknis, menempatkan informasi penting di balik tautan, atau menyembunyikan klausula tertentu dapat membuat konsumen secara formal memberikan persetujuan tetapi secara substantif tidak memahami akibatnya. Kajian mengenai kontrak digital menunjukkan adanya risiko ketika konsensualisme hanya terpenuhi secara formal-prosedural karena adanya *dark patterns*, panjangnya dokumen syarat, dan ketidakseimbangan informasi (Admiral dkk., 2025; Tito dkk., 2026).

Keabsahan kontrak juga berkaitan dengan hubungan antara hukum perdata dan hukum siber. Hukum perdata memberikan dasar mengenai perjanjian dan kewajiban para pihak, sedangkan hukum siber memberikan kerangka mengenai informasi elektronik, transaksi elektronik, sistem elektronik, dan tanda tangan elektronik. Keduanya tidak seharusnya dipertentangkan. Hubungan hukum yang lahir melalui sistem elektronik tetap merupakan hubungan hukum, sedangkan teknologi menjadi medium yang harus dapat diakomodasi oleh sistem hukum. Pendekatan tersebut membuat hukum tidak terjebak pada anggapan bahwa kontrak hanya sah apabila dituangkan dalam bentuk kertas.

Dalam transaksi lintas batas, persoalan keabsahan menjadi lebih rumit karena hukum negara para pihak dapat memiliki standar berbeda mengenai bentuk kontrak, tanda tangan, autentikasi, perlindungan konsumen, atau penggunaan klausula tertentu. Karena itu, kontrak digital internasional sebaiknya dirancang dengan ketentuan yang secara jelas mengatur hukum yang berlaku, mekanisme komunikasi, cara pemberian persetujuan, bukti transaksi, serta forum penyelesaian sengketa. Tanpa kejelasan tersebut, sengketa mengenai keabsahan dapat berubah menjadi sengketa mengenai hukum mana yang harus digunakan terlebih dahulu.

Dengan demikian, keabsahan kontrak elektronik tidak boleh ditentukan hanya berdasarkan pertanyaan apakah kontrak tersebut "digital". Fokus analisis harus diarahkan pada empat hal: apakah terdapat kehendak yang sah, apakah pihak yang menyatakan kehendak mempunyai kapasitas, apakah objek dan tujuan kontrak diperbolehkan, dan apakah terdapat mekanisme yang dapat menunjukkan hubungan antara pihak dengan tindakan elektroniknya. Teknologi memberikan sarana untuk mewujudkan kontrak, tetapi hukum tetap menentukan batas-batas keabsahannya.

4. Alat Bukti Elektronik dan Kekuatan Pembuktian Dalam Sengketa Transaksi Digital

Sengketa transaksi digital memperlihatkan satu persoalan yang sering luput dari perhatian ketika transaksi dilakukan. Pada saat transaksi berlangsung, para pihak biasanya lebih memikirkan

harga, barang, pembayaran, dan pengiriman. Persoalan bukti baru muncul ketika salah satu pihak menyangkal transaksi atau menyatakan bahwa prestasi tidak dilaksanakan. Pada titik tersebut, pihak yang sebelumnya menganggap transaksi telah selesai harus menunjukkan bukti mengenai apa yang terjadi. Dokumen elektronik, informasi elektronik, tanda tangan elektronik, data transaksi, rekaman komunikasi, *audit trail*, dan *timestamp* dapat menjadi bagian dari pembuktian, tetapi keberadaan bukti digital tidak otomatis menentukan kekuatan pembuktiannya (Awwad & Abdelsattar, 2025; Sunardi dkk., 2026; Syahmi dkk., 2026).

Bukti elektronik mempunyai karakter yang berbeda dari dokumen konvensional. Dokumen kertas secara fisik dapat diperiksa dan dibandingkan, sedangkan informasi elektronik dapat disalin berkali-kali tanpa perubahan yang tampak secara kasatmata. Satu dokumen dapat tersimpan pada perangkat pengguna, server perusahaan, sistem *backup*, dan penyedia *cloud*. Karena itu, sengketa tidak hanya menyangkut isi dokumen, tetapi juga asal dokumen, proses pembentukannya, lokasi penyimpanannya, serta kemungkinan perubahan setelah dokumen dibuat.

Autentikasi menjadi persoalan pertama. Pengadilan perlu memperoleh keyakinan bahwa bukti yang diajukan benar-benar berasal dari sumber yang diklaim. Dalam transaksi digital, autentikasi dapat didukung oleh data akun, sertifikat, log sistem, alamat surat elektronik, nomor transaksi, bukti

pembayaran, rekaman komunikasi, dan berbagai informasi teknis. Semakin kompleks transaksi, semakin penting membangun hubungan antara berbagai bukti tersebut sehingga terbentuk satu rangkaian yang koheren.

Persoalan kedua adalah integritas. Bukti digital memiliki nilai yang lebih kuat apabila dapat ditunjukkan bahwa data tidak berubah sejak dibuat atau sejak disimpan dalam sistem. *Hash*, tanda tangan elektronik, log sistem, kontrol akses, dan mekanisme penyimpanan tertentu dapat membantu menunjukkan integritas data. Dalam konteks hukum, integritas berarti bukan sekadar data masih dapat dibuka, tetapi terdapat dasar yang memadai untuk mempercayai bahwa isi data tidak telah dimodifikasi secara tidak sah.

Persoalan ketiga adalah *provenance*, yaitu asal-usul bukti. Pihak yang mengajukan bukti perlu dapat menjelaskan dari mana data tersebut berasal dan bagaimana data berpindah dari satu sistem ke sistem lain. Dalam sengketa digital, isu *provenance* dan *chain of custody* menjadi sangat penting karena bukti dapat berpindah melalui berbagai perangkat, penyedia layanan, atau sistem penyimpanan (Ferreira & Gromova, 2024; Haji dkk., 2026).

Chain of custody pada dasarnya membantu menunjukkan perjalanan suatu bukti sejak ditemukan, dikumpulkan, disimpan, dipindahkan, hingga diajukan. Konsep ini sangat penting ketika bukti berasal dari sistem yang kompleks. Misalnya, dalam sengketa transaksi, bukti dapat berupa log

pada server platform, bukti pembayaran dari bank, rekaman percakapan dari aplikasi, dan dokumen elektronik dari penjual. Apabila tidak ada penjelasan mengenai bagaimana data diperoleh dan disimpan, pihak lawan dapat mempertanyakan keasliannya.

Timestamp juga mempunyai fungsi penting. Waktu yang tercatat pada sistem dapat membantu menentukan kapan dokumen dibuat, kapan persetujuan diberikan, kapan pembayaran dilakukan, atau kapan suatu tindakan terjadi. Namun, waktu digital tidak selalu sederhana karena terdapat perbedaan antara waktu perangkat, waktu server, dan waktu pada sistem pihak ketiga. Oleh karena itu, *timestamp* perlu dilihat sebagai bagian dari keseluruhan sistem pencatatan, bukan sebagai satu-satunya bukti.

Audit trail memberikan gambaran mengenai rangkaian tindakan yang dilakukan dalam suatu sistem. Dalam transaksi digital, *audit trail* dapat menunjukkan siapa yang masuk ke sistem, tindakan apa yang dilakukan, kapan tindakan tersebut dilakukan, dan bagaimana suatu transaksi bergerak dari satu tahap ke tahap berikutnya. Keberadaan *audit trail* dapat membantu pengadilan memahami transaksi yang secara kasatmata tidak dapat diamati karena berlangsung sepenuhnya dalam sistem elektronik.

Bukti pembayaran digital juga mempunyai posisi penting. Bukti transfer, notifikasi pembayaran, nomor referensi, catatan *payment gateway*, atau catatan bank dapat menunjukkan bahwa sejumlah

uang telah dipindahkan. Namun, pembayaran saja belum tentu membuktikan seluruh isi kontrak. Pembayaran dapat menunjukkan adanya tindakan ekonomi, tetapi untuk membuktikan isi perjanjian masih diperlukan bukti mengenai barang, harga, syarat, tanggal penyerahan, serta kewajiban lain yang disepakati.

Rekaman komunikasi menjadi penting ketika kontrak terbentuk melalui *email*, pesan instan, atau sistem komunikasi internal. Rangkaian komunikasi dapat menunjukkan proses negosiasi, perubahan syarat, persetujuan, dan pelaksanaan kontrak. Tantangannya adalah memastikan bahwa komunikasi tersebut benar-benar berasal dari pihak yang diklaim, tidak dipotong sehingga mengubah konteks, dan tidak mengalami perubahan. Karena itu, menyimpan hanya tangkapan layar sering kali tidak cukup untuk menggambarkan keseluruhan konteks transaksi.

Tanda tangan elektronik mempunyai posisi khusus karena dirancang untuk menghubungkan dokumen dengan penanda tangan. Dalam keadaan ideal, tanda tangan elektronik dapat menunjukkan identitas, persetujuan, dan integritas dokumen. Namun, keandalan tersebut bergantung pada keamanan sistem. Pencurian identitas, penyalahgunaan *private key*, atau serangan terhadap infrastruktur sertifikasi dapat mengurangi kekuatan autentikasinya (Bendjerad, 2026; Faizin dkk., 2025).

Sengketa mengenai tanda tangan elektronik dapat muncul dalam bentuk sederhana: seseorang

mengakui bahwa tanda tangan terlihat seperti miliknya tetapi menyangkal bahwa ia memberikan persetujuan. Dalam kasus seperti ini, pembuktian tidak cukup berhenti pada bentuk tanda tangan. Perlu diperiksa bagaimana proses autentikasi berlangsung, apakah sertifikat masih berlaku, siapa yang menguasai kredensial, bagaimana dokumen disimpan, dan apakah terdapat catatan sistem yang menunjukkan proses penandatanganan. Literatur menempatkan kualitas autentikasi, sertifikat elektronik, keandalan sistem, dan kemampuan menunjukkan integritas dokumen sebagai faktor penting ketika terjadi penyangkalan terhadap persetujuan (Bendjerad, 2026; Ningsih dkk., 2026).

Dalam sengketa kontrak, bukti elektronik dapat digunakan untuk membuktikan setidaknya empat persoalan utama. Pertama, apakah kontrak benar-benar pernah terbentuk. Kedua, apa isi kontrak yang disepakati. Ketiga, apakah masing-masing pihak telah melaksanakan kewajibannya. Keempat, apakah salah satu pihak melakukan pelanggaran terhadap kontrak. Bukti digital karena itu tidak hanya relevan pada tahap pembentukan kontrak, tetapi juga sepanjang pelaksanaan hubungan kontraktual.

Untuk membuktikan adanya wanprestasi, misalnya, pembeli dapat menunjukkan bukti pesanan, bukti pembayaran, konfirmasi penjual, informasi pengiriman, dan komunikasi mengenai keterlambatan. Penjual sebaliknya dapat menunjukkan bukti bahwa barang telah dikirim,

diterima, atau ditolak oleh pembeli. Dalam sengketa layanan digital, bukti dapat berupa log penggunaan, catatan akses, laporan sistem, dan komunikasi antara pengguna dengan penyedia layanan. Semua bukti tersebut harus dibaca sebagai satu rangkaian, bukan secara terpisah.

Bukti elektronik juga dapat digunakan dalam perkara perbuatan melawan hukum. Misalnya, suatu pihak dapat mengeklaim bahwa data transaksi digunakan secara tidak sah atau sistem menyebabkan kerugian. Dalam kondisi tersebut, bukti digital dapat membantu menunjukkan hubungan antara tindakan, sistem, dan kerugian. Semakin kompleks infrastrukturnya, semakin penting dukungan ahli untuk menjelaskan bagaimana sistem bekerja.

Kekuatan bukti elektronik tidak ditentukan oleh label "digital" semata. Nilai pembuktiannya bergantung pada autentisitas, integritas, asal-usul, keandalan sistem, kesinambungan penyimpanan, dan kemampuan menjelaskan hubungan antara data dengan peristiwa hukum. Dengan demikian, organisasi yang melakukan transaksi elektronik seharusnya tidak hanya membangun sistem untuk memproses transaksi, tetapi juga membangun sistem untuk mempertahankan bukti transaksi. Dokumentasi digital pada akhirnya merupakan bagian dari manajemen risiko hukum.

5. Wanprestasi, Perlindungan Para Pihak, dan Penyelesaian Sengketa Transaksi Elektronik

Transaksi elektronik tidak selalu berakhir dengan pelaksanaan kewajiban secara sempurna.

Barang dapat tidak dikirim, pembayaran dapat tidak diterima, layanan dapat tidak tersedia, barang dapat berbeda dari deskripsi, atau sistem dapat gagal menjalankan kewajiban yang telah disepakati. Ketika kondisi tersebut terjadi, hubungan digital kembali berhadapan dengan prinsip dasar hukum perdata mengenai pemenuhan prestasi dan tanggung jawab. Digitalisasi tidak menghapus konsep wanprestasi. Pelanggaran terhadap kontrak digital tetap dapat menimbulkan konsekuensi hukum sebagaimana kontrak pada umumnya (Sunardi dkk., 2026).

Wanprestasi dalam transaksi elektronik dapat muncul dalam berbagai bentuk. Penjual mungkin tidak mengirimkan barang setelah pembayaran diterima. Pembeli dapat gagal melakukan pembayaran sesuai kesepakatan. Penyedia layanan digital dapat tidak memberikan layanan sebagaimana dijanjikan. Platform dapat gagal menjalankan mekanisme yang menjadi bagian dari layanan. Bahkan, dalam transaksi berbasis sistem otomatis, kegagalan kode atau sistem dapat menyebabkan kewajiban tidak terlaksana sebagaimana yang dipahami para pihak. Penentuan wanprestasi karena itu harus dimulai dari isi kontrak dan kewajiban yang sebenarnya disepakati.

Kontrak digital sering membuat pembuktian wanprestasi menjadi lebih mudah sekaligus lebih rumit. Lebih mudah karena sistem dapat menyimpan banyak catatan mengenai transaksi. Lebih rumit karena banyaknya catatan tidak selalu berarti mudah menentukan siapa yang bertanggung jawab. Apabila

barang tidak sampai, misalnya, kegagalan dapat terjadi pada penjual, perusahaan logistik, sistem pembayaran, atau platform. Karena itu, tanggung jawab harus ditentukan berdasarkan peran, kewajiban kontraktual, dan hubungan kausal antara tindakan pihak tertentu dengan kerugian.

Selain wanprestasi, transaksi elektronik juga dapat melahirkan perbuatan melawan hukum. Tidak semua kerugian yang terjadi dalam ekosistem digital berasal dari pelanggaran kontrak. Kerugian dapat timbul karena tindakan pihak ketiga, penggunaan sistem secara tidak sah, manipulasi data, penyebaran informasi yang merugikan, atau tindakan lain yang memenuhi unsur perbuatan melawan hukum. Dalam situasi tersebut, dasar tuntutan tidak semata-mata isi kontrak, tetapi juga kewajiban umum untuk tidak menimbulkan kerugian secara melawan hukum.

Akibat hukum dari pelanggaran dapat berbeda tergantung sifat hubungan dan pelanggarannya. Pemulihan dapat berupa pemenuhan kewajiban, penggantian barang, pengembalian pembayaran, pembatalan perjanjian, atau ganti rugi. Dalam hubungan konsumen, mekanisme pemulihan perlu mempertimbangkan posisi konsumen sebagai pihak yang sering memiliki akses lebih terbatas terhadap informasi dan bukti. UU Perlindungan Konsumen mengatur tanggung jawab pelaku usaha atas kerugian konsumen serta mekanisme ganti rugi tertentu.

Perlindungan konsumen menjadi semakin penting dalam kontrak digital karena sebagian besar

transaksi berlangsung melalui kontrak standar. Konsumen biasanya tidak mempunyai kesempatan untuk menegosiasikan isi kontrak. Kondisi tersebut dapat menjadi masalah apabila kontrak berisi pembatasan tanggung jawab yang berlebihan, larangan pengembalian dana, atau mekanisme penyelesaian sengketa yang sangat membebani konsumen. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen melarang sejumlah bentuk klausula baku yang merugikan konsumen dan menyatakan klausula tertentu batal demi hukum.

Persoalan tersebut semakin nyata dalam transaksi lintas negara. Platform dapat menetapkan bahwa sengketa harus diselesaikan berdasarkan hukum negara tertentu dan melalui forum tertentu. Konsumen Indonesia, misalnya, dapat melakukan transaksi dengan perusahaan asing yang menentukan bahwa setiap sengketa harus dibawa ke pengadilan di negara tempat perusahaan tersebut berdomisili. Secara kontraktual, klausula tersebut dapat terlihat sederhana, tetapi secara praktis dapat menimbulkan hambatan biaya, bahasa, jarak, dan akses terhadap keadilan. Literatur menunjukkan bahwa perlindungan konsumen dapat melemah ketika kontrak standar memilih forum asing atau membatasi *remedies* secara sepihak (Admiral dkk., 2025; Nabila, 2025).

Tanggung jawab *marketplace* juga perlu dianalisis secara hati-hati. Platform tidak selalu menjadi penjual, tetapi platform dapat memiliki fungsi yang sangat menentukan terhadap transaksi.

Platform dapat menerima pembayaran, menahan dana, mengatur komunikasi, menyediakan sistem ulasan, menentukan mekanisme pengembalian, dan melakukan moderasi terhadap penjual. Apabila platform hanya bertindak sebagai perantara teknis, tanggung jawabnya dapat berbeda dengan platform yang secara aktif mengendalikan seluruh proses transaksi. Karena itu, tanggung jawab tidak seharusnya ditentukan hanya berdasarkan label "*marketplace*".

Penyedia pembayaran juga memiliki posisi penting. Kegagalan pembayaran dapat menyebabkan transaksi tidak terlaksana meskipun penjual dan pembeli telah sepakat. Dalam situasi tersebut perlu ditentukan apakah kegagalan berada dalam ruang tanggung jawab penyedia pembayaran atau merupakan konsekuensi tindakan pengguna. Kontrak layanan, sistem keamanan, catatan transaksi, serta standar operasional menjadi penting untuk menentukan tanggung jawab.

Hubungan yang sama berlaku pada penyedia layanan logistik. Dalam transaksi digital, penjual dan pembeli dapat tidak pernah bertemu karena barang berpindah melalui perusahaan logistik. Ketika barang hilang atau rusak, kontrak antara penjual dan pembeli harus dibedakan dari hubungan antara penjual dengan perusahaan logistik. Bukti pengiriman, *tracking*, tanda terima elektronik, dan catatan serah terima menjadi bagian penting untuk menentukan kapan penguasaan barang berpindah dan siapa yang bertanggung jawab.

Penyelesaian sengketa melalui pengadilan tetap menjadi mekanisme penting. Pengadilan memiliki kewenangan untuk menilai keabsahan kontrak, menafsirkan kewajiban para pihak, menilai bukti elektronik, serta menentukan bentuk pemulihan. Namun, proses pengadilan dapat menghadapi kendala apabila transaksi melibatkan pihak yang berada di negara berbeda atau bukti tersimpan pada sistem yang berada di luar yurisdiksi. Kondisi tersebut membuat mekanisme alternatif semakin relevan.

Arbitrase dapat digunakan apabila para pihak telah menyepakati klausula arbitrase. Dalam transaksi B2B bernilai tinggi, arbitrase dapat memberikan keuntungan berupa forum yang lebih khusus dan fleksibel. Namun, arbitrase juga memiliki biaya dan prosedur yang harus dipertimbangkan. Dalam kontrak konsumen, klausula arbitrase yang dipaksakan melalui kontrak standar perlu diperiksa dari perspektif perlindungan konsumen dan fairness kontraktual.

Mediasi menawarkan pendekatan yang berbeda. Mediasi memungkinkan para pihak mencari penyelesaian yang dapat diterima bersama tanpa harus memperoleh putusan yang sepenuhnya memenangkan salah satu pihak. Dalam transaksi digital, mediasi dapat digunakan untuk menyelesaikan persoalan pengembalian dana, keterlambatan, barang yang tidak sesuai, atau sengketa layanan. Keunggulannya terletak pada

fleksibilitas dan kemungkinan mempertahankan hubungan bisnis.

Perkembangan yang semakin relevan adalah *Online Dispute Resolution* atau ODR. ODR menggunakan teknologi untuk mempertemukan para pihak, menyampaikan dokumen, mengelola komunikasi, dan memfasilitasi penyelesaian sengketa tanpa mengharuskan para pihak hadir pada satu tempat. Mekanisme ini sangat relevan bagi transaksi digital karena sengketa dapat melibatkan pihak yang berada jauh secara geografis. Literatur mengenai transaksi digital lintas batas menempatkan ODR dan harmonisasi sebagai salah satu arah penting dalam penyelesaian sengketa perdagangan digital (Kitov & Kartsev, 2025; Nabila, 2025).

ODR bukan berarti setiap sengketa harus diselesaikan melalui algoritma. Teknologi dapat menyediakan ruang dan prosedur, tetapi keputusan mengenai hak dan kewajiban tetap membutuhkan dasar hukum yang jelas. Sistem ODR yang baik harus menjamin identitas para pihak, keamanan dokumen, kesempatan untuk menyampaikan argumen, transparansi prosedur, serta akses terhadap mekanisme pemulihan. Tanpa perlindungan tersebut, ODR hanya akan menjadi bentuk digital dari prosedur yang tetap tidak seimbang.

Pilihan hukum (*choice of law*) menjadi persoalan utama dalam transaksi lintas negara. Para pihak dapat menentukan hukum negara tertentu sebagai hukum yang berlaku bagi kontrak. Namun, pilihan tersebut tidak selalu menyelesaikan seluruh

persoalan. Hukum yang dipilih mungkin mengatur hubungan kontraktual, tetapi aturan wajib mengenai perlindungan konsumen, keamanan data, atau ketertiban umum suatu negara tetap dapat berlaku. Karena itu, klausula pilihan hukum perlu dirancang dengan memahami batas-batas penerapannya.

Pilihan forum (*choice of forum*) juga perlu dibedakan dari pilihan hukum. Pilihan hukum menentukan hukum yang digunakan untuk menilai hubungan para pihak, sedangkan pilihan forum menentukan lembaga yang berwenang menyelesaikan sengketa. Kedua hal tersebut dapat menunjuk negara yang sama, tetapi tidak selalu demikian. Dalam transaksi digital, pemisahan ini penting karena para pihak dapat memilih hukum suatu negara tetapi menunjuk arbitrase atau pengadilan di negara lain.

Masalah pilihan hukum dan forum menjadi lebih sensitif ketika salah satu pihak adalah konsumen. Konsumen mungkin menyetujui syarat melalui satu klik tanpa menyadari bahwa sengketa harus dibawa ke negara lain. Karena itu, keberadaan klausula tersebut harus dibaca bersama prinsip perlindungan konsumen. Kontrak digital yang secara formal telah disetujui belum tentu bebas dari pemeriksaan mengenai keadilan klausulanya.

Dalam transaksi B2B, para pihak biasanya memiliki kemampuan yang lebih besar untuk bernegosiasi mengenai pilihan hukum dan forum. Mereka dapat menentukan hukum yang dianggap paling sesuai dengan transaksi dan memilih arbitrase

internasional apabila diperlukan. Namun, kebebasan tersebut tetap harus disertai dengan kejelasan. Klausula yang terlalu luas atau ambigu dapat justru menjadi sumber sengketa baru mengenai forum yang berwenang.

Transaksi lintas batas juga membutuhkan harmonisasi hukum. Perbedaan standar mengenai kontrak elektronik, tanda tangan, bukti elektronik, perlindungan konsumen, dan penyelesaian sengketa dapat meningkatkan biaya transaksi. Pelaku usaha harus memahami aturan di berbagai negara, sementara konsumen menghadapi ketidakpastian mengenai haknya. Literatur mengenai transaksi digital lintas negara menunjukkan bahwa pertumbuhan *E-commerce* global menghadirkan kebutuhan terhadap kerangka hukum yang lebih harmonis (Kitov & Kartsev, 2025; Nabila, 2025).

Harmonisasi tidak selalu berarti seluruh negara harus mempunyai hukum yang identik. Yang lebih realistis adalah membangun prinsip bersama mengenai pengakuan kontrak elektronik, tanda tangan elektronik, bukti digital, perlindungan konsumen, autentikasi, dan mekanisme kerja sama. Dengan prinsip yang lebih kompatibel, transaksi lintas negara dapat dilakukan dengan tingkat kepastian yang lebih tinggi. ODR dapat menjadi bagian dari arah tersebut karena memungkinkan sengketa diselesaikan melalui infrastruktur digital yang sesuai dengan karakter transaksi.

Perlindungan para pihak harus mencakup seluruh siklus transaksi. Perlindungan tidak cukup

diberikan setelah terjadi sengketa. Perlindungan harus dimulai dari pemberian informasi sebelum transaksi, desain mekanisme persetujuan, keamanan pembayaran, penyimpanan bukti, pelaksanaan kewajiban, mekanisme pengaduan, hingga penyelesaian sengketa. Pendekatan tersebut lebih sesuai dengan karakter transaksi digital yang seluruh prosesnya berlangsung melalui sistem.

Hubungan antara teknologi dan hukum juga menunjukkan bahwa tanggung jawab tidak dapat seluruhnya dialihkan kepada pengguna melalui klausula standar. Pelaku usaha yang merancang sistem memiliki pengetahuan dan kontrol yang lebih besar terhadap teknologi. Karena itu, pelaku usaha harus memiliki tanggung jawab untuk membangun sistem yang aman, transparan, dan dapat menyediakan bukti yang memadai. Konsumen tidak seharusnya menanggung seluruh risiko hanya karena transaksi dilakukan secara digital.

Secara konseptual, wanprestasi dalam transaksi elektronik tetap merupakan persoalan pemenuhan kewajiban kontraktual. Namun, cara membuktikan pelanggaran, menentukan pihak yang bertanggung jawab, serta memperoleh pemulihan menjadi lebih kompleks karena transaksi melibatkan sistem dan pihak ketiga. Bukti elektronik, *audit trail*, rekaman pembayaran, dan komunikasi digital menjadi instrumen penting dalam menentukan apa yang sebenarnya terjadi.

Oleh karena itu, penyelesaian sengketa transaksi digital sebaiknya tidak hanya memikirkan

tahap akhir ketika konflik sudah terjadi. Kontrak harus dirancang sejak awal dengan memperhatikan kemungkinan sengketa. Para pihak perlu menentukan standar komunikasi, mekanisme pemberitahuan, bukti transaksi, prosedur pengaduan, batas tanggung jawab yang wajar, hukum yang berlaku, dan forum penyelesaian sengketa. Dengan demikian, kontrak bukan hanya alat untuk menciptakan hubungan hukum, tetapi juga instrumen untuk mengelola risiko apabila hubungan tersebut mengalami masalah.

.

BAB VII
KEBEBASAN BEREKSPRESI, KONTEN ILEGAL, DAN SENSOR DI RUANG SIBER

Perkembangan internet telah mengubah cara manusia menyampaikan pendapat, memperoleh informasi, membangun komunitas, dan berpartisipasi dalam kehidupan publik. Jika sebelumnya komunikasi publik sangat bergantung pada media massa dengan struktur produksi informasi yang relatif terpusat, ruang siber memungkinkan hampir setiap orang menjadi pembuat sekaligus penyebar informasi. Seseorang dapat menyampaikan pandangan politik melalui media sosial, mengkritik kebijakan pemerintah melalui video, memberikan ulasan terhadap suatu produk, melakukan investigasi secara mandiri, atau membangun gerakan sosial melalui jaringan digital. Perubahan tersebut memperluas ruang kebebasan berekspresi, tetapi sekaligus menciptakan persoalan baru mengenai batas kebebasan, tanggung jawab pengguna, serta kewenangan negara dan platform digital dalam mengendalikan konten.

Kebebasan berekspresi di ruang digital karena itu tidak dapat dipahami hanya sebagai persoalan kebebasan berbicara melalui perangkat elektronik. Internet telah menjadi infrastruktur sosial yang

menghubungkan hak untuk mencari, menerima, dan menyebarkan informasi dengan berbagai kepentingan lainnya. Pendidikan, asosiasi, partisipasi politik, kebebasan pers, dan inklusi sosial semakin bergantung pada akses terhadap internet. Kebebasan berekspresi dalam lingkungan digital dengan demikian memiliki dimensi yang lebih luas karena pembatasan akses atau pembatasan distribusi informasi dapat secara langsung memengaruhi kemampuan seseorang untuk berpartisipasi dalam kehidupan masyarakat (Cohen & Fung, 2023; Jorgi & Firmansyah, 2026; Sˇramel & Michal, 2025).

Pada saat yang sama, ruang siber bukan ruang tanpa hukum. Kemampuan seseorang untuk menyampaikan informasi secara cepat dan luas dapat digunakan untuk tujuan yang konstruktif, tetapi juga dapat digunakan untuk menyebarkan ancaman, kebencian, penipuan, pornografi anak, hasutan kekerasan, atau informasi yang menimbulkan kerugian. Di sinilah hukum menghadapi persoalan yang sulit: membatasi ekspresi yang benar-benar merugikan tanpa mengubah pembatasan tersebut menjadi alat untuk membungkam kritik, perbedaan pendapat, atau ekspresi kelompok yang tidak populer.

Persoalan tersebut semakin kompleks karena pengendalian terhadap ekspresi tidak lagi hanya dilakukan oleh negara. Perusahaan teknologi yang mengoperasikan media sosial, *search engine*, *marketplace*, layanan video, dan platform komunikasi mempunyai kemampuan untuk menentukan apakah suatu konten dapat dipublikasikan, diperlihatkan kepada

pengguna lain, diturunkan peringkatnya, atau dihapus. Algoritme rekomendasi bahkan dapat memengaruhi tingkat visibilitas suatu ekspresi tanpa menghapusnya secara langsung. Ruang kebebasan berekspresi pada akhirnya dibentuk oleh interaksi antara negara, platform, algoritme, dan pengguna (Araujo, 2025; Are´valo Ramí´rez & Rousset Siri, 2025; Cohen & Fung, 2023).

Kondisi tersebut menimbulkan pertanyaan mendasar mengenai tata kelola ruang siber. Ketika negara menghapus suatu konten, dasar kewenangannya harus dapat dipertanggungjawabkan. Ketika platform menghapus konten pengguna, dasar keputusannya juga perlu dapat dipahami. Ketika algoritme menurunkan visibilitas suatu konten, pengguna harus memiliki kemungkinan untuk mengetahui dan, dalam keadaan tertentu, menggugat keputusan tersebut. Oleh sebab itu, isu kebebasan berekspresi digital tidak hanya berkaitan dengan substansi konten, tetapi juga dengan prosedur pengambilan keputusan terhadap konten.

1. Kebebasan Berekspresi Sebagai Hak Fundamental di Ruang Siber

Kebebasan berekspresi merupakan salah satu fondasi penting kehidupan demokratis. Hak tersebut memberikan ruang bagi individu untuk menyampaikan pendapat, mengkritik kebijakan, mengemukakan gagasan, menyebarkan informasi, dan berpartisipasi dalam perdebatan publik. Internet memperluas ruang tersebut secara signifikan. Seseorang yang sebelumnya tidak memiliki akses terhadap media massa dapat membuat akun media sosial dan menyampaikan pendapat kepada ribuan

bahkan jutaan orang. Dalam pengertian tersebut, ruang siber bukan sekadar alat komunikasi, melainkan telah berkembang menjadi infrastruktur yang memungkinkan pelaksanaan kebebasan berekspresi.

Kebebasan berekspresi dalam lingkungan digital mencakup hak untuk mencari, menerima, dan menyebarkan informasi melalui internet dan media digital. Hak tersebut tidak berhenti pada tindakan berbicara atau menulis. Kemampuan mengakses informasi juga merupakan bagian penting karena seseorang tidak dapat berpartisipasi secara bermakna dalam diskursus publik apabila informasi yang diperlukan tidak tersedia. Internet dengan demikian memiliki fungsi ganda: sebagai sarana seseorang menyampaikan pendapat dan sebagai sarana masyarakat memperoleh informasi yang diperlukan untuk membentuk pendapatnya sendiri (Cohen & Fung, 2023; Jorgi & Firmansyah, 2026; S˘ramel & Michal, 2025).

Hubungan antara internet dan kebebasan berekspresi menjadi semakin erat ketika teknologi digunakan untuk mendukung pendidikan, asosiasi, partisipasi politik, dan inklusi sosial. Masyarakat dapat menggunakan media digital untuk membangun komunitas, menggalang dukungan, menyampaikan aspirasi, mengawasi kebijakan publik, dan mengorganisasi kegiatan sosial. Karena itu, akses internet yang luas dan nondiskriminatif mempunyai arti penting bagi pelaksanaan hak-hak tersebut (Are´valo Ramí´rez & Rousset Siri, 2025).

Perubahan struktur komunikasi juga menjadikan ruang siber sebagai ruang publik baru. Dalam model media tradisional, produksi informasi cenderung dikendalikan oleh sejumlah organisasi media yang memiliki sumber daya untuk menentukan informasi apa yang dipublikasikan. Media sosial dan platform digital mengubah struktur tersebut dengan memberikan kemampuan publik untuk memproduksi dan mendistribusikan informasi sendiri. Ruang siber menjadi lebih inklusif karena masyarakat dapat menjadi penulis, pembicara, komentator, dan pengorganisasi tindakan kolektif tanpa harus terlebih dahulu memperoleh akses dari institusi media tradisional (Cohen & Fung, 2023).

Namun, perluasan akses tersebut tidak selalu menghasilkan ruang publik yang lebih sehat. Media sosial dapat menciptakan polarisasi karena pengguna cenderung berinteraksi dengan kelompok yang memiliki pandangan serupa. *Trolling*, *doxxing*, disinformasi, kampanye kebencian, dan manipulasi informasi dapat mengurangi kualitas diskursus publik. Ruang digital karena itu memiliki karakter ambivalen: di satu sisi memberikan kesempatan yang lebih luas untuk berbicara, tetapi di sisi lain dapat menciptakan lingkungan yang membuat sebagian orang takut berbicara atau menarik diri dari diskusi publik (Boutellier, 2026; Cohen & Fung, 2023).

Persoalan tersebut dapat dilihat melalui fenomena *user-generated content*. Pengguna tidak lagi hanya menjadi konsumen informasi, tetapi juga menjadi produsen informasi. Video, komentar,

podcast, unggahan media sosial, *blog*, ulasan, meme, dan berbagai bentuk ekspresi digital dapat mempunyai dampak sosial yang besar. Satu unggahan yang awalnya dibuat untuk audiens terbatas dapat menyebar secara luas melalui mekanisme rekomendasi dan *sharing*. Karakter viral tersebut membuat konsekuensi hukum suatu ekspresi menjadi jauh lebih sulit diprediksi dibandingkan komunikasi interpersonal.

Kebebasan berekspresi juga memiliki hubungan yang erat dengan kebebasan pers. Media digital memungkinkan jurnalis dan organisasi media mendistribusikan berita secara lebih cepat serta menjangkau audiens yang lebih luas. Pada saat yang sama, individu dapat melakukan aktivitas jurnalistik secara mandiri melalui platform digital. Batas antara jurnalis profesional, aktivis, akademisi, dan warga biasa menjadi lebih cair. Kondisi tersebut memperluas demokratisasi informasi, tetapi sekaligus meningkatkan persoalan mengenai verifikasi, akurasi, dan tanggung jawab atas informasi yang disebarkan.

Dalam demokrasi, kritik terhadap pemerintah merupakan salah satu bentuk ekspresi yang memiliki nilai sosial tinggi. Kritik memungkinkan masyarakat mengawasi kekuasaan dan mengoreksi kebijakan publik. Oleh karena itu, hukum perlu membedakan kritik terhadap kebijakan dari ekspresi yang menyerang individu secara melawan hukum. Kritik yang keras, tidak populer, atau menyinggung kepentingan tertentu tidak

dengan sendirinya kehilangan perlindungan hukum. Kajian mengenai demokrasi digital di Indonesia menunjukkan bahwa tantangan utama terletak pada bagaimana melindungi kebebasan berekspresi sekaligus mencegah penyalahgunaan ruang digital (Jorgi & Firmansyah, 2026).

Kebebasan berekspresi juga harus dipahami bersama dengan hak orang lain. Hak untuk menyampaikan pendapat tidak memberikan legitimasi untuk mengancam keselamatan orang lain, menyebarkan data pribadi secara melawan hukum, atau menghasut kekerasan. Dengan demikian, perlindungan kebebasan berekspresi bukan berarti seluruh bentuk komunikasi digital harus dilindungi tanpa pengecualian. Perlindungan justru membutuhkan mekanisme untuk membedakan ekspresi yang memiliki nilai demokratis dengan ekspresi yang menimbulkan kerugian yang secara hukum dapat dibenarkan untuk dibatasi.

Tantangan terbesar muncul ketika ekspresi yang sah berada sangat dekat dengan ekspresi yang berpotensi menimbulkan kerugian. Pernyataan politik dapat dianggap provokatif oleh sebagian orang tetapi menjadi kritik yang sah bagi pihak lain. Sebuah satire dapat dianggap menghina oleh orang yang menjadi objeknya, tetapi dipandang sebagai ekspresi artistik oleh masyarakat. Persoalan semacam ini menunjukkan bahwa hukum tidak dapat hanya menggunakan pendekatan mekanis terhadap kata-kata tertentu. Konteks, tujuan, dampak, dan posisi para pihak perlu diperhatikan.

Karena itu, kebebasan berekspresi digital tidak cukup dijamin melalui larangan sensor. Perlindungan juga membutuhkan akses terhadap internet, kebebasan mencari informasi, transparansi platform, mekanisme keberatan, dan perlindungan terhadap tindakan pembatasan yang sewenang-wenang. Ketika seseorang kehilangan akses terhadap platform atau kontennya diturunkan secara sistematis, dampaknya dapat menyerupai pembatasan ekspresi meskipun tidak terdapat larangan langsung dari negara.

Ruang siber memperluas kebebasan berekspresi sekaligus memperbesar tanggung jawab sosial dari setiap ekspresi. Internet telah menciptakan ruang publik yang lebih terbuka, tetapi keterbukaan tersebut membutuhkan tata kelola agar tidak berubah menjadi ruang yang didominasi oleh intimidasi, manipulasi, dan kebencian. Tantangan hukum bukan memilih antara kebebasan atau pengendalian, melainkan membangun kondisi yang memungkinkan kebebasan berekspresi tetap terlindungi tanpa membiarkan ekspresi yang benar-benar melanggar hukum merugikan pihak lain.

2. Batasan Kebebasan Berekspresi dan Pertanggungjawaban Hukum di Ruang Siber

Kebebasan berekspresi bukanlah hak yang tidak mempunyai batas. Dalam kehidupan sosial, ekspresi seseorang dapat berinteraksi dengan kepentingan dan hak orang lain. Negara karena itu dapat menetapkan pembatasan tertentu terhadap ekspresi apabila pembatasan tersebut mempunyai

dasar hukum dan ditujukan untuk melindungi kepentingan yang sah. Namun, kewenangan membatasi tidak berarti negara bebas menentukan ekspresi mana yang boleh atau tidak boleh ada. Pembatasan harus ditempatkan dalam kerangka hukum yang jelas dan dapat diuji.

Prinsip yang penting dalam menentukan legitimasi pembatasan adalah *necessity* dan *proportionality*. Pembatasan harus benar-benar diperlukan untuk mencapai tujuan yang sah dan tidak boleh melampaui apa yang diperlukan untuk mencapai tujuan tersebut (Are´valo Ramí´rez & Rousset Siri, 2025; Jorgi & Firmansyah, 2026; Petrov & Kumar, 2025; S˘ramel & Michal, 2025). Dengan pendekatan ini, hukum tidak hanya bertanya apakah pembatasan mempunyai dasar hukum, tetapi juga apakah pembatasan tersebut tepat dan proporsional terhadap persoalan yang hendak diselesaikan.

Penerapan prinsip proporsionalitas menjadi penting karena ruang siber memungkinkan suatu pembatasan berdampak sangat luas. Menghapus satu unggahan mungkin tampak sebagai tindakan sederhana, tetapi apabila unggahan tersebut merupakan bagian dari diskusi publik yang penting, penghapusan dapat memengaruhi banyak orang. Begitu pula pemblokiran suatu situs dapat menghentikan akses terhadap konten yang melanggar hukum sekaligus konten lain yang sebenarnya sah. Oleh sebab itu, semakin luas dampak suatu pembatasan, semakin kuat pula alasan hukum yang diperlukan untuk membenarkannya.

Salah satu batas penting adalah perlindungan reputasi. Seseorang tidak seharusnya menggunakan internet untuk menyebarkan tuduhan palsu yang secara sengaja merusak nama baik orang lain. Namun, perlindungan reputasi tidak boleh digunakan untuk menghapus kritik yang sah. Kritik terhadap tindakan pejabat publik, kebijakan pemerintah, atau perusahaan dapat mempunyai nilai kepentingan publik. Literatur menekankan perlunya membedakan kritik terhadap kebijakan publik dari penghinaan, pencemaran nama baik, ujaran kebencian, ancaman, dan bentuk ekspresi lain yang dapat dibatasi (Jorgi & Firmansyah, 2026).

Ancaman kekerasan mempunyai karakter berbeda dari kritik. Ketika seseorang menyampaikan ancaman yang nyata terhadap keselamatan orang lain, hukum memiliki kepentingan yang lebih kuat untuk melakukan intervensi. Hal yang sama berlaku terhadap hasutan yang secara nyata mendorong kekerasan. Namun, tidak setiap pernyataan keras dapat langsung dikategorikan sebagai ancaman atau hasutan. Konteks, sasaran, kemungkinan terjadinya kekerasan, dan hubungan antara pernyataan dengan tindakan nyata perlu diperhatikan.

Ujaran kebencian juga menjadi salah satu persoalan yang paling sulit. Ekspresi yang menyerang individu atau kelompok berdasarkan identitas tertentu dapat memperkuat diskriminasi dan kekerasan. Namun, definisi ujaran kebencian yang terlalu luas dapat mengubah pernyataan yang sebenarnya merupakan kritik atau perdebatan

menjadi konten yang dianggap terlarang. Karena itu, hukum perlu membangun batas yang jelas agar larangan terhadap ujaran kebencian tidak menjadi instrumen untuk membungkam perbedaan pandangan.

Persoalan yang sama muncul dalam pengaturan disinformasi. Tidak semua informasi yang salah secara otomatis merupakan tindak pidana. Seseorang dapat membagikan informasi yang ternyata tidak benar karena kesalahan, ketidaktahuan, atau sumber yang tidak dapat dipercaya. Jika setiap kesalahan informasi dipidana, ruang diskusi publik dapat menjadi terlalu represif. Kajian mengenai Indonesia bahkan mendorong agar kriminalisasi disinformasi dibatasi pada informasi yang disebarkan secara masif dan menimbulkan *significant harm*, bukan terhadap setiap informasi yang salah (Prahassacitta & Harkrisnowo, 2021).

Perbedaan antara kesalahan dan kesengajaan menjadi penting dalam menentukan pertanggungjawaban. Orang yang sengaja menciptakan informasi palsu untuk menimbulkan kepanikan memiliki karakter perbuatan yang berbeda dari orang yang membagikan informasi karena mengira informasi tersebut benar. Hukum perlu memperhatikan unsur kesalahan, tujuan, skala penyebaran, dan dampak yang ditimbulkan. Pendekatan yang hanya berfokus pada benar atau salahnya informasi dapat mengabaikan aspek subjektif dan kontekstual dari tindakan komunikasi.

Pertanggungjawaban hukum juga harus mempertimbangkan hubungan antara pengguna dan platform. Pengguna adalah pihak yang menghasilkan konten, tetapi platform menyediakan infrastruktur yang membuat konten dapat tersebar secara luas. Platform dapat mempunyai kebijakan internal yang mengatur konten, tetapi kebijakan tersebut tidak boleh dianggap identik dengan hukum negara. Platform mempunyai kepentingan bisnis dan tata kelola komunitas sendiri. Karena itu, penghapusan konten oleh platform perlu dibedakan dari pembatasan oleh negara.

Perbedaan tersebut penting karena sanksi negara memiliki konsekuensi hukum yang berbeda dari tindakan platform. Ketika negara menjatuhkan sanksi, tindakan tersebut harus didasarkan pada hukum dan tunduk pada mekanisme hukum. Ketika platform menghapus konten, tindakan tersebut didasarkan pada kontrak atau kebijakan layanan. Namun, karena platform mengendalikan ruang komunikasi yang sangat luas, keputusan privat tersebut dapat mempunyai dampak sosial yang menyerupai pembatasan publik.

Dalam lingkungan digital, satu orang juga dapat menjadi subjek dari beberapa rezim pertanggungjawaban sekaligus. Suatu unggahan dapat menimbulkan persoalan pidana apabila memenuhi unsur tindak pidana, persoalan perdata apabila merugikan pihak lain, dan persoalan administratif apabila melanggar kewajiban tertentu. Oleh karena itu, penentuan pertanggungjawaban

tidak dapat dilakukan hanya dengan melihat label "konten ilegal". Harus dilihat norma mana yang dilanggar dan jenis akibat hukum apa yang tersedia.

Pertanggungjawaban juga harus disertai perlindungan terhadap kebebasan berekspresi. Mekanisme penegakan hukum yang terlalu agresif dapat menghasilkan efek jera (*chilling effect*), yaitu keadaan ketika masyarakat memilih diam karena takut menghadapi konsekuensi hukum. Efek tersebut berbahaya bagi demokrasi karena masyarakat bukan hanya kehilangan hak untuk berbicara, tetapi juga kehilangan keberanian untuk mengkritik kebijakan atau mengemukakan informasi yang penting bagi kepentingan publik.

Dengan demikian, pembatasan kebebasan berekspresi membutuhkan tiga lapisan pengujian. Pertama, harus terdapat dasar hukum yang jelas. Kedua, tujuan pembatasan harus sah. Ketiga, cara pembatasan harus diperlukan dan proporsional. Kerangka tersebut membantu mencegah hukum berubah menjadi instrumen sensor yang berlebihan sekaligus tetap memungkinkan negara melindungi masyarakat dari ekspresi yang benar-benar menimbulkan kerugian.

3. Konten Ilegal dan Problematika Penentuan Batas Antara Konten Terlarang dan Konten yang Dilindungi

Istilah *illegal content* tampak sederhana, tetapi dalam praktik memiliki cakupan yang sangat luas. Konten dapat dianggap ilegal karena melanggar hukum pidana, hukum perdata, hak kekayaan

intelektual, perlindungan konsumen, privasi, atau ketentuan khusus lainnya. Bentuknya dapat berupa ujaran kebencian, hasutan kekerasan, pencemaran nama baik, pornografi anak, pelanggaran hak cipta, penipuan, perjudian daring, serta berbagai bentuk konten lain yang dilarang oleh hukum (Allakuliev, 2025; Gede dkk., 2024; Korpisaari, 2022).

Keragaman tersebut menciptakan persoalan bagi platform digital. Platform yang mengoperasikan media sosial dapat menerima laporan mengenai konten yang dianggap melanggar hukum, tetapi menentukan apakah suatu konten benar-benar ilegal sering membutuhkan penilaian hukum yang kompleks. Sebuah konten mungkin dianggap melanggar hak cipta, tetapi juga dapat mempunyai fungsi kritik atau pendidikan. Sebuah pernyataan mungkin dianggap sebagai ujaran kebencian oleh satu kelompok, tetapi dipandang sebagai perdebatan politik oleh kelompok lain. Karena itu, moderasi konten sering kali berada pada batas antara penilaian hukum dan penilaian kebijakan platform.

Masalah paling sulit terdapat pada *borderline content*. Konten semacam ini tidak dengan mudah dikategorikan sebagai legal atau ilegal. Contohnya adalah satire politik, kritik tajam, humor yang menyinggung kelompok tertentu, informasi yang belum terbukti kebenarannya, atau komentar yang kasar tetapi belum mencapai tingkat ancaman. Regulator dan pengadilan menghadapi kesulitan ketika menentukan kapan opini yang masih dilindungi berubah menjadi tindakan yang

menimbulkan *harm* dan dapat dibatasi (Caruso, 2024; Petrov & Kumar, 2025; S̆ramel & Michal, 2025).

Disinformasi merupakan contoh yang paling jelas. Informasi salah dapat mempunyai dampak negatif, terutama ketika menyangkut kesehatan publik, pemilu, keamanan, atau bencana. Namun, tidak semua informasi salah mempunyai tingkat bahaya yang sama. Informasi yang salah karena kesalahan jurnalistik dapat berbeda dengan informasi yang sengaja dibuat untuk memicu kepanikan. Bahkan sebagian informasi yang dianggap salah pada suatu waktu dapat berubah setelah bukti baru ditemukan. Karena itu, regulasi disinformasi harus mempertimbangkan konteks dan dampak, bukan hanya status benar atau salah.

Konsep *lawful but awful* menunjukkan persoalan tersebut. Ada konten yang secara moral dianggap buruk atau meresahkan, tetapi belum tentu melanggar hukum. Dalam keadaan demikian, keinginan untuk menghapus konten tersebut dapat berhadapan dengan prinsip kebebasan berekspresi. Kajian mengenai respons legislatif terhadap misinformasi, disinformasi, dan malinformasi menunjukkan bahwa sebagian ekspresi berada dalam wilayah yang tidak mudah dijangkau oleh hukum yang sudah ada (Chesterman, 2025; Petrov & Kumar, 2025).

Ujaran kebencian juga memperlihatkan kebutuhan terhadap definisi yang jelas. Konten yang menyerang kelompok tertentu dapat memiliki konsekuensi sosial yang serius, tetapi larangan yang

terlalu luas dapat mencakup perdebatan akademik, kritik agama, kritik politik, atau diskusi mengenai isu sensitif. Karena itu, penentuan apakah suatu konten termasuk ujaran kebencian harus mempertimbangkan sasaran ekspresi, isi, konteks, tujuan, kemungkinan menimbulkan diskriminasi atau kekerasan, serta dampak aktualnya.

Konten pornografi juga membutuhkan pembedaan. Tidak semua konten seksual memiliki status hukum yang sama. Pornografi anak, misalnya, memiliki karakter yang sangat berbeda karena menyangkut eksploitasi seksual terhadap anak. Konten lain dapat berkaitan dengan persoalan moral, perlindungan anak, atau hak orang dewasa. Hukum karena itu harus menggunakan kategori yang jelas agar tindakan perlindungan tidak berubah menjadi pelarangan yang terlalu luas.

Perjudian daring menunjukkan bagaimana perkembangan teknologi memperluas bentuk konten ilegal. Promosi perjudian dapat dilakukan melalui media sosial, iklan digital, situs, *influencer*, atau layanan komunikasi. Konten yang mengarahkan pengguna ke aktivitas perjudian dapat memiliki dampak berbeda dengan diskusi akademik mengenai perjudian. Pembedaan antara informasi mengenai suatu aktivitas dan promosi untuk mendorong partisipasi menjadi penting dalam menentukan batas hukum.

Pelanggaran hak cipta juga menunjukkan kompleksitas yang sama. Platform dapat menerima jutaan unggahan setiap hari dan tidak mungkin

memeriksa seluruh konten secara manual. Sistem otomatis kemudian digunakan untuk mendeteksi konten yang diduga melanggar hak cipta. Namun, sistem otomatis dapat melakukan kesalahan karena tidak selalu memahami konteks penggunaan. Materi yang digunakan untuk kritik, pendidikan, atau penelitian dapat secara keliru dianggap sebagai pelanggaran.

Ancaman kekerasan memiliki karakter yang lebih jelas ketika terdapat hubungan nyata antara pernyataan dan bahaya yang ditimbulkan. Namun, pernyataan yang menggunakan bahasa kasar atau emosional tidak selalu dapat dianggap sebagai ancaman. Hukum harus menghindari kecenderungan mengkriminalisasi ekspresi hanya karena ekspresi tersebut tidak menyenangkan. Tujuan perlindungan hukum adalah mencegah kerugian yang nyata dan bukan menghilangkan seluruh bentuk komunikasi yang kontroversial.

Risiko penggunaan hukum secara berlebihan telah menjadi perhatian dalam pengaturan disinformasi dan ujaran kebencian. Definisi yang kabur dapat memberikan diskresi yang terlalu luas kepada aparat atau platform sehingga memungkinkan penerapan yang tidak konsisten. Kajian menunjukkan bahwa hukum anti-disinformasi dan anti-*hate speech* berpotensi digunakan secara berlebihan apabila definisi dan kewenangan tidak dirancang secara hati-hati (Petrov & Kumar, 2025; Santos dkk., 2025; Sˇramel & Michal, 2025).

Dalam konteks tersebut, hukum perlu membedakan antara konten ilegal, konten berbahaya, dan konten yang sekadar tidak disukai. Konten ilegal merupakan konten yang memenuhi unsur pelanggaran hukum. Konten berbahaya dapat menimbulkan risiko sosial tetapi belum tentu memenuhi unsur pelanggaran. Konten yang tidak disukai adalah ekspresi yang mungkin dianggap buruk, ofensif, atau kontroversial tetapi tetap berada dalam wilayah kebebasan berekspresi. Ketiga kategori tersebut tidak boleh diperlakukan dengan instrumen hukum yang sama.

Perbedaan tersebut juga menentukan bentuk respons. Konten ilegal dapat dikenai penghapusan, pembatasan akses, atau sanksi sesuai hukum. Konten berbahaya mungkin lebih tepat ditangani melalui peringatan, pembatasan rekomendasi, *fact-checking*, atau peningkatan literasi. Sementara itu, konten yang hanya kontroversial seharusnya tidak menjadi objek sensor hanya karena menimbulkan ketidaknyamanan.

Model kategorisasi tersebut dapat membantu mencegah sensor berlebihan. Ketika setiap konten kontroversial langsung dikategorikan sebagai konten ilegal, hukum kehilangan kemampuan membedakan antara perlindungan masyarakat dan perlindungan terhadap kenyamanan sosial. Padahal, demokrasi membutuhkan ruang bagi gagasan yang tidak populer. Perlindungan kebebasan berekspresi justru menjadi paling penting ketika ekspresi tersebut menantang pandangan dominan.

Dengan demikian, penentuan konten ilegal harus selalu dikaitkan dengan norma yang jelas, konteks, tujuan, tingkat bahaya, dan akibat yang ditimbulkan. Pendekatan semacam ini memungkinkan hukum melindungi masyarakat tanpa menghapus ruang perdebatan publik. Batas antara kebebasan dan pelanggaran memang tidak selalu dapat dibuat secara matematis, tetapi hukum dapat membangun prosedur yang membuat penentuan batas tersebut lebih rasional, transparan, dan dapat dipertanggungjawabkan.

4. Sensor, Moderasi Konten, dan Tanggung Jawab Platform Digital

Sensor digital tidak selalu tampil dalam bentuk pemblokiran atau penghapusan konten. Dalam lingkungan digital, suatu konten dapat tetap tersedia tetapi dibuat lebih sulit ditemukan. Platform dapat menurunkan peringkat konten, membatasi rekomendasi, mengurangi jangkauan, memberikan label tertentu, membatasi akun, atau mengeluarkan pengguna dari platform. Perubahan tersebut menunjukkan bahwa kontrol terhadap ekspresi bekerja melalui berbagai tingkatan visibilitas. Literatur mengenai moderasi konten menunjukkan pergeseran dari fokus semata pada *removal* menuju bentuk seperti *demotion*, *downranking*, pembatasan rekomendasi, *shadow banning*, dan *de-platforming* (Gillespie, 2022).

Perbedaan antara penghapusan dan penurunan visibilitas penting secara hukum. Penghapusan mudah dikenali karena pengguna dapat

melihat bahwa kontennya tidak lagi tersedia. Penurunan visibilitas lebih sulit diketahui karena konten masih tampak tersedia bagi pemilik akun, tetapi tidak lagi muncul dalam rekomendasi atau hasil pencarian. Akibatnya, pengguna mungkin tidak mengetahui bahwa distribusi ekspresinya telah dibatasi. Kontrol semacam ini dapat memengaruhi ruang publik tanpa terlihat seperti sensor tradisional.

Algoritme memainkan peran besar dalam proses tersebut. Platform menggunakan sistem otomatis untuk mengidentifikasi, mengklasifikasikan, merekomendasikan, dan membatasi konten. Penggunaan AI dapat membantu memproses jumlah konten yang sangat besar, tetapi juga menimbulkan persoalan ketika sistem melakukan kesalahan. Algoritme dapat gagal memahami konteks, satire, bahasa lokal, atau istilah yang mempunyai makna berbeda dalam komunitas tertentu. Persoalan tersebut semakin serius ketika keputusan algoritme tidak transparan.

Opaque algorithms menjadi salah satu masalah utama dalam moderasi konten. Pengguna sering tidak mengetahui mengapa konten tertentu diturunkan, direkomendasikan, atau dihapus. Platform dapat menggunakan kombinasi AI, kebijakan internal, dan sistem peringkat yang kompleks. Dalam isu politik sensitif, keputusan semacam itu dapat memengaruhi distribusi gagasan tertentu tanpa mekanisme yang mudah dipahami oleh pengguna (Abokhodair dkk., 2024; Araujo, 2025; Petrov & Kumar, 2025).

Masalah tersebut dapat dilihat dari hubungan antara moderasi dan demokrasi. Jika platform mempunyai kemampuan menentukan informasi apa yang dilihat publik, platform pada dasarnya mempunyai kekuasaan terhadap struktur diskursus publik. Platform tidak sama dengan negara, tetapi keputusan platform dapat mempunyai konsekuensi publik yang besar. Hal ini menimbulkan pertanyaan apakah perusahaan swasta yang mengelola ruang komunikasi publik harus tunduk pada standar transparansi dan akuntabilitas tertentu.

Tanggung jawab platform tidak dapat ditentukan dengan satu formula untuk semua keadaan. Penyedia yang hanya menyediakan infrastruktur teknis memiliki posisi berbeda dengan platform yang aktif mengkurasi, memberi peringkat, merekomendasikan, dan memonetisasi konten. Semakin besar kemampuan platform untuk mengendalikan distribusi konten, semakin besar pula pertanyaan mengenai tanggung jawabnya terhadap konten yang berada dalam ekosistemnya (Allakuliev, 2025; Korpisaari, 2022).

Perbedaan tersebut penting untuk menghindari dua ekstrem. Ekstrem pertama adalah menganggap platform selalu bertanggung jawab atas seluruh konten pengguna. Pendekatan tersebut dapat membuat platform melakukan sensor berlebihan untuk menghindari risiko hukum. Ekstrem kedua adalah memberikan kekebalan mutlak kepada platform. Pendekatan tersebut dapat membuat platform mengabaikan risiko yang secara nyata

muncul dari sistem yang mereka kelola. Model yang lebih rasional perlu mempertimbangkan tingkat kontrol dan pengetahuan platform terhadap konten.

Mekanisme *notice and takedown* merupakan salah satu bentuk tata kelola yang dapat digunakan. Pihak yang merasa dirugikan dapat memberikan pemberitahuan kepada platform mengenai konten yang diduga melanggar hukum. Platform kemudian melakukan penilaian berdasarkan hukum dan kebijakannya. Mekanisme tersebut memberikan jalur yang relatif cepat untuk menangani konten bermasalah, tetapi memiliki risiko apabila laporan dapat dibuat secara berlebihan atau digunakan untuk menyerang pihak yang berbeda pendapat.

Risiko tersebut semakin besar apabila platform hanya mengandalkan laporan pengguna tanpa pemeriksaan yang memadai. Pihak yang ingin membungkam kritik dapat menggunakan sistem pelaporan untuk menyebabkan konten lawan dibatasi. Karena itu, *notice and takedown* membutuhkan prosedur pemeriksaan, dokumentasi alasan keputusan, dan kemungkinan pengajuan keberatan. Tanpa mekanisme tersebut, sistem pelaporan dapat berubah menjadi instrumen sensor privat.

Hak untuk mengajukan keberatan atau *appeal mechanism* menjadi bagian penting dari moderasi yang adil. Pengguna yang kontennya dihapus perlu mengetahui alasan penghapusan dan mempunyai kesempatan untuk menjelaskan konteksnya. Hal ini sangat penting ketika keputusan

dibuat secara otomatis. Sistem yang hanya memberikan pesan "konten melanggar kebijakan" tanpa penjelasan memadai membuat pengguna tidak dapat memahami atau menggugat keputusan tersebut.

Moderasi otomatis juga harus memperhatikan kesalahan algoritme. AI dapat mendeteksi pola tertentu, tetapi tidak selalu dapat memahami makna sosial suatu pernyataan. Satire, kutipan berita, diskusi akademik, atau dokumentasi pelanggaran hak asasi dapat mengandung kata-kata yang sama dengan konten yang dilarang. Jika sistem hanya membaca kata tanpa memahami konteks, konten yang sah dapat ikut dihapus. Kajian mengenai moderasi otomatis menunjukkan bahwa bias algoritmik dan kurangnya transparansi dapat memengaruhi keputusan terhadap konten, khususnya pada isu politik sensitif (Abokhodair dkk., 2024).

De-platforming menimbulkan persoalan yang lebih serius karena pengguna dapat kehilangan akses terhadap seluruh komunitas digital. Bagi sebagian individu atau organisasi, platform bukan hanya tempat berbagi informasi, tetapi juga sarana mencari pelanggan, menjalankan usaha, mengorganisasi kegiatan, atau membangun reputasi. Penghapusan akun dapat karena itu mempunyai konsekuensi ekonomi dan sosial yang besar. Tindakan tersebut perlu dibedakan dari penghapusan satu konten tertentu karena tingkat dampaknya jauh lebih luas.

Pemblokiran oleh negara mempunyai karakter berbeda dari moderasi platform. Negara menggunakan kewenangan publik untuk membatasi akses terhadap konten atau layanan tertentu. Karena itu, pemblokiran harus mempunyai dasar hukum yang jelas dan dapat dipertanggungjawabkan. Kajian komparatif menunjukkan bahwa pemblokiran dapat digunakan untuk melindungi ketertiban publik dan menangani konten ilegal, tetapi dapat menjadi persoalan demokratis apabila digunakan ketika unsur melawan hukum belum terbukti (Gede dkk., 2024).

Perbedaan antara sensor negara dan moderasi platform juga tidak berarti keduanya dapat berjalan tanpa batas. Keduanya harus memperhatikan hak pengguna. Negara harus menghormati prinsip legalitas dan proporsionalitas. Platform harus memiliki aturan yang jelas, transparan, dan menyediakan mekanisme keberatan. Dengan demikian, sumber kewenangan yang berbeda tetap membutuhkan standar perlindungan yang dapat mencegah kesewenang-wenangan.

Tata kelola yang baik juga memerlukan transparansi. Platform perlu memberikan informasi mengenai kategori konten yang dilarang, dasar keputusan moderasi, jumlah tindakan penghapusan, serta mekanisme keberatan. Transparansi tidak harus membuka seluruh rahasia teknis algoritme, tetapi pengguna setidaknya perlu mengetahui prinsip yang menentukan nasib kontennya. Tanpa

transparansi, kekuasaan platform terhadap ekspresi menjadi sulit diawasi.

Moderasi konten merupakan kebutuhan nyata dalam ekosistem digital. Platform tidak mungkin membiarkan seluruh konten beredar tanpa aturan. Namun, kebutuhan melakukan moderasi tidak dapat menjadi alasan untuk menghapus perlindungan terhadap kebebasan berekspresi. Model moderasi yang dapat dipertanggungjawabkan harus menggabungkan kejelasan aturan, pemeriksaan proporsional, transparansi, pengawasan, dan hak untuk mengajukan keberatan.

5. Menyeimbangkan Kebebasan Berekspresi, Perlindungan Publik, dan Tata Kelola Ruang Siber

Persoalan utama dalam tata kelola ruang siber bukan memilih antara kebebasan berekspresi dan perlindungan masyarakat. Keduanya merupakan kepentingan yang sama-sama penting. Masyarakat membutuhkan kebebasan untuk menyampaikan kritik dan memperoleh informasi, tetapi masyarakat juga membutuhkan perlindungan dari ancaman, eksploitasi, penipuan, kebencian, dan bentuk konten ilegal lainnya. Tantangannya adalah menentukan titik keseimbangan yang tidak memberikan kewenangan terlalu besar kepada negara maupun platform.

Model keseimbangan harus dimulai dari pengakuan bahwa pembatasan kebebasan berekspresi merupakan tindakan yang membutuhkan justifikasi. Negara atau platform yang membatasi suatu ekspresi harus mampu menjelaskan alasan pembatasan. Prinsip *necessity*

dan *proportionality* menjadi penting karena suatu tindakan pembatasan harus benar-benar diperlukan dan tidak boleh melampaui tujuan yang hendak dicapai (Are´valo Ramí´rez & Rousset Siri, 2025; Jorgi & Firmansyah, 2026; Petrov & Kumar, 2025; S˘ramel & Michal, 2025).

Prinsip *due process* juga harus menjadi bagian dari tata kelola digital. Pengguna yang dikenai pembatasan seharusnya memperoleh informasi mengenai alasan tindakan tersebut dan, dalam keadaan yang sesuai, kesempatan untuk mengajukan keberatan. Prosedur tersebut penting karena kesalahan dapat terjadi baik dalam keputusan manusia maupun keputusan otomatis. Hak untuk menggugat keputusan bukan berarti seluruh konten harus dipulihkan, tetapi memastikan bahwa keputusan pembatasan tidak bersifat final tanpa mekanisme pemeriksaan.

Transparansi merupakan lapisan berikutnya. Platform perlu menjelaskan kebijakan moderasinya dengan bahasa yang dapat dipahami. Negara juga perlu menjelaskan dasar hukum pemblokiran dan mekanisme pengawasannya. Ketika masyarakat tidak mengetahui alasan suatu konten dihapus atau situs diblokir, kepercayaan terhadap tata kelola digital akan menurun. Transparansi karena itu bukan sekadar kewajiban administratif, tetapi instrumen untuk menjaga legitimasi.

Pengawasan independen juga diperlukan. Apabila platform menjadi satu-satunya pihak yang menentukan apakah suatu konten dapat beredar,

terdapat risiko konsentrasi kekuasaan. Demikian pula, apabila pemerintah dapat memerintahkan pemblokiran tanpa mekanisme pengawasan, terdapat risiko penyalahgunaan kewenangan. Karena itu, keputusan yang mempunyai dampak besar terhadap kebebasan berekspresi perlu dapat diperiksa oleh lembaga yang independen atau, dalam keadaan tertentu, oleh pengadilan. Literatur mendorong model tata kelola campuran yang menggabungkan *due process*, transparansi, pengawasan independen, dan kewajiban kehati-hatian platform (Araujo, 2025; Petrov & Kumar, 2025; Santos dkk., 2025).

Pengawasan yudisial atau *judicial oversight* memiliki arti penting terutama ketika pembatasan dilakukan oleh negara. Pengadilan dapat menilai apakah dasar hukum pembatasan jelas, apakah tujuan pembatasan sah, apakah tindakan tersebut diperlukan, dan apakah dampaknya proporsional. Dalam konteks pemblokiran, pendekatan yang menempatkan pembuktian unsur melawan hukum sebelum penghentian akses dapat menjadi perlindungan terhadap penggunaan kewenangan secara berlebihan (Gede dkk., 2024).

Prinsip *clear definitions* juga sangat penting. Hukum yang menggunakan istilah seperti "konten berbahaya", "informasi negatif", atau "ujaran yang mengganggu" tanpa definisi yang jelas dapat memberikan ruang diskresi terlalu luas. Definisi yang kabur membuat masyarakat sulit mengetahui batas perilakunya dan membuat penerapan hukum tidak

konsisten. Literatur menempatkan definisi yang jelas sebagai salah satu *safeguard* penting dalam pengaturan konten digital (Caruso, 2024; Korpisaari, 2022; Petrov & Kumar, 2025; Santos dkk., 2025).

Perlindungan kelompok rentan juga harus diperhitungkan. Kebebasan berekspresi dapat digunakan untuk menyerang kelompok yang secara sosial sudah memiliki posisi lemah. Pada saat yang sama, moderasi yang terlalu agresif juga dapat menghapus ekspresi kelompok rentan yang justru membutuhkan ruang untuk menyampaikan pengalaman mereka. Kajian mengenai moderasi menunjukkan bahwa pembatasan yang terlalu ketat dapat menghapus konten yang bermanfaat, termasuk materi *harm reduction* dan ekspresi politik kelompok tertentu (Gomes & Sultan, 2024; Maia dkk., 2025).

Hal tersebut menunjukkan bahwa moderasi tidak dapat hanya berorientasi pada kata atau simbol. Konteks menjadi sangat penting. Sebuah kata yang muncul dalam ancaman dapat mempunyai konsekuensi berbeda apabila muncul dalam laporan jurnalistik mengenai ancaman tersebut. Demikian pula, gambar kekerasan dapat digunakan untuk glorifikasi kekerasan atau untuk dokumentasi kejahatan. Sistem moderasi yang tidak memperhatikan konteks berisiko menghapus informasi yang justru penting bagi masyarakat.

Literasi digital menjadi bagian penting dari solusi. Tidak semua persoalan informasi dapat diselesaikan melalui kriminalisasi atau penghapusan. Masyarakat perlu mempunyai kemampuan untuk

memeriksa sumber, membandingkan informasi, mengenali manipulasi, dan memahami konteks. Pencegahan ujaran kebencian dan disinformasi karena itu lebih efektif apabila digabungkan dengan pendidikan, literasi digital, desain platform yang bertanggung jawab, dan partisipasi masyarakat (Are´valo Ramí´rez & Rousset Siri, 2025; Cohen & Fung, 2023; Jorgi & Firmansyah, 2026; Petrov & Kumar, 2025).

Platform juga mempunyai peran dalam membangun lingkungan digital yang lebih sehat. Desain sistem rekomendasi, pengaturan komentar, mekanisme pelaporan, label informasi, dan pemberian konteks dapat digunakan sebagai alternatif terhadap penghapusan. Pendekatan semacam ini memungkinkan platform mengurangi risiko konten berbahaya tanpa selalu menghilangkan ekspresi dari ruang digital. Dalam konteks tersebut, moderasi dapat dipandang sebagai spektrum tindakan, bukan pilihan biner antara membiarkan dan menghapus.

Model *governance* campuran menjadi lebih relevan karena tidak ada satu aktor yang mempunyai seluruh kemampuan untuk mengatur ruang siber. Negara mempunyai kewenangan membuat dan menegakkan hukum. Platform mempunyai kontrol terhadap infrastruktur dan distribusi konten. Masyarakat mempunyai kemampuan untuk melaporkan, mengawasi, dan menilai informasi. Organisasi masyarakat sipil dan akademisi dapat memberikan evaluasi independen. Pembagian peran

tersebut perlu dirancang agar tidak terjadi dominasi salah satu aktor.

Hubungan antara negara dan platform harus ditempatkan secara hati-hati. Negara dapat menetapkan kewajiban tertentu terhadap platform, tetapi kewajiban tersebut tidak seharusnya menjadi mekanisme untuk mendelegasikan fungsi sensor tanpa batas. Sebaliknya, platform tidak dapat menggunakan kebijakan internal sebagai alasan untuk mengabaikan hukum. Relasi keduanya membutuhkan standar yang transparan sehingga tanggung jawab publik tidak hilang hanya karena suatu keputusan dibuat oleh perusahaan privat.

Regulasi *ex ante* dapat diperlukan untuk membangun standar sebelum sengketa terjadi. Pendekatan ini dapat mencakup kewajiban transparansi, prosedur pengaduan, penilaian risiko, mekanisme banding, dan pengawasan. Literatur menunjukkan bahwa adjudikasi kasus per kasus saja tidak selalu cukup untuk mengatasi ketidakseimbangan kekuasaan dalam ekosistem digital sehingga regulasi kelembagaan juga diperlukan (Caruso, 2024).

Pada sisi lain, regulasi tidak boleh dirancang sedemikian ketat sehingga platform memilih menghapus semua konten yang berpotensi menimbulkan masalah. Apabila biaya mempertahankan suatu konten lebih besar daripada biaya menghapusnya, platform dapat terdorong melakukan *over-removal*. Kondisi tersebut dapat mengurangi kualitas diskursus publik. Karena itu,

desain regulasi harus memberikan insentif agar platform mengambil tindakan yang proporsional, bukan sekadar sebanyak mungkin.

Dalam persoalan pemblokiran negara, prinsip kehati-hatian harus lebih kuat karena negara mempunyai kekuasaan koersif. Pemblokiran yang terlalu luas dapat menghambat akses masyarakat terhadap informasi. Karena itu, pemblokiran idealnya diarahkan pada konten yang memang terbukti melanggar hukum dan dilakukan berdasarkan prosedur yang dapat diuji. Beberapa kajian menekankan pentingnya pembuktian unsur melawan hukum sebelum akses dihentikan agar pemblokiran tidak berubah menjadi instrumen untuk mengontrol kritik politik (Gede dkk., 2024).

Tata kelola digital juga harus memperhatikan perubahan teknologi. Kecerdasan artifisial, *deepfake*, *generative AI*, dan sistem rekomendasi dapat menghasilkan persoalan yang belum sepenuhnya dipahami oleh hukum. Regulasi yang terlalu spesifik terhadap teknologi tertentu dapat cepat tertinggal. Sebaliknya, prinsip yang berorientasi pada risiko, transparansi, akuntabilitas, dan perlindungan hak dapat lebih mudah diterapkan terhadap teknologi baru.

Keseimbangan tersebut tidak berarti semua pihak harus puas. Kebebasan berekspresi selalu mengandung kemungkinan munculnya ekspresi yang mengganggu, kontroversial, atau tidak menyenangkan. Demokrasi membutuhkan toleransi terhadap sebagian ekspresi tersebut. Perlindungan

publik diperlukan ketika ekspresi telah mencapai tingkat kerugian yang dapat dibenarkan secara hukum. Di antara kedua titik tersebut terdapat ruang besar yang harus dikelola melalui prosedur, bukan melalui sensor otomatis.

Dengan demikian, tata kelola ruang siber yang ideal bukanlah *laissez-faire* yang membiarkan seluruh konten beredar tanpa batas, tetapi juga bukan sensor absolut yang menyerahkan keputusan mengenai ekspresi kepada negara atau algoritme. Model yang lebih dapat dipertanggungjawabkan adalah tata kelola yang membatasi konten secara sempit, berdasarkan hukum yang jelas, diperlukan untuk tujuan yang sah, proporsional terhadap risiko, transparan dalam pelaksanaannya, dapat digugat oleh pengguna, dan diawasi secara independen. Arah tersebut sejalan dengan kesimpulan literatur bahwa kebebasan berekspresi tetap merupakan hak fundamental, sementara pembatasannya harus sempit, proporsional, transparan, dan dapat dipertanggungjawabkan (Are´valo Ramí´rez & Rousset Siri, 2025; Petrov & Kumar, 2025; S˘ramel & Michal, 2025).

.

BAB VIII
KEAMANAN SIBER NASIONAL: ANTARA KEDAULATAN DIGITAL DAN ANCAMAN GLOBAL

1. Konsep dan Dimensi Keamanan Siber Nasional dalam Negara Digital

Perubahan teknologi informasi telah mengubah cara negara menjalankan fungsi pemerintahan, menyediakan pelayanan publik, mengelola perekonomian, menjaga keamanan, dan berhubungan dengan masyarakat. Infrastruktur digital tidak lagi sekadar menjadi fasilitas pendukung administrasi, melainkan telah menjadi bagian dari infrastruktur dasar yang memungkinkan negara berfungsi secara efektif. Sistem administrasi kependudukan, layanan kesehatan, pembayaran digital, jaringan komunikasi, sistem perpajakan, transportasi, energi, hingga sistem pertahanan semakin bergantung pada jaringan komputer dan pertukaran data secara elektronik. Keadaan tersebut menyebabkan gangguan terhadap sistem digital dapat berkembang menjadi gangguan terhadap fungsi negara secara keseluruhan. Keamanan siber nasional dengan demikian tidak dapat dipahami hanya sebagai persoalan perlindungan komputer dari serangan peretas, tetapi sebagai bagian dari

upaya mempertahankan kemampuan negara untuk menjalankan fungsi-fungsi strategisnya. Literatur menunjukkan bahwa keamanan siber nasional telah menjadi prasyarat bagi stabilitas negara, keberlanjutan pelayanan publik, serta keamanan ekonomi dalam masyarakat yang semakin terdigitalisasi (Chodyka dkk., 2025; Roshanaei, 2021; Vasylenko, 2025).

Pergeseran tersebut menghasilkan perubahan mendasar dalam konsep keamanan nasional. Pada masa ketika infrastruktur fisik menjadi tumpuan utama penyelenggaraan negara, ancaman keamanan lebih mudah dipetakan berdasarkan batas wilayah, objek fisik, dan aktor yang melakukan serangan. Dalam ekosistem digital, batas tersebut menjadi jauh lebih cair. Sebuah sistem pemerintahan yang secara fisik berada di dalam wilayah suatu negara dapat menggunakan perangkat lunak yang dikembangkan di negara lain, pusat data yang berlokasi di yurisdiksi berbeda, layanan *Cloud computing* yang dikelola perusahaan multinasional, serta jaringan komunikasi yang melewati sejumlah negara. Interdependensi tersebut menciptakan sistem sosio-teknis yang tidak berdiri sendiri. Ketergantungan negara terhadap *Information and Communication Technology* (ICT), *Internet of Things* (IoT), *smart grids*, *cloud*, dan sistem yang saling terhubung menyebabkan keamanan nasional harus mencakup perlindungan terhadap keseluruhan ekosistem digital tersebut (Chodyka dkk., 2025; Riggs dkk., 2023; Roshanaei, 2021).

Konsekuensi hukum dan kelembagaannya cukup penting. Apabila jaringan digital telah menjadi sarana utama penyelenggaraan fungsi negara, maka keamanan terhadap jaringan tersebut merupakan bagian dari perlindungan kepentingan publik. Perlindungan *critical information infrastructure* atau infrastruktur informasi kritis tidak dapat diserahkan semata-mata kepada administrator sistem atau bagian teknologi informasi suatu lembaga. Kegagalan sistem energi, misalnya, dapat memengaruhi rumah sakit, jaringan telekomunikasi, sistem pembayaran, transportasi, dan layanan pemerintahan secara bersamaan. Demikian pula gangguan terhadap sistem keuangan dapat menimbulkan efek yang melampaui kerugian satu perusahaan karena dapat mengganggu kepercayaan publik dan stabilitas ekonomi. Oleh sebab itu, perlindungan infrastruktur digital strategis harus ditempatkan sebagai prioritas kebijakan nasional (Kulugh dkk., 2022; Roshanaei, 2021; Vasylenko, 2025).

Persoalan tersebut memperlihatkan bahwa keamanan siber nasional memiliki dimensi yang lebih luas daripada keamanan teknis. Dimensi pertama adalah keamanan pemerintahan, yaitu kemampuan negara melindungi sistem, jaringan, aplikasi, dan data yang digunakan untuk menjalankan administrasi publik. Kebocoran data kependudukan, misalnya, bukan hanya persoalan kehilangan informasi, tetapi juga dapat menimbulkan risiko pencurian identitas, penipuan, pemalsuan dokumen, dan hilangnya kepercayaan masyarakat

terhadap negara. Serangan terhadap sistem pelayanan publik juga dapat membuat masyarakat tidak memperoleh layanan yang menjadi haknya. Negara digital karena itu membutuhkan jaminan bahwa transformasi digital tidak menghasilkan kerentanan baru yang justru mengurangi kapasitas pemerintah dalam memenuhi kewajibannya kepada masyarakat.

Dimensi kedua berkaitan dengan keamanan ekonomi digital. Aktivitas ekonomi semakin bergantung pada jaringan elektronik, mulai dari perdagangan daring, perbankan, pembayaran digital, logistik, platform perdagangan, hingga sistem produksi berbasis otomasi. Ketika sistem tersebut terganggu, kerugian tidak hanya dialami oleh pemilik sistem, tetapi juga oleh konsumen, pekerja, pemasok, dan pelaku usaha lain yang bergantung pada sistem tersebut. Keamanan siber dengan demikian memiliki hubungan langsung dengan kontinuitas kegiatan ekonomi. Perekonomian digital yang tidak memiliki tingkat keamanan memadai akan menghadapi risiko gangguan operasional, kehilangan data, penurunan kepercayaan konsumen, serta biaya pemulihan yang besar. Ketahanan digital pada akhirnya menjadi bagian dari daya saing ekonomi suatu negara.

Dimensi ketiga adalah perlindungan kepentingan publik. Negara memiliki kewajiban untuk memastikan bahwa masyarakat dapat menggunakan ruang digital tanpa menghadapi risiko yang tidak proporsional terhadap keselamatan, keamanan, dan hak-hak dasarnya. Kepentingan

publik dalam ruang siber mencakup keamanan data, kesinambungan pelayanan, perlindungan terhadap infrastruktur vital, keamanan transaksi, serta kemampuan masyarakat memperoleh informasi yang dapat dipercaya. Perubahan ini memperluas makna perlindungan negara. Negara tidak cukup hanya bertindak ketika serangan telah terjadi, tetapi perlu membangun lingkungan digital yang memiliki kemampuan untuk mencegah, mendeteksi, merespons, dan memulihkan gangguan.

Di sinilah konsep *cyber resilience* memperoleh arti strategis. Keamanan yang hanya berorientasi pada pencegahan mengandung kelemahan karena tidak ada sistem digital yang sepenuhnya kebal terhadap serangan. Ketika suatu sistem semakin kompleks dan terhubung dengan sistem lain, kemungkinan munculnya kerentanan baru selalu ada. *Cyber resilience* karena itu mengharuskan organisasi dan negara mempersiapkan kondisi sebelum serangan, kemampuan merespons ketika serangan berlangsung, serta kapasitas memulihkan fungsi setelah gangguan terjadi (Kulugh dkk., 2022; Lubis dkk., 2025). Dengan pendekatan ini, keberhasilan keamanan siber tidak semata-mata diukur dari kemampuan mencegah serangan, tetapi dari kemampuan mempertahankan fungsi penting meskipun serangan berhasil menembus sebagian sistem.

Perspektif tersebut menjadi penting karena pengalaman berbagai organisasi menunjukkan

bahwa kesiapan sebelum insiden tidak selalu diikuti oleh kesiapan pada tahap respons dan pemulihan. Banyak organisasi memiliki kebijakan keamanan, sistem deteksi, dan perangkat perlindungan, tetapi belum memiliki mekanisme pemulihan yang memadai ketika gangguan benar-benar terjadi. Celah tersebut menunjukkan bahwa keamanan siber tidak boleh berhenti pada pembangunan *firewall*, sistem autentikasi, atau perangkat deteksi. Organisasi perlu mengetahui layanan mana yang harus diprioritaskan, berapa lama sistem dapat berhenti, bagaimana data dipulihkan, siapa yang berwenang mengambil keputusan, dan bagaimana komunikasi publik dilakukan selama krisis. Penilaian terhadap kematangan ketahanan siber menunjukkan pentingnya memperhatikan seluruh siklus insiden, bukan hanya fase sebelum serangan (Chodyka dkk., 2025; Kulugh dkk., 2022).

Hubungan antara keamanan siber dan stabilitas nasional kemudian menjadi semakin jelas. Gangguan digital pada satu sektor dapat menghasilkan efek domino terhadap sektor lainnya. Sistem energi yang terganggu dapat menghentikan pusat data; pusat data yang terganggu dapat menghambat layanan pemerintahan; gangguan terhadap sistem pembayaran dapat menghambat aktivitas perdagangan; sementara gangguan komunikasi dapat menyulitkan koordinasi tanggap darurat. Interdependensi tersebut menunjukkan bahwa keamanan siber memiliki karakter sistemik. Negara tidak dapat memisahkan keamanan sektor

energi, keuangan, kesehatan, telekomunikasi, transportasi, dan pemerintahan secara mutlak karena seluruhnya berada dalam jaringan ketergantungan yang sama.

Keamanan siber nasional karena itu perlu dipahami sebagai kemampuan negara menjaga keberlangsungan fungsi strategis dalam lingkungan digital yang saling bergantung. Pemahaman tersebut menggeser orientasi dari perlindungan aset secara terpisah menuju perlindungan ekosistem. Negara harus mengetahui sistem mana yang paling vital, hubungan ketergantungan antarsistem, risiko yang muncul dari pihak ketiga, serta kapasitas pemulihan ketika terjadi gangguan. Pendekatan semacam ini sejalan dengan pandangan bahwa perlindungan infrastruktur kritis merupakan bagian inti dari keamanan nasional, terutama ketika infrastruktur tersebut menopang fungsi sosial, ekonomi, dan pemerintahan (Riggs dkk., 2023; Roshanaei, 2021; Vasylenko, 2025).

Dengan demikian, keamanan siber nasional dalam negara digital memiliki setidaknya empat dimensi yang saling berhubungan, yaitu keamanan pemerintahan, keamanan ekonomi, perlindungan infrastruktur kritis, dan perlindungan kepentingan publik. Keempatnya tidak dapat dikelola secara terpisah karena gangguan terhadap salah satu dimensi dapat menyebar kepada dimensi lainnya. Negara yang memiliki teknologi canggih tetapi tidak memiliki kemampuan pemulihan akan tetap rentan. Sebaliknya, negara yang memiliki regulasi tetapi

tidak memiliki kapasitas teknis dan sumber daya manusia juga menghadapi kesenjangan perlindungan. Keamanan siber nasional dengan demikian harus ditempatkan sebagai kombinasi antara teknologi, hukum, kelembagaan, sumber daya manusia, dan kemampuan koordinasi.

Persoalan tersebut juga menunjukkan bahwa keamanan siber bukan sekadar agenda lembaga keamanan. Kementerian dan lembaga pemerintah, perusahaan penyedia infrastruktur, operator telekomunikasi, lembaga keuangan, rumah sakit, institusi pendidikan, dan masyarakat merupakan bagian dari ekosistem yang sama. Setiap aktor memiliki tanggung jawab berbeda, tetapi kegagalan satu aktor dapat memberikan dampak kepada aktor lainnya. Model keamanan yang efektif karena itu membutuhkan pembagian tanggung jawab yang jelas, mekanisme pelaporan insiden, pertukaran informasi, serta koordinasi ketika terjadi krisis.

Negara di era digital membutuhkan paradigma keamanan yang tidak hanya bertanya "bagaimana mencegah serangan?", tetapi juga "bagaimana negara tetap berfungsi ketika serangan terjadi?" Pertanyaan kedua tersebut menjadi inti *cyber resilience*. Negara harus memiliki kemampuan mempertahankan layanan esensial, memprioritaskan fungsi yang paling kritis, memulihkan sistem dengan cepat, serta belajar dari setiap insiden untuk memperbaiki desain keamanan. Keamanan siber nasional dengan demikian merupakan bagian dari kapasitas negara untuk bertahan dan beradaptasi

terhadap perubahan teknologi dan ancaman yang menyertainya.

2. **Ancaman Siber Global dan Kerentanan Infrastruktur Digital Strategis**

Ancaman terhadap keamanan siber nasional berkembang seiring dengan meningkatnya ketergantungan masyarakat dan negara terhadap sistem digital. Semakin banyak fungsi strategis dipindahkan ke jaringan elektronik, semakin besar pula ruang yang dapat dimanfaatkan oleh pihak yang ingin mengganggu sistem tersebut. Ancaman tidak lagi terbatas pada serangan terhadap komputer individual, tetapi dapat diarahkan pada jaringan yang mengendalikan layanan publik, sistem keuangan, fasilitas energi, rumah sakit, jaringan telekomunikasi, dan infrastruktur pemerintahan. Dalam kondisi tertentu, serangan digital bahkan dapat menghasilkan konsekuensi yang menyerupai serangan terhadap infrastruktur fisik karena gangguan pada sistem pengendalian dapat menghentikan operasi fasilitas yang bersifat vital (Chodyka dkk., 2025; Roshanaei, 2021; Vasylenko, 2025).

Bentuk ancaman yang paling mudah dikenali adalah *malware*, yaitu perangkat lunak berbahaya yang dirancang untuk mengganggu, merusak, memata-matai, atau mengambil alih sistem. Perkembangan *malware* menunjukkan bahwa serangan semakin beragam dan adaptif. Di sisi lain, serangan *distributed denial-of-service* (DDoS) dapat membanjiri suatu layanan dengan permintaan dalam

jumlah besar sehingga sistem menjadi lambat atau tidak dapat diakses. Penelitian longitudinal menunjukkan bahwa *malware* dan DDoS terus berkembang dalam frekuensi maupun kompleksitas, sementara bentuk ancaman seperti *phishing*, *zero-day attack*, dan *attack-as-a-service* memperluas kemampuan pelaku untuk menyerang target dengan biaya dan kemampuan teknis yang semakin beragam (Aslan dkk., 2023; Falowo dkk., 2024).

Ransomware memperlihatkan perubahan penting dalam pola serangan siber. Serangan tidak hanya bertujuan mencuri informasi, tetapi juga mengunci atau mengenkripsi data dan sistem sehingga korban kehilangan kemampuan menjalankan operasi. Pelaku kemudian menuntut pembayaran sebagai syarat pemulihan akses. Dalam konteks infrastruktur kritis, konsekuensinya dapat sangat serius. Rumah sakit yang tidak dapat mengakses sistem pasien, perusahaan energi yang mengalami gangguan sistem, atau pemerintah yang kehilangan akses terhadap aplikasi pelayanan dapat mengalami kerugian jauh lebih besar daripada nilai tebusan yang diminta. *Ransomware* dan serangan terhadap rantai pasok juga dapat menghasilkan efek berantai karena satu titik kelemahan dapat memberikan akses terhadap sejumlah organisasi yang saling terhubung (Carroll, 2024; Simu & Zaman, 2023).

Spionase siber memiliki karakter yang berbeda. Tujuan utamanya tidak selalu menghentikan sistem, melainkan memperoleh

informasi strategis secara diam-diam. Targetnya dapat berupa data pemerintahan, penelitian teknologi, informasi pertahanan, strategi ekonomi, rahasia dagang, atau komunikasi pejabat. Dalam konteks hubungan antarnegara, spionase siber menimbulkan persoalan serius karena sulit membedakan aktivitas kriminal, kegiatan intelijen, dan operasi yang memiliki tujuan strategis negara. Penggunaan jaringan pihak ketiga, server yang berada di negara lain, serta teknik penyamaran identitas membuat proses atribusi menjadi kompleks. Kesulitan atribusi tersebut dapat memengaruhi keputusan negara dalam menentukan bentuk respons yang tepat.

Ancaman berikutnya muncul dari pencurian data. Data merupakan salah satu aset strategis dalam ekonomi digital karena dapat digunakan untuk mengidentifikasi individu, memahami perilaku konsumen, menjalankan pelayanan publik, mengembangkan kecerdasan artifisial, dan membuat keputusan ekonomi. Kebocoran data dalam jumlah besar dapat menciptakan risiko yang bertahan lama karena informasi yang telah tersebar tidak selalu dapat ditarik kembali. Dalam konteks negara, pencurian data kependudukan atau data strategis dapat mengganggu keamanan individu sekaligus kepentingan nasional. Karena itu, keamanan data perlu dipandang sebagai bagian dari keamanan siber nasional, bukan hanya sebagai persoalan perlindungan privasi.

Kerentanan menjadi semakin kompleks ketika serangan diarahkan pada sektor yang memiliki tingkat interdependensi tinggi. Energi merupakan salah satu contoh utama. Sistem pembangkit dan distribusi energi modern menggunakan jaringan digital untuk pemantauan dan pengendalian. Gangguan terhadap sistem tersebut dapat menyebabkan pemadaman dan pada tahap berikutnya memengaruhi telekomunikasi, rumah sakit, pusat data, transportasi, dan aktivitas ekonomi. Kondisi yang sama dapat terjadi pada sektor keuangan. Ketika sistem pembayaran atau perbankan terganggu, dampaknya dapat meluas karena masyarakat dan perusahaan tidak dapat melakukan transaksi secara normal. Keamanan siber dengan demikian menjadi faktor yang menentukan keberlangsungan aktivitas ekonomi sehari-hari.

Sektor kesehatan juga memiliki tingkat kerentanan tinggi karena ketergantungannya terhadap sistem informasi. Rumah sakit mengelola data pasien, sistem administrasi, perangkat medis, jadwal pelayanan, serta sistem komunikasi yang semakin terintegrasi secara digital. Serangan terhadap salah satu komponen dapat mengganggu keseluruhan layanan. Dalam kondisi tertentu, keamanan siber bahkan memiliki hubungan langsung dengan keselamatan manusia. Gangguan terhadap sistem kesehatan bukan hanya berarti kehilangan data, tetapi dapat menyebabkan keterlambatan pelayanan atau terganggunya proses pengambilan keputusan medis. Hal tersebut menunjukkan bahwa

penilaian risiko siber harus memperhitungkan dampak terhadap keselamatan publik, bukan sekadar nilai ekonomi aset yang terdampak.

Telekomunikasi dan transportasi juga merupakan sektor strategis. Jaringan telekomunikasi berfungsi sebagai fondasi bagi hampir seluruh aktivitas digital. Ketika jaringan tersebut terganggu, layanan pemerintahan, keuangan, perdagangan, dan komunikasi masyarakat ikut terdampak. Transportasi modern juga bergantung pada sistem digital untuk pengelolaan lalu lintas, pemesanan, navigasi, pengendalian, dan pertukaran informasi. Gangguan terhadap sistem tersebut dapat menciptakan konsekuensi fisik. Dalam konteks pertahanan, ketergantungan digital bahkan menjadi lebih sensitif karena sistem komunikasi, logistik, intelijen, dan pengawasan dapat menjadi sasaran operasi siber.

Rantai pasok teknologi memperluas lagi permukaan serangan. Organisasi tidak selalu membangun seluruh sistem digitalnya sendiri. Mereka menggunakan perangkat keras, perangkat lunak, layanan *cloud*, aplikasi, komponen jaringan, dan jasa pihak ketiga. Kerentanan pada satu pemasok dapat memengaruhi banyak pengguna sekaligus. Karena itu, keamanan suatu organisasi tidak hanya ditentukan oleh kualitas sistem internalnya, tetapi juga oleh keamanan ekosistem pemasok. *Supply-chain attack* menunjukkan bahwa strategi keamanan yang hanya memusatkan perhatian pada perimeter

organisasi menjadi semakin tidak memadai (Carroll, 2024; Simu & Zaman, 2023).

Perubahan karakter ancaman juga terlihat dari semakin kuatnya penggunaan kecerdasan artifisial. Teknologi AI dapat membantu organisasi mengenali pola anomali, mendeteksi aktivitas mencurigakan, dan mempercepat respons terhadap insiden. Namun, teknologi yang sama dapat dimanfaatkan untuk meningkatkan kemampuan pelaku serangan. Otomasi memungkinkan serangan dilakukan dalam skala lebih besar dan dengan kecepatan lebih tinggi. Sistem AI juga dapat digunakan untuk membantu menghasilkan konten palsu, melakukan rekayasa sosial, atau mengidentifikasi target yang rentan. Perlombaan antara penggunaan AI untuk pertahanan dan penggunaan AI untuk serangan menjadi salah satu tantangan baru keamanan nasional (Goffer dkk., 2025).

Ancaman berbasis AI juga mengubah persoalan mengenai kepercayaan terhadap informasi digital. *Deepfake*, suara hasil kloning, dan konten sintetis dapat digunakan untuk meniru individu tertentu atau menciptakan informasi palsu yang tampak meyakinkan. Dalam situasi krisis nasional, kemampuan memanipulasi informasi dapat menjadi bagian dari operasi yang lebih luas untuk menimbulkan kepanikan, mengurangi kepercayaan publik, atau memengaruhi keputusan masyarakat. Karena itu, keamanan siber perlu dipahami bersama

dengan keamanan informasi dan ketahanan masyarakat terhadap manipulasi digital.

Karakter global dari ancaman siber membuat batas antara ancaman domestik dan ancaman internasional semakin sulit ditentukan. Infrastruktur yang diserang dapat berada di satu negara, pelaku berada di negara kedua, server perantara berada di negara ketiga, sedangkan korban ekonomi tersebar di berbagai negara. Model tersebut memungkinkan pelaku memanfaatkan perbedaan kemampuan penegakan hukum dan regulasi antaryurisdiksi. Kecepatan serangan sering kali jauh lebih tinggi daripada kemampuan birokrasi negara untuk melakukan koordinasi. Kondisi tersebut membuat kerja sama internasional menjadi kebutuhan, sekaligus menempatkan negara pada posisi yang harus terus meningkatkan kapasitas domestiknya.

Ancaman siber juga semakin terorganisasi. Model *cybercrime -as-a-service* memungkinkan individu atau kelompok yang tidak memiliki kemampuan teknis tinggi memperoleh alat, infrastruktur, atau layanan yang dibutuhkan untuk melakukan serangan. Perkembangan ini menurunkan hambatan masuk bagi pelaku. Akibatnya, peningkatan kapasitas pertahanan tidak dapat hanya dilakukan dengan mengandalkan kemampuan teknis individu, tetapi harus mencakup penguatan sistem, proses, regulasi, sumber daya manusia, dan koordinasi antarlembaga (Aslan dkk., 2023).

Dari perspektif keamanan nasional, persoalan utama bukan sekadar banyaknya jenis

serangan, melainkan kemampuan serangan tersebut menghasilkan efek sistemik. Sebuah serangan mungkin dimulai dari satu akun, satu pemasok, atau satu server, tetapi dapat menyebar melalui jaringan yang saling bergantung. Oleh karena itu, strategi nasional perlu memetakan sektor yang paling kritis, hubungan ketergantungan antarsektor, serta titik kegagalan yang dapat menghasilkan dampak berantai. Perlindungan harus diberikan secara proporsional berdasarkan tingkat kepentingan dan konsekuensi apabila suatu sistem mengalami gangguan.

Dengan demikian, ancaman siber global dapat digambarkan melalui empat karakter utama, yaitu eskalasi ancaman, otomasi dan AI, ketergantungan terhadap infrastruktur digital, serta meningkatnya kompleksitas rantai pasok. Keempatnya saling berhubungan. Semakin tinggi ketergantungan terhadap teknologi, semakin besar dampak apabila sistem terganggu. Semakin kompleks rantai pasok, semakin banyak titik yang harus diamankan. Semakin canggih AI, semakin besar pula kemampuan pertahanan sekaligus potensi serangan. Keadaan tersebut membuat keamanan siber menjadi perlombaan adaptasi yang berlangsung terus-menerus.

3. Kedaulatan Digital, Ketergantungan Teknologi, dan Penguasaan Data Strategis

Kedaulatan negara pada era digital menghadapi persoalan yang berbeda dari kedaulatan dalam ruang fisik. Negara secara tradisional

menghubungkan kedaulatan dengan wilayah, penduduk, pemerintahan, dan kemampuan menjalankan kewenangan dalam batas teritorial. Infrastruktur digital tidak selalu mengikuti batas tersebut. Data dapat dibuat di satu negara, diproses di negara lain, disimpan di pusat data yang berbeda, dan diakses melalui jaringan global. Layanan digital juga dapat disediakan oleh perusahaan yang secara hukum dan ekonomis berada di luar wilayah negara pengguna. Kondisi tersebut menimbulkan pertanyaan mendasar mengenai sejauh mana negara benar-benar memiliki kendali terhadap sumber daya digital yang digunakan untuk menjalankan fungsi strategisnya.

Konsep kedaulatan digital berkembang dari persoalan tersebut. Kedaulatan digital dapat dipahami sebagai kemampuan negara untuk mempertahankan kendali bermakna atas data, infrastruktur, teknologi, standar, dan proses digital yang memiliki kepentingan strategis. Konsep tersebut tidak berarti bahwa negara harus mengendalikan seluruh aktivitas internet secara langsung. Fokus utamanya adalah memastikan bahwa ketergantungan teknologi tidak sampai menghilangkan kemampuan negara mengambil keputusan mengenai kepentingan strategisnya sendiri. Literatur menempatkan kedaulatan digital sebagai persoalan penguasaan terhadap data, infrastruktur, dan standar pemrosesan digital (Glasze dkk., 2022; Hummel dkk., 2021; Hutchinson dkk., 2024).

Salah satu persoalan yang paling penting adalah *data sovereignty* atau kedaulatan data. Data menjadi sumber daya strategis karena keputusan pemerintahan, kegiatan ekonomi, inovasi teknologi, dan pengembangan AI semakin bergantung pada kemampuan mengumpulkan serta memproses data. Negara yang tidak memiliki kontrol memadai atas data strategis berpotensi menghadapi ketergantungan dalam menentukan bagaimana data disimpan, diproses, dipindahkan, dan digunakan. Kedaulatan data karena itu bukan sekadar pertanyaan mengenai lokasi server, tetapi juga menyangkut siapa yang memiliki akses, siapa yang mengendalikan pemrosesan, standar hukum apa yang berlaku, dan bagaimana negara dapat melindungi kepentingan publik.

Lokasi pusat data menjadi relevan dalam konteks tersebut. Penempatan pusat data di wilayah nasional dapat memberikan keuntungan dari perspektif kontrol fisik, keamanan, dan kepatuhan terhadap hukum nasional. Namun, lokasi fisik tidak secara otomatis menjamin kedaulatan. Pengelolaan pusat data dapat dilakukan oleh perusahaan asing, perangkat lunaknya dapat berasal dari vendor luar negeri, dan sistemnya dapat bergantung pada komponen serta layanan yang berasal dari berbagai negara. Karena itu, kedaulatan digital tidak dapat direduksi menjadi kebijakan "data harus berada di dalam negeri". Kedaulatan membutuhkan kontrol yang lebih substantif terhadap keseluruhan ekosistem digital.

Ketergantungan terhadap *Cloud computing* memperlihatkan persoalan tersebut secara jelas. *Cloud* memberikan efisiensi, skalabilitas, fleksibilitas, dan kemampuan mengakses sumber daya komputasi secara cepat. Bagi pemerintah dan perusahaan, penggunaan *cloud* dapat mengurangi kebutuhan investasi pada infrastruktur fisik. Namun, ketergantungan pada penyedia *cloud* tertentu juga dapat menciptakan *vendor lock-in* dan ketergantungan strategis. Ketika penyedia layanan berada di luar negeri atau menggunakan infrastruktur global, negara perlu mempertimbangkan bagaimana akses terhadap data dan sistem dapat dipertahankan apabila terjadi konflik hukum, gangguan layanan, perubahan kebijakan perusahaan, atau tekanan geopolitik (Blancato, 2023).

Ketergantungan tersebut menghasilkan apa yang dapat disebut sebagai risiko kedaulatan teknologi. Sebuah negara mungkin memiliki jaringan internet yang luas dan masyarakat yang sangat terdigitalisasi, tetapi belum tentu memiliki kapasitas untuk memproduksi teknologi inti yang menopang ekosistem tersebut. Ketergantungan pada perangkat keras, sistem operasi, perangkat jaringan, chip, layanan *cloud*, sistem keamanan, dan platform digital tertentu dapat menciptakan kerentanan strategis. Apabila akses terhadap teknologi tersebut terganggu, negara dapat menghadapi kesulitan dalam mempertahankan fungsi digitalnya.

Persoalan ini menjadi lebih kompleks karena teknologi modern dibangun melalui rantai pasok global. Satu perangkat dapat menggunakan komponen dari berbagai negara dan perangkat lunak dari pengembang yang berbeda. Rantai pasok semacam itu menghasilkan efisiensi ekonomi, tetapi juga memperbesar permukaan risiko. Kerentanan dapat masuk melalui komponen pihak ketiga yang tidak mudah diawasi oleh pengguna akhir. Oleh sebab itu, keamanan rantai pasok digital harus menjadi bagian dari strategi kedaulatan digital. Negara perlu memahami bukan hanya siapa pemasok langsungnya, tetapi juga ketergantungan pada pemasok tingkat berikutnya.

Kedaulatan digital juga memiliki dimensi geopolitik. Negara-negara berusaha mengurangi ketergantungan terhadap teknologi tertentu karena teknologi dapat menjadi instrumen kekuatan ekonomi dan politik. Penguasaan terhadap standar teknologi, jaringan, platform, pusat data, sistem pembayaran, dan teknologi komputasi dapat memberikan pengaruh yang melampaui batas ekonomi. Dalam konteks tersebut, kedaulatan digital berhubungan dengan kemampuan suatu negara mempertahankan ruang pengambilan keputusan yang independen dalam menghadapi perubahan geopolitik. Kajian mengenai *digital sovereignty* menunjukkan bahwa ruang digital merupakan ruang yang diperebutkan oleh berbagai kepentingan negara, perusahaan, dan aktor lainnya (Glasze dkk., 2022).

Namun, kedaulatan digital tidak boleh diterjemahkan menjadi isolasi digital. Internet dibangun atas prinsip interkonektivitas. Perdagangan, penelitian, pendidikan, komunikasi, dan inovasi membutuhkan pertukaran data dan teknologi lintas batas. Kebijakan yang terlalu menekankan kontrol nasional dapat menghasilkan fragmentasi internet dan meningkatkan biaya bagi masyarakat maupun dunia usaha. Data *sovereignty* karena itu selalu berada dalam ketegangan dengan kebutuhan interoperabilitas, inovasi, dan arus data lintas negara (Bonnieu, 2026; Hutchinson dkk., 2024).

Ketegangan tersebut menunjukkan bahwa negara perlu membedakan antara kendali strategis dan kontrol total. Kendali strategis berarti negara memiliki kapasitas untuk melindungi aset digital yang vital, menetapkan standar keamanan, memastikan akses terhadap data strategis, mengelola risiko pihak ketiga, dan mempertahankan keberlangsungan layanan. Kontrol total, sebaliknya, mengandaikan negara harus menguasai seluruh teknologi dan arus data, sesuatu yang sulit diwujudkan dalam ekonomi digital global. Pendekatan pertama lebih realistis karena memungkinkan negara tetap terhubung dengan sistem global tanpa kehilangan kepentingan strategisnya.

Persoalan transfer data lintas negara juga menjadi bagian penting dari kedaulatan digital. Transfer tersebut dibutuhkan untuk perdagangan,

pembayaran, layanan *cloud*, riset, komunikasi, dan berbagai layanan digital lainnya. Pada saat yang sama, transfer data dapat menimbulkan persoalan mengenai perlindungan data, akses oleh otoritas asing, keamanan informasi, serta kepatuhan terhadap hukum nasional. Negara karena itu perlu memiliki mekanisme untuk menilai risiko transfer data berdasarkan jenis data, tujuan pemrosesan, pihak penerima, dan tingkat perlindungan yang tersedia.

Data strategis juga memiliki nilai yang berbeda-beda. Tidak seluruh data membutuhkan tingkat pengamanan yang sama. Data yang berkaitan dengan pertahanan, keamanan nasional, infrastruktur kritis, kebijakan strategis, atau identitas penduduk memiliki konsekuensi berbeda dengan data publik biasa. Pengelolaan kedaulatan digital karena itu membutuhkan klasifikasi aset dan data berdasarkan tingkat kepentingannya. Pendekatan berbasis risiko memungkinkan negara memusatkan sumber daya pada aset yang apabila terganggu akan menimbulkan dampak paling besar.

Penguasaan data juga tidak dapat dipisahkan dari perkembangan kecerdasan artifisial. AI membutuhkan data dalam jumlah besar untuk dilatih, diuji, dan dikembangkan. Negara yang memiliki kemampuan mengakses data berkualitas dan infrastruktur komputasi memiliki posisi strategis dalam pengembangan AI. Sebaliknya, negara yang hanya menjadi pengguna teknologi dapat mengalami ketergantungan baru. Kedaulatan digital pada masa

depan karena itu tidak hanya berkaitan dengan lokasi penyimpanan data, tetapi juga kemampuan mengembangkan teknologi, mengelola infrastruktur komputasi, dan membangun sumber daya manusia yang mampu memahami serta mengendalikan teknologi tersebut.

Dari perspektif hukum, kedaulatan digital membutuhkan keseimbangan antara kepentingan negara dan keterbukaan jaringan global. Regulasi perlu memberikan kepastian mengenai data apa yang harus dilindungi, standar keamanan yang harus dipenuhi, kewajiban penyedia layanan, serta mekanisme ketika terjadi konflik lintas batas. Namun, regulasi juga perlu menghindari fragmentasi yang tidak diperlukan. Harmonisasi standar dan pengakuan terhadap mekanisme perlindungan yang setara dapat membantu mempertahankan arus data tanpa mengorbankan kepentingan keamanan.

Pada akhirnya, kedaulatan digital bukan berarti negara harus berdiri sendiri dalam ekosistem digital global. Justru, negara membutuhkan kemampuan untuk bekerja sama sambil mempertahankan kendali atas kepentingan strategisnya. Konsep tersebut dapat dirumuskan sebagai kemampuan untuk terhubung tanpa menjadi sepenuhnya bergantung, berbagi data tanpa kehilangan kendali, menggunakan teknologi global tanpa kehilangan kapasitas strategis, serta membuka ekonomi digital tanpa mengorbankan keamanan nasional. Dengan pendekatan demikian, kedaulatan digital menjadi instrumen untuk mempertahankan

otonomi strategis, bukan alasan untuk menutup diri dari perkembangan teknologi global.

4. **Strategi Ketahanan Siber dan Tata Kelola Keamanan Siber Nasional**

Keamanan siber nasional tidak dapat dibangun hanya melalui satu regulasi atau satu lembaga. Kompleksitas ancaman digital menuntut sistem tata kelola yang mampu menghubungkan kebijakan, teknologi, kelembagaan, sumber daya manusia, sektor bisnis, dan masyarakat. Ancaman dapat muncul dari jaringan pemerintah, perusahaan swasta, pemasok teknologi, perangkat individu, maupun infrastruktur global. Negara karena itu harus membangun mekanisme koordinasi yang memungkinkan informasi mengenai risiko dan insiden bergerak secara cepat di antara aktor yang memiliki kewenangan dan kemampuan berbeda. Strategi ketahanan siber yang berkembang dalam literatur cenderung menempatkan regulasi, CSIRT/CERT, perlindungan infrastruktur kritis, berbagi informasi ancaman, dan koordinasi lintas sektor sebagai elemen penting (Chodyka dkk., 2025; Sukma, 2026; Vasylenko, 2025).

Regulasi menjadi fondasi awal karena menentukan siapa yang bertanggung jawab, standar apa yang harus dipenuhi, bagaimana insiden dilaporkan, serta bagaimana negara dapat melakukan intervensi ketika terjadi gangguan. Regulasi yang baik tidak hanya menetapkan larangan dan sanksi, tetapi juga menciptakan struktur tanggung jawab preventif. Operator infrastruktur

kritis, misalnya, perlu mengetahui standar keamanan minimum, kewajiban melakukan penilaian risiko, prosedur pelaporan insiden, serta kewajiban memulihkan layanan. Dengan demikian, hukum berfungsi bukan hanya sebagai instrumen represif setelah serangan terjadi, tetapi sebagai mekanisme untuk membentuk perilaku keamanan sebelum insiden.

Kelembagaan menjadi lapisan berikutnya. Negara membutuhkan lembaga yang mampu melakukan koordinasi, deteksi, analisis, respons, dan pemulihan. Keberadaan CSIRT atau CERT menjadi penting karena insiden siber membutuhkan respons teknis yang cepat. Pada saat yang sama, respons teknis harus terhubung dengan pengambilan keputusan administratif dan hukum. Sebuah insiden pada infrastruktur kritis mungkin memerlukan isolasi sistem, tetapi tindakan tersebut juga dapat memengaruhi pelayanan publik. Keputusan semacam itu membutuhkan koordinasi antara administrator sistem, pimpinan lembaga, aparat keamanan, regulator, dan pihak lain yang berkepentingan.

Perlindungan infrastruktur kritis perlu menggunakan pendekatan berbasis risiko. Tidak semua sistem memiliki tingkat kepentingan yang sama. Negara perlu menentukan sistem yang apabila mengalami gangguan dapat menimbulkan dampak besar terhadap keselamatan, ekonomi, pemerintahan, atau ketertiban sosial. Setelah objek prioritas ditentukan, perlindungan harus mencakup identifikasi aset, pemetaan ketergantungan,

penilaian kerentanan, pengujian sistem, penguatan kontrol keamanan, serta penyusunan rencana pemulihan. Model penilaian ketahanan infrastruktur kritis menekankan pentingnya pengukuran kemampuan organisasi menghadapi keseluruhan siklus ancaman (Kulugh dkk., 2022; Lubis dkk., 2025).

Salah satu perubahan penting adalah pergeseran dari model pertahanan berbasis perimeter menuju pendekatan yang lebih adaptif. Sistem tidak dapat lagi menganggap bahwa seluruh aktivitas di dalam jaringan secara otomatis aman. Penggunaan *secure-by-design* dan pendekatan *zero trust* mengharuskan keamanan dipertimbangkan sejak tahap perancangan dan setiap akses diverifikasi berdasarkan identitas, konteks, serta tingkat kewenangan. Pendekatan tersebut menjadi semakin relevan ketika organisasi menggunakan *cloud*, perangkat bergerak, aplikasi pihak ketiga, dan sistem kerja jarak jauh. Keamanan tidak lagi berada pada satu gerbang, melainkan dibangun melalui berbagai lapisan pengendalian.

Incident response merupakan komponen yang tidak kalah penting. Ketika serangan terjadi, keterlambatan dapat memperbesar dampak. Organisasi perlu mengetahui bagaimana insiden diidentifikasi, siapa yang diberi kewenangan, sistem apa yang harus diisolasi, bagaimana bukti dipertahankan, dan bagaimana layanan dipulihkan. Respons yang tidak terkoordinasi dapat menyebabkan kerugian tambahan, misalnya dengan

menghapus bukti atau mematikan sistem yang sebenarnya masih dibutuhkan untuk analisis. Karena itu, prosedur respons harus diuji melalui latihan dan simulasi secara berkala.

Ketahanan siber juga membutuhkan *threat intelligence sharing*. Informasi mengenai teknik serangan, indikator kompromi, pola aktivitas, dan kerentanan baru dapat membantu organisasi lain mencegah serangan yang sama. Namun, berbagi informasi tidak selalu mudah. Organisasi mungkin khawatir bahwa pengungkapan insiden akan merusak reputasi, menimbulkan konsekuensi hukum, atau membuka informasi sensitif. Karena itu, mekanisme berbagi informasi membutuhkan standar, kepercayaan, perlindungan data, dan aturan mengenai bagaimana informasi digunakan. *Threat intelligence sharing* dapat meningkatkan kemampuan deteksi dan respons, tetapi manfaatnya sangat bergantung pada kualitas mekanisme pertukaran informasi (Lubis dkk., 2025; Qudus, 2025).

Sumber daya manusia menjadi faktor yang sering kali menentukan keberhasilan seluruh sistem. Teknologi keamanan dapat gagal apabila tidak dikelola oleh manusia yang memiliki kompetensi memadai. Negara membutuhkan tenaga yang mampu memahami keamanan jaringan, analisis ancaman, forensik digital, keamanan aplikasi, perlindungan data, manajemen risiko, hingga aspek hukum dan kebijakan. Kebutuhan tersebut tidak hanya berlaku bagi lembaga keamanan, tetapi juga bagi operator infrastruktur dan organisasi sektor swasta.

Pengembangan tenaga kerja harus dilakukan melalui pendidikan, pelatihan, sertifikasi, latihan bersama, serta pengembangan jalur karier yang mampu mempertahankan talenta siber (Lubis dkk., 2025; Qudus, 2025; Simu & Zaman, 2023).

Hubungan pemerintah dan sektor swasta menjadi aspek yang tidak dapat dihindari. Sebagian besar infrastruktur digital penting dimiliki atau dioperasikan oleh perusahaan swasta. Pemerintah dapat menetapkan kebijakan dan standar, tetapi tidak dapat secara langsung mengendalikan seluruh infrastruktur yang menjadi bagian dari kehidupan digital masyarakat. *Public-private partnership* karena itu menjadi salah satu mekanisme yang dibutuhkan untuk membangun ketahanan siber nasional (Kala, 2024; Qudus, 2025; Sukma, 2026). Kerja sama tersebut dapat mencakup pertukaran informasi, pengembangan standar keamanan, latihan respons, koordinasi insiden, dan pengembangan kapasitas.

Meskipun demikian, kemitraan pemerintah dan swasta harus dirancang dengan hati-hati. Kerja sama tidak boleh berubah menjadi pemindahan tanggung jawab secara sepihak kepada perusahaan atau menjadi alasan bagi negara untuk memperluas kewenangan tanpa mekanisme akuntabilitas. Literatur menunjukkan bahwa *public-private partnership* tidak selalu menghasilkan tata kelola yang sepenuhnya *polycentric* karena dalam banyak situasi tujuan dan kerangka kerja tetap ditentukan oleh negara (Sukma, 2026). Oleh karena itu, kerja sama harus disertai pembagian kewenangan yang

jelas, transparansi, perlindungan kepentingan publik, dan mekanisme pengawasan.

Tata kelola keamanan siber juga harus melibatkan aparat penegak hukum. Ketika insiden mengandung unsur pidana, proses teknis perlu berjalan bersama proses hukum. Bukti digital harus diamankan sejak awal agar dapat digunakan dalam penyelidikan dan proses peradilan. Aparat penegak hukum membutuhkan kemampuan memahami karakteristik sistem digital, sementara tenaga teknis perlu memahami kebutuhan pembuktian hukum. Hubungan antara keahlian teknis dan hukum menjadi penting karena kesalahan pada tahap awal dapat menyebabkan bukti tidak dapat digunakan secara optimal.

Akademisi memiliki peran yang berbeda tetapi tetap penting. Perkembangan teknologi berlangsung lebih cepat daripada siklus pembentukan kebijakan. Penelitian akademik dapat membantu negara memahami pola ancaman, mengevaluasi efektivitas regulasi, mengembangkan metode pengukuran ketahanan, serta mengidentifikasi risiko teknologi baru. Kerja sama antara universitas, pemerintah, dan industri juga dapat menghasilkan inovasi keamanan yang lebih sesuai dengan kebutuhan nasional. Dalam jangka panjang, kemampuan penelitian domestik menjadi bagian dari kedaulatan teknologi.

Masyarakat juga merupakan bagian dari sistem ketahanan siber. Banyak serangan bermula dari faktor manusia, seperti penggunaan kata sandi

yang lemah, klik terhadap *phishing*, penggunaan perangkat lunak ilegal, atau ketidakmampuan mengenali komunikasi palsu. Literasi digital tidak dapat menggantikan sistem keamanan teknis, tetapi dapat mengurangi sejumlah risiko yang berasal dari perilaku pengguna. Masyarakat juga perlu mengetahui bagaimana melaporkan insiden dan apa yang harus dilakukan ketika mengalami serangan. Ketahanan nasional dengan demikian memiliki dimensi sosial, bukan hanya teknis.

Kerja sama internasional tetap dibutuhkan karena karakter ancaman siber tidak berhenti pada batas wilayah. Informasi ancaman dapat berasal dari satu negara, infrastruktur pelaku berada di negara lain, dan target berada di negara ketiga. Negara membutuhkan mekanisme pertukaran informasi, kerja sama investigasi, pengembangan kapasitas, dan koordinasi ketika insiden memiliki dampak lintas batas. Kerja sama internasional menjadi bagian penting dari strategi nasional justru karena tidak ada negara yang sepenuhnya dapat mengamankan ekosistem digitalnya sendiri (Goffer dkk., 2025; Qudus, 2025; Simu & Zaman, 2023).

Strategi ketahanan juga perlu mengintegrasikan pengelolaan risiko rantai pasok. Organisasi harus mengetahui teknologi dan layanan apa saja yang berasal dari pihak ketiga, bagaimana keamanan pemasok dinilai, bagaimana pembaruan perangkat dilakukan, dan apa yang terjadi apabila pemasok mengalami gangguan. Pendekatan ini semakin penting ketika organisasi menggunakan

cloud dan perangkat lunak sebagai layanan. Keamanan sistem tidak dapat dipisahkan dari keamanan pihak yang menyediakan komponen sistem tersebut. Pengelolaan risiko rantai pasok harus menjadi bagian dari pengadaan teknologi, bukan baru dilakukan setelah insiden terjadi.

Pengembangan *sovereign cloud* juga dapat dipertimbangkan sebagai salah satu strategi untuk sektor yang memiliki kebutuhan strategis tinggi. Tujuannya bukan meniadakan penggunaan layanan global, tetapi memastikan bahwa fungsi yang sangat sensitif memiliki tingkat kontrol, keamanan, dan keberlanjutan yang sesuai dengan kepentingan nasional. Strategi tersebut harus disertai analisis biaya dan manfaat karena pembangunan kapasitas domestik dapat membutuhkan investasi besar. Pendekatan yang rasional adalah menentukan fungsi yang benar-benar strategis dan membangun kemandirian secara bertahap, sambil tetap memanfaatkan teknologi global untuk kebutuhan yang risikonya lebih rendah (Blancato, 2023; Bonnieu, 2026).

Pada tingkat yang lebih luas, *cyber resilience* membutuhkan perubahan cara berpikir. Keamanan tidak boleh dianggap sebagai proyek yang selesai setelah sistem dipasang. Ancaman berubah, teknologi berubah, dan ketergantungan berubah. Sistem yang aman hari ini belum tentu aman beberapa tahun kemudian. Negara karena itu perlu membangun siklus berkelanjutan berupa identifikasi risiko, pencegahan, deteksi, respons, pemulihan, evaluasi,

dan adaptasi. Pendekatan tersebut menjadikan setiap insiden sebagai sumber pembelajaran untuk meningkatkan ketahanan.

Strategi tersebut dapat diringkas dalam lima kemampuan utama. Pertama, mencegah, melalui regulasi, desain aman, pengamanan infrastruktur, dan peningkatan kesadaran. Kedua, mendeteksi, melalui pemantauan, analisis ancaman, dan berbagi informasi. Ketiga, merespons, melalui CSIRT/CERT, prosedur insiden, koordinasi, dan pengambilan keputusan cepat. Keempat, memulihkan, melalui pencadangan, redundansi, rencana kontinuitas, dan pemulihan sistem. Kelima, beradaptasi, melalui evaluasi, pembelajaran, penelitian, pembaruan regulasi, dan pengembangan teknologi. Kerangka tersebut memperlihatkan bahwa *cyber resilience* jauh lebih luas daripada sekadar pertahanan teknis (Kulugh dkk., 2022; Lubis dkk., 2025).

Tata kelola keamanan siber nasional membutuhkan model yang menghubungkan negara, pasar, masyarakat, dan komunitas pengetahuan. Negara tetap memiliki posisi sentral karena memiliki kewenangan regulasi dan tanggung jawab terhadap keamanan nasional. Namun, negara tidak dapat bekerja sendiri karena sebagian besar teknologi dan infrastruktur berada dalam ekosistem swasta dan global. Sektor bisnis memiliki kemampuan teknis dan sumber daya yang besar, tetapi membutuhkan kerangka hukum yang jelas. Akademisi menghasilkan pengetahuan dan inovasi, sementara masyarakat merupakan pengguna sekaligus bagian dari sistem

keamanan. Kolaborasi tersebut harus dibangun berdasarkan pembagian tanggung jawab yang jelas dan orientasi pada kepentingan publik.

Dengan demikian, tujuan akhir keamanan siber nasional bukanlah menciptakan ruang digital yang sepenuhnya bebas dari serangan. Tujuan yang lebih realistis adalah membangun negara yang mampu mempertahankan fungsi strategisnya meskipun menghadapi serangan, mampu memulihkan layanan ketika terjadi gangguan, dan mampu beradaptasi terhadap ancaman yang belum pernah muncul sebelumnya. Pandangan tersebut menempatkan keamanan siber sebagai bagian dari ketahanan nasional. Keamanan siber bukan lagi sekadar persoalan teknis yang berada di ruang server, melainkan bagian dari kemampuan negara mempertahankan stabilitas, kedaulatan, pelayanan publik, dan keamanan ekonomi.

Arah perkembangan keamanan siber menunjukkan kebutuhan untuk menggabungkan *secure-by-design*, *zero trust*, pengelolaan risiko rantai pasok, *sovereign cloud*, penguatan infrastruktur kritis, serta investasi jangka panjang dalam sumber daya manusia dan inovasi domestik (Bonnieu, 2026; Carroll, 2024). Keseluruhan strategi tersebut harus berjalan secara terpadu karena kelemahan pada satu aspek dapat mengurangi efektivitas aspek lainnya. Regulasi tanpa kapasitas teknis tidak cukup. Teknologi tanpa tata kelola tidak cukup. Infrastruktur tanpa sumber daya manusia juga tidak cukup.

Ketahanan hanya dapat tercapai apabila seluruh komponen tersebut bekerja sebagai satu sistem.

Bab ini memperlihatkan bahwa keamanan siber nasional berada di antara dua kepentingan yang harus terus diseimbangkan. Di satu sisi, negara membutuhkan kedaulatan digital, yaitu kemampuan mempertahankan kendali atas data, teknologi, infrastruktur, dan kepentingan strategisnya. Di sisi lain, negara tidak dapat melepaskan diri dari sifat global dan saling terhubungnya internet. Ancaman pun tidak mengenal batas, sehingga kerja sama internasional tetap menjadi kebutuhan. Karena itu, keamanan siber nasional tidak seharusnya dibangun melalui isolasi, melainkan melalui ketahanan, pengendalian risiko, kapasitas domestik, dan kerja sama yang memungkinkan negara tetap terhubung tanpa kehilangan otonomi strategis.

Dalam kerangka tersebut, keamanan siber dapat dipandang sebagai kemampuan negara untuk menjaga tiga hal sekaligus: keberlangsungan fungsi, perlindungan kepentingan strategis, dan kemampuan beradaptasi. Keberlangsungan fungsi memastikan pelayanan publik dan kegiatan ekonomi tetap berjalan. Perlindungan kepentingan strategis memastikan data, infrastruktur, dan teknologi vital tidak mudah dikendalikan oleh pihak lain. Kemampuan beradaptasi memastikan negara mampu merespons perubahan ancaman dan teknologi. Ketiga kemampuan tersebut merupakan fondasi bagi negara digital yang tangguh dalam menghadapi ancaman global.

BAB IX
KECEERDASAN BUATAN, BLOCKCHAIN, DAN TANTANGAN REGULASI TEKNOLOGI BARU

1. Kecerdasan Buatan dan Transformasi Hubungan Hukum di Era Digital

Perkembangan kecerdasan buatan atau *artificial intelligence* (AI) telah membawa perubahan dari sekadar penggunaan teknologi sebagai alat bantu menuju penggunaan sistem yang mampu melakukan analisis, memberikan rekomendasi, menghasilkan konten, dan mengambil keputusan berdasarkan data serta pola yang dipelajari. Perubahan tersebut memiliki konsekuensi yang lebih luas daripada persoalan teknis karena keputusan yang dihasilkan oleh sistem AI dapat memengaruhi hak, kewajiban, kepentingan ekonomi, bahkan posisi hukum seseorang. Pemerintah dapat menggunakan AI untuk membantu pelayanan publik, perusahaan dapat menggunakannya untuk menyeleksi calon pekerja atau menentukan kelayakan kredit, sedangkan lembaga penegak hukum dapat memanfaatkannya untuk menganalisis informasi dan mendukung proses pengambilan keputusan. Penggunaan AI dalam pemerintahan, bisnis, pelayanan publik, kesehatan, keuangan, dan

penegakan hukum menunjukkan bahwa teknologi tersebut telah masuk ke wilayah yang sebelumnya sangat bergantung pada penilaian manusia (Aliliele dkk., 2025; Satyo dkk., 2026; Stepanov & Stepanov, 2026).

Perubahan tersebut menjadi penting secara hukum karena sistem otomatis mulai mengambil alih sebagian fungsi yang sebelumnya dilakukan manusia. Pada model konvensional, seseorang yang menerima keputusan administratif dapat mengetahui siapa pejabat atau institusi yang mengambil keputusan tersebut. Dalam sistem berbasis AI, proses pengambilan keputusan dapat melibatkan kumpulan data, model algoritmik, parameter teknis, perangkat lunak, dan proses komputasi yang kompleks. Pihak yang menerima keputusan mungkin hanya mengetahui hasil akhirnya tanpa memahami bagaimana hasil tersebut diperoleh. Perubahan ini menggeser persoalan hukum dari sekadar pertanyaan mengenai apa keputusan yang dibuat menuju pertanyaan mengenai bagaimana keputusan tersebut dibuat dan siapa yang bertanggung jawab atasnya (Greenstein, 2021; Satyo dkk., 2026).

AI sendiri bukan merupakan satu teknologi tunggal. Machine learning, misalnya, bekerja dengan memanfaatkan data untuk menemukan pola dan menghasilkan prediksi atau klasifikasi. Sistem generative AI memiliki kemampuan yang lebih kompleks karena dapat menghasilkan teks, gambar, suara, kode, dan bentuk konten lainnya berdasarkan pola yang dipelajari. Sementara itu, automated

decision-making memungkinkan sistem menggunakan data dan aturan tertentu untuk menghasilkan keputusan tanpa harus melalui intervensi manusia pada setiap tahap. Perbedaan kemampuan tersebut penting karena tingkat risiko hukumnya tidak sama. Sistem yang hanya memberikan rekomendasi kepada manusia memiliki struktur tanggung jawab yang berbeda dengan sistem yang secara otomatis menentukan akses seseorang terhadap layanan atau mengambil tindakan yang menghasilkan akibat hukum.

Dalam hubungan hukum, persoalan utama muncul ketika manusia memberikan sebagian kewenangan pengambilan keputusan kepada sistem algoritmik. Pendelegasian tersebut memang dapat meningkatkan efisiensi. Sistem AI mampu memproses data dalam jumlah besar dengan kecepatan yang tidak mungkin dilakukan manusia secara manual. Dalam administrasi pemerintahan, teknologi dapat membantu mengidentifikasi pola atau memprioritaskan pelayanan. Dalam dunia bisnis, AI dapat membantu melakukan analisis risiko dan memberikan rekomendasi. Dalam bidang hukum, sistem AI dapat membantu pencarian dokumen, analisis kontrak, atau pengelompokan informasi. Namun, efisiensi tidak dengan sendirinya berarti legitimasi hukum. Keputusan yang cepat tetap harus dapat dipertanggungjawabkan apabila keputusan tersebut memengaruhi hak atau kepentingan seseorang.

Persoalan semakin rumit ketika sistem AI memiliki karakter black box. Dalam sistem semacam itu, bahkan pengguna teknologi tidak selalu mampu menjelaskan secara sederhana mengapa sistem menghasilkan suatu keluaran tertentu. Kurangnya keterjelasan dapat mengganggu prinsip fairness, due process, dan hak seseorang untuk mempertanyakan keputusan yang merugikannya (Greenstein, 2021; Rajendra & Thuraisingam, 2025; Satyo dkk., 2026). Jika seseorang ditolak memperoleh suatu layanan berdasarkan hasil algoritmik, misalnya, maka ia secara hukum membutuhkan kesempatan untuk mengetahui alasan keputusan tersebut dan memperoleh mekanisme untuk mengajukan keberatan. Tanpa mekanisme tersebut, otomatisasi berpotensi mengubah keputusan yang seharusnya dapat diperdebatkan menjadi keputusan yang seolah-olah objektif hanya karena dihasilkan oleh mesin.

Di sinilah konsep *explainability* memperoleh arti penting. *Explainability* tidak selalu berarti membuka seluruh kode sumber suatu sistem kepada publik. Yang lebih penting adalah kemampuan memberikan penjelasan yang relevan mengenai dasar keputusan, faktor yang berpengaruh, batasan sistem, serta alasan mengapa suatu keluaran dihasilkan. Tingkat penjelasan dapat disesuaikan dengan risiko. Keputusan yang berdampak kecil terhadap seseorang tidak selalu membutuhkan mekanisme penjelasan yang sama dengan keputusan yang menentukan akses terhadap kredit, pekerjaan,

pelayanan kesehatan, bantuan sosial, atau proses hukum. Pendekatan tersebut membuat *explainability* tidak sekadar persoalan teknis, tetapi menjadi bagian dari perlindungan hak.

Risiko lain muncul dari kualitas data yang digunakan AI. Algoritma dapat menghasilkan keputusan yang tampak objektif, tetapi hasilnya dapat mencerminkan bias yang terdapat dalam data pelatihan. Apabila data historis mengandung ketimpangan atau diskriminasi, sistem dapat mempelajari pola tersebut dan mereproduksinya dalam keputusan baru. Algorithmic bias dapat muncul dalam berbagai bentuk dan menghasilkan perlakuan yang tidak setara terhadap kelompok tertentu (Wang dkk., 2024). Persoalan ini menunjukkan bahwa netralitas teknologi tidak dapat diasumsikan hanya karena keputusan dibuat melalui komputer. Teknologi dapat mengotomatisasi bias sebagaimana ia dapat mengotomatisasi proses yang efisien.

Dalam konteks pelayanan publik, risiko tersebut menjadi lebih sensitif karena pemerintah memiliki posisi yang berbeda dengan perusahaan biasa. Keputusan administratif dapat menentukan akses masyarakat terhadap hak atau layanan tertentu. Ketika AI digunakan untuk membantu keputusan pemerintahan, prinsip legalitas, transparansi, akuntabilitas, dan perlindungan hak harus tetap dipertahankan. Sistem otomatis tidak dapat menjadi alasan untuk mengurangi kewajiban pemerintah memberikan perlakuan yang adil.

Penggunaan AI justru harus diikuti dengan mekanisme pengawasan yang memastikan bahwa teknologi bekerja dalam kerangka hukum.

Hal yang sama berlaku dalam penegakan hukum. AI dapat digunakan untuk membantu analisis data, mengidentifikasi pola, atau mendukung proses investigasi. Namun, penggunaan sistem tersebut dalam bidang yang memiliki konsekuensi terhadap kebebasan dan hak individu membutuhkan kehati-hatian lebih tinggi. Keputusan yang dibuat atau dipengaruhi algoritma harus tetap dapat diuji oleh manusia yang memiliki kewenangan hukum. Literatur mengenai penggunaan AI dalam *law enforcement* menekankan adanya peluang sekaligus risiko dalam pemanfaatan teknologi tersebut (Stepanov & Stepanov, 2026). Teknologi seharusnya memperkuat kemampuan penegakan hukum, bukan menghilangkan tanggung jawab manusia dalam membuat keputusan yang memiliki konsekuensi hukum.

Prinsip tersebut dapat dirumuskan melalui gagasan bahwa AI sebaiknya berfungsi sebagai pendukung keputusan, bukan pengganti mutlak penilaian manusia, terutama pada keputusan yang berisiko tinggi. Sistem AI dapat memberikan rekomendasi, mengidentifikasi pola, atau menyajikan alternatif. Keputusan akhir tetap membutuhkan manusia yang memahami konteks hukum dan sosial dari keputusan tersebut. Pendekatan ini dipandang lebih dapat dipertanggungjawabkan karena manusia tetap menjadi aktor yang melakukan penilaian

normatif (Bailo dkk., 2026; Pashentsev & Babaeva, 2024).

Kendati demikian, keberadaan manusia dalam proses tersebut belum tentu cukup. Pengawasan manusia dapat menjadi formalitas apabila manusia hanya menerima hasil AI tanpa melakukan pemeriksaan yang berarti. Kondisi tersebut dikenal sebagai *automation bias*, yaitu kecenderungan manusia terlalu mempercayai rekomendasi sistem otomatis. Apabila pengawasan hanya dilakukan dengan cara menandatangani keputusan yang telah dihasilkan AI, maka keberadaan manusia tidak memberikan perlindungan yang substantif. Karena itu, *human oversight* harus dirancang sebagai mekanisme kontrol yang nyata, bukan sekadar mencantumkan manusia dalam prosedur (Laux & Ruschemeier, 2025).

Transformasi hubungan hukum oleh AI juga mengubah hubungan antara pihak yang mengembangkan dan menggunakan teknologi. Dalam sistem tradisional, seseorang yang menggunakan alat biasanya memiliki kontrol yang relatif mudah dipahami terhadap alat tersebut. Dalam AI, hubungan tersebut dapat melibatkan pengembang model, penyedia layanan, integrator, operator, pengguna akhir, dan institusi yang memperoleh manfaat dari sistem. Masing-masing dapat memiliki tingkat kendali yang berbeda terhadap sistem. Perbedaan tingkat kendali tersebut nantinya menjadi penting dalam menentukan siapa

yang harus bertanggung jawab ketika teknologi menghasilkan kerugian.

Dengan demikian, AI menciptakan bentuk baru hubungan hukum yang bersifat teknologis, multipihak, dan berbasis data. Hubungan tersebut tidak lagi hanya terjadi antara dua subjek hukum, tetapi dapat melibatkan manusia, perusahaan pengembang, penyedia infrastruktur, platform, pemilik data, dan institusi pengguna. Hukum perlu memahami struktur hubungan tersebut agar tidak hanya melihat pihak yang berada paling dekat dengan korban, tetapi juga menilai siapa yang merancang sistem, siapa yang mengendalikan risiko, siapa yang memperoleh manfaat, dan siapa yang memiliki kemampuan mencegah kerugian.

Transformasi AI tidak menghilangkan kebutuhan terhadap hukum, tetapi justru memperbesar kebutuhan tersebut. Semakin besar peran AI dalam kehidupan masyarakat, semakin penting memastikan bahwa keputusan teknologi tetap berada dalam kerangka akuntabilitas. Transparansi, *explainability*, *human oversight*, audit, dan mekanisme pemulihan menjadi unsur penting agar otomatisasi tidak menghasilkan keputusan yang tidak dapat dipertanggungjawabkan. Arah perkembangan hukum dengan demikian bukan melarang AI, tetapi memastikan bahwa AI berkembang dalam struktur yang tetap menempatkan manusia dan hak-haknya sebagai pusat perlindungan.

2. Pertanggungjawaban Hukum dan Risiko Algoritmik dalam Penggunaan Kecerdasan Buatan

Persoalan pertanggungjawaban menjadi salah satu tantangan terbesar ketika AI digunakan dalam aktivitas yang memiliki konsekuensi hukum. Sistem dapat menghasilkan rekomendasi yang salah, memberikan informasi yang tidak akurat, mendiskriminasi kelompok tertentu, melanggar privasi, atau menghasilkan keputusan yang menyebabkan kerugian. Pertanyaan hukumnya kemudian tidak sederhana. Apakah kesalahan tersebut merupakan kesalahan pengembang, penyedia sistem, pengguna, operator, atau institusi yang menggunakan AI? Jawaban terhadap pertanyaan tersebut membutuhkan pendekatan yang tidak hanya melihat siapa yang mengoperasikan sistem, tetapi juga bagaimana risiko diciptakan dan siapa yang memiliki kemampuan untuk mengendalikannya.

AI pada dasarnya bukan subjek hukum yang dapat dimintai pertanggungjawaban sebagaimana manusia atau badan hukum. Sistem AI tidak memiliki kehendak hukum, kapasitas hukum, atau kemampuan menanggung kewajiban dalam pengertian konvensional. Karena itu, pertanggungjawaban tetap ditempatkan pada manusia dan institusi yang terlibat dalam pengembangan, penyediaan, pengoperasian, atau pemanfaatan sistem (Pashentsev & Babaeva, 2024; Qutieshat dkk., 2026). Prinsip tersebut penting agar

munculnya teknologi otonom tidak menyebabkan kekosongan pertanggungjawaban. Ketika sistem melakukan kesalahan, hukum tetap harus menemukan subjek yang dapat dimintai pertanggungjawaban.

Model pertanggungjawaban yang lebih realistis adalah *shared responsibility*. Pengembang memiliki tanggung jawab terhadap desain dan keamanan sistem. Penyedia layanan bertanggung jawab terhadap cara teknologi disediakan dan dipelihara. *Deployer* atau institusi pengguna bertanggung jawab terhadap konteks penggunaan. Operator memiliki kewajiban mengikuti prosedur dan melakukan pengawasan yang diperlukan. Sementara itu, institusi yang memperoleh manfaat dari penggunaan AI dapat memiliki kewajiban memastikan sistem digunakan secara aman dan sesuai hukum (Bailo dkk., 2026; Satyo dkk., 2026). Pembagian tersebut memungkinkan hukum menilai tanggung jawab berdasarkan tingkat kendali dan peran masing-masing pihak.

Contoh sederhana dapat menggambarkan kompleksitas tersebut. Sebuah perusahaan menggunakan AI untuk melakukan seleksi kandidat pekerja. Sistem secara konsisten menghasilkan tingkat penolakan yang lebih tinggi terhadap kelompok tertentu. Kandidat yang dirugikan kemudian menggugat keputusan tersebut. Perusahaan mungkin berpendapat bahwa keputusan dihasilkan sistem AI. Penyedia teknologi dapat berpendapat bahwa perusahaan memasukkan data

dan parameter sendiri. Pengembang model mungkin menyatakan bahwa model hanya menyediakan alat dan pengguna bertanggung jawab terhadap penggunaannya. Jika hukum hanya mencari satu pihak yang bersalah secara sederhana, proses pertanggungjawaban dapat menjadi sulit. Model tanggung jawab berbasis peran memungkinkan pengadilan atau regulator menilai kontribusi dan kontrol setiap pihak.

Risiko algoritmik juga dapat muncul sebelum sistem digunakan. Pengujian yang tidak memadai dapat menyebabkan kesalahan tidak terdeteksi. Data pelatihan dapat mengandung bias. Dokumentasi mungkin tidak menjelaskan batas kemampuan sistem. Model dapat bekerja dengan baik dalam kondisi tertentu tetapi menghasilkan kesalahan dalam kondisi lain. Karena itu, kewajiban hukum tidak seharusnya dimulai ketika kerugian telah terjadi. Pengembang dan pengguna perlu memiliki kewajiban preventif, termasuk pengujian, dokumentasi, penilaian risiko, pemantauan, dan pembaruan sistem.

Algorithmic bias merupakan salah satu bentuk risiko yang paling penting. Sistem AI dapat menghasilkan perlakuan berbeda berdasarkan karakteristik tertentu apabila pola tersebut terdapat dalam data atau desain model. Bias tidak selalu muncul karena seseorang secara sengaja memasukkan aturan diskriminatif. Bias dapat muncul melalui variabel pengganti (*proxy variables*), distribusi data yang tidak seimbang, cara pelabelan

data, atau tujuan optimasi tertentu. Karena itu, pemeriksaan terhadap sistem AI harus memperhatikan bukan hanya aturan yang tertulis, tetapi juga hasil yang dihasilkan sistem (Wang dkk., 2024).

Risiko bias memiliki konsekuensi hukum yang berbeda tergantung sektor penggunaannya. Dalam rekomendasi konten, bias mungkin memengaruhi informasi yang diterima pengguna. Dalam sektor keuangan, bias dapat memengaruhi akses terhadap kredit. Dalam ketenagakerjaan, bias dapat memengaruhi peluang seseorang memperoleh pekerjaan. Dalam kesehatan, kesalahan prediksi dapat memengaruhi keputusan pelayanan. Semakin besar dampak keputusan terhadap kehidupan seseorang, semakin tinggi kebutuhan akan pengawasan, transparansi, dan mekanisme koreksi.

Persoalan berikutnya adalah *hallucination* pada sistem AI generatif. Sistem dapat menghasilkan informasi yang tampak meyakinkan tetapi sebenarnya tidak akurat atau tidak memiliki dasar yang memadai. Dalam konteks umum, kesalahan tersebut mungkin hanya menyebabkan ketidaknyamanan. Namun, apabila digunakan untuk membuat dokumen hukum, keputusan bisnis, informasi kesehatan, atau komunikasi resmi, kesalahan dapat menghasilkan kerugian yang lebih besar. Pengguna tidak dapat sepenuhnya melepaskan tanggung jawab dengan alasan bahwa informasi tersebut berasal dari AI. Pihak yang menggunakan

keluaran AI tetap harus menilai kesesuaian dan kebenarannya berdasarkan konteks penggunaannya.

Perlindungan data juga berkaitan erat dengan pertanggungjawaban AI. Sistem AI membutuhkan data untuk dilatih dan dioperasikan. Penggunaan data yang berlebihan, tidak sah, atau tidak aman dapat menimbulkan persoalan hukum. Risiko semakin tinggi apabila data yang digunakan mengandung informasi pribadi atau data sensitif. Pengembang dan pengguna harus memahami sumber data, dasar pemrosesan, tujuan penggunaan, serta mekanisme keamanan. Dengan demikian, tata kelola AI tidak dapat dipisahkan dari tata kelola data.

Keamanan sistem merupakan dimensi lainnya. Sistem AI yang terhubung dengan jaringan dapat menjadi sasaran manipulasi, *prompt injection*, pencurian data, atau serangan lainnya. Serangan terhadap sistem dapat menyebabkan AI menghasilkan keluaran yang berbeda dari kondisi normal. Dalam konteks tertentu, manipulasi tersebut dapat menyebabkan keputusan yang salah. Karena itu, keamanan AI harus mencakup keseluruhan siklus hidup sistem, mulai dari data, model, infrastruktur, sampai penggunaan akhir.

Human oversight kemudian menjadi mekanisme penting untuk mengurangi risiko. Namun, sebagaimana telah dijelaskan, pengawasan tidak boleh sekadar prosedural. Manusia yang melakukan pengawasan harus memiliki kewenangan untuk menolak rekomendasi AI, meminta pemeriksaan tambahan, atau menghentikan

penggunaan sistem apabila ditemukan risiko. Mereka juga perlu memiliki pengetahuan yang cukup untuk memahami keterbatasan teknologi. Tanpa kompetensi tersebut, manusia hanya menjadi pelaksana keputusan yang sebenarnya dibuat oleh sistem.

Audit dapat menjadi mekanisme untuk memastikan bahwa pengawasan tersebut berjalan. Audit AI dapat menilai kualitas data, kinerja model, potensi diskriminasi, keamanan, dokumentasi, dan kesesuaian penggunaan. Dokumentasi juga memungkinkan organisasi menjelaskan bagaimana sistem dikembangkan dan digunakan. Ketika sengketa muncul, dokumentasi dapat membantu menentukan siapa yang mengambil keputusan, data apa yang digunakan, versi model apa yang digunakan, dan prosedur apa yang berlaku pada saat keputusan dibuat.

Mekanisme pemulihan (*remedies*) merupakan bagian yang sama pentingnya. Orang yang dirugikan oleh keputusan AI harus memiliki jalur untuk mengajukan keberatan, meminta pemeriksaan manusia, memperoleh koreksi, atau mendapatkan kompensasi apabila memenuhi dasar pertanggungjawaban. Hak untuk memperoleh pemulihan menjadi sangat penting karena teknologi tidak boleh menciptakan keputusan yang secara praktis tidak dapat digugat. Prinsip hukum membutuhkan adanya mekanisme untuk mengoreksi kesalahan, termasuk kesalahan yang dihasilkan oleh sistem otomatis (Rajendra & Thuraisingam, 2025).

Dalam menentukan tanggung jawab, hukum juga perlu mempertimbangkan tingkat risiko penggunaan AI. Tidak semua penggunaan AI membutuhkan kontrol yang sama. Sistem yang membantu menyusun rekomendasi hiburan memiliki risiko berbeda dengan sistem yang menentukan akses seseorang terhadap layanan kesehatan atau kebijakan publik. Pendekatan berbasis risiko memungkinkan kewajiban hukum disesuaikan dengan potensi dampak. Semakin tinggi risikonya, semakin tinggi pula tuntutan terhadap pengujian, dokumentasi, pengawasan, transparansi, dan mekanisme pemulihan.

Model tersebut memungkinkan hukum tetap mempertahankan prinsip dasar pertanggungjawaban tanpa memaksakan konsep yang tidak sesuai terhadap teknologi. Tidak perlu menjadikan AI sebagai subjek hukum baru hanya untuk menjawab persoalan pertanggungjawaban. Yang lebih penting adalah memastikan bahwa seluruh aktor yang berada dalam rantai pengembangan dan penggunaan AI memiliki kewajiban yang jelas. Dengan demikian, teknologi tidak menjadi "subjek tanpa tanggung jawab", sementara manusia dan institusi tetap menjadi pusat akuntabilitas.

Pertanggungjawaban AI harus dibangun berdasarkan prinsip bahwa otonomi teknologi tidak boleh berarti pelepasan tanggung jawab manusia. Semakin besar kemampuan sistem untuk menghasilkan keputusan secara mandiri, semakin

penting pula mekanisme untuk memastikan adanya manusia atau institusi yang dapat dimintai pertanggungjawaban. Pendekatan tersebut menghubungkan inovasi teknologi dengan prinsip hukum yang lebih fundamental: adanya pihak yang bertanggung jawab, keputusan yang dapat dipertanyakan, dan korban yang memperoleh akses terhadap pemulihan.

3. *Blockchain*, *Smart Contract*, dan Rekonstruksi Keabsahan Hukum Transaksi Digital

Blockchain memperkenalkan cara berbeda dalam mencatat dan memvalidasi transaksi digital. Berbeda dengan sistem konvensional yang biasanya bergantung pada satu institusi atau pusat pencatatan, *blockchain* menggunakan mekanisme *distributed ledger* yang memungkinkan catatan transaksi disimpan dan diverifikasi melalui jaringan. Karakter tersebut menghasilkan tingkat transparansi dan ketahanan terhadap perubahan data yang berbeda dari sistem basis data konvensional. Dalam transaksi digital, *blockchain* dapat digunakan untuk pencatatan aset, pembayaran, identitas digital, pelacakan transaksi, dan berbagai bentuk aktivitas ekonomi lainnya (Abigail dkk., 2025; Maydanyk, 2024).

Keunggulan teknis tersebut kemudian melahirkan gagasan bahwa transaksi dapat dijalankan dengan lebih sedikit perantara. Namun, berkurangnya perantara tidak berarti berkurangnya kebutuhan terhadap hukum. Ketika transaksi konvensional melibatkan bank, notaris, perusahaan, atau lembaga lainnya sebagai pihak yang melakukan

verifikasi dan pencatatan, sistem berbasis *blockchain* mendistribusikan sebagian fungsi tersebut ke jaringan dan protokol teknologi. Perubahan ini menimbulkan pertanyaan hukum mengenai siapa yang menjadi pihak dalam transaksi, kapan kesepakatan dianggap terjadi, bagaimana identitas dibuktikan, dan siapa yang bertanggung jawab ketika sistem mengalami kesalahan.

Salah satu perkembangan yang paling menarik adalah *Smart Contract*. Istilah tersebut sering digunakan untuk menggambarkan kode komputer yang dirancang untuk menjalankan tindakan tertentu secara otomatis apabila kondisi yang telah ditentukan terpenuhi. Ketika suatu kondisi terjadi, sistem dapat secara otomatis mentransfer aset, mencatat transaksi, atau menjalankan tindakan lain yang telah diprogram. Otomatisasi tersebut dapat meningkatkan efisiensi, tetapi sekaligus mengubah cara hukum memandang pelaksanaan kontrak. Dalam kontrak konvensional, manusia atau lembaga biasanya melakukan tindakan pelaksanaan. Dalam *Smart Contract*, sebagian pelaksanaan dapat dilakukan oleh kode.

Persoalan pertama adalah apakah *Smart Contract* dapat dianggap sebagai kontrak dalam pengertian hukum. Jawabannya tidak cukup ditentukan oleh keberadaan kode. Keabsahan hukum tetap membutuhkan terpenuhinya syarat kontraktual, termasuk adanya kehendak yang sah, objek yang jelas, dan tujuan yang diperbolehkan hukum (Aslina & Noviya, 2026; Maydanyk, 2024).

Kode komputer dapat menjadi sarana untuk mengeksekusi kesepakatan, tetapi kode tersebut tidak otomatis menciptakan kesepakatan yang sah. Harus terdapat hubungan antara kehendak para pihak dan tindakan teknis yang dijalankan oleh sistem.

Dalam konteks ini, konsep persetujuan menjadi sangat penting. Persetujuan terhadap *Smart Contract* dapat diwujudkan melalui tindakan digital tertentu, tetapi tindakan tersebut harus dapat dikaitkan dengan kehendak para pihak. Pengakuan terhadap *automated consent* berkembang dalam transaksi elektronik, tetapi validitasnya pada dasarnya tetap bergantung pada persetujuan manusia yang kemudian diterjemahkan ke dalam instruksi atau kode (Al-Mezel dkk., 2026). Kode dapat menjalankan apa yang telah disepakati, tetapi kode tidak seharusnya dianggap sebagai pengganti kehendak hukum.

Masalah berikutnya berkaitan dengan bahasa kontrak. Kontrak konvensional menggunakan bahasa yang dapat ditafsirkan dengan mempertimbangkan konteks, kebiasaan, itikad baik, dan keadaan para pihak. Kode komputer membutuhkan instruksi yang lebih spesifik agar dapat dijalankan. Tidak semua klausula hukum mudah diterjemahkan menjadi kondisi otomatis. Klausula mengenai itikad baik, kewajaran, perubahan keadaan, atau kewajiban untuk bernegosiasi kembali dapat sulit diwujudkan dalam bentuk *if-then* yang sederhana. Karena itu,

tidak semua kontrak cocok sepenuhnya diotomatisasi (Maydanyk, 2024).

Kondisi tersebut dapat menimbulkan kesenjangan antara bahasa hukum dan bahasa kode. Bahasa hukum memiliki ruang interpretasi yang diperlukan agar kontrak dapat beradaptasi dengan keadaan. Kode, sebaliknya, bekerja berdasarkan instruksi yang telah ditentukan. Apabila kode menjalankan suatu tindakan yang secara teknis sesuai dengan program tetapi bertentangan dengan maksud para pihak, muncul pertanyaan mengenai mana yang harus diprioritaskan. Pertanyaan tersebut tidak dapat dijawab hanya melalui teknologi karena membutuhkan interpretasi hukum.

Persoalan *force majeure* memperlihatkan kesulitan tersebut. Kontrak konvensional dapat memberikan ruang untuk menyesuaikan kewajiban ketika terjadi keadaan di luar kendali para pihak. *Smart Contract* yang dirancang untuk menjalankan transaksi secara otomatis mungkin tidak memiliki mekanisme fleksibel untuk menghadapi perubahan keadaan. Gangguan jaringan, serangan siber, kegagalan *oracle*, perubahan regulasi, atau kondisi pasar ekstrem dapat memengaruhi pelaksanaan kontrak. Literatur menunjukkan bahwa doktrin klasik *force majeure* belum selalu memadai untuk menghadapi risiko teknologi yang muncul dalam kontrak digital otomatis (Abigail dkk., 2025).

Persoalan lainnya adalah kesalahan kode. Kesalahan kecil dalam pemrograman dapat menghasilkan konsekuensi ekonomi yang besar

apabila kode digunakan untuk mengelola aset dalam jumlah besar. Ketika sistem telah dirancang untuk mengeksekusi transaksi secara otomatis, kesalahan tersebut dapat berjalan tanpa menunggu pemeriksaan manusia. Di sinilah muncul pertanyaan mengenai pihak yang bertanggung jawab. Apakah tanggung jawab berada pada pengembang kode, pemilik *Smart Contract*, pengguna, operator platform, atau pihak lain yang memperoleh manfaat dari sistem?

Model tanggung jawab multipihak menjadi relevan dalam kondisi tersebut. Literatur menunjukkan bahwa tanggung jawab dapat bergantung pada peran operator, pemilik, pengembang, validator, atau platform (Al-Mezel dkk., 2026; Aslina & Noviya, 2026; Maydanyk, 2024). Penentuan tanggung jawab perlu mempertimbangkan siapa yang memiliki kemampuan untuk mencegah kesalahan, siapa yang mengetahui risiko, dan siapa yang memperoleh manfaat dari aktivitas tersebut. Pendekatan semacam ini lebih sesuai dibandingkan menganggap bahwa seluruh risiko otomatis menjadi tanggung jawab satu pihak.

Karakter *blockchain* yang sulit diubah juga menciptakan persoalan tersendiri. Immutability merupakan salah satu keunggulan teknologi karena mengurangi kemungkinan manipulasi catatan transaksi. Namun, karakter tersebut dapat menjadi masalah apabila transaksi ternyata salah, tidak sah, atau dilakukan akibat penipuan. Dalam kontrak

konvensional, pembatalan atau restitusi dapat dilakukan melalui mekanisme hukum tertentu. Dalam sistem berbasis *blockchain*, pembatalan teknis tidak selalu mudah dilakukan. Kondisi tersebut dapat memperbesar risiko bagi konsumen dan pihak yang berada dalam posisi tawar lebih lemah (Aslina & Noviya, 2026).

Pseudonimitas juga dapat mempersulit penegakan hukum. Identitas yang digunakan dalam transaksi berbasis *blockchain* tidak selalu secara langsung menunjukkan identitas hukum seseorang. Alamat digital dapat terhubung dengan transaksi, tetapi menghubungkannya dengan subjek hukum tertentu dapat membutuhkan proses tambahan. Kesulitan tersebut berpengaruh terhadap pembuktian, terutama ketika terjadi sengketa atau dugaan pelanggaran hukum. Teknologi yang meningkatkan privasi atau desentralisasi dengan demikian dapat sekaligus meningkatkan tantangan identifikasi.

Keadaan tersebut tidak berarti bahwa *blockchain* atau *Smart Contract* tidak dapat digunakan dalam hubungan hukum. Sebaliknya, teknologi tersebut dapat memberikan manfaat besar apabila digunakan untuk jenis transaksi yang struktur kewajibannya jelas dan dapat diotomatisasi. Persoalannya adalah menentukan bagian mana dari kontrak yang cocok untuk dieksekusi secara otomatis dan bagian mana yang tetap membutuhkan penilaian manusia. Pendekatan yang lebih realistis adalah menggabungkan kode dengan ketentuan hukum

tertulis, sehingga kode menjalankan aspek teknis sementara ketentuan hukum tetap mengatur hak, kewajiban, interpretasi, dan penyelesaian sengketa.

Kontrak hibrida dapat menjadi salah satu bentuk kompromi tersebut. Para pihak dapat menyusun kontrak dalam bahasa hukum dan menghubungkan bagian tertentu dengan *Smart Contract*. Klausula mengenai pembayaran otomatis, misalnya, dapat diterjemahkan ke dalam kode, sedangkan ketentuan mengenai *force majeure*, sengketa, pembatalan, dan interpretasi tetap berada dalam dokumen hukum. Model tersebut memungkinkan efisiensi teknologi tanpa menghilangkan fleksibilitas hukum.

Dari perspektif hukum perdata, hal terpenting bukanlah apakah kontrak dibuat dalam dokumen biasa atau kode komputer. Pertanyaan utamanya adalah apakah terdapat kesepakatan yang sah, apakah para pihak dapat diidentifikasi, apakah objek dan tujuan kontrak diperbolehkan, serta bagaimana hak dan kewajiban dapat ditegakkan. Teknologi merupakan sarana. Keabsahan hukum tetap membutuhkan dasar normatif. *Smart Contract* karena itu sebaiknya dipahami sebagai bentuk teknologi untuk menjalankan kesepakatan, bukan sebagai sistem hukum yang berdiri sendiri.

Blockchain dan *Smart Contract* menunjukkan bahwa hukum harus beradaptasi terhadap perubahan cara transaksi dilakukan. Immutability, otomatisasi, pseudonimitas, dan desentralisasi memberikan manfaat sekaligus risiko. Tantangan

hukum bukan menghapus karakter teknologi tersebut, tetapi membangun mekanisme yang memungkinkan manfaatnya digunakan tanpa menghilangkan perlindungan hukum. Kejelasan klausula, alokasi risiko, mekanisme pembatalan, *force majeure*, dan pertanggungjawaban multipihak menjadi unsur penting dalam membangun transaksi berbasis *Smart Contract* yang dapat dipertanggungjawabkan secara hukum.

4. Regulasi Teknologi Baru: Antara Inovasi, Kepastian Hukum, dan Perlindungan Masyarakat

Teknologi berkembang melalui siklus inovasi yang jauh lebih cepat dibandingkan proses pembentukan peraturan. Sebuah teknologi dapat mengalami beberapa generasi perubahan sebelum regulator menyelesaikan proses pembentukan atau perubahan undang-undang. Keadaan tersebut menimbulkan apa yang dikenal sebagai *regulatory lag*, yaitu kondisi ketika hukum belum mampu memberikan respons memadai terhadap perkembangan teknologi. Persoalannya bukan hanya bahwa regulasi terlambat, tetapi juga bahwa kategori hukum yang dirancang untuk teknologi lama belum tentu cocok untuk teknologi yang memiliki karakter berbeda (Ahern, 2025; Currie dkk., 2025).

AI menjadi contoh nyata dari persoalan tersebut. Sistem yang sama dapat digunakan untuk berbagai tujuan dengan tingkat risiko berbeda. Teknologi generatif dapat digunakan untuk membuat konten kreatif, membantu pekerjaan administratif, mengembangkan perangkat lunak, atau mendukung

proses pengambilan keputusan. Apabila regulasi hanya berfokus pada jenis teknologinya, aturan dapat menjadi terlalu luas atau terlalu sempit. Karena itu, pendekatan berbasis risiko menjadi semakin penting agar kewajiban hukum disesuaikan dengan dampak penggunaan teknologi, bukan hanya label teknologinya (Corfmat dkk., 2025; Currie dkk., 2025).

Pendekatan *risk-based regulation* mengharuskan regulator mengidentifikasi kemungkinan dampak sebelum menentukan tingkat kewajiban. Sistem AI berisiko rendah tidak harus dibebani persyaratan yang sama dengan sistem yang memengaruhi hak fundamental. Pendekatan ini memungkinkan inovasi tetap berkembang pada wilayah yang risikonya dapat diterima, sementara penggunaan berisiko tinggi memperoleh pengawasan lebih ketat. Dengan demikian, regulasi tidak semata-mata berfungsi sebagai pembatas, tetapi juga sebagai instrumen untuk membentuk ekosistem inovasi yang lebih aman.

Persoalan tersebut memperlihatkan keterbatasan pendekatan *technology-neutral regulation* apabila diterapkan secara mutlak. Prinsip netralitas teknologi memiliki keunggulan karena hukum tidak cepat usang ketika teknologi berubah. Namun, teknologi baru dapat menghasilkan risiko yang tidak dikenal ketika hukum lama dibuat. Regulasi yang terlalu umum mungkin tidak memberikan instrumen yang cukup untuk mengatasi risiko tertentu. Karena itu, regulasi teknologi baru membutuhkan kombinasi antara prinsip yang relatif

tahan terhadap perubahan teknologi dan ketentuan khusus untuk risiko tertentu (Currie dkk., 2025).

Salah satu instrumen yang berkembang adalah *regulatory sandbox*. Melalui *sandbox*, inovasi dapat diuji dalam lingkungan terbatas dengan pengawasan regulator. Tujuannya bukan memberikan pengecualian hukum tanpa batas, tetapi menciptakan ruang untuk mempelajari teknologi dan risiko sebelum diterapkan secara luas. Regulator dapat memperoleh pengalaman langsung mengenai bagaimana suatu teknologi bekerja, risiko apa yang muncul, dan aturan apa yang perlu disesuaikan (Johnson, 2022; Novelli dkk., 2026).

Meskipun demikian, *sandbox* bukan solusi otomatis. Proses seleksi peserta, penentuan ruang uji, pengawasan, perlindungan peserta, dan keputusan setelah pengujian menimbulkan persoalan legitimasi. Apabila regulator terlalu dekat dengan pelaku industri, terdapat risiko pengawasan menjadi lemah. Sebaliknya, apabila aturan terlalu ketat, inovasi yang seharusnya dapat diuji justru tidak berkembang. Literatur menunjukkan bahwa *regulatory sandbox* juga memiliki persoalan terkait partisipasi, akuntabilitas, legitimasi, serta pengawasan setelah fase uji coba berakhir (Johnson, 2022; Novelli dkk., 2026).

Kepastian hukum menjadi tantangan lain. Pelaku usaha membutuhkan kepastian mengenai apa yang diperbolehkan, apa yang dilarang, dan apa yang harus dilakukan untuk memenuhi kewajiban. Ketidakjelasan dapat meningkatkan biaya kepatuhan

dan menghambat investasi. Namun, regulasi yang terlalu rinci dapat cepat menjadi usang. Regulator karena itu perlu membangun aturan yang cukup jelas untuk memberikan kepastian tetapi cukup fleksibel untuk mengikuti perubahan teknologi.

Dokumentasi dan audit dapat menjadi jembatan antara fleksibilitas dan kepastian tersebut. Regulator tidak harus selalu menentukan bagaimana teknologi harus dibangun secara teknis. Regulator dapat menentukan hasil yang harus dicapai, seperti keamanan, transparansi, perlindungan data, pengelolaan risiko, dan kemampuan memberikan penjelasan. Perusahaan kemudian memiliki ruang memilih teknologi untuk mencapai standar tersebut. Model ini memungkinkan regulasi lebih adaptif terhadap inovasi tanpa kehilangan tujuan perlindungan.

Transparansi juga menjadi instrumen penting. Pengguna dan regulator perlu mengetahui kapan AI digunakan, untuk tujuan apa, dengan risiko apa, serta siapa yang bertanggung jawab. Dalam sistem berisiko tinggi, registri atau dokumentasi sistem AI dapat membantu regulator melakukan pengawasan. Audit juga dapat digunakan untuk menilai kepatuhan terhadap standar. Literatur menunjukkan bahwa audit, dokumentasi, *transparency registries*, dan harmonisasi lintas yurisdiksi dapat menjadi elemen penting dalam membangun tata kelola AI (Currie dkk., 2025; Rajendra & Thuraisingam, 2025).

Perlindungan konsumen harus menjadi bagian dari desain regulasi. Konsumen sering kali tidak memiliki kemampuan teknis untuk memahami bagaimana AI atau *blockchain* bekerja. Ketimpangan informasi dapat menyebabkan konsumen menerima risiko yang tidak mereka pahami. Dalam transaksi berbasis teknologi, klausula standar juga dapat menempatkan konsumen pada posisi tawar yang lebih lemah. Regulasi perlu memastikan bahwa inovasi tidak menjadi alasan untuk mengurangi perlindungan terhadap pihak yang tidak memiliki kemampuan negosiasi atau pengetahuan teknis yang setara.

Privasi merupakan persoalan lain yang harus diperhatikan. AI membutuhkan data, sementara *blockchain* dapat menciptakan catatan yang sulit diubah. Dua karakter tersebut dapat menciptakan ketegangan dengan prinsip perlindungan data. Sistem yang membutuhkan data dalam jumlah besar harus memiliki batasan tujuan dan keamanan yang memadai. Sebaliknya, teknologi pencatatan permanen harus dirancang dengan mempertimbangkan hak subjek data. Regulasi perlu mencari solusi teknis dan hukum yang memungkinkan inovasi tetap berjalan tanpa menghilangkan hak individu.

Hak kekayaan intelektual juga mengalami tekanan baru. Sistem AI generatif dapat menghasilkan konten berdasarkan data dalam jumlah besar. *Blockchain* dapat digunakan untuk mencatat kepemilikan atau transaksi aset digital.

Pertanyaan mengenai siapa pemilik hasil yang dihasilkan AI, bagaimana data digunakan untuk pelatihan, dan bagaimana hak pencipta dilindungi menunjukkan bahwa hukum kekayaan intelektual harus berhadapan dengan model produksi yang berbeda dari masa sebelumnya. Persoalan tersebut membutuhkan dialog antara prinsip hukum yang telah ada dan karakter teknologi baru.

Persaingan usaha juga tidak dapat diabaikan. Teknologi digital dapat menciptakan konsentrasi pasar karena perusahaan yang menguasai data, komputasi, platform, atau infrastruktur dapat memperoleh keunggulan besar. Ketergantungan terhadap teknologi tertentu dapat menciptakan *lock-in* dan mengurangi pilihan pengguna. Regulasi teknologi karena itu tidak hanya berkaitan dengan keamanan dan privasi, tetapi juga dengan struktur pasar dan distribusi kekuasaan ekonomi.

Pendekatan regulasi adaptif membutuhkan regulator yang juga mampu belajar. Regulator tidak cukup membuat aturan kemudian menunggu sampai terjadi pelanggaran. Perubahan teknologi mengharuskan regulator melakukan pemantauan, evaluasi, konsultasi, pengujian, dan pembaruan kebijakan secara berkala. Inilah yang disebut sebagai *regulatory learning*. Regulasi tidak dipandang sebagai produk akhir, tetapi sebagai proses yang terus disempurnakan berdasarkan perkembangan teknologi dan pengalaman penerapannya (Ahern, 2025).

Model tersebut mengarah pada gagasan *anticipatory governance*. Regulasi seharusnya tidak hanya merespons masalah setelah terjadi, tetapi berusaha mengantisipasi risiko yang mungkin muncul. Antisipasi bukan berarti melarang teknologi berdasarkan dugaan semata. Antisipasi berarti mengidentifikasi skenario risiko, menilai kemungkinan dampaknya, dan menyiapkan mekanisme mitigasi sebelum teknologi digunakan secara luas. Pendekatan ini sangat relevan untuk AI karena kemampuan teknologi dapat berkembang lebih cepat daripada pengalaman regulator.

Harmonisasi menjadi penting karena teknologi digital beroperasi lintas batas. Perusahaan dapat mengembangkan sistem di satu negara, menyediakan layanan di negara lain, dan memproses data di negara ketiga. Perbedaan regulasi dapat menciptakan konflik kepatuhan. Karena itu, negara membutuhkan dialog dan kerja sama internasional untuk mengembangkan prinsip dasar yang dapat saling dikenali. Harmonisasi tidak selalu berarti semua negara harus memiliki aturan identik, tetapi setidaknya terdapat standar minimum dan mekanisme kompatibilitas.

Regulasi yang baik pada akhirnya harus menjaga tiga kepentingan secara bersamaan. Pertama, inovasi, agar masyarakat dan dunia usaha dapat memanfaatkan manfaat teknologi. Kedua, kepastian hukum, agar pelaku mengetahui kewajiban dan batasannya. Ketiga, perlindungan masyarakat, agar risiko teknologi tidak dibebankan secara tidak

proporsional kepada individu atau kelompok yang rentan. Ketiga kepentingan tersebut tidak selalu berjalan searah. Karena itu, regulasi teknologi baru membutuhkan penilaian berbasis risiko dan mekanisme pembelajaran yang berkelanjutan.

Dengan demikian, tantangan regulasi teknologi baru bukan sekadar memilih antara "mengatur" atau "tidak mengatur". Persoalan yang lebih penting adalah bagaimana mengatur dengan cara yang tepat. Regulasi yang terlalu lemah dapat membiarkan risiko berkembang tanpa kontrol. Regulasi yang terlalu berat dapat menghambat inovasi. Regulasi yang tidak jelas dapat menciptakan ketidakpastian. Jalan keluarnya adalah membangun regulasi adaptif, berbasis risiko, proporsional, transparan, dan memungkinkan pembelajaran kelembagaan.

5. Masa Depan Hukum di Tengah Konvergensi AI, Blockchain, dan Teknologi Otonom

Perkembangan teknologi tidak selalu berlangsung dalam bentuk teknologi yang berdiri sendiri. AI, *blockchain*, *cloud computing*, *Internet of Things*, dan sistem otonom semakin dapat diintegrasikan dalam satu ekosistem. Konvergensi tersebut mengubah persoalan hukum karena suatu tindakan dapat melibatkan beberapa lapisan teknologi sekaligus. Data dapat disimpan dalam infrastruktur terdistribusi, dianalisis oleh AI, kemudian digunakan untuk memicu *Smart Contract* yang melakukan transaksi otomatis. Ketika terjadi kesalahan, sulit menentukan titik tunggal tempat

kesalahan tersebut terjadi. Persoalan hukum kemudian bergerak dari pengaturan satu teknologi menuju pengaturan hubungan antarteknologi.

Konvergensi tersebut menciptakan bentuk baru otomatisasi. AI dapat melakukan analisis dan menghasilkan keputusan. *Smart Contract* dapat menerjemahkan keputusan tersebut menjadi tindakan. *Blockchain* dapat mencatat tindakan tersebut secara permanen. Sistem otonom kemudian dapat melakukan tindakan berikutnya berdasarkan informasi yang diterima. Rangkaian tersebut dapat berlangsung dengan sedikit atau tanpa intervensi manusia secara langsung. Dalam kondisi seperti itu, pertanyaan hukum yang penting bukan lagi sekadar apakah suatu teknologi sah, tetapi siapa yang mengendalikan rangkaian proses dan siapa yang harus bertanggung jawab apabila rangkaian tersebut menghasilkan kerugian.

Pertanggungjawaban menjadi semakin kompleks karena tidak semua aktor memiliki kendali terhadap seluruh sistem. Pengembang AI mungkin tidak mengendalikan *Smart Contract*. Pengembang *Smart Contract* mungkin tidak mengendalikan data yang digunakan AI. Operator *blockchain* mungkin hanya menyediakan infrastruktur validasi. Pengguna mungkin hanya menjalankan sistem yang telah dirancang oleh pihak lain. Model pertanggungjawaban karena itu harus memperhatikan distribusi kontrol dan manfaat. Pendekatan *shared responsibility* menjadi semakin

relevan dalam kondisi konvergensi tersebut (Al-Mezel dkk., 2026; Qutieshat dkk., 2026).

Pertanyaan mengenai subjek hukum juga dapat muncul kembali. Sistem otonom dapat melakukan tindakan tanpa perintah manusia pada setiap langkah. Namun, memberikan status subjek hukum kepada sistem tidak secara otomatis menyelesaikan masalah pertanggungjawaban. Sistem tidak memiliki aset, kehendak, atau kemampuan moral dalam pengertian yang sama dengan manusia. Memberikan status hukum tertentu kepada teknologi juga dapat berisiko digunakan untuk mengalihkan tanggung jawab dari manusia dan perusahaan kepada mesin. Karena itu, perkembangan teknologi otonom lebih tepat dihadapi dengan memperkuat struktur pertanggungjawaban manusia dan institusi yang berada di balik sistem.

Konsep *human-centered regulation* menjadi penting dalam konteks tersebut. Orientasi utama regulasi bukan pada kepentingan teknologi itu sendiri, tetapi pada manusia yang terkena dampaknya. Teknologi dikembangkan untuk meningkatkan kehidupan manusia, bukan sebaliknya. Prinsip tersebut berarti bahwa efisiensi tidak boleh mengalahkan hak, inovasi tidak boleh menghapus akuntabilitas, dan otomatisasi tidak boleh menghilangkan kesempatan seseorang untuk memperoleh pemulihan. Pendekatan human-centered menempatkan perlindungan hak sebagai parameter utama dalam menentukan batas

penggunaan teknologi (Ahern, 2025; Satyo dkk., 2026).

Dalam sistem AI, prinsip tersebut berarti manusia harus memiliki kemampuan untuk mempertanyakan keputusan. Dalam *Smart Contract*, manusia harus memiliki mekanisme untuk menangani keadaan yang tidak diprediksi oleh kode. Dalam *blockchain*, sistem harus mempertimbangkan kebutuhan hukum untuk memperbaiki kesalahan. Dalam sistem otonom, harus terdapat pihak yang bertanggung jawab terhadap desain, pengoperasian, dan pengawasan. Setiap teknologi dapat memiliki mekanisme berbeda, tetapi prinsip dasarnya sama: tidak boleh ada keputusan atau tindakan yang menimbulkan akibat hukum tanpa adanya jalur pertanggungjawaban.

Konvergensi teknologi juga mengubah konsep bukti. Dalam sistem digital, bukti dapat berasal dari log AI, rekaman transaksi *blockchain*, *Smart Contract*, data sensor, *cloud*, dan sistem komunikasi. Jumlah bukti dapat sangat besar dan berasal dari berbagai sistem. Tantangan hukum bukan hanya bagaimana memperoleh bukti, tetapi bagaimana memahami hubungan antara berbagai sumber data tersebut. Pengadilan atau regulator membutuhkan mekanisme untuk menentukan keaslian, integritas, asal-usul, serta konteks bukti.

Karakter *blockchain* yang sulit diubah dapat membantu membangun jejak transaksi. Namun, keberadaan catatan yang tidak mudah berubah tidak otomatis membuktikan bahwa informasi yang dicatat

sejak awal benar. *Garbage in, garbage out* tetap berlaku. Apabila data yang dimasukkan ke sistem salah, pencatatan yang permanen hanya membuat kesalahan tersebut tercatat secara permanen. Oleh karena itu, hukum perlu membedakan antara integritas catatan dan kebenaran isi catatan.

AI juga menimbulkan persoalan terhadap konsep pengetahuan dan keputusan. Sistem dapat menghasilkan rekomendasi berdasarkan pola yang tidak mudah dipahami manusia. Apabila keputusan tersebut digunakan dalam proses hukum, pihak yang terkena dampak perlu memiliki kemampuan untuk memahami dasar keputusan secara memadai. *Explainability* menjadi semakin penting karena keputusan algoritmik tidak boleh menciptakan "ruang hitam" yang kebal terhadap pemeriksaan (Rajendra & Thuraisingam, 2025).

Kebutuhan terhadap audit juga akan meningkat. Audit tidak hanya dilakukan terhadap perusahaan, tetapi dapat mencakup model AI, proses data, *Smart Contract*, keamanan sistem, dan mekanisme pengambilan keputusan. Audit menjadi instrumen untuk memastikan bahwa teknologi tetap berada dalam parameter hukum dan etika. Dalam sistem yang berubah secara terus-menerus, audit berkala lebih relevan daripada pemeriksaan satu kali pada saat sistem pertama kali diluncurkan.

Regulasi masa depan juga harus semakin berbasis risiko. Tidak masuk akal menerapkan kontrol yang sama terhadap seluruh teknologi. Sistem AI yang digunakan untuk rekomendasi musik

memiliki risiko berbeda dari AI yang menentukan kelayakan seseorang memperoleh layanan publik. *Smart Contract* untuk transaksi kecil memiliki konsekuensi berbeda dengan sistem yang mengelola aset bernilai besar. Pendekatan berbasis risiko memungkinkan hukum memberikan perlindungan yang proporsional sekaligus mencegah beban regulasi yang tidak diperlukan (Corfmat dkk., 2025; Currie dkk., 2025).

Regulator juga harus memiliki kemampuan untuk beradaptasi. Teknologi yang muncul saat ini mungkin akan berubah secara mendasar dalam beberapa tahun. Karena itu, hukum perlu memiliki mekanisme evaluasi dan pembaruan. *Regulatory sandbox*, konsultasi dengan industri, penelitian akademik, audit, dan pengumpulan data mengenai insiden dapat menjadi sumber pembelajaran bagi regulator (Novelli dkk., 2026). Proses pembentukan hukum dengan demikian tidak berhenti pada pengesahan peraturan, tetapi berlanjut melalui evaluasi terhadap dampaknya.

Konvergensi teknologi juga memperkuat kebutuhan kerja sama lintas disiplin. Hukum tidak dapat memahami AI tanpa bekerja sama dengan ilmu komputer dan ilmu data. Regulasi *blockchain* membutuhkan pemahaman terhadap arsitektur jaringan dan mekanisme konsensus. Perlindungan konsumen membutuhkan perspektif ekonomi dan perilaku. Perlindungan hak membutuhkan perspektif sosial dan etika. Model regulasi masa depan karena itu harus membuka ruang dialog antara ahli hukum,

teknologi, bisnis, akademisi, pemerintah, dan masyarakat.

Kerja sama lintas negara juga menjadi semakin penting. Sistem digital dapat dikembangkan, dioperasikan, dan digunakan di berbagai negara sekaligus. Perbedaan aturan dapat menimbulkan konflik mengenai data, tanggung jawab, kontrak, dan bukti. Harmonisasi prinsip dan mekanisme pengakuan dapat membantu mengurangi konflik tersebut. Namun, kerja sama internasional tetap perlu menghormati kepentingan nasional dan perlindungan hak masing-masing negara.

Masa depan hukum teknologi juga akan dipengaruhi oleh kemampuan hukum membedakan antara risiko yang dapat diterima dan risiko yang tidak dapat diterima. Tidak semua risiko harus dihilangkan karena inovasi selalu mengandung ketidakpastian. Yang penting adalah memastikan bahwa risiko dipahami, dikelola, dialokasikan secara adil, dan terdapat mekanisme pemulihan ketika risiko berubah menjadi kerugian. Pendekatan tersebut lebih realistis dibandingkan mengharuskan teknologi mencapai kondisi tanpa risiko.

Pada titik ini, pertanyaan hukum yang paling mendasar dapat dirumuskan dalam tiga pertanyaan: siapa yang mengendalikan, siapa yang menanggung risiko, dan siapa yang dapat menggugat? Ketiga pertanyaan tersebut menjadi semakin penting ketika AI, *blockchain*, dan sistem otonom saling terhubung (Al-Mezel dkk., 2026; Pashentsev & Babaeva, 2024; Qutieshat dkk., 2026). Jika seseorang dirugikan oleh

sistem yang bekerja secara otomatis, ia harus dapat mengetahui siapa yang bertanggung jawab dan bagaimana memperoleh pemulihan. Jika tidak, teknologi akan menghasilkan kesenjangan akuntabilitas.

Paradigma tersebut menunjukkan bahwa masa depan hukum bukanlah perlombaan untuk menciptakan aturan bagi setiap teknologi baru. Hukum perlu membangun prinsip yang mampu bertahan menghadapi perubahan teknologi, sekaligus menyediakan mekanisme untuk merespons risiko baru. Prinsip pertanggungjawaban, transparansi, perlindungan hak, proporsionalitas, pengawasan manusia, keamanan, dan akses terhadap pemulihan dapat menjadi fondasi yang relatif stabil. Sementara itu, instrumen regulasi dapat disesuaikan berdasarkan perkembangan teknologi.

Konvergensi AI, *blockchain*, dan teknologi otonom pada akhirnya tidak mengurangi peran hukum. Sebaliknya, teknologi tersebut membuat hukum semakin penting karena keputusan dan transaksi semakin banyak dilakukan melalui sistem yang tidak selalu mudah dipahami oleh manusia. Hukum harus memastikan bahwa kompleksitas teknologi tidak berubah menjadi alasan untuk menghilangkan tanggung jawab. Inovasi tetap harus diberi ruang, tetapi ruang tersebut harus dibangun dengan pagar hukum yang melindungi manusia.

Dengan demikian, paradigma masa depan dapat diarahkan pada empat karakter utama: adaptif, antisipatif, berbasis risiko, dan berpusat pada

manusia. Regulasi adaptif memungkinkan hukum mengikuti perubahan teknologi. Regulasi antisipatif memungkinkan risiko dipersiapkan sebelum menjadi krisis. Regulasi berbasis risiko memungkinkan kewajiban disesuaikan dengan tingkat dampak. Regulasi berpusat pada manusia memastikan bahwa teknologi tetap menjadi sarana untuk meningkatkan kesejahteraan, bukan sumber baru ketidakadilan. Arah tersebut sejalan dengan perkembangan pemikiran hukum teknologi yang menekankan pentingnya tata kelola AI, pertanggungjawaban manusia, dan adaptasi regulasi terhadap inovasi (Ahern, 2025; Aslina & Noviya, 2026; Satyo dkk., 2026).

Bab ini menunjukkan bahwa tantangan terbesar teknologi baru bukan terletak pada kemampuan mesin melakukan sesuatu yang sebelumnya hanya dapat dilakukan manusia. Tantangan yang lebih mendasar adalah bagaimana hukum mempertahankan prinsip pertanggungjawaban ketika tindakan tersebut dilakukan melalui sistem yang semakin otomatis dan kompleks. AI dapat mengambil keputusan, *blockchain* dapat mencatat transaksi, dan *Smart Contract* dapat mengeksekusi kewajiban. Namun, ketika keputusan tersebut menghasilkan akibat hukum, manusia tetap membutuhkan jawaban mengenai dasar keputusan, pihak yang bertanggung jawab, dan mekanisme pemulihan.

Oleh karena itu, masa depan hukum teknologi tidak seharusnya diarahkan pada pilihan antara

inovasi dan regulasi. Keduanya justru harus ditempatkan dalam hubungan yang saling memperkuat. Regulasi yang baik menciptakan kepercayaan, sementara kepercayaan menjadi salah satu syarat berkembangnya inovasi. Teknologi yang aman dan dapat dipertanggungjawabkan akan lebih mudah diterima masyarakat dibandingkan teknologi yang menghasilkan manfaat ekonomi tetapi meninggalkan korban tanpa mekanisme pemulihan.

Dengan perspektif tersebut, hukum dapat memainkan peran sebagai penjaga keseimbangan antara kebebasan berinovasi dan perlindungan manusia. AI, *blockchain*, dan sistem otonom tidak harus dipandang sebagai ancaman terhadap hukum. Teknologi tersebut merupakan tantangan yang memaksa hukum memperbarui cara berpikir mengenai subjek, tanggung jawab, kontrak, bukti, privasi, kepemilikan, dan pengawasan. Hukum yang mampu beradaptasi dengan perubahan tersebut akan tetap relevan dalam masyarakat digital, sedangkan hukum yang hanya bergantung pada kategori teknologi masa lalu akan semakin tertinggal dari realitas yang hendak diaturnya.

BAB X
MENUJU ARSITEKTUR HUKUM SIBER YANG ADAFTIF: REKOMENDASI DAN PROSPEK

Perkembangan teknologi digital telah mengubah cara negara, masyarakat, dan pelaku usaha menjalankan aktivitas hukum. Ruang siber tidak lagi dapat dipandang sebagai ruang tambahan yang berdiri di luar kehidupan sosial, ekonomi, dan pemerintahan, melainkan telah menjadi bagian integral dari kehidupan modern. Transaksi ekonomi berlangsung melalui sistem elektronik, data pribadi menjadi sumber daya strategis, layanan publik bergantung pada infrastruktur digital, komunikasi sosial berlangsung melalui platform, sementara kecerdasan artifisial (*artificial intelligence*/AI), *blockchain*, *cloud computing*, *Internet of Things* (IoT), dan sistem otonom terus memperluas bentuk hubungan yang sebelumnya tidak dikenal dalam praktik hukum konvensional. Kondisi tersebut menyebabkan hukum siber menghadapi persoalan yang lebih kompleks daripada sekadar kebutuhan membentuk aturan mengenai kejahatan komputer. Hukum siber harus mampu mengatur hubungan hukum, mendistribusikan tanggung jawab, melindungi hak, menjaga keamanan, serta menyediakan mekanisme

penyelesaian sengketa dalam lingkungan yang berubah dengan cepat.

Persoalan utama yang muncul pada tahap perkembangan hukum siber bukan semata-mata tidak adanya hukum. Indonesia telah memiliki berbagai perangkat hukum yang bersinggungan dengan aktivitas digital, baik dalam hukum pidana, hukum perdata, transaksi elektronik, perlindungan data pribadi, perlindungan konsumen, keamanan siber, maupun bidang sektoral lainnya. Permasalahan justru terletak pada bagaimana berbagai rezim hukum tersebut dapat bekerja sebagai satu kesatuan. Perkembangan aturan secara sektoral berpotensi menciptakan fragmentasi apabila masing-masing regulasi dibangun dengan terminologi, tujuan, mekanisme pengawasan, dan konsepsi pertanggungjawaban yang berbeda. Literatur mengenai hukum siber menunjukkan bahwa tantangan tersebut semakin penting ketika perkembangan teknologi berlangsung lebih cepat daripada kemampuan hukum untuk melakukan penyesuaian. Dengan demikian, persoalan hukum siber perlu dilihat sebagai persoalan arsitektur hukum, bukan hanya persoalan jumlah regulasi (Ababneh dkk., 2026; Ahern, 2025; Johari & Prakash, 2026; Khan, 2025).

Arsitektur hukum siber yang diperlukan pada masa depan harus mampu menghubungkan berbagai cabang hukum tanpa menghilangkan karakteristik masing-masing. Hukum pidana tetap dibutuhkan untuk merespons serangan dan perbuatan yang merugikan kepentingan publik. Hukum perdata tetap diperlukan untuk mengatur kontrak, ganti rugi, tanggung jawab, dan

hubungan antarpihak. Perlindungan data pribadi memberikan batas terhadap pengumpulan dan penggunaan informasi individu. Hukum transaksi elektronik memberikan legitimasi terhadap hubungan hukum yang berlangsung melalui sistem elektronik. Keamanan siber memberikan dimensi perlindungan terhadap sistem dan infrastruktur. Perlindungan konsumen menjaga pihak yang berada dalam posisi tawar yang lebih lemah. Hak kekayaan intelektual memberikan perlindungan terhadap kreativitas dan inovasi digital. Sementara itu, regulasi teknologi baru dibutuhkan untuk menghadapi risiko yang lahir dari teknologi yang sebelumnya belum dikenal.

Atas dasar tersebut, Bab X diarahkan untuk merumuskan agenda pembaruan hukum siber yang tidak berhenti pada pembentukan norma. Pembaruan harus mencakup empat dimensi yang saling berhubungan, yaitu harmonisasi norma, kapasitas kelembagaan, desain regulasi adaptif, dan orientasi global. Keempat dimensi tersebut membentuk satu rangkaian. Harmonisasi tanpa kapasitas penegakan hanya menghasilkan aturan yang sulit bekerja. Kapasitas penegakan tanpa regulasi yang adaptif akan membuat institusi terus mengejar perkembangan teknologi. Regulasi adaptif tanpa perlindungan hak dapat berubah menjadi instrumen kontrol yang berlebihan. Sebaliknya, keterbukaan global tanpa perlindungan kepentingan nasional dapat menciptakan ketergantungan strategis. Karena itu, arsitektur hukum siber harus dibangun secara terpadu, adaptif, berorientasi pada manusia, dan tetap mempertahankan kepentingan nasional.

1. **Rekonstruksi dan Harmonisasi Kerangka Hukum Siber Nasional**

Kebutuhan untuk merekonstruksi kerangka hukum siber Indonesia berangkat dari kenyataan bahwa aktivitas digital tidak mengenal batas-batas tradisional antarcabang hukum. Satu peristiwa digital dapat sekaligus mengandung persoalan pidana, perdata, perlindungan data, perlindungan konsumen, keamanan sistem, dan bahkan hak kekayaan intelektual. Misalnya, kebocoran data pelanggan dalam suatu layanan digital tidak hanya menyangkut keamanan sistem. Peristiwa tersebut dapat menimbulkan persoalan mengenai kewajiban pengendali data, kerugian konsumen, tanggung jawab kontraktual, kemungkinan tindak pidana, kewajiban pemberitahuan insiden, serta kewajiban pemulihan. Apabila setiap aspek tersebut ditangani secara terpisah tanpa mekanisme koordinasi normatif, penyelesaian masalah dapat menghasilkan kesimpulan yang tidak konsisten. Karena itu, hukum siber harus diposisikan sebagai sebuah arsitektur yang menghubungkan berbagai rezim hukum yang sebelumnya berkembang secara relatif terpisah.

Rekonstruksi tersebut tidak harus dimaknai sebagai pembentukan satu undang-undang yang menghapus seluruh aturan sektoral. Model unifikasi total justru berpotensi menimbulkan persoalan baru karena karakter setiap sektor berbeda. Hukum pidana memiliki orientasi perlindungan kepentingan publik dan pemberian sanksi, hukum perdata menekankan hubungan hak dan kewajiban

antarpihak, perlindungan data berorientasi pada kontrol individu atas informasi personal, sedangkan keamanan siber menitikberatkan pada integritas dan keberlangsungan sistem. Yang lebih diperlukan adalah harmonisasi fungsi dan prinsip. Artinya, setiap aturan sektoral tetap dapat dipertahankan, tetapi memiliki titik temu berupa prinsip umum, definisi yang kompatibel, pembagian kewenangan yang jelas, dan mekanisme penyelesaian konflik norma. Pendekatan tersebut lebih realistis dibandingkan memaksakan seluruh bidang ke dalam satu instrumen hukum yang seragam (Gussman & Jannah, 2026; Johari & Prakash, 2026).

Salah satu persoalan yang perlu mendapat perhatian adalah penggunaan terminologi hukum yang tidak seragam. Teknologi digital menghasilkan objek dan aktivitas yang sering kali berada di antara kategori hukum yang telah ada. Definisi mengenai sistem, data, informasi, layanan digital, penyedia platform, pengguna, operator, serta pelaku teknologi dapat menghasilkan konsekuensi hukum yang berbeda apabila digunakan secara tidak konsisten. Definisi yang terlalu sempit berisiko cepat kehilangan relevansi ketika teknologi berubah. Sebaliknya, definisi yang terlalu luas dapat menciptakan ketidakpastian karena aparat, pelaku usaha, dan masyarakat tidak mengetahui secara pasti tindakan apa yang termasuk dalam cakupan suatu ketentuan. Ketidakjelasan tersebut dapat memengaruhi konsistensi interpretasi dan penegakan hukum (Gussman & Jannah, 2026; Hasnia dkk., 2025).

Persoalan definisi menjadi semakin rumit ketika hukum harus berhadapan dengan teknologi baru. AI, *blockchain*, komputasi awan, IoT, dan sistem otonom tidak selalu dapat ditempatkan secara sederhana dalam kategori hukum konvensional. Sebuah sistem AI, misalnya, dapat digunakan untuk mengambil keputusan yang memengaruhi seseorang tanpa adanya tindakan manusia secara langsung pada setiap tahap. *Blockchain* dapat menyimpan catatan transaksi secara terdistribusi dan sulit diubah. *Cloud computing* menyebabkan data dan proses komputasi dapat tersebar pada berbagai lokasi dan yurisdiksi. IoT menghubungkan benda fisik dengan sistem digital sehingga gangguan terhadap sistem digital dapat menghasilkan akibat di dunia fisik. Perubahan tersebut menunjukkan bahwa rekonstruksi hukum tidak cukup dilakukan dengan menambahkan istilah teknologi ke dalam peraturan lama. Yang harus direkonstruksi adalah hubungan antara teknologi, risiko, hak, tanggung jawab, dan akibat hukum (Johari & Prakash, 2026; Khan, 2025; Othman, 2025).

Harmonisasi juga diperlukan untuk mengantisipasi kemungkinan konflik antara aturan khusus dan aturan umum. Konflik dapat muncul ketika suatu tindakan digital telah memenuhi unsur suatu ketentuan pidana khusus, tetapi pada saat yang sama memiliki konsekuensi yang diatur dalam hukum pidana umum. Konflik serupa dapat terjadi dalam hubungan antara aturan perlindungan data dan aturan sektoral mengenai penyimpanan

informasi, antara kewajiban keamanan sistem dengan kewajiban membuka informasi, atau antara perlindungan konsumen dengan ketentuan kontrak digital. Perkembangan hukum siber menunjukkan bahwa tumpang tindih seperti ini tidak dapat diselesaikan hanya dengan menambahkan aturan baru. Dibutuhkan metode harmonisasi yang secara sistematis menentukan hubungan antara norma umum, norma khusus, norma sektoral, dan prinsip perlindungan hak (Gussman & Jannah, 2026).

Harmonisasi juga tidak berarti seluruh aturan harus mempunyai redaksi identik. Yang lebih penting adalah terciptanya *functional equivalence*, yaitu kemampuan berbagai instrumen hukum untuk mencapai tujuan perlindungan yang sejalan meskipun menggunakan mekanisme yang berbeda. Pendekatan ini penting karena sistem hukum memiliki tradisi, institusi, dan sektor yang berbeda. Dalam konteks nasional, hukum pidana, hukum perdata, perlindungan data, keamanan siber, dan perlindungan konsumen tidak perlu dilebur menjadi satu. Namun, semuanya harus dapat memberikan jawaban yang kompatibel ketika menghadapi peristiwa digital yang sama. Prinsip *compatibility* semacam ini lebih memungkinkan hukum tetap fleksibel tanpa kehilangan kepastian (Johari & Prakash, 2026; Kaya & Shahid, 2025).

Rekonstruksi juga harus memperhatikan kemungkinan kekosongan hukum. Kekosongan tidak selalu berarti tidak terdapat satu pun aturan yang dapat diterapkan. Kekosongan dapat terjadi ketika

aturan yang ada tidak memberikan jawaban terhadap persoalan tertentu, ketika tidak jelas siapa yang bertanggung jawab, atau ketika mekanisme pemulihan tidak tersedia. Dalam teknologi digital, kekosongan semacam ini dapat muncul karena hubungan hukum melibatkan banyak aktor sekaligus. Dalam sebuah ekosistem digital, misalnya, terdapat pengembang, penyedia infrastruktur, operator, platform, pengguna, penyedia layanan awan, serta pihak ketiga lainnya. Apabila terjadi kerugian, penentuan pihak yang harus bertanggung jawab dapat menjadi rumit. Karena itu, hukum siber perlu mengembangkan prinsip alokasi tanggung jawab yang tidak hanya bergantung pada siapa yang secara formal melakukan tindakan, tetapi juga pada siapa yang mempunyai kemampuan mengendalikan risiko.

Prinsip umum hukum siber dapat menjadi instrumen penting untuk menjembatani berbagai rezim tersebut. Prinsip pertama adalah kepastian hukum (*legal certainty*), yang menuntut agar individu dan pelaku usaha dapat mengetahui hak, kewajiban, larangan, serta konsekuensi hukum dari tindakan digitalnya. Prinsip kedua adalah akuntabilitas, yaitu adanya pihak yang dapat dimintai pertanggungjawaban atas sistem, keputusan, data, atau aktivitas digital yang berada dalam kendalinya. Prinsip ketiga adalah perlindungan hak, yang memastikan bahwa digitalisasi tidak menghilangkan privasi, kebebasan, perlindungan konsumen, dan hak-hak fundamental lainnya. Prinsip keempat adalah interoperabilitas, agar sistem hukum dapat

berfungsi dalam ekosistem teknologi dan hubungan lintas yurisdiksi. Prinsip kelima adalah klasifikasi berdasarkan risiko, sehingga beban hukum dapat disesuaikan dengan tingkat dampak suatu teknologi atau aktivitas (Ababneh dkk., 2026; Johari & Prakash, 2026).

Dengan demikian, rekonstruksi kerangka hukum siber Indonesia sebaiknya tidak dimulai dari pertanyaan "teknologi apa yang harus diatur?", tetapi dari pertanyaan "risiko hukum apa yang harus dikendalikan dan hak apa yang harus dilindungi?". Pergeseran cara berpikir tersebut sangat penting. Jika hukum dibangun berdasarkan nama teknologi, maka setiap inovasi baru berpotensi memerlukan regulasi baru. Sebaliknya, apabila hukum dibangun berdasarkan risiko dan fungsi, prinsip yang sama dapat diterapkan pada teknologi yang berbeda. Sistem AI dan sistem berbasis teknologi lain mungkin mempunyai mekanisme teknis yang berbeda, tetapi apabila keduanya menghasilkan keputusan berisiko tinggi terhadap hak seseorang, keduanya dapat dikenai prinsip transparansi, auditabilitas, pengawasan manusia, dan mekanisme keberatan.

Rekonstruksi hukum juga harus menghasilkan mekanisme evaluasi regulasi. Setiap peraturan mengenai ruang siber seharusnya tidak dianggap sebagai produk final yang tidak perlu ditinjau kembali. Perkembangan teknologi dapat membuat suatu ketentuan menjadi tidak efektif, terlalu membebani inovasi, atau justru gagal melindungi masyarakat. Oleh sebab itu, perlu

terdapat mekanisme *regulatory review* yang memungkinkan pemerintah dan pembentuk peraturan mengevaluasi efektivitas norma berdasarkan perkembangan teknologi, putusan pengadilan, pola pelanggaran, perubahan model bisnis, dan perkembangan internasional. Hukum siber dengan demikian tidak lagi dipahami sebagai kumpulan aturan yang statis, tetapi sebagai sistem normatif yang terus belajar.

Harmonisasi kerangka hukum siber harus menghasilkan tiga kepastian sekaligus. Pertama, masyarakat harus mengetahui hak dan perlindungannya ketika menggunakan teknologi digital. Kedua, pelaku usaha harus memahami kewajiban dan risiko hukum yang melekat pada layanan yang mereka tawarkan. Ketiga, negara harus memiliki dasar kewenangan yang jelas untuk melakukan pencegahan, pengawasan, penegakan, dan pemulihan. Ketiganya tidak dapat dicapai apabila hukum terus berkembang secara terfragmentasi. Harmonisasi karena itu merupakan prasyarat agar hukum siber dapat berfungsi sebagai sistem, bukan sekadar kumpulan norma yang kebetulan berkaitan dengan teknologi.

2. Penguatan Kelembagaan, Penegakan Hukum, dan Kapasitas Digital Negara

Kekuatan hukum siber pada akhirnya tidak ditentukan oleh seberapa banyak peraturan yang dimiliki suatu negara, tetapi oleh kemampuan institusinya untuk menerapkan aturan tersebut secara konsisten. Norma yang jelas dapat kehilangan

efektivitas ketika aparat tidak mempunyai kemampuan teknis untuk mengidentifikasi pelanggaran, mengamankan bukti, memahami arsitektur sistem, atau menelusuri pelaku. Dalam kejahatan siber, persoalan tersebut menjadi lebih serius karena bukti dapat berubah, dipindahkan, dienkripsi, disimpan dalam yurisdiksi lain, atau berada pada sistem yang dikelola oleh perusahaan swasta. Oleh karena itu, penguatan kelembagaan harus menjadi bagian yang sama pentingnya dengan reformasi legislasi (Lazaro & Mzurikwao, 2026; Lestari dkk., 2026).

Pembuktian merupakan salah satu titik paling menentukan dalam penegakan hukum siber. Informasi digital mempunyai karakter berbeda dari bukti konvensional. Bukti digital dapat dengan cepat berubah atau hilang, dapat memiliki banyak salinan, dan dapat bergantung pada sistem yang menghasilkan metadata tertentu. Integritas bukti karena itu tidak hanya ditentukan oleh isi informasi, tetapi juga oleh bagaimana bukti tersebut diperoleh, disimpan, diperiksa, dan dipresentasikan. Keterbatasan fasilitas forensik dan perbedaan pemahaman mengenai validitas bukti digital dapat mengurangi efektivitas proses penegakan hukum. Kondisi tersebut menunjukkan bahwa reformasi hukum pembuktian harus berjalan beriringan dengan pembangunan kapasitas forensik digital (Klase´n dkk., 2024; Lestari dkk., 2026).

Institusi penegak hukum juga membutuhkan spesialisasi. Penyidik yang menangani kejahatan

siber harus memahami bukan hanya hukum pidana, tetapi juga jaringan komputer, keamanan informasi, metode serangan, jejak digital, teknik penyamaran identitas, dan karakteristik layanan digital. Jaksa membutuhkan kemampuan untuk menjelaskan hubungan antara bukti teknis dan unsur tindak pidana. Hakim membutuhkan kompetensi untuk menilai reliabilitas bukti digital, argumentasi ahli, serta implikasi teknologi terhadap hak para pihak. Praktisi hukum juga harus memahami teknologi agar dapat memberikan nasihat hukum yang relevan. Kesenjangan antara kompetensi hukum dan kompetensi teknologi dapat menjadi salah satu hambatan terbesar dalam penerapan hukum siber (Klase´n dkk., 2024; Lazaro & Mzurikwao, 2026; Mugamba, 2026).

Penguatan kapasitas tersebut tidak dapat dilakukan melalui pelatihan satu kali. Teknologi berubah terlalu cepat sehingga kompetensi yang relevan hari ini dapat menjadi tidak memadai beberapa tahun kemudian. Negara membutuhkan sistem pendidikan dan pelatihan berkelanjutan yang menghubungkan perkembangan teknologi dengan perkembangan hukum. Pendidikan hukum perlu memperlakukan teknologi digital bukan sebagai bidang tambahan, melainkan sebagai bagian dari kompetensi hukum modern. Dengan demikian, pendidikan hukum dapat berfungsi sebagai infrastruktur preventif yang membentuk kemampuan aparat dan praktisi sebelum persoalan

digital berkembang menjadi sengketa atau tindak pidana (Mugamba, 2026).

Koordinasi antarlembaga merupakan dimensi lain yang harus diperkuat. Satu insiden siber dapat melibatkan lembaga penegak hukum, lembaga keamanan siber, regulator sektoral, operator infrastruktur, penyedia layanan digital, serta lembaga lain yang memiliki kewenangan berbeda. Apabila masing-masing lembaga bekerja tanpa mekanisme koordinasi, respons terhadap insiden dapat terlambat. Keterlambatan tersebut bukan hanya persoalan administratif, tetapi dapat mengakibatkan hilangnya bukti, meluasnya serangan, atau meningkatnya kerugian. Karena itu, arsitektur kelembagaan harus menetapkan dengan jelas siapa yang memimpin respons, siapa yang menyediakan informasi, siapa yang melakukan investigasi, dan siapa yang bertanggung jawab terhadap pemulihan.

Mekanisme respons terhadap insiden juga harus dipandang sebagai bagian dari penegakan hukum. Selama ini, keamanan siber sering dipahami dalam kerangka teknis, sementara hukum baru masuk setelah kerugian terjadi. Pendekatan tersebut perlu diubah. Respons insiden harus sejak awal memperhitungkan kebutuhan hukum, termasuk preservasi bukti, perlindungan data, kewajiban pelaporan, hak korban, dan kemungkinan proses pidana atau perdata. Dengan demikian, proses *incident response* tidak hanya bertujuan memulihkan sistem, tetapi juga mempertahankan kemampuan

negara dan korban untuk mencari pertanggungjawaban hukum.

Sektor swasta harus menjadi bagian integral dari arsitektur tersebut. Banyak sistem digital yang digunakan masyarakat tidak sepenuhnya dimiliki atau dioperasikan oleh negara. Infrastruktur telekomunikasi, layanan awan, platform digital, layanan pembayaran, sistem perdagangan elektronik, dan berbagai layanan lainnya bergantung pada perusahaan swasta. Oleh sebab itu, negara tidak dapat membangun ketahanan siber hanya melalui lembaga pemerintah. Kerja sama pemerintah dan swasta dibutuhkan dalam berbagi informasi ancaman, respons insiden, pengamanan infrastruktur, serta pemulihan layanan (Hwang, 2025; Kingshuk & Rahman, 2026; Lestari dkk., 2026).

Kendati demikian, kemitraan pemerintah-swasta tidak boleh dipahami sebagai pemindahan tanggung jawab negara kepada perusahaan. Negara tetap memiliki kewajiban untuk memastikan kepentingan publik terlindungi. Kemitraan harus disertai pembagian tanggung jawab yang jelas, standar minimum keamanan, mekanisme pengawasan, serta aturan mengenai penggunaan dan pertukaran data. Dalam hal tertentu, perusahaan dapat memiliki pengetahuan teknis yang lebih tinggi daripada negara. Kondisi tersebut harus dimanfaatkan melalui kolaborasi, tetapi tidak boleh menghasilkan ketergantungan yang membuat regulator kehilangan kapasitas independennya.

Penguatan kelembagaan juga membutuhkan sistem berbagi informasi mengenai ancaman. Serangan terhadap satu organisasi dapat memberikan pelajaran bagi organisasi lain. Jika informasi mengenai pola serangan, kerentanan, indikator kompromi, dan metode mitigasi tidak dibagikan, setiap organisasi akan menghadapi ancaman secara terpisah. Karena itu, perlu dibangun mekanisme *threat intelligence sharing* yang memungkinkan informasi dibagikan secara cepat dengan tetap memperhatikan kerahasiaan dan perlindungan data. Kolaborasi semacam ini menjadi penting karena serangan siber dapat berlangsung lintas sektor dan lintas yurisdiksi (Lubis dkk., 2025; Qudus, 2025; Simu & Zaman, 2023).

Kapasitas digital negara juga harus mencakup kemampuan melakukan evaluasi terhadap teknologi yang digunakan oleh pemerintah sendiri. Negara tidak dapat secara kredibel mengatur keamanan digital masyarakat apabila sistem internal pemerintah masih rentan. Sistem pelayanan publik, basis data pemerintah, infrastruktur komunikasi, dan layanan digital negara harus menjadi contoh penerapan keamanan. Prinsip *security by design* perlu diterapkan sejak tahap perencanaan sistem, bukan setelah terjadi insiden. Penguatan ini juga berkaitan dengan kebutuhan membangun ketahanan digital jangka panjang melalui pengembangan sumber daya manusia, inovasi domestik, dan pengelolaan risiko rantai pasok teknologi (Bonnieu, 2026; Carroll, 2024).

Penegakan hukum yang efektif membutuhkan pendekatan yang bergerak dari reaktif menuju preventif dan resilien. Negara tidak cukup hanya bertindak setelah serangan terjadi. Negara harus memiliki kemampuan mendeteksi ancaman, mencegah kerentanan, merespons insiden, memulihkan layanan, dan mengambil pelajaran dari kejadian tersebut. Model semacam ini menempatkan hukum, institusi, teknologi, dan sumber daya manusia dalam satu sistem. Hukum memberikan dasar kewenangan dan tanggung jawab, institusi menjalankan fungsi, teknologi menyediakan kemampuan teknis, sedangkan sumber daya manusia memastikan semuanya dapat bekerja.

Dengan demikian, reformasi kelembagaan hukum siber harus diarahkan pada pembentukan kapasitas yang berkelanjutan. Ukuran keberhasilan tidak semata-mata jumlah peraturan atau jumlah perkara yang berhasil diproses. Keberhasilan harus dilihat dari kemampuan mendeteksi dan merespons insiden, kualitas pembuktian digital, konsistensi putusan, kecepatan pemulihan, koordinasi antarlembaga, kemampuan melindungi korban, dan kapasitas negara untuk belajar dari setiap insiden. Pada titik inilah hukum siber berubah dari sekadar sistem larangan menjadi sistem ketahanan hukum dan digital.

3. Model Regulasi Adaptif dan Tata Kelola Teknologi yang Berorientasi pada Hak

Salah satu persoalan terbesar dalam regulasi teknologi adalah adanya jarak waktu antara

munculnya inovasi dan terbentuknya respons hukum. Ketika teknologi berkembang sangat cepat, proses legislasi konvensional sering membutuhkan waktu lebih lama daripada siklus inovasi. Akibatnya, aturan yang baru dibentuk dapat segera menghadapi teknologi atau model bisnis yang tidak sepenuhnya sesuai dengan asumsi ketika aturan tersebut dirancang. Kondisi ini dikenal sebagai *regulatory lag*. Karena itu, masa depan hukum siber membutuhkan pendekatan yang memungkinkan hukum belajar dan menyesuaikan diri tanpa kehilangan legitimasi (Ahern, 2025; Currie dkk., 2025).

Regulasi berbasis risiko (*risk-based regulation*) menawarkan salah satu jalan keluar. Pendekatan ini tidak memperlakukan semua teknologi dengan tingkat pengawasan yang sama. Teknologi yang mempunyai dampak rendah dapat dikenai kewajiban yang lebih ringan, sedangkan teknologi yang berpotensi memengaruhi keselamatan, hak fundamental, keamanan nasional, atau kepentingan publik secara signifikan harus mendapatkan pengawasan yang lebih ketat. Model tersebut memungkinkan sumber daya regulator diarahkan pada risiko yang paling serius. Pendekatan berbasis risiko juga lebih mudah disesuaikan dengan perubahan teknologi karena fokus utamanya bukan pada nama teknologi, tetapi pada dampak yang ditimbulkan (Ababneh dkk., 2026; Khan, 2025).

Namun, klasifikasi risiko tidak boleh dianggap sebagai proses sekali jadi. Risiko teknologi dapat berubah seiring perubahan penggunaan, skala,

data yang diproses, dan konteks penerapan. Sistem yang pada awalnya memiliki risiko rendah dapat menjadi berisiko tinggi ketika digunakan pada sektor kesehatan, keuangan, penegakan hukum, atau layanan publik. Oleh sebab itu, klasifikasi harus bersifat dinamis. Regulator perlu memiliki kemampuan untuk meninjau ulang kategori risiko berdasarkan bukti empiris, insiden yang terjadi, dan perkembangan teknologi (Novelli dkk., 2026).

Pendekatan *technology-neutral regulation* juga penting untuk mengurangi risiko keusangan hukum. Regulasi yang terlalu terikat pada teknologi tertentu akan cepat kehilangan relevansi ketika teknologi tersebut digantikan. Hukum sebaiknya mengatur fungsi dan konsekuensi, bukan semata-mata bentuk teknologinya. Misalnya, kewajiban menjaga keamanan informasi dapat diterapkan pada berbagai sistem tanpa harus menentukan teknologi tertentu yang wajib digunakan. Demikian pula prinsip transparansi dan perlindungan hak dapat berlaku pada berbagai sistem pengambilan keputusan otomatis. Pendekatan netral teknologi membuat norma lebih tahan terhadap perubahan (*technology obsolescence*) (Johari & Prakash, 2026).

Akan tetapi, netralitas teknologi juga mempunyai batas. Norma yang terlalu abstrak dapat gagal memberikan panduan konkret untuk teknologi dengan karakteristik khusus. AI, misalnya, menghadirkan persoalan mengenai bias algoritmik, kemampuan menjelaskan keputusan, dan pengawasan manusia yang tidak selalu dapat

diselesaikan hanya dengan prinsip umum. Karena itu, regulasi yang ideal perlu menggabungkan prinsip netral teknologi dengan aturan khusus berbasis risiko. Prinsip umum memberikan stabilitas, sedangkan aturan khusus memberikan perlindungan ketika risiko tertentu membutuhkan intervensi lebih detail (Ababneh dkk., 2026).

Regulatory sandbox dapat menjadi instrumen untuk mengatasi persoalan tersebut. Melalui *sandbox*, teknologi atau model bisnis baru dapat diuji dalam lingkungan yang terkendali sebelum diterapkan secara lebih luas. Regulator dapat mempelajari risiko yang sebenarnya, sementara inovator mendapatkan ruang untuk mengembangkan teknologi tanpa langsung menghadapi seluruh beban kepatuhan yang berlaku pada skala penuh. Dengan demikian, *sandbox* tidak hanya menjadi ruang bagi inovasi, tetapi juga menjadi ruang belajar bagi regulator (Ahern, 2025; Novelli dkk., 2026).

Namun, *sandbox* tidak boleh dipahami sebagai zona bebas hukum. Eksperimen regulasi tetap membutuhkan kriteria masuk, pembatasan risiko, mekanisme pengawasan, evaluasi, serta aturan keluar (*exit rules*). Tanpa mekanisme tersebut, *sandbox* dapat menciptakan ketidakpastian, ketidakadilan antarpelaku usaha, atau bahkan dimanfaatkan sebagai cara untuk menghindari pengawasan. Persoalan legitimasi juga perlu diperhatikan karena keputusan regulator untuk memberikan pengecualian atau kelonggaran dapat memengaruhi pihak yang tidak ikut serta dalam

eksperimen. Karena itu, desain *sandbox* harus transparan, akuntabel, dan mempunyai dasar hukum yang jelas (Novelli dkk., 2026; Zarra, 2026).

Selain *sandbox*, regulator perlu mengembangkan *regulatory foresight*. Pendekatan ini mengajak negara melihat bukan hanya teknologi yang sudah ada, tetapi juga kemungkinan perkembangan teknologi dan konsekuensinya. Hukum tidak harus menunggu sampai suatu risiko menjadi kenyataan dalam skala besar. Regulator dapat menggunakan skenario, konsultasi ahli, analisis tren, simulasi, dan evaluasi teknologi untuk mengantisipasi risiko. Dengan demikian, regulasi dapat bergerak dari pola reaktif menuju pola antisipatif (Ahern, 2025).

Model *co-regulation* dan *self-regulation* juga dapat digunakan, khususnya dalam sektor yang berkembang cepat. Pelaku industri sering mempunyai pengetahuan teknis yang lebih rinci mengenai teknologi dibandingkan regulator. Pelibatan industri dalam penyusunan standar dapat membantu menghasilkan aturan yang lebih realistis. Namun, *self-regulation* memiliki risiko apabila tidak disertai pengawasan. Kepentingan ekonomi dapat membuat pelaku industri menetapkan standar yang terlalu ringan atau lebih mengutamakan efisiensi daripada perlindungan pengguna. Karena itu, *co-regulation* perlu ditempatkan dalam kerangka tanggung jawab publik, bukan sebagai pengganti fungsi negara (Kalenzi, 2022).

Orientasi hak menjadi batas penting dari seluruh model regulasi tersebut. Regulasi adaptif tidak boleh hanya diarahkan untuk mempercepat inovasi. Teknologi digunakan oleh manusia dan dapat memengaruhi kehidupan manusia. Karena itu, kepentingan efisiensi ekonomi harus diseimbangkan dengan privasi, kebebasan berekspresi, keamanan, perlindungan konsumen, dan hak asasi manusia. Sistem digital yang efisien tetapi menghasilkan diskriminasi atau menghilangkan kemampuan seseorang untuk menggugat keputusan tidak dapat dianggap sebagai sistem hukum yang baik.

Prinsip *human-centered governance* karena itu harus menjadi fondasi. Teknologi seharusnya membantu manusia, bukan menghilangkan kemampuan manusia untuk mengontrol keputusan yang mempunyai konsekuensi serius. Pada teknologi berisiko tinggi, pengawasan manusia harus memiliki substansi, bukan sekadar formalitas. Pengambil keputusan manusia harus memiliki kompetensi, akses terhadap informasi, dan kewenangan nyata untuk menolak atau mengubah keluaran sistem. Jika manusia hanya menerima keputusan algoritmik tanpa memahami atau mampu mengoreksinya, maka keberadaan "pengawasan manusia" menjadi sekadar simbol.

Regulasi juga harus menjamin mekanisme keberatan dan pemulihan. Setiap keputusan digital yang berdampak signifikan terhadap seseorang seharusnya dapat dipertanyakan melalui mekanisme yang jelas. Individu harus memiliki kesempatan

untuk mengetahui dasar keputusan, mengoreksi informasi yang salah, dan memperoleh peninjauan manusia ketika diperlukan. Prinsip tersebut sangat penting dalam penggunaan AI karena sistem algoritmik dapat menghasilkan kesalahan atau bias. Dengan demikian, regulasi adaptif harus memperhatikan bukan hanya bagaimana teknologi bekerja, tetapi juga bagaimana seseorang dapat mempertahankan haknya ketika teknologi menghasilkan keputusan yang merugikan.

Dengan demikian, regulasi adaptif bukan berarti hukum menjadi lemah atau tidak pasti. Adaptif justru berarti hukum mempunyai mekanisme untuk berubah secara terukur ketika kondisi berubah. Kepastian hukum tidak harus berarti aturan tidak pernah berubah. Kepastian dapat diwujudkan melalui kejelasan prinsip, prosedur perubahan, transparansi pengawasan, dan kemampuan masyarakat memahami hak serta kewajibannya. Dengan kerangka tersebut, hukum dapat berubah mengikuti teknologi tanpa menciptakan ketidakpastian yang tidak terkendali.

4. Prospek Arsitektur Hukum Siber Indonesia dalam Ekosistem Digital Global

Masa depan hukum siber Indonesia tidak dapat dipisahkan dari kenyataan bahwa ruang digital bersifat lintas batas. Data dapat dikumpulkan di satu negara, diproses di negara lain, disimpan melalui layanan awan di wilayah berbeda, dan digunakan oleh pengguna yang berada di banyak yurisdiksi. Serangan siber juga dapat dilakukan dari satu negara

terhadap sistem yang berada di negara lain dengan menggunakan infrastruktur yang tersebar di beberapa lokasi. Situasi tersebut membuat hukum nasional tetap penting, tetapi tidak lagi cukup. Indonesia membutuhkan kemampuan untuk bekerja dalam sistem hukum global yang semakin terhubung.

Persoalan lintas batas paling jelas terlihat dalam arus data. Perdagangan digital, layanan awan, penelitian, komunikasi, dan inovasi membutuhkan perpindahan data lintas negara. Di sisi lain, negara mempunyai kepentingan untuk memastikan bahwa data strategis dan data pribadi terlindungi. Ketegangan antara keterbukaan dan kedaulatan data menjadi salah satu persoalan utama dalam tata kelola digital global. Kebijakan yang terlalu terbuka dapat meningkatkan risiko keamanan dan kehilangan kendali atas data, sedangkan pembatasan yang terlalu ketat dapat menghambat perdagangan, inovasi, dan interoperabilitas digital (Gulia, 2025; Hwang, 2025; Kaya & Shahid, 2025).

Indonesia karena itu perlu menghindari dua ekstrem. Ekstrem pertama adalah liberalisasi tanpa perlindungan yang mengabaikan kepentingan keamanan dan hak masyarakat. Ekstrem kedua adalah isolasi digital yang membatasi pertukaran data dan teknologi secara berlebihan. Posisi yang lebih realistis adalah membangun interoperabilitas dengan mekanisme perlindungan yang memadai. Instrumen seperti *mutual recognition*, *adequacy*, perjanjian regional, dan kerja sama berbasis konvensi dapat digunakan untuk menciptakan hubungan lintas

batas yang tetap melindungi kepentingan nasional (Hwang, 2025; Kaya & Shahid, 2025; Zhuang, 2026).

Harmonisasi internasional juga diperlukan dalam penanganan kejahatan siber. Pelaku dapat berada di yurisdiksi yang berbeda dengan korban. Bukti dapat disimpan oleh penyedia layanan yang tunduk pada hukum negara lain. Permintaan akses data dapat membutuhkan prosedur kerja sama internasional. Tanpa mekanisme yang efektif, perbedaan yurisdiksi dapat menciptakan ruang aman bagi pelaku. Karena itu, Indonesia perlu memperkuat kerja sama internasional dalam pertukaran informasi, bantuan hukum timbal balik, investigasi bersama, pengembangan standar bukti digital, dan mekanisme ekstradisi atau bentuk kerja sama lain yang relevan.

Dalam konteks tersebut, kedaulatan digital perlu dipahami secara substantif. Kedaulatan digital bukan semata-mata keinginan untuk menempatkan seluruh data dan teknologi di dalam wilayah nasional. Kedaulatan lebih tepat dipahami sebagai kemampuan negara untuk mempertahankan kendali yang bermakna atas infrastruktur strategis, data penting, standar, keamanan, dan kebijakan digital. Ketergantungan yang terlalu besar pada teknologi asing dapat menimbulkan risiko apabila negara kehilangan kemampuan untuk memastikan keberlanjutan layanan atau keamanan sistem. Persoalan tersebut semakin penting ketika teknologi yang digunakan menyangkut infrastruktur kritis (Hwang, 2025; Othman, 2025).

Kendati demikian, kedaulatan digital yang terlalu proteksionis juga dapat menimbulkan persoalan. Ekosistem internet pada dasarnya dibangun melalui konektivitas dan pertukaran informasi. Pembatasan yang terlalu luas dapat meningkatkan biaya, menghambat inovasi, dan menciptakan fragmentasi digital. Karena itu, kedaulatan perlu diseimbangkan dengan interoperabilitas. Negara harus mampu melindungi kepentingan strategis tanpa menutup diri dari jaringan global. Tantangan tersebut mengharuskan hukum siber Indonesia untuk membangun kemampuan nasional sekaligus menjaga keterhubungan internasional (Kaya & Shahid, 2025; Othman, 2025).

Arsitektur hukum siber global saat ini juga menghadapi persoalan *regulatory patchwork*. Setiap negara dapat memiliki definisi, kewajiban, standar keamanan, dan mekanisme perlindungan data yang berbeda. Bagi perusahaan yang beroperasi lintas negara, perbedaan tersebut dapat meningkatkan biaya kepatuhan dan ketidakpastian hukum. Bagi masyarakat, perbedaan standar perlindungan dapat menghasilkan tingkat perlindungan yang berbeda ketika data berpindah yurisdiksi. Karena itu, Indonesia perlu aktif dalam forum internasional dan regional untuk mendorong kesesuaian prinsip tanpa harus menghilangkan karakter hukum nasional (Hwang, 2025; Kaya & Shahid, 2025; Khan, 2025).

Perlindungan data lintas batas menjadi salah satu bidang yang membutuhkan perhatian khusus.

Sistem perlindungan data nasional harus mampu menentukan kapan data dapat dipindahkan ke negara lain, standar perlindungan apa yang harus dipenuhi, siapa yang bertanggung jawab ketika terjadi pelanggaran, dan bagaimana hak subjek data dapat ditegakkan ketika data berada di luar wilayah Indonesia. Persoalan ini tidak dapat diselesaikan hanya melalui aturan domestik. Diperlukan mekanisme kerja sama dan pengakuan antarsistem hukum agar hak individu tetap dapat dilindungi ketika data bergerak melewati batas negara.

Prospek hukum siber Indonesia juga sangat dipengaruhi oleh perkembangan AI dan sistem otonom. Teknologi tersebut dapat menghasilkan keputusan, melakukan tindakan, dan berinteraksi dengan sistem lain dengan tingkat intervensi manusia yang semakin rendah. Kondisi tersebut akan menimbulkan pertanyaan hukum yang lebih kompleks mengenai pertanggungjawaban. Ketika sebuah sistem otonom menghasilkan kerugian, siapa yang bertanggung jawab? Apakah pengembang, penyedia, operator, pengguna, atau institusi yang menggunakan sistem tersebut? Pertanyaan semacam ini menunjukkan bahwa hukum masa depan perlu mengembangkan prinsip pertanggungjawaban berdasarkan kontrol, kemampuan mencegah risiko, manfaat yang diperoleh, dan kewajiban kehati-hatian.

Teknologi AI juga akan semakin terhubung dengan infrastruktur digital. Sistem deteksi ancaman dapat menggunakan AI untuk mengidentifikasi

serangan, tetapi AI pada saat yang sama dapat digunakan oleh pelaku untuk meningkatkan kualitas serangan. Karena itu, perkembangan AI tidak hanya menghadirkan peluang bagi keamanan, tetapi juga memperbesar kompleksitas ancaman. Negara membutuhkan strategi yang mampu menggunakan AI untuk pertahanan sekaligus membangun batas hukum terhadap penggunaannya. Prinsip keamanan, transparansi, pengawasan manusia, dan akuntabilitas menjadi semakin penting dalam konteks tersebut.

Keamanan infrastruktur digital strategis harus menjadi prioritas dalam arsitektur hukum siber masa depan. Infrastruktur digital bukan lagi sekadar alat pendukung administrasi. Gangguan terhadap energi, telekomunikasi, layanan kesehatan, transportasi, keuangan, pemerintahan, dan sistem strategis lainnya dapat mengganggu fungsi negara dan kehidupan masyarakat. Karena itu, perlindungan infrastruktur kritis membutuhkan pendekatan yang menggabungkan standar teknis, kewajiban hukum, mekanisme pelaporan insiden, pengawasan, dan kerja sama dengan operator. Ketahanan digital harus dibangun sebelum serangan terjadi, bukan hanya setelah kerugian muncul.

Pendekatan tersebut mengharuskan Indonesia mengembangkan konsep *digital resilience* yang lebih luas. Ketahanan bukan berarti sistem tidak pernah mengalami gangguan. Tidak ada sistem digital yang sepenuhnya bebas dari risiko. Ketahanan berarti sistem memiliki kemampuan untuk

mengantisipasi, menyerap dampak, merespons, memulihkan diri, dan belajar dari insiden. Karena itu, hukum tidak hanya perlu menentukan larangan dan sanksi, tetapi juga kewajiban membangun kapasitas pencegahan dan pemulihan. Prinsip *secure-by-design*, *zero trust*, pengelolaan risiko rantai pasok, dan penguatan kapasitas domestik dapat menjadi bagian dari strategi tersebut (Bonnieu, 2026; Carroll, 2024).

Masa depan arsitektur hukum siber juga akan dipengaruhi oleh kemampuan Indonesia mengembangkan sumber daya manusia. Teknologi dapat dibeli, tetapi kapasitas manusia untuk memahami, mengelola, dan mengaturnya harus dibangun secara berkelanjutan. Indonesia membutuhkan lebih banyak ahli yang mampu bekerja pada persimpangan hukum dan teknologi. Hakim, jaksa, penyidik, regulator, akademisi, pengacara, insinyur, ahli keamanan informasi, dan pembuat kebijakan perlu mempunyai ruang kolaborasi. Perkembangan hukum siber tidak dapat hanya diserahkan kepada satu kelompok profesi karena masalah digital sendiri bersifat multidisipliner.

Dalam jangka panjang, hukum siber Indonesia juga perlu memiliki kemampuan untuk mengatur teknologi yang saat ini belum sepenuhnya dikenal. Prinsip ini sangat penting karena hukum selalu mempunyai keterbatasan jika dibangun hanya berdasarkan teknologi yang telah ada. Teknologi baru dapat muncul dalam bentuk yang tidak diperkirakan sebelumnya. Karena itu, hukum masa depan harus

mempunyai prinsip yang cukup umum untuk menghadapi teknologi baru, tetapi cukup konkret untuk memberikan perlindungan. Kombinasi antara *technology-neutral regulation*, pendekatan berbasis risiko, *regulatory foresight*, dan evaluasi berkala dapat menjadi fondasi untuk menghadapi ketidakpastian tersebut.

Visi hukum siber Indonesia bukanlah menciptakan sistem hukum yang paling banyak mengatur teknologi. Visi yang lebih tepat adalah membangun sistem hukum yang mampu memastikan bahwa teknologi berkembang dalam lingkungan yang aman, adil, dapat dipertanggungjawabkan, dan menghormati manusia. Regulasi tidak boleh menjadi penghambat inovasi tanpa alasan, tetapi inovasi juga tidak boleh menjadi alasan untuk mengabaikan hak masyarakat. Keseimbangan tersebut merupakan inti dari tata kelola digital yang berkelanjutan.

Arsitektur hukum siber Indonesia dapat dibayangkan sebagai sebuah sistem yang memiliki empat lapisan. Lapisan pertama adalah **norma**, yaitu hukum yang harmonis dan mempunyai prinsip umum. Lapisan kedua adalah **institusi**, yaitu lembaga yang mempunyai kapasitas untuk melaksanakan dan menegakkan hukum. Lapisan ketiga adalah mekanisme adaptasi, yaitu kemampuan regulasi untuk belajar, mengevaluasi, dan menyesuaikan diri. Lapisan keempat adalah konektivitas global, yaitu kemampuan Indonesia untuk bekerja sama dengan negara lain tanpa kehilangan kepentingan nasional.

Keempat lapisan tersebut harus bekerja secara bersamaan.

Dalam kerangka tersebut, prinsip kepastian hukum tetap menjadi fondasi. Hukum yang adaptif tidak boleh menghasilkan aturan yang berubah tanpa arah. Setiap perubahan harus mempunyai dasar, prosedur, alasan, dan tujuan yang dapat dipertanggungjawabkan. Masyarakat dan pelaku usaha harus mampu memprediksi konsekuensi hukum dari tindakan mereka. Pada saat yang sama, negara harus mampu mengubah aturan ketika teknologi dan risiko berubah. Keseimbangan antara stabilitas dan kemampuan beradaptasi inilah yang menjadi karakter utama arsitektur hukum siber masa depan.

Prinsip kedua adalah orientasi pada manusia. Teknologi tidak boleh ditempatkan sebagai tujuan akhir regulasi. Tujuan akhirnya adalah memastikan bahwa teknologi memberikan manfaat bagi manusia sekaligus tidak menciptakan risiko yang tidak dapat diterima. Prinsip ini mengharuskan hukum memperhatikan privasi, keamanan, kebebasan, kesetaraan, perlindungan konsumen, dan hak untuk memperoleh pemulihan. Dalam konteks AI dan sistem otonom, prinsip tersebut juga berarti mempertahankan ruang bagi manusia untuk memahami, mengontrol, dan menggugat keputusan yang berdampak pada dirinya.

Prinsip ketiga adalah berbasis risiko. Tidak semua teknologi membutuhkan tingkat regulasi yang sama. Negara harus mampu mengidentifikasi

teknologi dan aktivitas yang mempunyai dampak terbesar terhadap masyarakat, keamanan, ekonomi, dan hak fundamental. Pendekatan tersebut memungkinkan regulasi menjadi lebih proporsional. Teknologi dengan risiko rendah tidak perlu dibebani mekanisme yang sama dengan teknologi yang dapat memengaruhi keselamatan publik atau hak fundamental.

Prinsip keempat adalah kapasitas. Hukum yang baik harus didukung oleh institusi yang mampu menjalankannya. Kapasitas teknis, sumber daya manusia, forensik digital, koordinasi antarlembaga, kemampuan investigasi, dan kerja sama internasional harus menjadi bagian dari arsitektur hukum. Tanpa kapasitas tersebut, hukum hanya akan menjadi norma formal yang tidak mempunyai daya implementasi yang memadai.

Prinsip kelima adalah interoperabilitas. Indonesia perlu mempertahankan kemampuan untuk berinteraksi dengan sistem hukum dan teknologi global. Keterhubungan tersebut penting untuk perdagangan, investasi, inovasi, keamanan, dan penegakan hukum lintas batas. Namun, interoperabilitas tidak berarti menyerahkan seluruh kendali. Indonesia tetap harus memiliki kemampuan untuk menentukan standar perlindungan yang sesuai dengan kepentingan nasional.

Dengan demikian, masa depan hukum siber Indonesia sebaiknya tidak diarahkan menuju hukum yang semakin represif atau semakin permisif, melainkan menuju hukum yang semakin adaptif,

responsif, proporsional, dan berorientasi pada hak. Hukum harus mampu merespons ancaman tanpa mengorbankan kebebasan, mendukung inovasi tanpa mengabaikan keamanan, membuka arus data tanpa kehilangan kontrol atas kepentingan strategis, dan memberikan ruang bagi teknologi tanpa menghilangkan tanggung jawab manusia.

Arsitektur hukum siber yang adaptif bukanlah sebuah produk hukum yang selesai dibentuk dalam satu waktu. Ia merupakan proses berkelanjutan yang membutuhkan evaluasi, pembelajaran, koordinasi, dan pembaruan. Perubahan teknologi akan terus berlangsung, sehingga hukum harus memiliki kemampuan untuk bergerak bersamanya. Tantangan terbesar bukan memprediksi setiap teknologi yang akan muncul, melainkan memastikan bahwa ketika teknologi baru hadir, negara sudah mempunyai prinsip, institusi, dan mekanisme yang mampu menghadapinya.

Visi tersebut menempatkan Indonesia pada posisi yang tidak sekadar menjadi pengguna teknologi, tetapi juga menjadi negara yang mampu mengatur, melindungi, dan mengarahkan perkembangan ekosistem digitalnya. Arsitektur hukum siber yang demikian akan menjadikan hukum bukan sebagai penghalang inovasi, melainkan sebagai fondasi kepercayaan. Kepercayaan tersebut dibangun melalui kepastian hukum, perlindungan hak, keamanan sistem, akuntabilitas pelaku, kapasitas institusi, dan kerja sama internasional. Inilah arah yang diperlukan agar transformasi digital

tidak hanya menghasilkan kemajuan teknologi, tetapi juga menghasilkan tata kehidupan digital yang adil, aman, dan berkelanjutan.

DAFTAR PUSTAKA

Ababneh, J., Alzara, A., Attar, H., Al-Shaikh, A., Abu-Jassar, A., & Hafez, M. (2026). Cybersecurity laws, digital crimes, and ethical considerations: a multidimensional perspective on Cyber Risk Regulation (MPoCRR). *Journal of Cloud Computing*, *15*. https://doi.org/10.1186/s13677-025-00824-y

Abdelkarim, Y. (2025). UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age. *Journal of Digital Technologies and Law*. https://doi.org/10.21202/jdtl.2025.22

Abigail, A. D., Tyas, D. A., Setyawan, F., & Amrullah, M. (2025). Legal Liability for Force Majeure in Digital Crypto Asset Contracts Reviewed from the Perspective of Legal Rationality in the Digital Age. *Academia Open*. https://doi.org/10.21070/acopen.10.2025.12855

Abokhodair, N., Skop, Y., Rüller, S., Aal, K., & Elmimouni, H. (2024). Opaque algorithms, transparent biases: Automated content moderation during the Sheikh Jarrah Crisis. *First Monday*, *29*. https://doi.org/10.5210/fm.v29i4.13620

Admiral, A., Arifin, R., Adinda, F., & Ezzerouali, S. (2025). Unfair Terms in Standard Digital Contracts: A Hidden Threat to Human Rights and Consumer Justice. *Yustisia Jurnal Hukum*. https://doi.org/10.20961/yustisia.v14i3.109656

Adytia, N. A. P., Wachdin, S. Z. S., & Said, S. (2024). The Legal Framework for Personal Data Protection in the Digital Era as Fulfillment of Privacy Rights in

Indonesia. *KnE Social Sciences*. https://doi.org/10.18502/kss.v8i21.14785

Ahern, D. (2025). The New Anticipatory Governance Culture for Innovation: Regulatory Foresight, Regulatory Experimentation and Regulatory Learning. *European Business Organization Law Review*, *26*, 241–283. https://doi.org/10.1007/s40804-025-00348-7

Al-Mezel, S., AlDalalah, S., AlShatnawi, N., Matalkaha, M. F., Alhade, A., & Hasan, M. (2026). Contemporary Islamic Economic Law: Autonomous Smart Contracts and the Legal Dilemma of Liability for Technical Errors. *MILRev: Metro Islamic Law Review*. https://doi.org/10.32332/milrev.v5i1.13661

AlDesouki, M. M. A. (2024). legal regulation of digital rights and freedoms. *International Journal of Advanced Research on Law and Governance*. https://doi.org/10.21608/ijarlg.2024.275161.1076

Alifah, D. (2024). The Evolution of Cyber Law: Protecting Privacy and Data in the Digital Age. *LAWYER: Jurnal Hukum*. https://doi.org/10.58738/lawyer.v2i2.652

Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025). Explainable Artificial Intelligence Models for Automated Regulatory Compliance and Policy Enforcement. *Shodhshauryam International Scientific Refereed Research*. https://doi.org/10.32628/shisrrj258474

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021).

Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *3*. https://doi.org/10.3389/fcomp.2021.563060

Allahrakha, N. (2024). Rethinking Digital Borders to Address Jurisdiction and Governance in the Global Digital Economy. *International Journal of Law and Policy*. https://doi.org/10.59022/ijlp.124

Allahrakha, N. (2025). Human Rights in Cyberspace: Digital Freedom and Security in the Age of Global Connectivity. *Uzbek Journal of Law and Digital Policy*. https://doi.org/10.59022/ujldp.353

Allakuliev, M. (2025). Tort Liability of Digital Platforms for User-Generated Content. *Uzbek Journal of Law and Digital Policy*. https://doi.org/10.59022/ujldp.376

Ansari, Y., Sunarmi, & Sukarja, D. (2024). Legal Aspects of Cross-Border Electronic Commerce Transactions with Quick Response Code (QR Code) Based Payments in the ASEAN Cooperation Framework. *Journal of Law, Politic and Humanities*. https://doi.org/10.38035/jlph.v4i6.767

Antony, A., Sandoval, E. B., & Louis, J. E. (2025). Legal Reform in Indonesia's Response to the Digital Manipulation Era: A Responsive Legal Theory Approach. *Trunojoyo Law Review*. https://doi.org/10.21107/tlr.v8i1.30732

Arafat, Z., Asyhadi, F., Amaliya, L., & Dewi, S. (2025). THE EXISTENCE OF LEGAL PHILOSOPHY IN THE TRANSFORMATION OF THE INDONESIAN LEGAL SYSTEM IN THE ERA OF DIGITALIZATION. *MSJ : Majority Science Journal*.

https://doi.org/10.61942/msj.v3i2.319
Araujo, L. H. D. (2025). Digital Constitutionalism: freedom of speech and platforms accountability. *Revista de Investigações Constitucionais*. https://doi.org/10.5380/rinc.v12i2.97417
Are´valo Rami´rez, W., & Rousset Siri, A. (2025). FREEDOM OF SPEECH AND ITS DIGITAL TRANSFORMATION AND PROTECTION: guidelines and principles from the Inter-American Court Of Human Rights case-law and other human right protection bodies. *Latin American Journal of European Studies*. https://doi.org/10.51799/2763-8685v5n1003
Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, *37*, 29–51. https://doi.org/10.1080/13600869.2022.2061888
Asan, M. L., & Azis, R. A. (2026). Legal Validity of Smart Contracts as a Digital Contract Mechanism in Online Buying and Selling Transactions (E-Commerce) on the Opensea Application. *International Journal of Science and Environment (IJSE)*. https://doi.org/10.51601/ijse.v6i1.351
Aslan, Ö., Aktug˘, S. S., Ozkan-Okay, M., Yílmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*. https://doi.org/10.3390/electronics12061333
Aslina, N., & Noviya, A. (2026). Legal Responsibility in

Smart Contracts in Blockchain Transactions. *Ipso Jure*. https://doi.org/10.62872/d8kn5x96

Asyari, H. Al. (2023). Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law. *AUC IURIDICA*. https://doi.org/10.14712/23366478.2023.56

Awwad, A., & Abdelsattar, A. (2025). Digital Evidence in Forensic Accounting- A study in Saudi Legislation. *Cogent Social Sciences*, *11*. https://doi.org/10.1080/23311886.2025.2522958

Bailo, P., Nittari, G., Pesel, G., Basello, E., Spasari, T., & Ricci, G. (2026). Governing Healthcare AI in the Real World: How Fairness, Transparency, and Human Oversight Can Coexist: A Narrative Review. *Sci*. https://doi.org/10.3390/sci8020036

Bartoli, L. (2025). Cybersecurity and the Fight against Cybercrime: Partners or Competitors? *European Journal of Risk Regulation*, *16*, 498–513. https://doi.org/10.1017/err.2025.31

Bendjerad, A. (2026). Protecting Electronic Signatures from Cyber Threats in Electronic Contracts. *Public Administration and Law Review*. https://doi.org/10.36690/2674-5216-2026-2-104-117

Bhange, M. (2025). Understanding Cyber Law and Security. *Gurukul International Multidisciplinary Research Journal*. https://doi.org/10.69758/gimrj/2503i3iivxiiip0007

Blancato, F. (2023). The cloud sovereignty nexus: How

the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*. https://doi.org/10.1002/poi3.358

Bonnieu, J.-N. B. (2026). Future Digital Resilience in Safeguarding Critical Infrastructure and Securing Digital Economy. *Proceeding Jakarta Geopolitical Forum*. https://doi.org/10.55960/jgf.v10i1.319

Borgesius, F. (2025). Discrimination, artificial intelligence, and algorithmic decision-making. *ArXiv*, *abs/2510.1*. https://doi.org/10.48550/arxiv.2510.13465

Boutellier, H. (2026). Het ondermijnde paradijs. *Justitiële verkenningen*. https://doi.org/10.5553/jv/01675850202605200 1005

Campione, R. (2025). The Legal–Digital Metamorphosis of the Individual. *Philosophies*. https://doi.org/10.3390/philosophies10010002

Carroll, J. (2024). The U.S. National Cybersecurity Strategy: A Vehicle with an International Journey. *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.23.1.2300

Caruso, C. (2024). Towards the Institutions of Freedom: The European Public Discourse in the Digital Era. *German Law Journal*, *26*, 114–137. https://doi.org/10.1017/glj.2024.68

Chaudhary, A., & Asghar, A. (2026). Cross-Border Cybercrime Investigations: Legal Challenges and The Impact of Distinct National Laws on Digital Evidence and Admissibility. *UCP Journal of Law &*

Legal Education. https://doi.org/10.24312/ucp-jlle.03.03.546
Chesterman, S. (2025). Lawful but Awful: Evolving Legislative Responses to Address Online Misinformation, Disinformation, and Mal-Information in the Age of Generative AI. *ArXiv*, *abs/2505.1*. https://doi.org/10.48550/arxiv.2505.15067
Chodyka, M., Z˙urawski, S., Wojciechowska-Filipek, S., Ciekanowski, Z., & Mazur, S. (2025). Critical Infrastructure Security Management in the Era of Cyber Threats. *EUROPEAN RESEARCH STUDIES JOURNAL*. https://doi.org/10.35808/ersj/4000
Christodoulou, P., & Limniotis, K. (2024). Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges. *Network*, *4*, 91–113. https://doi.org/10.3390/network4010005
Christopher, Y., & Fitria, A. (2026). Tanggung Jawab E-Commerce Terhadap Konsumen Serta Penerapan Choice of Law dan Jurisdiction Clause dalam Transaksi Lintas Negara. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*. https://doi.org/10.31004/jerkin.v4i3.4936
Coche, E., Kolk, A., & Ocelí´k, V. (2023). Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, *7*, 112–127. https://doi.org/10.1057/s42214-023-00172-1
Coetzee, J. (2024). Cross-Border Data Flows and the

Protection of Personal Information Act 4 of 2013 – Part II: The Data Transfer Provision. *Potchefstroom Electronic Law Journal*. https://doi.org/10.17159/1727-3781/2024/v27i0a15234

Cohen, J., & Fung, A. (2023). Democratic responsibility in the digital public sphere. *Constellations*. https://doi.org/10.1111/1467-8675.12670

Çora, H., & Mikail, E. (2026). CYBERSECURITY, SOVEREIGNTY, AND INTERNATIONAL LAW: NORMATIVE CHALLENGES IN THE DIGITAL AGE. *Veredas do Direito*. https://doi.org/10.18623/rvd.v23.4381

C'orac, S. (2025). ZAS˘TITA LJUDSKIH PRAVA U DIGITALNOM OKRUZ˘ENJU: „PRAVO NA ZABORAV" U PRAKSI EVROPSKOG SUDA ZA LJUDSKA PRAVA. *Savremeno pravo u eri digitalizacije i održivog razvoja*. https://doi.org/10.46793/xximajsko.551c

Corfmat, M., Martineau, J., & Re´gis, C. (2025). High-reward, high-risk technologies? An ethical and legal account of AI development in healthcare. *BMC Medical Ethics*, *26*. https://doi.org/10.1186/s12910-024-01158-1

Currie, W., Leimeister, J., Schlagwein, D., & Willcocks, L. (2025). Rethinking technology regulation in the age of AI risks. *Journal of Information Technology*, *40*, 236–245. https://doi.org/10.1177/02683962251378815

Drechsler, L. (2023). Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation. *Review of European*

Administrative Law. https://doi.org/10.7590/187479823x16800083010347

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*, 76–92. https://doi.org/10.1177/00048658211003925

Ennan, R. (2024). Digitalization of Law and formation of Digital Law. *Uzhhorod National University Herald. Series: Law*. https://doi.org/10.24144/2307-3322.2024.83.1.29

Fachran, S., Rosadi, S. D., & Amalia, P. (2026). PROTECTION OF DATA SUBJECT RIGHTS IN THE TRANSFER OF PERSONAL DATA BETWEEN DATA CONTROLLERS IN INDONESIA: A COMPARATIVE ANALYSIS OF THE PDP LAW AND THE EU GDPR. *Awang Long Law Review*. https://doi.org/10.56301/awl.v8i2.1827

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. *Journal of European Integration*, *46*, 1073–1088. https://doi.org/10.1080/07036337.2024.2411240

Faizin, M., Ezzerouali, S., Jibril, A. M., & Bahari, R. (2025). Redefining Consent in Digital Contracts through Electronic Signatures in Islamic Law. *International Journal of Islamic Thought and Humanities*. https://doi.org/10.54298/ijith.v4i2.637

Falowo, O., Ozer, M., Li, C., & Abdo, J. B. (2024). Evolving Malware and DDoS Attacks: Decadal Longitudinal Study. *IEEE Access*, *12*, 39221–39237. https://doi.org/10.1109/access.2024.3376682

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*, 435–453. https://doi.org/10.1080/09662839.2022.2102896
Ferreira, B., & Gromova, E. (2024). Digital Evidence in Disputes Involving States. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4
Firdaus, A., Lubis, M. A., Frensh, W., & Harahap, M. (2025). Legal Transformation in the Digital Era: Building Adaptive Regulations to the Dynamics of Technological Development. *East Asian Journal of Multidisciplinary Research*. https://doi.org/10.55927/eajmr.v4i9.381
Gafarova, K., & Jabbarova, M. (2025). The legal-theoretical character of cybercrime and the integration of Azerbaijan to international cybersecurity levels. *Azerbaijan Law Journal*. https://doi.org/10.61638/jvdq7012
Gajic´, G. (2026). Criminalistic and Legal Challenges of Electronic Communications Surveillance in the Era of Encrypted Platforms. *Годишњак факултета правних наука - АПЕИРОН*. https://doi.org/10.7251/gfp2616095g
Gede, I., Mulyawarman, A., Arya, P., Yasa, S., & Cait, L. (2024). Blocking Dangerous Content in Electronic Communications Networks: Evidence from Netherlands, United States and Singapore. *Journal of Human Rights, Culture and Legal System*. https://doi.org/10.53955/jhcls.v4i1.216
Ghazi-Tehrani, A., & Pontell, H. (2021). Phishing Evolves:

Analyzing the Enduring Cybercrime. *Victims & Offenders*, *16*, 316–342. https://doi.org/10.1080/15564886.2020.1829224

Gillespie, T. (2022). Do Not Recommend? Reduction as a Form of Content Moderation. *Social Media + Society*, *8*. https://doi.org/10.1177/20563051221117552

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., B o ̂mont, C., Braun, M., Danet, D., Desforges, A., Ge´ry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pe´tiniaud, L., Winkler, J., & Zanin, C. (2022). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*, 919–958. https://doi.org/10.1080/14650045.2022.2050070

Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., Das, N., Chakraborty, P., & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. *Journal of Posthumanism*. https://doi.org/10.63332/joph.v5i3.965

Gomes, A. B., & Sultan, A. (2024). Problematizing content moderation by social media platforms and its impact on digital harm reduction. *Harm Reduction Journal*, *21*. https://doi.org/10.1186/s12954-024-01104-9

Greenstein, S. (2021). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Guama´n, D., Del Alamo, J., & Caiza, J. (2021). GDPR

Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps. *IEEE Access*, *9*, 15961–15982. https://doi.org/10.1109/access.2021.3053130

Gulia, J. (2025). cross - border data transfers : international cooperation and conflicts. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2025.v07i02.41439

Gulyaeva, E., Grace, H., & Fe´lix, D. (2025). Impact of Digital Technologies on Legal Theory and Practice. *Qubahan Techno Journal*. https://doi.org/10.48161/qtj.v4n4a76

Gussman, A. A., & Jannah, R. (2026). Countering cybercrime in a criminal law perspective: the challenges of law enforcement in the digital age. *Journal of Strafvordering Indonesian*. https://doi.org/10.62872/vt6zyw84

Haji, I. A., Mohammed, S., & Mousa, K. (2026). Blockchain based chain of custody and digital evidence legality in post conflict prosecutions. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2026.1801364

Hanandini, D. (2024). Social Transformation in Modern Society: A Literature Review on the Role of Technology in Social Interaction. *Jurnal Ilmiah Ekotrans & Erudisi*. https://doi.org/10.69989/j0m6cg84

Hasnia, H., Hafiz, A., Rasna, R., Nurahman, D., & Parhusip, J. (2025). Reconstruction of Criminal Law Policy in

Handling Cyber Crime: Perspectives of Technology Law and Human Rights. *Jurnal Smart Hukum (JSH)*. https://doi.org/10.55299/jsh.v3i3.1328

Häuselmann, A., & Custers, B. (2025). The Right to Rectification and Inferred Personal Data. *Eur. J. Law Technol.*, *15*. https://doi.org/10.2139/ssrn.5116221

Hefjullah. (2025). Cybersecurity and International Law: The Challenge of Sovereignty in Cyberspace. *RESEARCH HUB International Multidisciplinary Research Journal*. https://doi.org/10.53573/rhimrj.2025.v12n9.012

Homonai, V. (2024). The impact of digitalization on the development of e-commerce and its legal regulation. *Uzhhorod National University Herald. Series: Law*. https://doi.org/10.24144/2307-3322.2024.85.2.43

Humin, O. (2026). DIGITAL JUSTICE: THE PHILOSOPHICAL AND LEGAL DIMENSION. *Наукові інновації та передові технології*. https://doi.org/10.52058/2786-5274-2026-1(53)-2118-2126

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*. https://doi.org/10.1177/2053951720982012

Hutchinson, J., Stilinovic, M., & Gray, J. (2024). Data sovereignty: The next frontier for internet policy? *Policy & Internet*. https://doi.org/10.1002/poi3.386

Hwang, J. Y. (2025). Digital sovereignty in an era of cyber threats and global connectivity. *International*

Journal of Multidisciplinary Research Updates. https://doi.org/10.53430/ijmru.2025.9.2.0023
Islami, Z. (2025). Tantangan Penegakan Hukum di Era Globalisasi Digital: Strategi Nasional Menghadapi Kejahatan Siber Lintas Batas. *AKSIOMA : Jurnal Sains Ekonomi dan Edukasi*. https://doi.org/10.62335/aksioma.v2i12.1985
Jadala, S. K. (2026). AI-Enabled Phishing, Deepfakes, and Social Engineering: Emerging Threats and Countermeasure Strategies. *International Journal of AI, BigData, Computational and Management Studies*. https://doi.org/10.63282/3050-9416.ijaibdcms-v7i2p130
Johari, A., & Prakash, L. (2026). The Need for Cybercrime Regulation on a Global Scale by International Law and Cyber Conventions. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2026.v08i02.70459
Johnson, W. (2022). Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. *Regulation & Governance*. https://doi.org/10.1111/rego.12487
Jorgi, J., & Firmansyah, H. (2026). Digital Democracy and the Challenges of Freedom of Expression in Indonesia. *JIHK*. https://doi.org/10.46924/jihk.v8i1.476
Kala, E. M. (2024). Public-Private Synergy in Cybersecurity Advanced Strategies for Bridging Regulatory Gaps and Enhancing Digital Resilience.

International Journal of Research Studies in Computer Science and Engineering. https://doi.org/10.20431/2349-4859.1002003

Kalenzi, C. (2022). Artificial Intelligence and Blockchain: How Should Emerging Technologies Be Governed? *Frontiers in Research Metrics and Analytics*, *7*. https://doi.org/10.3389/frma.2022.801549

Kang, W. (2025). A Typological and Prioritization Analysis of Key Indicators in Cyber-Enabled Financial Crimes. *2025 11th International Conference on Systems and Informatics (ICSAI)*, 1–3. https://doi.org/10.1109/icsai68704.2025.11345875

Kashyap, A., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law and Safety*. https://doi.org/10.32631/pb.2023.2.19

Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics*. https://doi.org/10.61838/kman.isslp.4.2.20

Ke, T., & Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Manag. Sci.*, *69*, 4389–4412. https://doi.org/10.1287/mnsc.2022.4614

Khaled, B. (2026). The Legal Foundations of Electronic Commerce: A Comparative and Analytical Examination of Definitions, Evolution, and Regulatory Challenges in the Digital Economy. *Science, Education and Innovations in the context of modern problems*.

https://doi.org/10.56334/sei/9.6.8
Khan, M. N. I. (2025). CROSS-BORDER DATA PRIVACY AND LEGAL SUPPORT: A SYSTEMATIC REVIEW OF INTERNATIONAL COMPLIANCE STANDARDS AND CYBER LAW PRACTICES. *American Journal of Scholarly Research and Innovation*. https://doi.org/10.63125/a4gbeb22
Khanna, R. (2024). Cybersecurity Law: Challenges and Legal Frameworks for Protecting Digital Assets and Privacy Rights. *Indian Journal of Law*. https://doi.org/10.36676/ijl.v2.i2.05
Kingshuk, N. H., & Rahman, S. S. (2026). Cybercrime and Criminal Justice in Bangladesh. *ABC Journal of Advanced Research*. https://doi.org/10.18034/abcjar.v15i1.804
Kirani, A. A., & Lie, G. (2026). STRATEGI E-COMMERCE dalam MEMILIH HUKUM dan FORUM UNTUK MENGHINDARI KONFLIK YURISDIKSI pada TRANSAKSI LINTAS BATAS. *Mahkamah : Jurnal Riset Ilmu Hukum*. https://doi.org/10.62383/mahkamah.v3i2.1611
Kitov, A., & Kartsev, M. (2025). Legal Considerations for Cross-Border Digital Transactions. *International Journal of Commerce, Finance and Digital Economy*. https://doi.org/10.67228/3071642x/ijcfde-2025pi6b3q
Klase´n, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic science international*, *362*, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

Klevtsov, K. (2022). International cooperation in the fight against cyberpression in the context of response to new challenges and threats. *Vestnik of Saint Petersburg University. Law*. https://doi.org/10.21638/spbu14.2022.306

Korpisaari, P. (2022). From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act. *Journal of Media Law*, *14*, 352–377. https://doi.org/10.1080/17577632.2022.2148335

Kovalenko, Y. (2022). The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights. *Masaryk University Journal of Law and Technology*. https://doi.org/10.5817/mujlt2022-1-2

Kulugh, V., Mbanaso, U., & Chukwudebe, G. (2022). Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure. *SN Computer Science*, *3*. https://doi.org/10.1007/s42979-022-01108-x

Lalova-Spinks, T., Saesen, R., Silva, M., Geissler, J., Shakhnenko, I., Camaradou, J. C., & Huys, I. (2024). Patients' knowledge, preferences, and perspectives about data protection and data control: an exploratory survey. *Frontiers in Pharmacology*, *14*. https://doi.org/10.3389/fphar.2023.1280173

Laux, J., & Ruschemeier, H. (2025). Automation Bias in the AI Act: On the Legal Implications of Attempting

to De-Bias Human Oversight of AI. *ArXiv*, *abs/2502.10036*. https://doi.org/10.1017/err.2025.10033

Lazari, C. (2025). Cybersecurity and Sovereignty in Cyberspace: Challenges and Prospects of International Law. *Moscow Journal of International Law*. https://doi.org/10.24833/0869-0049-2025-1-125-137

Lazaro, M., & Mzurikwao, A. (2026). Bridging the Prosecutorial Gap: Capacity Building for Cybercrime Prosecution in Tanzania. *Journal of Policy and Development Studies*. https://doi.org/10.4314/jpds.v20i2.2

Lee, G. (2024). Personal Data Protection Issues in the Era of Artificial Intelligence. *Journal of Medical Imaging*. https://doi.org/10.31916/sjmi2024-01-03

Lestari, E. F., Rahmayanti, R., & Aruan, D. C. (2026). Problematika Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia. *Dewantara : Jurnal Pendidikan Sosial Humaniora*. https://doi.org/10.30640/dewantara.v5i2.6623

Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. (2025). Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors (Basel, Switzerland)*, *25*. https://doi.org/10.3390/s25154545

Luhina, N., & Paliukh, O. (2025). PECULIARITIES OF PROOF IN CRIMINAL PROCEEDINGS RELATED TO CYBERCRIME. *Social Development: Economic and Legal Issues*. https://doi.org/10.70651/3083-

6018/2025.4.27
Lukmana, N. (2025). Legal Protection Of Criminal Acts Of Electronic Selling And Buying Transactions From A Cyber Law Perspective. *Proceedings of the First International Cyber Law Conference, ICL-C 2023, 11 November 2023, Jakarta, Indonesia*. https://doi.org/10.4108/eai.11-11-2023.2351701
Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime? *Annual Review of Law and Social Science*. https://doi.org/10.1146/annurev-lawsocsci-041822-044042
Mahfud, T. A., Subekti, S., Suyono, Y. U., & Widodo, E. (2026). The Legal Certainty of Digital Consent In The Formation of Electronic Contracts is Reviewed From The Principle of Consensualism. *Journal of Law, Politic and Humanities*. https://doi.org/10.38035/jlph.v6i5.3509
Maia, R. B., De Assis, K. R. S., & Da Costa, P. J. C. (2025). O direito e o discurso de o´dio nas redes sociais: limites da liberdade de expressa˜o. *RCMOS - Revista Científica Multidisciplinar O Saber*. https://doi.org/10.51473/rcmos.v1i2.2025.1623
Maydanyk, R. (2024). Smart Contract on a Crypto Assets in the Civil Law and Common Law Jurisdictions: Implementation of Best Practices. *Open Journal for Legal Studies*. https://doi.org/10.32591/coas.ojls.0702.01015m
Miller, C. (2022). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, *6*.

https://doi.org/10.1016/j.fsisyn.2022.100296
Moussa, A. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, *11*, 1–10. https://doi.org/10.1186/s41935-021-00234-6
Mugamba, E. (2026). CO-CREATED LEGAL EDUCATION AND THE PREVENTIVE ARCHITECTURE OF EU CYBERCRIME GOVERNANCE. *Journal of Political Science, Law & Governance*. https://doi.org/10.63456/jpslg-2-2-109
Muharman, D. (2025). The Evolution of Cyber Law: Protecting Privacy and Security in the Digital Age. *Journal of Information Systems Engineering and Management*. https://doi.org/10.52783/jisem.v10i51s.10397
Mujianto, M. (2025). Cybercrime Regulations as an Instrument of Legal Protection for Victims of Cybercrime in Indonesia. *Proceeding of International Conference on The Law Development For Public Welfare*. https://doi.org/10.30659/picldpw.v4i0.50191
Nabila, A. (2025). Asrar Digital Transactions: An International Legal Review of Global E-Commerce. *International Journal of Law and Policy*. https://doi.org/10.59022/ijlp.324
Nafi'ah, L. S., & Prastyanti, R. (2025). The Right to Privacy in International Law: Evolving Standards for Personal Data Protection in the Digital Era. *West Science Law and Human Rights*. https://doi.org/10.58812/wslhr.v3i03.2018
Ningsih, S. F., Hurairah, H., & Timur, W. (2026). Digital

Agreements On The Legal Validity Of Electronic Signatures In Online Lending From The Perspective Of Indonesian Legislation. *JURNAL HUKUM SEHASEN*. https://doi.org/10.37676/jhs.v12i2.10799

Noor, M. (2025). Cybercrime and Data Protection Emerging Legal Challenges. *International Journal of Law and Policy*. https://doi.org/10.59022/ijlp.369

Novelli, C., Hacker, P., McDougall, S., Morley, J., Rotolo, A., & Floridi, L. (2026). Getting Regulatory Sandboxes Right: Design and Governance Under the AI Act. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10096

Nur, I., Hadisiswati, I., Fajarwati, H., Nuruddienil, H., & Rais, M. D. (2026). Wisdom in the Digital Era: Bridging Human Rights, Indonesian Cyber Law, and Progressive Fiqh. *The Journal of Society and Media*. https://doi.org/10.26740/jsm.v10n1.p315-340

Octaviandini, E. C., & Listyani, A. A. (2025). Cyber Law Reform in Indonesia: Regulatory Challenges, Technological Dynamics, and Adaptive Policy Directions in Digital Era. *Jurnal Idea Hukum*. https://doi.org/10.20884/1.jih.2025.11.2.664

Okonkwo, O. A. (2025). Evolving interpretations of digital privacy, free expression, and data protection within international human rights jurisprudence and governance frameworks. *International Journal of Science and Research Archive*. https://doi.org/10.30574/ijsra.2025.17.1.2876

Othman, D. M. O. D. M. (2025). Cyber Threats and Legal Gaps: A Study on Egypt and UAE Laws". المجلة

القانونية.
https://doi.org/10.21608/jlaw.2025.410577.1301
Pashentsev, D., & Babaeva, Y. (2024). Artificial intelligence in law-making and law enforcement: Risks and new opportunities. *Vestnik of Saint Petersburg University. Law*. https://doi.org/10.21638/spbu14.2024.214
Paul, J., Ueno, A., Dennis, C., Alamanos, E., Curtis, L., Foroudi, P., Kacprzak, A., Kunz, W., Liu, J., Marvi, R., Nair, S., Ozdemir, O., Pantano, E., Papadopoulos, T., Petit, O., Tyagi, S., & Wirtz, J. (2024). Digital transformation: A multidisciplinary perspective and future research agenda. *International Journal of Consumer Studies*. https://doi.org/10.1111/ijcs.13015
Petrov, I., & Kumar, R. (2025). Disinformation and Legal Responsibility: Regulating Digital Speech Without Curtailing Dissent. *Interdisciplinary Studies in Society, Law, and Politics*. https://doi.org/10.61838/kman.isslp.4.2.26
Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*. https://doi.org/10.3390/forensicsci2020028
Pohle, J., Nanni, R., & Santaniello, M. (2025). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. *Policy & Internet*. https://doi.org/10.1002/poi3.437
Prahassacitta, V., & Harkrisnowo, H. (2021). Criminal Disinformation in Relation to the Freedom of

Expression in Indonesia: A Critical Study. *Comparative Law Review*. https://doi.org/10.12775/clr.2021.005

Praja, B. A. (2026). Cross-Border Cyberbullying Law Enforcement from a Cyber Law Perspective. *Progressive Law Review*. https://doi.org/10.36448/prolev.v8i1.336

Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive*. https://doi.org/10.30574/ijsra.2025.14.1.0225

Qutieshat, E., Adwan, M. Al, & Khater, M. (2026). Artificial Intelligence in Islamic Law: Ethics, Governance, and Accountability. *Journal of Sustainable Development and Regulatory Issues (JSDERI)*. https://doi.org/10.53955/jsderi.v4i2.236

Rahmadani, S., & Prastyanti, R. (2025). Human Rights and Cybersecurity: Reinforcing Legal Protections for Personal Data. *International Journal of Law Dynamics Review*. https://doi.org/10.62039/ijldr.v3i1.80

Rajendra, J. B., & Thuraisingam, A. (2025). The role of explainability and human intervention in AI decisions: jurisdictional and regulatory aspects. *Information & Communications Technology Law*, *35*, 152–183. https://doi.org/10.1080/13600834.2025.2537514

Rawat, S., Anand, M., Bharti, S., Kumar, V., & Mehta, N.

(2026). Legal aspect of Click-Wrap and Browse-Wrap Agreements in India: A Comparative Analysis and the Way Forward. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2026.v08i01.66948

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors (Basel, Switzerland)*, *23*. https://doi.org/10.3390/s23084060

Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam*. https://doi.org/10.54471/dakwatuna.v7i2.1202

Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*. https://doi.org/10.4236/jcc.2021.98006

Santos, A., Cazzamatta, R., & Napolitano, C. J. (2025). Holding platforms accountable in the fight against misinformation: A cross-national analysis of state-established content moderation regulations. *International Communication Gazette*, *87*, 729–750. https://doi.org/10.1177/17480485251348550

Sari, A., & Herman, K. (2025). Transforming Cybercriminal Law Governance through an Interdisciplinary Approach as an Effort to Achieve

Global Prosperity. *Greenation International Journal of Law and Social Sciences*. https://doi.org/10.38035/gijlss.v3i3.587

Satbayeva, A., Alimbetova, A., & Beissenbayeva, M. (2024). CYBERCRIME CHALLENGES: EXPERIENCE OF INTERNATIONAL COOPERATION. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*. https://doi.org/10.52026/2788-5291_2024_78_3_211

Satyo, B. K., M.Kn, Agung, B., & Prasetyo, Y. (2026). Artificial Intelligence and the Future of Human Rights: Legal Accountability for Algorithmic Decision-Making in Democratic Societies. *International Journal of Law and Social Sciences*. https://doi.org/10.65960/ijlss.2.1.2026.12

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marque´s, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Gov. Inf. Q.*, *39*, 101679. https://doi.org/10.1016/j.giq.2022.101679

Schmitt, M., & Flechais, I. (2023). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*. https://doi.org/10.1007/s10462-024-10973-2

Shehu, V. P., & Shehu, V. (2023). Human rights in the technology era – Protection of data rights. *European Journal of Economics, Law and Social Sciences*, *7*, 1–10. https://doi.org/10.2478/ejels-2023-0001

Shyshenko, A. (2025). Digital evidences in criminal proceedings: problems of authenticity and admissibility. *Analytical and Comparative Jurisprudence*. https://doi.org/10.24144/2788-6018.2025.05.3.46

Simu, S. J., & Zaman, F. (2023). Advanced Cybersecurity Strategies for Protecting Critical Infrastructure: Strengthening the Backbone of National Security. *International Journal of Scientific Research and Management (IJSRM)*. https://doi.org/10.18535/ijsrm/v11i12.ec07

Situmeang, S., Kamilia, E. R., Lutfiyah, N., & Aurora, D. M. (2026). Enforcement of the universality principle in combating cybercrime as a transnational crime. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*. https://doi.org/10.35295/sz.iisl.2411

Solodovnik, V. (2026). International legal assistance in criminal cases: current state, problems and development prospects. *Международное право и международные организации / International Law and International Organizations*. https://doi.org/10.7256/2454-0633.2026.1.78653

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. *ERA Forum*, *23*, 101–108. https://doi.org/10.1007/s12027-022-00707-8

Sˇramel, B., & Michal, S. (2025). From Liberty to Liability: EU Responses to the Abuse of Freedom of Expression Online. *Social Sciences*. https://doi.org/10.3390/socsci14090557

Stepanov, O., & Stepanov, M. (2026). Approaches to the legal regulation of artificial intelligence application in law enforcement. *Law Enforcement Review*. https://doi.org/10.52468/2542-1514.2025.9(4).15-25

Sukirno, Lisdiyono, E., & Mulyani, S. (2021). Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website. *International Journal of Criminology and Sociology*. https://doi.org/10.6000/1929-4409.2021.10.105

Sukma, I. M. (2026). Partnerships without polycentricity? Cybersecurity governance in the Indo-Pacific. *Society Register*. https://doi.org/10.14746/sr.53184

Sunardi, H., Jamaludin, J., Amrulloh, M. A., & Ulya, D. H. (2026). Digital Evidence And Its Challenges In Indonesian Civil Law. *Journal of Law, Politic and Humanities*. https://doi.org/10.38035/jlph.v6i4.3232

Syahmi, T. F., & Subekti, S. (2026). Binding Power of Contracts Formed Through Click-Wrap And Browse Wrap Mechanisms in the Perspective of Indonesian Contract Law. *Journal of Law, Politic and Humanities*. https://doi.org/10.38035/jlph.v6i4.3409

Syahmi, T. F., Wardhono, A., Borman, M., & Prawesthi, W. (2026). Legal Certainty and Evidentiary Strength of Digital Signatures in Electronic Contracts under Indonesian Law. *AL-MANHAJ: Jurnal Hukum dan*

Pranata Sosial Islam. https://doi.org/10.37680/almanhaj.v8i1.8904

Tan, Y. N., Alhakim, A., & Nurlaily, N. (2026). Human Rights Protection in the Digital Sphere: The Problematics of Legal Certainty and Its Relevance to the SDGs. *SIGn Jurnal Hukum*. https://doi.org/10.37276/sjh.v8i1.652

Taufiqurokhman, Sara, R., Suseno, W., & Zakaria, R. M. (2025). Cross-Border Consumer Disputes in the Digital Marketplace: Rethinking Jurisdiction and Law in Global E-Commerce Governance. *Legalis : Journal of Law Review*. https://doi.org/10.61978/legalis.v3i4.1122

Tebenkova, V. (2024). International Legal Principles for Establishing the Jurisdiction of States in Cyberspace. *Actual Problems of Russian Law*. https://doi.org/10.17803/1994-1471.2024.162.5.177-191

Tito, N. W., Putri, Y. M., Zamansyah, F. A., & Kadir, S. A. (2026). THE PRINCIPLE OF CONSENSUALISM IN THE FORMATION OF DIGITAL STANDARD CONTRACTS: A STUDY ON THE MECHANISM OF CLICK-WRAP AGREEMENTS ON PAY LATER PLATFORMS IN INDONESIA. *HERMENEUTIKA : Jurnal Ilmu Hukum*. https://doi.org/10.33603/hermeneutika.v10i2.12548

Tobing, A. N., & Fitria, A. (2025). Jurisdiction and Locus Delicti of Transnational Cybercrime: a Normative Study Of International Law and Indonesian Telematics Law. *Interdisciplinary Social Studies*.

https://doi.org/10.55324/iss.v5i1.951
Touria, M. (2025). Cybersecurity as a Legal and Social Pillar for Protecting Digital Rights and Enhancing Trust in the Digital Space. *Science, Education and Innovations in the Context of Modern Problems*. https://doi.org/10.56334/sei/8.6.28
Van Veldhoven, Z., & Vanthienen, J. (2021). Digital transformation as an interaction-driven perspective between business, society, and technology. *Electronic Markets*, *32*, 629–644. https://doi.org/10.1007/s12525-021-00464-5
Vasylenko, V. (2025). National Cybersecurity in the Context of Society Digitalization: the Role of Police in Protecting Critical Infrastructure. *Bulletin of Kharkiv National University of Internal Affairs*. https://doi.org/10.32631/v.2025.2.33
Vrabec, H. (2021). *Data Subject Rights under the GDPR*. https://doi.org/10.1093/oso/9780198868422.001.0001
Wang, X., Wu, Y., Ji, X., & Fu, H. (2024). Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. *Frontiers in Artificial Intelligence*, *7*. https://doi.org/10.3389/frai.2024.1320277
Whitty, M., & Young, G. (2025). Relational Cybercrimes: A New Way Forward in Classifying Cybercrimes. *IEEE Security & Privacy*, *23*, 80–90. https://doi.org/10.1109/msec.2025.3576909
Widayanti, T., Dwi, A., Nuril, A., Haris, Z., Djafar, E., & Zulfan, M. (2025). ENHANCING CYBERSECURITY AND LEGAL INTEGRATION: REFORMING

INDONESIA'S CYBER LAW TO FOSTER SUSTAINABLE GROWTH IN THE DIGITAL ECONOMY. *Diponegoro Law Review*. https://doi.org/10.14710/dilrev.10.1.2025.105-119

Wu, Z. (2025). Jurisdictional Conflicts and Applicable Law in Cross-Border E-Commerce: A Comparative Study on Consumer Protection. *Elder Law*. https://doi.org/10.47297/wspelwsp2515-824411.20250902

Zarra, A. (2026). Experimentalism beyond ex ante regulation: A law and economics perspective on AI regulatory sandboxes. *Cambridge Forum on AI: Law and Governance*. https://doi.org/10.1017/cfl.2025.10039

Zhuang, J. (2026). The Connection Path Between International Criminal Law Governance and Network Information Law for Transnational Cybercrimes under Data Sovereignty Conflicts. *Lecture Notes in Education Psychology and Public Media*. https://doi.org/10.54254/2753-7048/2026.zju31772

Zisu, M.-A. (2025). Personal Data Protection in the Era of Artificial Intelligence: Legal Challenges and Solutions. *Anuarul Universitatii Petre Andrei din Iasi - Fascicula: Drept, Stiinte Economice, Stiinte Politice*. https://doi.org/10.63331/upalaw/34/23