PENGANTAR HUKUM TEKNOLOGI INFORMASI

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

PENGANTAR HUKUM TEKNOLOGI INFORMASI

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

PENGANTAR HUKUM TEKNOLOGI INFORMASI

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

yash media
IKAPI
IKATAN PENERBIT INDONESIA

PENGANTAR HUKUM TEKNOLOGI INFORMASI

Editor : Muhammad Fairuzabadi
Tata Letak : Tim Yash Media
Rancang Sampul : Darmas
Halaman : xxii + 508 hlm.
Ukuran : 15 x 23 cm
Cetakan Pertama : 2026

ISBN : 978-634-7327-91-8

Diterbitkan pertama kali oleh :
Yash Media
Anggota IKAPI 205/DIY/2025
Dusun Tapan No.03 RT06, RW.01, Karanglo, Purwomartani,
Kec. Kalasan, Kabupaten Sleman, DI Yogyakarta 55571
Email: yashmediaco@gmail.com
https://yashmedia.id/

Kata Pengantar

Puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga buku referensi berjudul *Pengantar Hukum Teknologi Informasi* ini dapat diselesaikan. Buku ini disusun sebagai salah satu sumber pembelajaran untuk membantu pembaca memahami hubungan antara perkembangan teknologi informasi dan dinamika hukum yang mengaturnya.

Perkembangan teknologi digital telah membawa perubahan besar dalam kehidupan masyarakat. Internet, media sosial, kecerdasan buatan, perdagangan elektronik, teknologi finansial, komputasi awan, dan berbagai platform digital telah menciptakan pola interaksi, transaksi, serta hubungan hukum yang semakin kompleks. Kemajuan tersebut memberikan banyak manfaat, tetapi juga menimbulkan berbagai persoalan, seperti penyalahgunaan data pribadi, penipuan digital, pelanggaran hak cipta, serangan siber, sengketa transaksi elektronik, serta ketidakjelasan tanggung jawab para pihak dalam ekosistem digital.

Buku ini membahas hukum teknologi informasi secara bertahap dan sistematis. Pembahasan diawali dengan pengenalan konsep, ruang lingkup, sejarah perkembangan, serta prinsip-prinsip hukum siber. Bagian selanjutnya menguraikan sistem hukum informasi dan transaksi elektronik, kedudukan informasi serta dokumen elektronik, pelindungan data pribadi, perlindungan konsumen digital, kejahatan siber, pembuktian dan forensik digital, serta kekayaan intelektual dalam lingkungan digital.

Pembahasan juga mencakup aspek hukum perdagangan elektronik, teknologi finansial, ekonomi digital, kebijakan keamanan siber nasional dan internasional, serta etika dan tanggung jawab dalam penggunaan teknologi. Pada bagian akhir, disajikan analisis sejumlah kasus hukum teknologi informasi di Indonesia agar pembaca dapat menghubungkan konsep dan ketentuan hukum dengan persoalan yang muncul dalam praktik.

Buku ini terutama ditujukan bagi mahasiswa, dosen, peneliti, praktisi hukum, pengelola sistem informasi, pelaku usaha digital, serta masyarakat yang ingin memperoleh pemahaman dasar mengenai hukum teknologi informasi. Penyajian materi diupayakan menggunakan bahasa yang sistematis dan mudah dipahami tanpa mengabaikan ketepatan konsep serta

dasar hukum yang relevan. Dengan pendekatan tersebut, buku ini diharapkan dapat digunakan sebagai referensi dalam kegiatan pembelajaran, penelitian, diskusi akademik, maupun pengambilan keputusan yang berkaitan dengan aktivitas digital.

Penyusunan buku ini tidak terlepas dari dukungan, kontribusi, dan pemikiran berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada seluruh pihak yang telah membantu dalam proses penyusunan, penelaahan, penyuntingan, dan penerbitan buku ini. Penghargaan juga disampaikan kepada para akademisi, praktisi, lembaga pemerintah, dan organisasi yang karya serta kebijakannya menjadi sumber penting dalam pengembangan pembahasan buku.

Penulis menyadari bahwa hukum teknologi informasi merupakan bidang yang berkembang sangat cepat. Perubahan teknologi, regulasi, kebijakan, dan praktik penegakan hukum dapat terjadi dalam waktu yang relatif singkat. Oleh sebab itu, buku ini masih memiliki keterbatasan dan memerlukan penyempurnaan secara berkelanjutan. Kritik dan saran yang membangun sangat diharapkan sebagai bahan perbaikan untuk edisi berikutnya.

Akhir kata, semoga buku *Pengantar Hukum Teknologi Informasi* ini dapat memberikan manfaat, memperluas wawasan, dan meningkatkan kesadaran hukum pembaca dalam menggunakan serta mengembangkan teknologi secara aman, bertanggung jawab, beretika, dan sesuai dengan ketentuan hukum yang berlaku.

Sleman, Juli 2026

Penulis

Daftar Isi

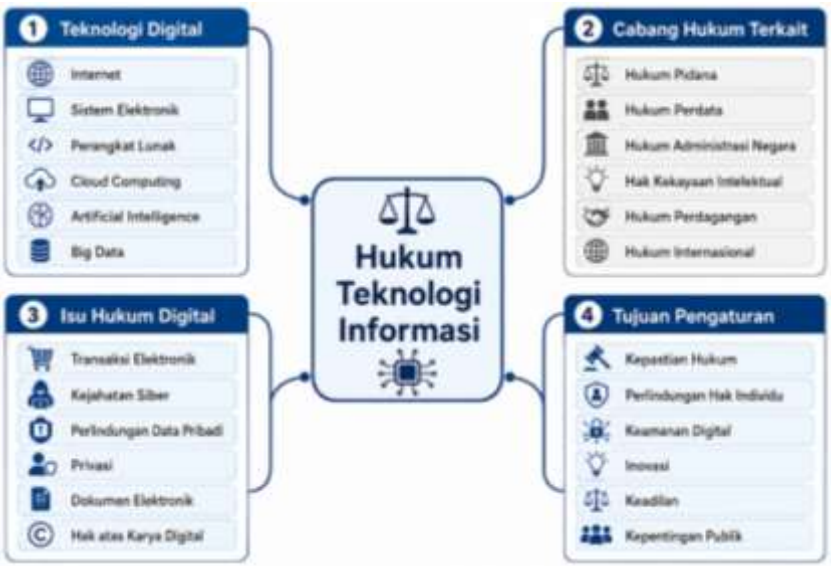
Daftar Gambar

Daftar Tabel

Bab 1
Pengantar Hukum Teknologi Informasi

1.1 Definisi Hukum Teknologi Informasi

Hukum Teknologi Informasi, atau yang juga dikenal sebagai *Information Technology Law* (*IT Law*), merupakan bidang hukum yang mengatur berbagai aspek hukum yang berkaitan dengan penggunaan, pengembangan, pengelolaan, dan penyebaran teknologi informasi dan komunikasi. Bidang ini lahir karena aktivitas manusia semakin banyak dilakukan melalui sistem elektronik, jaringan komputer, internet, perangkat lunak, komputasi awan (*cloud computing*), kecerdasan buatan (*artificial intelligence*), *big data*, serta berbagai layanan digital lainnya. Perkembangan tersebut menimbulkan hubungan hukum baru yang membutuhkan kepastian, perlindungan, dan mekanisme pertanggungjawaban yang jelas (Murray, 2019; Ramli, 2004).



Gambar 1.1: Peta konseptual ruang kajian Hukum Teknologi Informasi

Secara substansial, Hukum Teknologi Informasi tidak berdiri sendiri sebagai disiplin hukum yang terlepas dari sistem hukum yang telah ada. Bidang ini merupakan hasil pertemuan antara berbagai cabang hukum, seperti hukum

pidana, hukum perdata, hukum administrasi negara, hukum hak kekayaan intelektual, hukum perdagangan, hukum perlindungan konsumen, hukum ketenagakerjaan, dan hukum internasional. Namun, karena teknologi informasi memiliki karakter yang dinamis, transnasional, dan sering kali melampaui batas yurisdiksi negara, Hukum Teknologi Informasi menuntut pendekatan yang lebih adaptif, responsif, dan multidisipliner (Murray, 2019; Reed, 2012).

Salah satu ciri penting Hukum Teknologi Informasi adalah sifatnya yang *technology-neutral* sekaligus *technology-responsive*. Prinsip *technology-neutral* berarti aturan hukum sebaiknya tidak terlalu bergantung pada satu jenis teknologi tertentu, sehingga tetap dapat digunakan meskipun bentuk teknologinya berubah. Sementara itu, prinsip *technology-responsive* menunjukkan bahwa hukum tetap harus mampu merespons risiko, dampak, dan kebutuhan baru yang muncul akibat perkembangan teknologi. Dalam praktiknya, hukum sering kali tertinggal dari laju inovasi teknologi. Kondisi ini dikenal sebagai *technology gap*, yaitu kesenjangan antara perkembangan teknologi dengan kemampuan hukum untuk mengaturnya secara tepat waktu dan efektif (Brownsword & Goodwin, 2012; Murray, 2019).

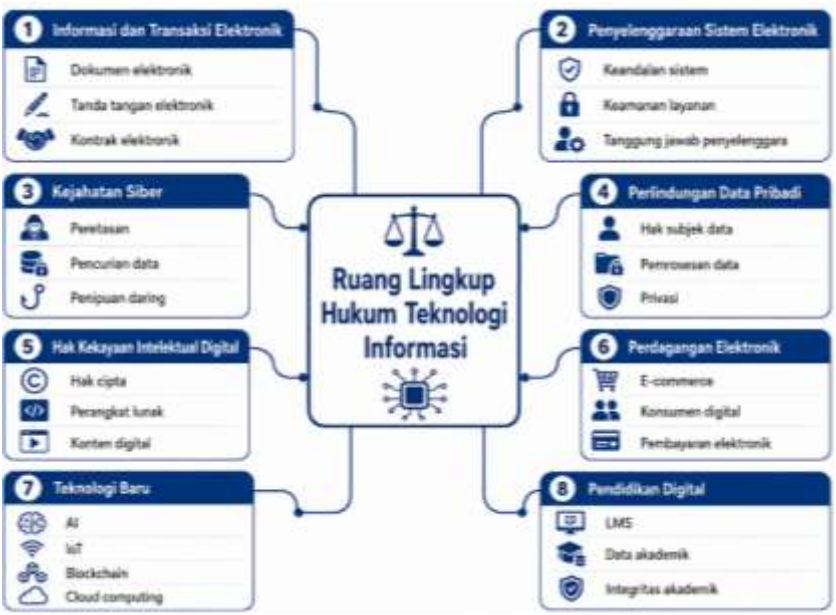
Di Indonesia, pengakuan terhadap Hukum Teknologi Informasi semakin kuat dengan lahirnya berbagai peraturan perundang-undangan yang mengatur aktivitas digital. Salah satu regulasi utama adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan diubah kembali melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, pelindungan data pribadi secara khusus diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Keberadaan regulasi tersebut menjadi dasar penting dalam mengatur transaksi elektronik, dokumen elektronik, tanda tangan elektronik, penyelenggaraan sistem elektronik, pelindungan data pribadi, serta penanganan berbagai bentuk penyalahgunaan teknologi digital (Republik Indonesia, 2008, 2016sb, 2019b, 2022, 2024).

Dengan demikian, Hukum Teknologi Informasi dapat dipahami sebagai instrumen normatif yang berperan dalam menjaga keseimbangan antara inovasi teknologi, kepastian hukum, perlindungan hak individu, keamanan sistem elektronik, dan kepentingan publik di era digital. Kehadiran hukum

dalam bidang teknologi informasi tidak hanya bertujuan untuk memberikan sanksi terhadap penyalahgunaan teknologi, tetapi juga untuk membangun ekosistem digital yang aman, terpercaya, adil, dan bertanggung jawab.

1.2 Ruang Lingkup Hukum Teknologi Informasi

Ruang lingkup Hukum Teknologi Informasi mencakup berbagai aspek hukum yang berkaitan dengan penciptaan, penggunaan, pengelolaan, penyebaran, dan pemanfaatan teknologi informasi dalam kehidupan masyarakat. Perkembangan teknologi digital telah melahirkan berbagai aktivitas baru yang sebelumnya belum sepenuhnya dikenal dalam sistem hukum konvensional, seperti transaksi elektronik, komunikasi digital, penyelenggaraan sistem elektronik, komputasi awan (*cloud computing*), kecerdasan buatan (*artificial intelligence*), serta pengolahan data dalam skala besar (*big data*). Oleh karena itu, Hukum Teknologi Informasi hadir untuk memberikan kepastian hukum terhadap hubungan hukum yang terjadi di ruang digital (Murray, 2019; Ramli, 2004).



Gambar 1.2: Ruang Lingkup Hukum Teknologi Informasi

Salah satu ruang lingkup utama Hukum Teknologi Informasi adalah pengaturan mengenai informasi dan transaksi elektronik. Bidang ini

mencakup legalitas informasi elektronik, dokumen elektronik, tanda tangan elektronik, kontrak elektronik, pembayaran digital, serta pembuktian elektronik dalam proses hukum. Pengaturan ini bertujuan untuk memastikan bahwa aktivitas ekonomi, sosial, administratif, dan komunikasi yang dilakukan melalui media elektronik memiliki kedudukan hukum yang jelas. Di Indonesia, aspek ini diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 (Republik Indonesia, 2008, 2016, 2024).

Ruang lingkup berikutnya adalah penyelenggaraan sistem elektronik. Sistem elektronik menjadi infrastruktur utama dalam berbagai layanan digital, baik yang diselenggarakan oleh pemerintah, lembaga pendidikan, pelaku usaha, maupun masyarakat. Pengaturan terhadap penyelenggaraan sistem elektronik mencakup aspek keandalan, keamanan, tanggung jawab penyelenggara, perlindungan pengguna, pengelolaan data, dan kewajiban menjaga sistem agar berjalan secara aman dan terpercaya. Dalam konteks ini, penyelenggara sistem elektronik memiliki tanggung jawab untuk memastikan bahwa layanan digital yang digunakan masyarakat tidak menimbulkan kerugian hukum, teknis, maupun sosial (Republik Indonesia, 2019a).

Hukum Teknologi Informasi juga mencakup pengaturan mengenai kejahatan siber (*cybercrime*). Perkembangan internet dan sistem informasi telah melahirkan berbagai bentuk pelanggaran hukum, seperti akses tanpa hak terhadap sistem elektronik, pencurian data, penipuan daring, penyebaran *malware*, pencemaran nama baik melalui media elektronik, penyebaran konten melanggar hukum, serta serangan siber terhadap infrastruktur digital. Dalam bidang ini, hukum berfungsi sebagai instrumen untuk mencegah, menindak, dan memberikan perlindungan hukum terhadap korban kejahatan siber, sekaligus menjaga keamanan ruang digital (Reed, 2012).

Aspek penting lainnya adalah pelindungan data pribadi dan privasi. Dalam era ekonomi digital, data telah menjadi aset strategis yang memiliki nilai sosial, ekonomi, dan hukum. Data pribadi dapat digunakan untuk kepentingan layanan, analisis perilaku pengguna, personalisasi sistem, hingga pengambilan keputusan berbasis algoritma. Namun, pengumpulan, penyimpanan, penggunaan, dan penyebaran data pribadi tanpa dasar hukum yang sah dapat menimbulkan pelanggaran terhadap hak privasi individu.

Oleh sebab itu, pelindungan data pribadi menjadi bagian penting dalam Hukum Teknologi Informasi untuk menjamin keamanan data, hak subjek data pribadi, dan tanggung jawab pihak yang memproses data (Republik Indonesia, 2022b; Solove & Schwartz, 2020).

Ruang lingkup Hukum Teknologi Informasi juga mencakup perlindungan hak kekayaan intelektual di lingkungan digital. Kemajuan teknologi memungkinkan karya cipta, perangkat lunak, basis data, desain digital, video, musik, gambar, dan berbagai konten digital disebarluaskan dengan sangat cepat. Kondisi ini memberi peluang bagi perkembangan ekonomi kreatif, tetapi juga meningkatkan risiko pelanggaran hak cipta, pembajakan perangkat lunak, penggunaan karya tanpa izin, dan distribusi konten digital secara ilegal. Oleh karena itu, pengaturan hak kekayaan intelektual di ruang digital diperlukan untuk melindungi hak moral dan hak ekonomi pencipta serta mendorong pemanfaatan karya digital secara sah (Lessig, 2006; Ramli, 2004).

Selain itu, Hukum Teknologi Informasi mencakup perdagangan melalui sistem elektronik atau *e-commerce*. Aktivitas jual beli daring, pemasaran digital, layanan platform, pembayaran elektronik, perlindungan konsumen digital, dan tanggung jawab pelaku usaha merupakan bagian dari ruang lingkup ini. Pengaturan perdagangan elektronik diperlukan agar transaksi yang dilakukan melalui media digital memiliki kepastian hukum, melindungi konsumen dari praktik yang merugikan, serta memberikan kejelasan tanggung jawab bagi pelaku usaha dan penyelenggara platform digital (Republik Indonesia, 2019b).

Secara lebih luas, ruang lingkup Hukum Teknologi Informasi tidak hanya terbatas pada transaksi elektronik, keamanan siber, pelindungan data pribadi, dan hak kekayaan intelektual, tetapi juga mencakup tata kelola internet, tanggung jawab platform digital, komputasi awan, kecerdasan buatan, *Internet of Things* (*IoT*), *blockchain*, aset digital, dan teknologi berbasis algoritma. Setiap perkembangan teknologi tersebut dapat melahirkan hubungan hukum baru antara individu, organisasi, pelaku usaha, dan negara. Karena itu, Hukum Teknologi Informasi dituntut untuk selalu adaptif terhadap perubahan teknologi yang berlangsung cepat dan sering kali melampaui batas yurisdiksi negara (Brownsword & Goodwin, 2012; Murray, 2019).

Dalam konteks pendidikan, ruang lingkup Hukum Teknologi Informasi juga berkaitan dengan pemanfaatan teknologi digital dalam proses pembelajaran, penelitian, dan pengelolaan institusi pendidikan. Penggunaan platform pembelajaran daring, sistem manajemen pembelajaran (*Learning Management System*), perpustakaan digital, penyimpanan data akademik berbasis komputasi awan, serta pemanfaatan kecerdasan buatan dalam kegiatan akademik menimbulkan berbagai konsekuensi hukum. Persoalan seperti pelindungan data pribadi mahasiswa dan dosen, kepemilikan hak cipta atas materi pembelajaran digital, keabsahan dokumen akademik elektronik, keamanan sistem informasi kampus, dan etika penggunaan kecerdasan buatan menjadi bagian dari kajian Hukum Teknologi Informasi di sektor pendidikan.

Transformasi digital di bidang pendidikan juga memunculkan tantangan terkait integritas akademik dan tata kelola pendidikan berbasis teknologi. Penggunaan aplikasi berbasis kecerdasan buatan untuk menyusun tugas, karya ilmiah, maupun penelitian menimbulkan pertanyaan mengenai batas antara pemanfaatan teknologi sebagai alat bantu pembelajaran dan potensi pelanggaran etika akademik, seperti plagiarisme, manipulasi karya, atau misrepresentasi kontribusi akademik. Institusi pendidikan memiliki tanggung jawab untuk memastikan bahwa teknologi yang digunakan dalam kegiatan akademik memenuhi prinsip keamanan, keandalan, aksesibilitas, perlindungan data, dan penghormatan terhadap hak-hak pengguna.

Ruang lingkup Hukum Teknologi Informasi menunjukkan bahwa hukum tidak hanya berfungsi sebagai instrumen pengendalian terhadap penyalahgunaan teknologi, tetapi juga sebagai dasar untuk membangun ekosistem digital yang aman, tertib, inklusif, dan berkeadilan. Pemahaman terhadap ruang lingkup ini penting agar masyarakat, pelaku usaha, penyelenggara sistem elektronik, institusi pendidikan, dan pemerintah dapat memanfaatkan teknologi secara bertanggung jawab sesuai dengan prinsip hukum yang berlaku.

1.3 Hubungan Hukum, Teknologi, dan Masyarakat Digital

Hukum, teknologi, dan masyarakat merupakan tiga elemen yang saling memengaruhi dan berkembang secara dinamis. Dalam konteks masyarakat

digital, perkembangan teknologi informasi tidak hanya membawa perubahan pada aspek teknis dan ekonomi, tetapi juga mengubah pola komunikasi, interaksi sosial, budaya, politik, pendidikan, dan aktivitas sehari-hari. Transformasi tersebut melahirkan berbagai hubungan hukum baru yang sebelumnya belum sepenuhnya dikenal dalam masyarakat konvensional. Oleh karena itu, norma, regulasi, dan mekanisme penegakan hukum perlu menyesuaikan diri dengan karakteristik ruang digital yang cepat, terbuka, dan lintas batas (Castells, 2010; Murray, 2019).

Teknologi pada dasarnya dapat dipahami sebagai alat yang penggunaannya bergantung pada tujuan, nilai, dan kepentingan manusia. Di satu sisi, teknologi informasi memberikan kemudahan dalam komunikasi, akses informasi, transaksi ekonomi, pelayanan publik, pendidikan, penelitian, dan inovasi bisnis. Di sisi lain, teknologi juga dapat menimbulkan risiko hukum dan sosial, seperti penyebaran informasi palsu, pelanggaran privasi, kejahatan siber, eksploitasi data pribadi, pelanggaran hak cipta, serta penyalahgunaan kecerdasan buatan (*artificial intelligence*). Kondisi ini menunjukkan bahwa perkembangan teknologi selalu diikuti oleh kebutuhan terhadap instrumen hukum yang mampu menjaga keseimbangan antara inovasi dan perlindungan kepentingan masyarakat (Brownsword & Goodwin, 2012; Reed, 2012).

Hukum memiliki fungsi sebagai sarana pengendalian sosial (*social control*) sekaligus sebagai sarana pembaruan atau rekayasa sosial (*social engineering*). Dalam masyarakat digital, hukum tidak hanya berperan memberikan sanksi terhadap pelanggaran yang terjadi di ruang siber, tetapi juga mengarahkan pemanfaatan teknologi agar selaras dengan nilai keadilan, keamanan, kemanfaatan, kepastian hukum, dan penghormatan terhadap hak asasi manusia. Dengan adanya hukum, aktivitas digital diharapkan dapat berlangsung secara tertib dan bertanggung jawab. Hukum juga berperan membangun kepercayaan (*trust*) yang menjadi fondasi penting dalam ekosistem digital, terutama dalam transaksi elektronik, layanan digital, dan pengelolaan data pribadi (Lessig, 2006; Murray, 2019).

Hubungan antara hukum dan teknologi sering kali ditandai oleh adanya kesenjangan antara kecepatan inovasi dan kemampuan regulasi untuk menyesuaikan diri. Teknologi berkembang sangat cepat, sedangkan proses pembentukan hukum membutuhkan waktu yang lebih panjang karena harus melalui kajian akademik, penyusunan kebijakan, pembahasan legislasi,

konsultasi publik, dan pertimbangan berbagai kepentingan. Fenomena ini sering disebut sebagai *lag of law* atau *technology gap*, yaitu kondisi ketika hukum tertinggal dari perkembangan teknologi yang hendak diaturnya. Oleh karena itu, pendekatan hukum yang adaptif, berbasis prinsip, dan berorientasi pada masa depan menjadi penting dalam menghadapi perubahan teknologi yang terus berlangsung (Brownsword & Goodwin, 2012; Reed, 2012).

Masyarakat digital sebagai subjek utama dalam pemanfaatan teknologi juga memiliki peran penting dalam pembentukan dan efektivitas hukum teknologi informasi. Tingkat literasi digital, kesadaran hukum, etika bermedia, dan budaya penggunaan teknologi akan menentukan keberhasilan suatu regulasi. Regulasi yang baik tidak akan berjalan efektif apabila masyarakat tidak memahami hak, kewajiban, dan risiko hukum dalam menggunakan teknologi. Karena itu, pembangunan masyarakat digital tidak cukup hanya bertumpu pada infrastruktur teknologi, tetapi juga perlu didukung oleh literasi hukum, etika digital, dan tanggung jawab sosial dalam menggunakan teknologi informasi.

Dalam konteks Indonesia, hubungan antara hukum, teknologi, dan masyarakat digital tampak dalam berbagai pengaturan hukum yang mengatur aktivitas digital, seperti informasi elektronik, transaksi elektronik, penyelenggaraan sistem elektronik, pelindungan data pribadi, dan larangan terhadap penyalahgunaan teknologi. Undang-Undang Informasi dan Transaksi Elektronik menjadi salah satu dasar penting dalam pengaturan aktivitas digital, sedangkan Undang-Undang Pelindungan Data Pribadi memberikan dasar hukum bagi perlindungan hak individu atas data pribadi. Kedua ranah pengaturan tersebut menunjukkan bahwa hukum berperan dalam memberikan kepastian hukum, melindungi hak masyarakat, dan membangun tata kelola digital yang lebih bertanggung jawab (Republik Indonesia, 2008, 2016, 2022, 2024).

Dalam konteks pendidikan, hubungan antara hukum, teknologi, dan masyarakat digital menjadi semakin penting untuk dipahami oleh sivitas akademika. Perguruan tinggi tidak hanya berfungsi sebagai pengguna teknologi, tetapi juga sebagai pusat pengembangan ilmu pengetahuan, inovasi, dan pembentukan karakter masyarakat digital yang bertanggung jawab. Pemanfaatan teknologi dalam pembelajaran, penelitian, publikasi ilmiah, administrasi akademik, dan pengelolaan data pendidikan

menimbulkan berbagai implikasi hukum. Oleh karena itu, pemahaman terhadap hukum teknologi informasi diperlukan agar penggunaan teknologi di lingkungan akademik tetap sejalan dengan prinsip kejujuran akademik, perlindungan data, penghormatan hak cipta, dan etika penggunaan teknologi.

Pemahaman mengenai hubungan antara hukum, teknologi, dan masyarakat digital menunjukkan bahwa regulasi tidak dapat dipandang semata-mata sebagai instrumen pembatas atau pengendalian. Regulasi juga berfungsi sebagai mekanisme untuk mendorong inovasi yang bertanggung jawab, melindungi kepentingan publik, dan membangun kepercayaan dalam masyarakat digital. Dengan hubungan yang seimbang antara hukum, teknologi, dan masyarakat, transformasi digital dapat diarahkan agar memberi manfaat yang luas tanpa mengabaikan keadilan, keamanan, dan hak-hak individu.

1.4 Peran Hukum dalam Mengatur Aktivitas Digital

Transformasi digital telah mengubah hampir seluruh aspek kehidupan manusia, mulai dari komunikasi, perdagangan, pendidikan, layanan kesehatan, administrasi pemerintahan, hingga hubungan sosial sehari-hari. Aktivitas yang sebelumnya dilakukan secara konvensional kini banyak beralih ke ruang digital melalui internet, sistem elektronik, aplikasi, platform digital, komputasi awan (*cloud computing*), dan berbagai layanan berbasis teknologi informasi. Perubahan tersebut memberikan manfaat berupa efisiensi, kecepatan, kemudahan akses, dan perluasan jangkauan layanan. Namun, di sisi lain, perkembangan teknologi juga menimbulkan berbagai persoalan hukum yang memerlukan pengaturan yang jelas dan memadai (Murray, 2019; Reed, 2012).

Hukum memiliki peran strategis dalam mengatur aktivitas digital agar pemanfaatan teknologi informasi dapat berlangsung secara tertib, aman, adil, dan bertanggung jawab. Keberadaan hukum diperlukan untuk menciptakan keseimbangan antara kebebasan berinovasi dengan perlindungan terhadap hak dan kepentingan masyarakat. Tanpa pengaturan yang memadai, ruang digital berpotensi menimbulkan ketidakpastian, penyalahgunaan teknologi, pelanggaran privasi, penyebaran informasi yang merugikan, dan berbagai bentuk pelanggaran hak individu maupun organisasi (Brownsword & Goodwin, 2012; Lessig, 2006).

Salah satu peran utama hukum dalam aktivitas digital adalah menciptakan kepastian hukum. Kepastian hukum memberikan kejelasan mengenai hak, kewajiban, tanggung jawab, serta konsekuensi hukum dari setiap tindakan yang dilakukan melalui media elektronik. Dalam transaksi elektronik, misalnya, hukum memberikan dasar bagi pengakuan informasi elektronik, dokumen elektronik, tanda tangan elektronik, kontrak elektronik, serta alat bukti elektronik. Dengan adanya kepastian hukum, masyarakat, pelaku usaha, dan penyelenggara sistem elektronik memiliki dasar yang jelas dalam melakukan aktivitas digital (Republik Indonesia, 2008, 2016, 2024).

Selain menciptakan kepastian hukum, hukum juga berperan memberikan perlindungan terhadap hak dan kepentingan para pihak yang terlibat dalam aktivitas digital. Data dan informasi telah menjadi aset penting dalam ekosistem digital, sehingga rentan terhadap pencurian, penyalahgunaan, pengungkapan tanpa izin, dan pemrosesan yang tidak sesuai dengan tujuan. Oleh karena itu, hukum hadir untuk memberikan perlindungan terhadap privasi, data pribadi, keamanan informasi, dan hak-hak pengguna teknologi informasi. Perlindungan ini penting agar masyarakat dapat menggunakan teknologi secara aman dan percaya terhadap layanan digital yang digunakan (Republik Indonesia, 2022b; Solove & Schwartz, 2020).

Hukum juga berperan menjaga ketertiban dan keamanan di ruang digital. Internet yang bersifat terbuka dan lintas batas memberikan peluang bagi munculnya berbagai bentuk kejahatan siber (*cybercrime*), seperti akses tanpa hak terhadap sistem elektronik, penipuan daring, pencurian identitas, penyebaran *malware*, manipulasi informasi, dan serangan terhadap sistem elektronik. Dalam kondisi tersebut, hukum berfungsi sebagai instrumen pengendalian sosial (*social control*) yang menetapkan batas perilaku yang diperbolehkan dan yang dilarang dalam ruang digital. Melalui mekanisme penegakan hukum, pelaku pelanggaran dapat dimintai pertanggungjawaban sehingga masyarakat memperoleh perlindungan yang lebih baik (Reed, 2012; Republik Indonesia, 2008, 2016, 2024).

Di samping fungsi perlindungan dan pengendalian, hukum juga memiliki peran penting dalam mendukung pertumbuhan ekonomi digital. Kepercayaan merupakan faktor utama dalam perkembangan ekonomi berbasis teknologi. Pelaku usaha, konsumen, investor, dan penyelenggara platform memerlukan jaminan bahwa aktivitas bisnis yang dilakukan melalui media elektronik memiliki dasar hukum yang jelas. Oleh sebab itu,

pengaturan mengenai transaksi elektronik, perdagangan melalui sistem elektronik, perlindungan konsumen digital, keamanan sistem elektronik, dan tata kelola data menjadi bagian penting dalam membangun ekosistem ekonomi digital yang sehat dan berkelanjutan (Murray, 2019; Republik Indonesia, 2019a, 2019b).

Perkembangan teknologi yang berlangsung cepat juga menuntut hukum untuk bersifat adaptif dan responsif. Munculnya teknologi baru seperti kecerdasan buatan (*artificial intelligence*), *Internet of Things* (*IoT*), komputasi awan (*cloud computing*), *blockchain*, aset digital, dan sistem berbasis algoritma menghadirkan tantangan hukum yang sebelumnya belum sepenuhnya dikenal. Dalam situasi tersebut, hukum perlu mampu mengikuti perkembangan teknologi tanpa menghambat inovasi. Regulasi yang terlalu kaku dapat menghambat perkembangan teknologi, sedangkan regulasi yang terlalu longgar dapat menimbulkan ketidakpastian dan meningkatkan risiko penyalahgunaan teknologi (Brownsword & Goodwin, 2012; Murray, 2019).

Hukum juga berfungsi menciptakan akuntabilitas dalam penyelenggaraan aktivitas digital. Setiap individu, pelaku usaha, lembaga pemerintah, maupun penyelenggara sistem elektronik harus bertanggung jawab atas tindakan, keputusan, dan layanan yang diselenggarakan dalam lingkungan digital. Prinsip akuntabilitas menjadi penting karena aktivitas digital sering kali melibatkan banyak pihak, penggunaan data dalam jumlah besar, sistem otomatis, serta proses yang tidak selalu mudah dipahami oleh pengguna. Dengan adanya aturan mengenai tanggung jawab hukum, setiap pihak memiliki kewajiban untuk memastikan bahwa aktivitas digital yang dilakukan tidak merugikan pihak lain dan sesuai dengan prinsip hukum yang berlaku.

Dalam konteks pendidikan, peran hukum dalam mengatur aktivitas digital juga semakin penting. Penggunaan platform pembelajaran daring, sistem informasi akademik, penyimpanan data mahasiswa, perpustakaan digital, publikasi ilmiah, dan aplikasi berbasis kecerdasan buatan menimbulkan berbagai konsekuensi hukum. Persoalan seperti pelindungan data pribadi, hak cipta materi pembelajaran, keabsahan dokumen akademik elektronik, keamanan sistem informasi kampus, dan etika penggunaan teknologi perlu diatur agar kegiatan pendidikan digital berjalan secara aman, tertib, dan bertanggung jawab.

Secara keseluruhan, peran hukum dalam mengatur aktivitas digital tidak hanya terbatas pada pemberian sanksi terhadap pelanggaran. Hukum juga berfungsi sebagai dasar untuk menciptakan kepastian, perlindungan, keamanan, akuntabilitas, dan kepercayaan dalam ekosistem digital. Dengan pengaturan yang tepat, hukum dapat menjaga keseimbangan antara perkembangan inovasi teknologi dan perlindungan terhadap kepentingan masyarakat.

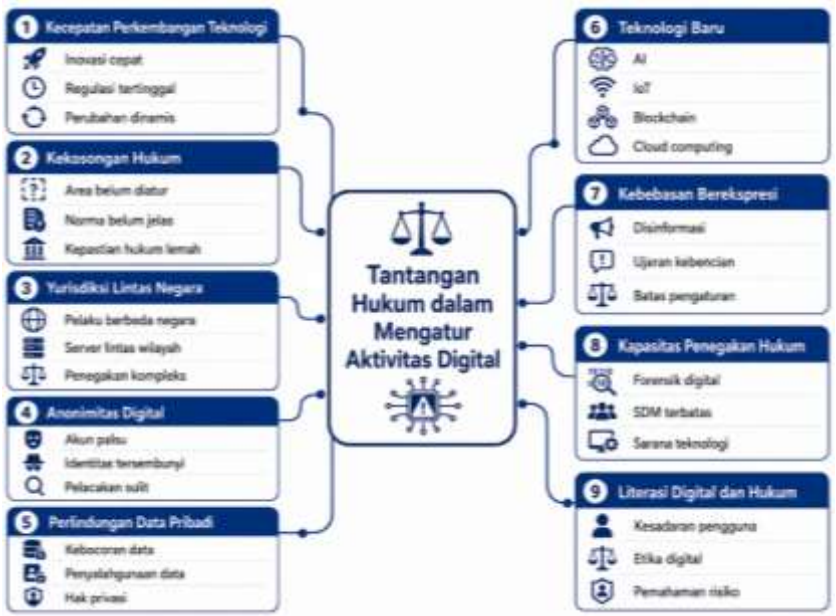
1.5 Tantangan Hukum dalam Mengatur Aktivitas Digital

Perkembangan teknologi informasi yang berlangsung sangat cepat telah membawa perubahan mendasar dalam berbagai aspek kehidupan masyarakat. Aktivitas ekonomi, sosial, pendidikan, pemerintahan, layanan kesehatan, hingga hubungan antarindividu kini banyak dilakukan melalui media digital yang memanfaatkan jaringan internet dan sistem elektronik. Meskipun memberikan berbagai manfaat berupa efisiensi, kemudahan akses, dan perluasan jangkauan layanan, perkembangan tersebut juga menghadirkan tantangan besar bagi sistem hukum dalam menjalankan fungsinya sebagai instrumen pengatur kehidupan masyarakat (Murray, 2019; Reed, 2012).

Salah satu tantangan utama adalah kecepatan perkembangan teknologi yang sering kali melampaui kemampuan hukum untuk menyesuaikan diri. Proses pembentukan peraturan perundang-undangan pada umumnya memerlukan waktu yang relatif panjang karena harus melalui tahapan perencanaan, kajian akademik, pembahasan, pengesahan, dan implementasi. Sebaliknya, inovasi teknologi dapat berkembang dalam waktu yang sangat singkat dan menghasilkan model bisnis, layanan, pola komunikasi, serta bentuk interaksi baru yang sebelumnya belum dikenal dalam sistem hukum. Akibatnya, dapat muncul kekosongan hukum (*legal vacuum*) atau ketidakjelasan pengaturan terhadap teknologi baru yang berkembang di masyarakat (Brownsword & Goodwin, 2012).

Tantangan berikutnya adalah karakteristik ruang digital yang bersifat lintas batas negara (*borderless*). Aktivitas digital tidak selalu terikat pada batas wilayah geografis. Suatu tindakan dapat dilakukan oleh pengguna di satu negara, menggunakan sistem elektronik atau server di negara lain, dan menimbulkan akibat hukum di negara yang berbeda. Kondisi ini menimbulkan persoalan mengenai yurisdiksi, hukum yang berlaku,

kewenangan lembaga penegak hukum, serta mekanisme penyelesaian sengketa atau tindak pidana yang melibatkan unsur lintas negara. Oleh karena itu, kerja sama internasional menjadi faktor penting dalam penegakan hukum di ruang siber (Reed, 2012; Murray, 2019).



Gambar 1.3: Tantangan Hukum dalam Mengatur Aktivitas Digital

Selain persoalan yurisdiksi, identifikasi pelaku juga menjadi tantangan tersendiri dalam aktivitas digital. Penggunaan identitas anonim, akun palsu, teknologi enkripsi, jaringan privat virtual (*virtual private network*), serta berbagai teknik penyamaran identitas menyebabkan proses pelacakan pelaku pelanggaran hukum menjadi lebih kompleks dibandingkan dengan pelanggaran dalam ruang fisik. Aparat penegak hukum dituntut memiliki kemampuan teknis, sumber daya manusia, prosedur investigasi digital, dan teknologi pendukung yang memadai agar dapat menangani kasus digital secara efektif dan tetap sesuai dengan prinsip hukum yang berlaku.

Tantangan lain yang sangat penting berkaitan dengan pelindungan data pribadi dan privasi pengguna. Dalam era ekonomi digital, data telah menjadi sumber daya strategis yang memiliki nilai sosial, ekonomi, dan hukum. Berbagai organisasi, platform digital, lembaga pendidikan, perusahaan, dan institusi pemerintah mengumpulkan, menyimpan, mengolah, serta

memanfaatkan data pengguna untuk berbagai tujuan. Namun, pengelolaan data yang tidak disertai dasar hukum dan mekanisme perlindungan yang memadai dapat menimbulkan risiko kebocoran data, pencurian identitas, penyalahgunaan informasi pribadi, diskriminasi berbasis data, hingga pelanggaran hak privasi individu (Solove & Schwartz, 2020; Republik Indonesia, 2022).

Perkembangan teknologi baru seperti kecerdasan buatan (*artificial intelligence*), *Internet of Things* (*IoT*), *blockchain*, komputasi awan (*cloud computing*), dan sistem berbasis algoritma juga menimbulkan tantangan hukum yang semakin kompleks. Penggunaan kecerdasan buatan, misalnya, menimbulkan pertanyaan mengenai transparansi algoritma, keadilan hasil keputusan, bias data, pelindungan data pribadi, serta pihak yang harus bertanggung jawab apabila sistem menghasilkan keputusan yang merugikan. Demikian pula, teknologi *blockchain* menghadirkan tantangan terkait pengawasan, pertanggungjawaban, validitas transaksi, dan mekanisme penyelesaian sengketa karena sifatnya yang terdesentralisasi (Brownsword & Goodwin, 2012; Murray, 2019).

Di sisi lain, keseimbangan antara kebebasan berekspresi dan perlindungan terhadap kepentingan umum juga menjadi persoalan penting dalam ruang digital. Internet memberikan kesempatan bagi setiap individu untuk menyampaikan pendapat, memperoleh informasi, dan berpartisipasi dalam ruang publik secara luas. Namun, kebebasan tersebut dapat disalahgunakan untuk menyebarkan ujaran kebencian, disinformasi, fitnah, penipuan, maupun konten yang merugikan masyarakat. Dalam kondisi demikian, hukum menghadapi tantangan untuk menentukan batas yang proporsional antara perlindungan kebebasan berekspresi dan upaya menjaga ketertiban, keamanan, serta hak orang lain di ruang digital (Lessig, 2006; Murray, 2019).

Tantangan berikutnya adalah keterbatasan kapasitas lembaga penegak hukum dalam menghadapi kompleksitas kejahatan digital. Penanganan kasus yang melibatkan teknologi informasi memerlukan pemahaman mengenai forensik digital, keamanan siber, analisis data elektronik, pelacakan transaksi digital, serta pengamanan barang bukti elektronik. Tidak semua lembaga penegak hukum memiliki sumber daya manusia, infrastruktur teknologi, dan kemampuan teknis yang memadai untuk menghadapi modus kejahatan siber yang terus berkembang. Oleh karena itu,

peningkatan kapasitas kelembagaan menjadi kebutuhan penting dalam penegakan hukum teknologi informasi.

Selain itu, rendahnya tingkat literasi digital dan literasi hukum masyarakat juga menjadi tantangan dalam implementasi Hukum Teknologi Informasi. Banyak pelanggaran di ruang digital terjadi karena kurangnya pemahaman masyarakat mengenai hak, kewajiban, etika, dan risiko hukum dalam menggunakan teknologi informasi. Sebagian pengguna belum memahami bahwa aktivitas seperti menyebarkan data pribadi orang lain, menggunakan karya digital tanpa izin, menyebarkan informasi yang belum terverifikasi, atau mengakses sistem elektronik tanpa hak dapat memiliki konsekuensi hukum. Upaya penegakan hukum perlu disertai edukasi dan peningkatan kesadaran masyarakat agar tercipta budaya digital yang aman dan bertanggung jawab.

Dalam konteks pendidikan, tantangan hukum aktivitas digital juga tampak pada penggunaan teknologi dalam proses pembelajaran, penelitian, administrasi akademik, dan publikasi ilmiah. Penggunaan platform pembelajaran daring, sistem informasi akademik, penyimpanan data mahasiswa, serta aplikasi berbasis kecerdasan buatan dapat menimbulkan persoalan mengenai pelindungan data pribadi, hak cipta materi ajar, integritas akademik, plagiarisme, dan keabsahan dokumen elektronik. Institusi pendidikan perlu memiliki tata kelola digital yang jelas agar pemanfaatan teknologi dapat mendukung proses akademik tanpa mengabaikan prinsip hukum dan etika.

Berdasarkan berbagai tantangan tersebut, Hukum Teknologi Informasi dituntut untuk bersifat adaptif, fleksibel, dan responsif terhadap perubahan masyarakat digital. Pendekatan regulasi yang terlalu kaku berpotensi menghambat inovasi, sedangkan pendekatan yang terlalu longgar dapat menimbulkan ketidakpastian hukum dan meningkatkan risiko penyalahgunaan teknologi. Oleh karena itu, pembentukan hukum di bidang teknologi informasi perlu mempertimbangkan keseimbangan antara perlindungan hukum, kepastian hukum, keamanan digital, penghormatan terhadap hak individu, dan dukungan terhadap inovasi.

Pada akhirnya, tantangan hukum dalam mengatur aktivitas digital tidak hanya terletak pada penyusunan regulasi, tetapi juga pada kemampuan negara, lembaga penegak hukum, pelaku usaha, institusi pendidikan, dan

masyarakat untuk beradaptasi dengan perubahan teknologi yang berlangsung dinamis. Keberhasilan pengaturan aktivitas digital sangat bergantung pada sinergi antara regulasi yang efektif, penegakan hukum yang kuat, tata kelola teknologi yang bertanggung jawab, dan peningkatan kesadaran hukum dalam masyarakat digital.

1.6 Urgensi Hukum Teknologi Informasi Bagi Mahasiswa S1

Perkembangan teknologi informasi telah mengubah cara manusia belajar, bekerja, berkomunikasi, mencari informasi, melakukan transaksi, dan berinteraksi dalam kehidupan sehari-hari. Mahasiswa pada jenjang pendidikan sarjana merupakan bagian dari masyarakat digital yang sangat dekat dengan pemanfaatan teknologi informasi. Penggunaan media sosial, platform pembelajaran daring, layanan komputasi awan (*cloud computing*), aplikasi berbasis kecerdasan buatan (*artificial intelligence*), sistem informasi akademik, dan transaksi elektronik telah menjadi bagian penting dalam aktivitas akademik maupun kehidupan sosial. Oleh karena itu, pemahaman mengenai Hukum Teknologi Informasi menjadi kebutuhan penting agar mahasiswa mampu menggunakan teknologi secara aman, etis, dan bertanggung jawab (Murray, 2019; Ramli, 2004).

Urgensi pertama terletak pada kebutuhan untuk meningkatkan kesadaran hukum dalam penggunaan teknologi digital. Banyak aktivitas yang dilakukan di ruang digital memiliki konsekuensi hukum, seperti menyebarkan informasi melalui media sosial, menggunakan perangkat lunak, mengunduh dan membagikan materi digital, memanfaatkan karya ilmiah orang lain, mengelola data pribadi, serta melakukan transaksi elektronik. Kurangnya pemahaman terhadap aspek hukum dapat menyebabkan seseorang melakukan pelanggaran secara tidak sengaja, misalnya pelanggaran hak cipta, penyebaran konten yang melanggar hukum, penyalahgunaan data pribadi, atau penggunaan informasi elektronik secara tidak bertanggung jawab (Lessig, 2006; Republik Indonesia, 2008, 2016, 2024).

Selain itu, pemahaman mengenai Hukum Teknologi Informasi penting untuk melindungi mahasiswa sebagai pengguna teknologi. Dalam aktivitas digital, mahasiswa dapat menjadi korban berbagai bentuk pelanggaran,

seperti pencurian identitas, penipuan daring, peretasan akun, penyalahgunaan data pribadi, penyebaran data tanpa izin, maupun bentuk kejahatan siber (*cybercrime*) lainnya. Pengetahuan mengenai hak-hak pengguna teknologi informasi akan membantu mahasiswa memahami cara melindungi data pribadi, mengenali risiko digital, serta mengetahui langkah yang dapat dilakukan apabila mengalami pelanggaran di ruang digital (Solove & Schwartz, 2020; Republik Indonesia, 2022).

Hukum Teknologi Informasi juga memiliki peran penting dalam mendukung integritas akademik di lingkungan perguruan tinggi. Kemudahan akses terhadap informasi dan teknologi digital meningkatkan peluang mahasiswa untuk memperoleh sumber belajar yang luas. Namun, kemudahan tersebut juga dapat menimbulkan risiko seperti plagiarisme, pelanggaran hak cipta, manipulasi data penelitian, penggunaan karya orang lain tanpa atribusi, dan penyalahgunaan teknologi kecerdasan buatan dalam penyusunan tugas akademik. Pemahaman terhadap aspek hukum dan etika penggunaan teknologi informasi dapat mendorong mahasiswa untuk menjunjung tinggi kejujuran akademik, menghormati hak kekayaan intelektual, dan bertanggung jawab dalam memanfaatkan teknologi untuk kegiatan pendidikan dan penelitian.

Di samping itu, penguasaan Hukum Teknologi Informasi menjadi kompetensi yang relevan dengan kebutuhan dunia kerja di era transformasi digital. Hampir seluruh sektor industri saat ini memanfaatkan teknologi informasi dalam kegiatan operasional, pelayanan, pemasaran, pengelolaan data, komunikasi, dan pengambilan keputusan. Isu mengenai pelindungan data pribadi, keamanan informasi, transaksi elektronik, hak kekayaan intelektual, kepatuhan terhadap regulasi digital, dan tanggung jawab penggunaan teknologi semakin mendapat perhatian dalam dunia profesional. Mahasiswa yang memahami aspek hukum teknologi informasi akan memiliki kesiapan yang lebih baik dalam menghadapi tuntutan kerja di berbagai bidang.

Bagi mahasiswa dari bidang non-hukum, pemahaman Hukum Teknologi Informasi diperlukan agar mereka mampu mengidentifikasi risiko hukum yang mungkin muncul dalam pemanfaatan teknologi sesuai bidang keahliannya. Mahasiswa bidang teknologi informasi, ekonomi, pendidikan, kesehatan, komunikasi, dan bidang lainnya akan berhadapan dengan persoalan digital yang memiliki dimensi hukum. Sementara itu, bagi

mahasiswa bidang hukum, penguasaan bidang ini menjadi penting karena Hukum Teknologi Informasi merupakan salah satu cabang hukum yang berkembang pesat dan semakin dibutuhkan dalam praktik hukum modern.

Selain sebagai pengguna teknologi, mahasiswa juga merupakan agen perubahan sosial yang memiliki peran penting dalam membangun budaya digital yang sehat. Pemahaman terhadap Hukum Teknologi Informasi dapat mendorong mahasiswa untuk menggunakan teknologi secara bijaksana, menghormati hak orang lain di ruang digital, menjaga keamanan data pribadi, memeriksa kebenaran informasi sebelum menyebarkannya, serta berpartisipasi dalam menciptakan ekosistem digital yang aman, etis, produktif, dan berkeadilan.

Dalam konteks kehidupan akademik, pemahaman Hukum Teknologi Informasi juga membantu mahasiswa memahami batas penggunaan teknologi sebagai alat bantu belajar. Teknologi dapat digunakan untuk mencari referensi, mengelola data, menyusun ide, melakukan analisis, dan meningkatkan produktivitas akademik. Namun, penggunaan teknologi tetap perlu memperhatikan etika akademik, keaslian karya, perlindungan data, dan aturan institusi pendidikan. Dengan pemahaman hukum yang baik, mahasiswa dapat memanfaatkan teknologi secara optimal tanpa mengabaikan tanggung jawab akademik dan sosial.

Pada akhirnya, urgensi Hukum Teknologi Informasi bagi mahasiswa jenjang sarjana tidak hanya berkaitan dengan kebutuhan untuk memahami aturan hukum, tetapi juga berkaitan dengan pembentukan kompetensi, etika, tanggung jawab, dan kesadaran digital. Di era masyarakat informasi dan ekonomi digital, literasi hukum di bidang teknologi informasi menjadi salah satu kemampuan dasar yang perlu dimiliki agar mahasiswa mampu beradaptasi dengan perkembangan teknologi, melindungi haknya, menghormati hak orang lain, dan berkontribusi dalam membangun masyarakat digital yang aman dan berkeadilan.

Bab 2
Sejarah Perkembangan Hukum Teknologi

2.1 Perkembangan Teknologi Informasi dan Dampaknya terhadap Hukum

Perkembangan teknologi informasi telah mengubah hampir seluruh aspek kehidupan manusia, mulai dari komunikasi, perdagangan, pendidikan, hingga pelayanan publik. Perubahan tersebut turut melahirkan bentuk hubungan, hak, kewajiban, dan risiko hukum yang sebelumnya belum dikenal. Oleh karena itu, hukum dituntut untuk terus beradaptasi agar mampu memberikan kepastian, perlindungan, dan keadilan dalam menghadapi perkembangan teknologi yang berlangsung semakin cepat (Bainbridge, 2008; Koops, 2010).

2.1.1 Revolusi Teknologi Informasi: Dari Analog ke Digital

Perkembangan teknologi informasi merupakan salah satu fenomena paling transformatif dalam sejarah peradaban manusia. Dalam kurun waktu kurang dari satu abad, umat manusia telah menyaksikan transformasi yang luar biasa, yaitu dari penggunaan perangkat mekanis sederhana menuju sistem komputasi yang mampu memproses miliaran data dalam hitungan detik. Revolusi ini tidak hanya mengubah cara manusia bekerja dan berkomunikasi, tetapi juga secara fundamental merombak tatanan sosial, ekonomi, dan hukum yang telah berlaku selama berabad-abad.

Pada dekade 1940-an, komputer generasi awal, seperti ENIAC (*Electronic Numerical Integrator and Computer*), muncul sebagai mesin berukuran sangat besar yang memenuhi satu ruangan dan digunakan terutama untuk keperluan militer serta ilmiah. Memasuki dekade 1950-an dan 1960-an, teknologi transistor menggantikan tabung vakum sehingga memungkinkan terciptanya komputer yang lebih kecil dan lebih terjangkau. Revolusi sirkuit terpadu (*integrated circuit*) pada dekade 1960-an kemudian membuka jalan bagi penggunaan komputasi secara luas serta mengubah wajah industri dan bisnis secara permanen.

Dekade 1970-an dan 1980-an menandai lahirnya era komputer pribadi (*personal computer* atau PC). Apple, IBM, dan Microsoft menjadi perusahaan yang merevolusi cara individu berinteraksi dengan teknologi informasi. Pada periode ini, data mulai dipahami sebagai aset yang berharga. Kebutuhan untuk melindungi informasi digital juga mulai menjadi isu serius bagi pelaku bisnis dan pemerintah. Era inilah yang kemudian mendorong lahirnya berbagai regulasi hukum pertama yang secara khusus mengatur penggunaan komputer dan data elektronik (Bainbridge, 2008).

Tonggak Penting Perkembangan Teknologi Informasi

- **1940-an:** lahirnya komputer generasi awal, seperti ENIAC dan UNIVAC, untuk keperluan militer dan ilmiah.
- **1950-an–1960-an:** berkembangnya teknologi transistor dan sirkuit terpadu serta dimulainya penggunaan komputasi dalam kegiatan bisnis.
- **1970-an–1980-an:** berkembangnya era komputer pribadi atau PC dengan Apple, IBM, dan Microsoft sebagai perusahaan utama dalam revolusi tersebut.
- **1990-an:** lahirnya *World Wide Web* dan mulai berkembangnya internet komersial yang dapat diakses oleh masyarakat umum.
- **2000-an:** berkembangnya jaringan pita lebar (*broadband*), perdagangan elektronik (*e-commerce*), dan media sosial berbasis platform.
- **2010-an:** berkembangnya telepon pintar (*smartphone*), *big data*, komputasi awan (*cloud computing*), dan Internet untuk Segala (*Internet of Things* atau IoT).
- **2020-an:** berkembangnya kecerdasan buatan generatif, *blockchain*, metaverse, dan komputasi kuantum.

2.1.2 Dampak Teknologi terhadap Sistem Hukum

Setiap gelombang perubahan teknologi membawa implikasi yang mendalam bagi sistem hukum. Hukum, sebagai instrumen yang lahir dari masyarakat dan digunakan untuk mengatur hubungan antarmanusia, selalu dituntut untuk beradaptasi ketika realitas sosial berubah. Namun, teknologi informasi menghadirkan tantangan adaptasi yang jauh lebih kompleks dibandingkan dengan perubahan sosial sebelumnya. Kompleksitas tersebut muncul karena

teknologi informasi melampaui batas geografis, berkembang dengan sangat cepat, serta menciptakan berbagai entitas dan hubungan hukum baru.

Pertama, teknologi informasi mengubah konsep identitas dan subjek hukum. Dalam hukum tradisional, subjek hukum terdiri atas orang perseorangan (*natural person*) dan badan hukum (*legal entity*) yang keberadaannya dapat diidentifikasi secara fisik. Namun, di dunia digital muncul identitas virtual, pseudonim, dan bahkan agen kecerdasan buatan. Kondisi tersebut menimbulkan pertanyaan mendasar mengenai pihak yang harus bertanggung jawab secara hukum atas tindakan yang dilakukan oleh entitas digital. Pertanyaan ini belum sepenuhnya terjawab secara memadai oleh sistem hukum di berbagai negara (Bainbridge, 2008; Koops, 2010).

Kedua, teknologi mengubah konsep kepemilikan dan hak atas suatu benda atau karya. Hak kekayaan intelektual, yang telah diatur melalui hukum hak cipta, paten, dan merek sejak abad ke-18 dan ke-19, menghadapi tantangan besar pada era digital. Kemampuan untuk menyalin, mendistribusikan, dan memodifikasi karya digital secara sempurna dengan biaya yang hampir tidak ada telah mendorong pembentuk undang-undang di berbagai negara untuk terus memperbarui kerangka hukum kekayaan intelektual. Perdebatan antara perlindungan hak eksklusif pencipta dan kepentingan akses publik terhadap informasi pun menjadi semakin kompleks (Bainbridge, 2008).

Ketiga, teknologi mengubah konsep yurisdiksi dan kedaulatan. Internet tidak mengenal batas negara. Sebuah situs web yang datanya disimpan pada peladen di Amerika Serikat dapat diakses oleh pengguna di Indonesia dan memengaruhi warga negara Malaysia. Kondisi tersebut menimbulkan persoalan hukum yang signifikan. Persoalan tersebut mencakup hukum negara yang harus diberlakukan, pengadilan yang berwenang memeriksa perkara, serta mekanisme pelaksanaan putusan pengadilan terhadap pelaku yang berada dalam yurisdiksi berbeda. Pertanyaan-pertanyaan tersebut menjadi bagian penting dalam perdebatan akademik dan perumusan kebijakan hukum internasional hingga saat ini (Koops, 2010).

2.1.3 Tantangan Hukum di Era Digital

Era digital menghadirkan serangkaian tantangan hukum yang belum pernah dihadapi sebelumnya. Tantangan tersebut tidak hanya bersifat teknis, tetapi juga berkaitan dengan nilai-nilai fundamental, seperti kebebasan, privasi,

keadilan, dan kedaulatan. Pemahaman terhadap berbagai tantangan tersebut penting untuk menjelaskan mengapa perkembangan hukum teknologi berlangsung secara kompleks dan tidak selalu linier.

Beberapa tantangan utama yang dihadapi hukum pada era digital meliputi hal-hal berikut.

1. **Kecepatan Perubahan Teknologi dan Kelambatan Proses Legislasi**

   Teknologi berkembang dengan kecepatan yang sangat tinggi, sedangkan proses pembentukan peraturan perundang-undangan membutuhkan waktu yang relatif panjang. Ketika suatu undang-undang di bidang teknologi selesai dibentuk, teknologi yang diaturnya sering kali telah berkembang jauh melampaui asumsi awal para perancang undang-undang tersebut.

2. **Sifat Lintas Batas Internet**

   Kejahatan siber, pelanggaran privasi, dan penyebaran konten ilegal dapat dilakukan oleh pelaku yang berada di suatu negara dengan korban yang tersebar di berbagai negara serta menggunakan infrastruktur yang berlokasi di negara lain. Keadaan tersebut menyulitkan penentuan yurisdiksi dan koordinasi penegakan hukum antarnegara (Koops, 2010).

3. **Anonimitas dan Pseudonimitas**

   Internet memungkinkan pengguna menyembunyikan atau menyamarkan identitas aslinya. Kemampuan tersebut dapat melindungi privasi dan kebebasan berekspresi, tetapi juga dapat mempersulit proses identifikasi pelaku, penegakan hukum, dan pertanggungjawaban hukum (Koops, 2010; A. Raharjo, 2002).

4. **Pembuktian Digital**

   Barang bukti digital dapat dengan mudah diubah, disalin, dipindahkan, atau dimanipulasi. Oleh karena itu, hukum acara pidana dan hukum acara perdata tradisional belum sepenuhnya memadai untuk menangani karakteristik khusus bukti digital. Penanganan bukti digital memerlukan prosedur yang dapat menjamin keaslian, integritas, dan keterlacakan bukti (Casey, 2011; ISO/IEC, 2012).

5. **Monopoli Platform Digital**

   Perusahaan teknologi besar, seperti Google, Meta, Amazon, dan Apple, telah mengakumulasi kekuatan pasar serta menguasai data pengguna

dalam jumlah yang sangat besar. Kondisi tersebut menimbulkan kekhawatiran mengenai persaingan usaha, perlindungan privasi, pengelolaan informasi, dan kebebasan berekspresi.

6. Konvergensi Teknologi

Batas antara telekomunikasi, media, dan komputasi semakin kabur. Sementara itu, regulasi untuk masing-masing sektor pada awalnya dikembangkan secara terpisah. Kondisi tersebut menyebabkan berbagai peraturan berpotensi tumpang tindih, tidak selaras, atau tidak sesuai dengan perkembangan teknologi yang telah terintegrasi.

2.2 Awal Mula Regulasi Teknologi dan Komunikasi Digital

Regulasi teknologi dan komunikasi digital berkembang sebagai respons terhadap perubahan cara manusia menyampaikan, menyimpan, dan memproses informasi. Sebelum internet digunakan secara luas, pengaturan hukum telah diterapkan pada telegraf, telepon, radio, televisi, dan pemrosesan data komputer. Berbagai regulasi awal tersebut kemudian menjadi dasar bagi pembentukan hukum komunikasi dan teknologi digital modern.

2.2.1 Sejarah Awal Regulasi Komunikasi

Regulasi teknologi komunikasi tidak dimulai sejak munculnya internet. Jauh sebelum era digital, berbagai negara telah mengembangkan kerangka hukum untuk mengatur beragam sarana komunikasi, mulai dari telegraf dan telepon hingga radio dan televisi. Pemahaman mengenai sejarah regulasi komunikasi penting karena berbagai konsep, prinsip, dan struktur kelembagaan yang lahir pada era pradigital kemudian diadaptasi dalam regulasi teknologi informasi modern. Perkembangan hukum teknologi pada dasarnya selalu mengikuti perubahan sarana komunikasi, pola distribusi informasi, dan bentuk hubungan antara penyedia layanan dengan masyarakat (Bainbridge, 2008).

Telegraf yang berkembang pada pertengahan abad ke-19 merupakan salah satu teknologi komunikasi pertama yang memerlukan regulasi lintas negara secara terkoordinasi. Pesatnya pembangunan jaringan telegraf internasional

mendorong pembentukan *International Telegraph Union* pada tahun 1865. Organisasi tersebut kemudian berubah menjadi *International Telecommunication Union* (ITU) dan menjadi badan khusus Perserikatan Bangsa-Bangsa yang berperan dalam standardisasi serta tata kelola telekomunikasi internasional.

Di Amerika Serikat, regulasi komunikasi modern memiliki landasan penting dalam *Communications Act of 1934*. Undang-undang tersebut membentuk *Federal Communications Commission* (FCC) sebagai lembaga federal yang berwenang mengatur radio, televisi, dan telekomunikasi. Regulasi tersebut juga memperkenalkan prinsip bahwa spektrum frekuensi merupakan sumber daya publik dan bahwa penyelenggara komunikasi memiliki kewajiban untuk melayani kepentingan umum. Prinsip tersebut kemudian turut memengaruhi perdebatan mengenai netralitas jaringan dan kewajiban pelayanan universal pada era internet.

Di Eropa, perkembangan regulasi komunikasi mengikuti pola yang berbeda dengan memberikan peran lebih besar kepada negara dalam kepemilikan dan pengelolaan infrastruktur komunikasi. Sebagian besar negara Eropa memiliki perusahaan telekomunikasi nasional yang dikuasai pemerintah dan dikenal sebagai PTT, yaitu *Post, Telegraph, and Telephone*. Struktur tersebut bertahan hingga berlangsungnya gelombang privatisasi dan liberalisasi telekomunikasi pada dekade 1980-an dan 1990-an.

Peralihan dari monopoli negara menuju pasar telekomunikasi yang lebih kompetitif meninggalkan struktur regulasi yang kompleks. Negara tidak lagi hanya bertindak sebagai pemilik dan operator jaringan, tetapi juga sebagai regulator yang bertugas menjaga persaingan usaha, ketersediaan layanan, keamanan jaringan, dan perlindungan konsumen.

2.2.2 Lahirnya Regulasi Komputer dan Data

Ketika komputer mulai digunakan secara luas dalam kegiatan bisnis dan pemerintahan pada dekade 1960-an, kekhawatiran mengenai privasi data mulai meningkat. Kemampuan komputer untuk menyimpan, memproses, menggabungkan, dan mencocokkan data dalam jumlah besar menciptakan kondisi yang sebelumnya sulit diwujudkan. Pemerintah maupun perusahaan dapat membangun profil individu secara terperinci dengan menggabungkan data dari berbagai sumber.

Perkembangan tersebut mengubah orientasi hukum dari sekadar perlindungan terhadap perangkat komputer menuju perlindungan terhadap informasi yang diproses di dalamnya. Regulasi komputer kemudian berkembang untuk mengatur pengumpulan data, keamanan penyimpanan, akses terhadap informasi, penggunaan data sesuai tujuan, dan hak individu atas data pribadinya. Perlindungan data menjadi salah satu bidang utama dalam perkembangan hukum komputer karena pemrosesan informasi secara otomatis dapat menimbulkan risiko pengawasan, diskriminasi, dan penyalahgunaan data (Bainbridge, 2008).

Negara bagian Hessen di Jerman mengesahkan undang-undang perlindungan data pada tahun 1970. Regulasi tersebut sering dipandang sebagai undang-undang perlindungan data pertama di dunia, meskipun ruang berlakunya terbatas pada tingkat negara bagian. Jerman kemudian mengesahkan undang-undang perlindungan data federal atau *Bundesdatenschutzgesetz* pada tahun 1977.

Swedia mengesahkan *Data Act* pada tahun 1973 dan menjadi salah satu negara pertama yang memiliki regulasi perlindungan data nasional secara komprehensif. Inggris selanjutnya mengesahkan *Data Protection Act* pada tahun 1984 sebagai respons terhadap meningkatnya penggunaan komputer untuk memproses data pribadi oleh lembaga pemerintah dan perusahaan.

Pada tingkat internasional, *Organisation for Economic Co-operation and Development* (OECD) menerbitkan *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* pada tahun 1980. Meskipun tidak memiliki sifat mengikat seperti perjanjian internasional, pedoman tersebut memberikan pengaruh besar terhadap pembentukan kebijakan perlindungan data di berbagai negara.

Pedoman OECD memperkenalkan delapan prinsip dasar perlindungan data, yaitu pembatasan pengumpulan, kualitas data, penentuan tujuan, pembatasan penggunaan, perlindungan keamanan, keterbukaan, partisipasi individu, dan akuntabilitas. Prinsip-prinsip tersebut menjadi fondasi bagi berbagai peraturan perlindungan data modern.

Tabel 2.1: Tonggak Awal Regulasi Teknologi dan Komunikasi Digital

Tahun	Peristiwa atau Regulasi	Keterangan
1865	Pendirian *International Telegraph Union*	Organisasi internasional yang dibentuk untuk mengoordinasikan jaringan dan layanan telegraf antarnegara.
1934	*Communications Act of 1934* Amerika Serikat	Membentuk FCC dan memperkuat prinsip kepentingan publik dalam penyelenggaraan komunikasi.
1970	Undang-Undang Perlindungan Data Hessen	Regulasi perlindungan data pertama pada tingkat negara bagian di Jerman.
1973	*Data Act* Swedia	Salah satu undang-undang perlindungan data nasional pertama yang bersifat komprehensif.
1980	*OECD Privacy Guidelines*	Menetapkan prinsip-prinsip dasar perlindungan privasi dan arus data lintas negara.
1981	*Convention 108*	Perjanjian internasional mengikat mengenai perlindungan individu dalam pemrosesan data pribadi secara otomatis.
1984	*Data Protection Act* Inggris	Regulasi awal Inggris yang mengatur perlindungan data pribadi dalam sistem komputer.
1986	*Computer Fraud and Abuse Act* Amerika Serikat	Mengatur akses tanpa hak dan tindak pidana tertentu yang melibatkan sistem komputer.
1991	Peluncuran *Pretty Good Privacy*	Memperluas akses masyarakat terhadap teknologi enkripsi dan perlindungan komunikasi digital.

2.2.3 Tonggak Awal Regulasi Internasional

Pada tingkat internasional, perkembangan regulasi teknologi informasi berjalan seiring dengan meningkatnya kesadaran mengenai risiko yang ditimbulkan oleh pemrosesan data dan penggunaan jaringan komputer. Risiko tersebut mencakup akses tanpa hak, pencurian data, manipulasi informasi, gangguan terhadap sistem komputer, serta pelanggaran privasi.

Kemunculan tindak pidana yang menggunakan komputer menunjukkan bahwa hukum pidana tradisional tidak selalu mampu menjangkau karakteristik khusus kejahatan digital (Raharjo, 2002; Koops, 2010).

Amerika Serikat mengambil langkah penting dengan mengesahkan *Computer Fraud and Abuse Act* (CFAA) pada tahun 1986. Undang-undang tersebut mengatur berbagai perbuatan yang berkaitan dengan akses tanpa hak terhadap komputer, pengambilan informasi, penipuan berbasis komputer, dan tindakan yang menyebabkan kerusakan pada sistem komputer. CFAA kemudian menjadi salah satu landasan utama penanganan tindak pidana komputer di Amerika Serikat.

Meskipun demikian, penerapan CFAA juga menimbulkan perdebatan. Salah satu persoalan utamanya adalah penafsiran mengenai batas antara akses yang sah dan akses yang melampaui kewenangan. Persoalan tersebut menunjukkan bahwa rumusan hukum yang terlalu luas dapat menimbulkan ketidakpastian dalam penerapannya, terutama ketika teknologi dan pola penggunaan sistem berkembang lebih cepat daripada perubahan peraturan.

Dewan Eropa mengadopsi *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* atau *Convention 108* pada tahun 1981. Konvensi tersebut merupakan salah satu instrumen internasional pertama yang mengikat secara hukum dalam bidang perlindungan data pribadi. Konvensi ini mengatur prinsip pemrosesan data yang adil, keamanan data, kualitas informasi, serta perlindungan terhadap data sensitif.

Pada tahun 2018, *Convention 108* dimodernisasi melalui protokol perubahan yang dikenal sebagai *Convention 108+*. Pembaruan tersebut dilakukan untuk menyesuaikan prinsip perlindungan data dengan perkembangan pemrosesan data berskala besar, arus data lintas negara, teknologi digital, dan kebutuhan pengawasan independen.

Perkembangan penting lainnya adalah munculnya konsep kejahatan komputer sebagai kategori tindak pidana tersendiri. Sebelum komputer digunakan secara luas, hukum pidana belum mengenal secara spesifik perbuatan seperti akses ilegal, penyebaran perangkat lunak berbahaya, pencurian identitas digital, atau gangguan terhadap sistem elektronik. Karakteristik dunia digital memungkinkan kejahatan dilakukan dari jarak jauh, dalam waktu singkat, dan melibatkan korban di banyak negara (Koops, 2010).

Berbagai negara kemudian mengembangkan pendekatan yang berbeda untuk mengatasi kejahatan komputer. Sebagian negara memilih memperluas atau mengubah ketentuan dalam hukum pidana yang telah ada, sedangkan negara lainnya membentuk undang-undang khusus mengenai kejahatan komputer. Perbedaan pendekatan tersebut dipengaruhi oleh sistem hukum, tingkat perkembangan teknologi, kapasitas penegakan hukum, dan kebijakan keamanan nasional masing-masing negara (Hardjaloka, 2015).

Perkembangan regulasi pada periode awal tersebut menunjukkan bahwa hukum teknologi informasi pada mulanya berfokus pada tiga aspek utama, yaitu pengaturan infrastruktur komunikasi, perlindungan data pribadi, dan kriminalisasi akses tanpa hak terhadap sistem komputer. Ketiga aspek tersebut kemudian menjadi landasan bagi perkembangan hukum siber yang lebih luas pada era internet.

2.3 Perkembangan Hukum Siber di Dunia

Perkembangan hukum siber di berbagai negara berlangsung seiring dengan meningkatnya penggunaan komputer, internet, dan layanan digital dalam kehidupan masyarakat. Setiap negara mengembangkan pendekatan yang berbeda sesuai dengan sistem hukum, kebutuhan keamanan, perlindungan privasi, dan tingkat kemajuan teknologinya. Perbedaan tersebut kemudian membentuk beragam model pengaturan hukum siber yang memengaruhi tata kelola ruang digital secara global.

2.3.1 Definisi dan Ruang Lingkup Hukum Siber

Hukum siber (*cyber law*), yang juga dikenal sebagai hukum internet atau hukum dunia maya, merupakan bidang hukum yang mengatur berbagai aktivitas manusia dalam lingkungan digital. Berbeda dengan cabang hukum tradisional yang memiliki batas relatif jelas, hukum siber bersifat multidisipliner karena beririsan dengan hukum pidana, hukum perdata, hukum perdagangan, hukum kekayaan intelektual, hukum perlindungan data, hukum telekomunikasi, dan hukum internasional.

Kemunculan hukum siber tidak terlepas dari perubahan karakter kejahatan dan hubungan hukum akibat penggunaan komputer serta jaringan internet. Teknologi memungkinkan suatu perbuatan dilakukan dari jarak jauh, melintasi batas negara, dan melibatkan sistem elektronik yang tersebar di

berbagai yurisdiksi. Karakter tersebut membuat penerapan konsep hukum konvensional menjadi lebih kompleks, terutama dalam menentukan pelaku, lokasi tindak pidana, alat bukti, dan hukum yang berlaku (Raharjo, 2002; Koops, 2010).

Secara umum, ruang lingkup hukum siber mencakup beberapa bidang utama berikut.

1. **Kejahatan siber**

   Kejahatan siber (*cybercrime*) mencakup akses tanpa hak, peretasan, penipuan elektronik, penyebaran perangkat lunak berbahaya (*malware*), pencurian identitas digital, manipulasi data, dan serangan terhadap sistem atau infrastruktur digital. Komputer dapat berkedudukan sebagai sasaran kejahatan, sarana untuk melakukan kejahatan, maupun tempat penyimpanan barang bukti (Raharjo, 2002).

2. **Privasi dan perlindungan data pribadi**

   Bidang ini mengatur cara data pribadi dikumpulkan, digunakan, disimpan, dibagikan, dan dihapus. Perlindungan data juga mencakup hak individu untuk mengetahui tujuan pemrosesan, mengakses data, memperbaiki informasi yang tidak akurat, serta menolak penggunaan tertentu atas data pribadinya.

3. **Hak kekayaan intelektual digital**

   Hukum kekayaan intelektual digital mencakup perlindungan hak cipta terhadap konten digital, perlindungan perangkat lunak, paten teknologi, merek dalam lingkungan elektronik, dan sengketa nama domain. Kemudahan menyalin serta mendistribusikan karya digital menjadi salah satu tantangan utama dalam penerapan hukum kekayaan intelektual.

4. **Perdagangan dan transaksi elektronik**

   Bidang ini mencakup kontrak elektronik, tanda tangan elektronik, pembayaran digital, perlindungan konsumen, transaksi melalui platform, dan keabsahan dokumen elektronik. Salah satu persoalan utamanya adalah memastikan bahwa transaksi yang dilakukan tanpa pertemuan fisik tetap memiliki kepastian dan kekuatan hukum (Bainbridge, 2008).

5. **Konten digital dan kebebasan berekspresi**

   Hukum siber juga mengatur penyebaran konten ilegal, pencemaran nama baik, ujaran kebencian, pornografi, disinformasi, dan moderasi konten oleh platform digital. Pengaturan tersebut perlu menyeimbangkan kepentingan ketertiban umum dengan perlindungan kebebasan berekspresi.

6. **Privasi komunikasi**

   Bidang ini berkaitan dengan penyadapan, intersepsi komunikasi, penggunaan enkripsi, kerahasiaan korespondensi elektronik, dan kewenangan pemerintah untuk mengakses komunikasi dalam rangka penegakan hukum atau keamanan nasional.

7. **Tata kelola internet**

   Tata kelola internet mencakup pengelolaan nama domain, sistem penamaan domain (*Domain Name System* atau DNS), alokasi alamat internet, netralitas jaringan, keamanan infrastruktur, dan koordinasi kebijakan internet internasional.

Dengan cakupan tersebut, hukum siber tidak dapat dipandang sebagai satu cabang hukum yang sepenuhnya berdiri sendiri. Hukum siber lebih tepat dipahami sebagai bidang hukum yang mengintegrasikan berbagai prinsip hukum untuk menjawab persoalan yang muncul akibat pemanfaatan teknologi digital.

2.3.2 Perkembangan di Amerika Serikat

Amerika Serikat memiliki peran penting dalam perkembangan hukum siber karena banyak inovasi, perusahaan, dan infrastruktur awal internet berkembang di negara tersebut. Regulasi siber Amerika Serikat pada mulanya berfokus pada akses tanpa hak terhadap komputer, perlindungan komunikasi elektronik, dan tanggung jawab penyedia layanan internet.

Setelah mengesahkan *Computer Fraud and Abuse Act* (CFAA) pada tahun 1986, Amerika Serikat mengembangkan berbagai regulasi untuk menghadapi tindak pidana berbasis komputer. CFAA mengatur akses tanpa hak, pengambilan data, penipuan dengan menggunakan komputer, dan tindakan yang menimbulkan kerusakan terhadap sistem komputer. Undang-

undang tersebut menjadi salah satu dasar utama penuntutan tindak pidana komputer di Amerika Serikat.

Pada tahun yang sama, Amerika Serikat mengesahkan *Electronic Communications Privacy Act* (ECPA). Regulasi tersebut memperluas perlindungan terhadap penyadapan komunikasi dari layanan telepon tradisional ke komunikasi elektronik dan data yang disimpan secara digital. Akan tetapi, perkembangan komputasi awan (*cloud computing*), media sosial, dan penyimpanan data berskala besar kemudian menimbulkan perdebatan mengenai relevansi sejumlah ketentuan ECPA.

Tahun 1996 menjadi salah satu tonggak penting dalam perkembangan hukum internet di Amerika Serikat melalui pengesahan *Communications Decency Act* (CDA). Undang-undang tersebut pada awalnya dimaksudkan untuk mengendalikan penyebaran konten yang dianggap tidak pantas di internet. Sejumlah ketentuannya kemudian dibatalkan oleh Mahkamah Agung Amerika Serikat karena dianggap bertentangan dengan perlindungan kebebasan berbicara.

Salah satu ketentuan yang tetap berlaku adalah Pasal 230 CDA atau *Section 230*. Ketentuan tersebut pada prinsipnya membatasi tanggung jawab penyedia layanan interaktif terhadap konten yang dibuat dan diunggah oleh pengguna. Perlindungan tersebut memungkinkan platform digital berkembang tanpa diperlakukan sepenuhnya sebagai penerbit setiap konten pengguna.

Meskipun demikian, *Section 230* terus menjadi objek perdebatan. Sebagian pihak menilai ketentuan tersebut diperlukan untuk melindungi inovasi dan kebebasan berkomunikasi di internet. Sebaliknya, pihak lain berpendapat bahwa perlindungan yang terlalu luas dapat mengurangi akuntabilitas platform terhadap penyebaran konten ilegal, disinformasi, kekerasan, dan ujaran kebencian.

Setelah serangan 11 September 2001, orientasi regulasi siber Amerika Serikat bergeser ke arah keamanan nasional. Pengesahan *USA PATRIOT Act* pada tahun 2001 memperluas kewenangan pemerintah dalam melakukan pengawasan, memperoleh data komunikasi, dan mengakses informasi untuk kepentingan keamanan nasional. Perkembangan tersebut diikuti oleh penguatan kelembagaan keamanan dalam negeri dan koordinasi keamanan siber nasional.

Pengungkapan program pengawasan digital oleh Edward Snowden pada tahun 2013 kemudian memicu perdebatan internasional mengenai batas kewenangan negara dalam mengakses data komunikasi. Peristiwa tersebut menunjukkan adanya ketegangan antara kepentingan keamanan nasional, kebutuhan penegakan hukum, dan perlindungan hak atas privasi.

2.3.3 Perkembangan di Eropa

Eropa mengembangkan pendekatan hukum siber yang lebih menekankan perlindungan hak fundamental, khususnya privasi dan perlindungan data pribadi. Pendekatan tersebut berbeda dengan Amerika Serikat yang cenderung mengatur perlindungan data berdasarkan sektor dan jenis industri.

Salah satu landasan awal perlindungan data di Eropa adalah *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* atau *Convention 108* yang diadopsi oleh Dewan Eropa pada tahun 1981. Konvensi tersebut menjadi instrumen internasional yang mengikat dalam perlindungan individu terhadap pemrosesan data pribadi secara otomatis.

Uni Eropa selanjutnya mengadopsi Direktif Perlindungan Data 1995 atau *Directive 95/46/EC*. Direktif tersebut bertujuan menyelaraskan perlindungan data di antara negara-negara anggota Uni Eropa sekaligus menjamin pergerakan data dalam pasar internal. Salah satu prinsip pentingnya adalah bahwa pemindahan data pribadi ke negara di luar Uni Eropa hanya dapat dilakukan apabila negara tujuan menyediakan tingkat perlindungan yang memadai.

Perkembangan paling signifikan dalam perlindungan data Eropa adalah penerapan *General Data Protection Regulation* (GDPR) sejak 25 Mei 2018. GDPR menggantikan Direktif 1995 dan memperkuat perlindungan data pribadi melalui ketentuan yang berlaku langsung di seluruh negara anggota Uni Eropa.

GDPR memperkenalkan dan memperkuat beberapa prinsip penting, antara lain:

- persetujuan yang jelas dalam pemrosesan data;
- pembatasan tujuan penggunaan data;
- pengumpulan data secara minimal;

- akurasi dan pembaruan data;
- pembatasan jangka waktu penyimpanan;
- keamanan serta kerahasiaan data; dan
- akuntabilitas pengendali data.

GDPR juga memberikan sejumlah hak kepada subjek data, seperti hak memperoleh akses, hak memperbaiki data, hak menghapus data atau hak untuk dilupakan (*right to be forgotten*), hak membatasi pemrosesan, hak portabilitas data, dan hak mengajukan keberatan. Selain itu, GDPR memperkenalkan pendekatan perlindungan data sejak tahap perancangan sistem (*privacy by design*) dan perlindungan data sebagai pengaturan standar (*privacy by default*).

Organisasi yang melanggar ketentuan GDPR dapat dikenai sanksi administratif yang besar. Sanksi tersebut dimaksudkan untuk memastikan bahwa perlindungan data tidak hanya dipandang sebagai kewajiban administratif, tetapi menjadi bagian dari tata kelola dan manajemen risiko organisasi.

Selain perlindungan data, Dewan Eropa juga mengadopsi *Convention on Cybercrime* atau Konvensi Budapest pada tahun 2001. Konvensi tersebut menjadi salah satu instrumen internasional utama untuk menangani kejahatan yang dilakukan melalui sistem komputer dan internet (Council of Europe, 2001).

Konvensi Budapest mengatur beberapa kategori tindak pidana, yaitu:

- tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data serta sistem komputer;
- tindak pidana yang dilakukan dengan menggunakan komputer;
- tindak pidana yang berkaitan dengan konten;
- pelanggaran hak cipta dan hak terkait; serta
- mekanisme penyelidikan dan kerja sama internasional.

Konvensi tersebut juga menyediakan kerangka kerja sama lintas negara dalam pengamanan data, pertukaran informasi, investigasi digital, dan bantuan hukum timbal balik. Kerja sama tersebut penting karena tindak pidana siber sering melibatkan pelaku, korban, dan infrastruktur yang berada di negara berbeda.

2.3.4 Perkembangan di Asia

Perkembangan hukum siber di Asia berlangsung dengan pola yang beragam. Perbedaan tersebut dipengaruhi oleh sistem politik, tingkat pembangunan ekonomi, kapasitas teknologi, budaya hukum, dan kebijakan keamanan masing-masing negara. Singapura, Jepang, India, dan Tiongkok merupakan beberapa negara yang memiliki pengaruh penting dalam perkembangan regulasi teknologi di kawasan Asia.

Singapura menjadi salah satu negara Asia yang relatif awal mengembangkan kerangka hukum teknologi informasi. *Computer Misuse Act* yang disahkan pada tahun 1993 mengatur akses tanpa hak, modifikasi data, gangguan sistem, dan berbagai tindak pidana yang menggunakan komputer. Regulasi tersebut kemudian mengalami beberapa perubahan untuk menyesuaikan diri dengan perkembangan ancaman siber.

Singapura juga mengesahkan *Personal Data Protection Act* (PDPA) pada tahun 2012. Undang-undang tersebut mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi. PDPA berupaya menyeimbangkan kebutuhan perlindungan konsumen dengan kepentingan organisasi dalam menggunakan data untuk kegiatan bisnis yang sah.

Jepang mengembangkan pendekatan yang menggabungkan perlindungan privasi dan dukungan terhadap inovasi digital. *Act on the Protection of Personal Information* (APPI) menjadi dasar utama perlindungan data pribadi di Jepang. Regulasi tersebut terus diperbarui untuk menyesuaikan diri dengan pemrosesan data berskala besar, perkembangan ekonomi digital, dan arus data lintas negara.

Jepang juga memperkenalkan gagasan *Data Free Flow with Trust* (DFFT). Konsep tersebut mendorong pergerakan data lintas negara dengan tetap memperhatikan kepercayaan, privasi, keamanan, dan perlindungan hak kekayaan intelektual. Pendekatan tersebut berupaya mencegah fragmentasi ekonomi digital akibat perbedaan regulasi nasional.

Tiongkok mengembangkan pendekatan yang lebih menekankan kedaulatan siber (*cyber sovereignty*), keamanan nasional, dan kontrol negara terhadap ruang digital. Pendekatan tersebut terlihat dalam pembangunan sistem penyaringan internet yang dikenal sebagai *Great Firewall of China* serta pembentukan sejumlah undang-undang di bidang keamanan dan data.

Cybersecurity Law yang diberlakukan pada tahun 2017 mengatur keamanan jaringan, kewajiban operator infrastruktur informasi kritis, perlindungan data, dan pengawasan terhadap layanan digital. Selanjutnya, *Data Security Law* tahun 2021 mengatur klasifikasi data, keamanan pemrosesan, dan perlindungan data yang dinilai penting bagi negara.

Pada tahun yang sama, Tiongkok memberlakukan *Personal Information Protection Law* (PIPL). Regulasi tersebut mengatur dasar pemrosesan informasi pribadi, kewajiban pengendali data, hak individu, dan pemindahan data lintas negara. Meskipun memiliki beberapa kesamaan dengan GDPR, penerapan PIPL berlangsung dalam kerangka tata kelola digital yang memberikan kewenangan luas kepada negara.

Perbedaan pendekatan di Asia menunjukkan bahwa regulasi hukum siber tidak berkembang dalam satu model yang seragam. Negara dengan ekonomi terbuka cenderung menekankan fasilitasi perdagangan digital dan perlindungan konsumen, sedangkan negara yang berorientasi pada keamanan lebih menekankan kontrol terhadap data, infrastruktur, dan arus informasi. Keragaman tersebut menjadi tantangan dalam membangun kerja sama hukum siber regional (Hardjaloka, 2015).

Tabel 2.2: Perkembangan Regulasi Hukum Siber di Dunia

Tahun	Peristiwa atau Regulasi	Keterangan
1981	*Convention 108*	Instrumen internasional yang mengatur perlindungan individu dalam pemrosesan data pribadi secara otomatis.
1986	CFAA Amerika Serikat	Mengatur akses tanpa hak dan tindak pidana yang melibatkan sistem komputer.
1986	ECPA Amerika Serikat	Memperluas perlindungan komunikasi terhadap data dan komunikasi elektronik.
1993	*Computer Misuse Act* Singapura	Salah satu regulasi awal kejahatan komputer di Asia Tenggara.
1995	Direktif Perlindungan Data Uni Eropa	Menyelaraskan perlindungan data pribadi di negara-negara anggota Uni Eropa.

Tahun	Peristiwa atau Regulasi	Keterangan
1996	CDA Amerika Serikat	Mengatur konten internet dan memuat ketentuan mengenai tanggung jawab platform.
2000	*Information Technology Act* India	Memberikan dasar hukum bagi transaksi elektronik dan penanganan tindak pidana komputer.
2001	Konvensi Budapest	Menjadi kerangka internasional penanganan kejahatan siber dan kerja sama lintas negara.
2003	APPI Jepang	Menjadi dasar perlindungan informasi pribadi di Jepang.
2012	PDPA Singapura	Mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi.
2017	*Cybersecurity Law* Tiongkok	Mengatur keamanan jaringan, infrastruktur informasi kritis, dan kewajiban operator digital.
2018	GDPR mulai berlaku	Memperkuat hak subjek data dan kewajiban organisasi dalam pemrosesan data pribadi.
2021	*Data Security Law* Tiongkok	Mengatur klasifikasi, pemrosesan, dan keamanan data.
2021	PIPL Tiongkok	Mengatur pemrosesan informasi pribadi dan hak individu atas data pribadinya.

2.4 Perkembangan Hukum Teknologi Informasi di Indonesia

Perkembangan hukum teknologi informasi di Indonesia berlangsung secara bertahap, mengikuti pertumbuhan penggunaan komputer, internet, transaksi elektronik, dan pemrosesan data pribadi. Pada awalnya, persoalan yang muncul akibat penggunaan teknologi ditangani melalui ketentuan hukum umum. Seiring dengan meningkatnya kompleksitas aktivitas digital, Indonesia kemudian membentuk sejumlah regulasi khusus yang mengatur informasi elektronik, transaksi digital, keamanan siber, penyelenggaraan sistem elektronik, dan pelindungan data pribadi.

2.4.1 Era Pradigital dan Landasan Awal

Perkembangan hukum teknologi informasi di Indonesia tidak dapat dilepaskan dari konteks sejarah, politik, ekonomi, dan perkembangan infrastruktur komunikasi nasional. Sebelum terbentuknya regulasi khusus di bidang teknologi informasi, berbagai persoalan yang berkaitan dengan penggunaan komputer dan komunikasi elektronik ditangani dengan menggunakan peraturan yang pada awalnya tidak dirancang untuk aktivitas digital.

Kitab Undang-Undang Hukum Pidana, ketentuan hukum perdata, Undang-Undang Hak Cipta, dan peraturan di bidang telekomunikasi menjadi landasan awal dalam menangani persoalan hukum yang melibatkan teknologi. Namun, ketentuan tersebut memiliki keterbatasan ketika diterapkan pada perbuatan yang menggunakan komputer, data elektronik, atau jaringan internet. Karakter kejahatan komputer, seperti akses tanpa hak, manipulasi data, dan pencurian informasi, tidak selalu dapat disamakan dengan tindak pidana konvensional yang melibatkan benda berwujud (A. Raharjo, 2002).

Penggunaan jaringan internet di Indonesia mulai berkembang pada awal dekade 1990-an melalui komunitas akademik dan kelompok pengguna teknologi. Pada pertengahan dekade tersebut, akses internet komersial mulai tersedia dan mendorong pertumbuhan penyedia jasa internet, situs web, surat elektronik, serta berbagai layanan komunikasi digital.

Perkembangan internet memperluas ruang komunikasi masyarakat dan memungkinkan pertukaran informasi berlangsung secara lebih cepat. Pada saat yang sama, internet juga menimbulkan persoalan baru, seperti penyebaran konten ilegal, pelanggaran hak cipta, penipuan elektronik, akses tanpa hak, dan pelanggaran privasi.

Krisis ekonomi dan perubahan politik pada periode 1997–1998 turut memengaruhi perkembangan penggunaan internet di Indonesia. Pada masa Reformasi, internet berkembang sebagai sarana penyebaran informasi, komunikasi politik, aktivitas masyarakat sipil, dan media alternatif. Semangat keterbukaan, transparansi, dan kebebasan memperoleh informasi mendorong peningkatan penggunaan media digital dalam kehidupan masyarakat.

Pemerintah kemudian mulai memandang teknologi informasi sebagai bagian penting dari pembangunan nasional. Berbagai kebijakan mengenai telematika, telekomunikasi, pemerintahan elektronik, dan pengembangan infrastruktur digital mulai disusun. Namun, hingga awal dekade 2000-an, Indonesia belum memiliki satu undang-undang khusus yang secara komprehensif mengatur informasi dan transaksi elektronik.

Ketiadaan regulasi khusus tersebut menimbulkan persoalan dalam menentukan keabsahan dokumen elektronik, tanda tangan elektronik, kontrak digital, dan alat bukti elektronik. Penegak hukum juga menghadapi kesulitan ketika menangani perbuatan yang dilakukan melalui sistem komputer karena ketentuan pidana konvensional belum sepenuhnya menjangkau karakteristik kejahatan digital.

2.4.2 UU ITE dan Kelahiran Hukum Siber Indonesia

Tonggak utama perkembangan hukum teknologi informasi di Indonesia adalah pengesahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau UU ITE pada 21 April 2008. Undang-undang tersebut memberikan landasan hukum bagi penggunaan informasi elektronik, dokumen elektronik, tanda tangan elektronik, dan transaksi elektronik di Indonesia (Republik Indonesia, 2008).

Pengesahan UU ITE menandai terbentuknya kerangka hukum khusus untuk mengatur aktivitas di ruang siber. Undang-undang tersebut didasarkan pada pemikiran bahwa penggunaan teknologi informasi harus mendukung perdagangan, pertumbuhan ekonomi, pelayanan publik, dan kesejahteraan masyarakat. Pada saat yang sama, pemanfaatan teknologi perlu diselenggarakan dengan memperhatikan kepastian hukum, kehati-hatian, keamanan, dan perlindungan terhadap kepentingan masyarakat.

Salah satu kontribusi utama UU ITE adalah pengakuan terhadap informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah. Pengakuan tersebut memperluas jenis alat bukti yang sebelumnya dikenal dalam hukum acara Indonesia. Dokumen yang dibuat, dikirimkan, diterima, atau disimpan secara elektronik dapat digunakan dalam proses hukum selama memenuhi persyaratan yang ditentukan oleh peraturan perundang-undangan.

UU ITE juga memberikan pengakuan terhadap tanda tangan elektronik. Dalam konteks transaksi digital, tanda tangan elektronik berfungsi sebagai alat autentikasi dan verifikasi identitas penanda tangan. Penggunaannya dapat memberikan kekuatan hukum dan akibat hukum selama memenuhi persyaratan mengenai identitas, penguasaan data pembuatan tanda tangan, serta mekanisme pendeteksian perubahan informasi.

Selain mengatur transaksi elektronik, UU ITE memuat sejumlah larangan terhadap perbuatan di ruang digital. Larangan tersebut mencakup distribusi konten tertentu, akses tanpa hak terhadap komputer atau sistem elektronik, intersepsi tanpa hak, manipulasi data, gangguan terhadap sistem elektronik, dan perbuatan lain yang menimbulkan kerugian bagi pihak lain.

Secara garis besar, materi UU ITE Nomor 11 Tahun 2008 meliputi hal-hal berikut.

Bab II: Asas dan tujuan

Bagian ini mengatur asas pemanfaatan teknologi informasi dan transaksi elektronik, seperti kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi.

Bab III: Informasi, dokumen, dan tanda tangan elektronik

Bagian ini memuat pengakuan terhadap informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah serta ketentuan mengenai tanda tangan elektronik.

Bab IV: Penyelenggaraan sertifikasi elektronik dan sistem elektronik

Bagian ini mengatur penyelenggara sertifikasi elektronik serta kewajiban penyelenggara sistem elektronik untuk mengoperasikan sistem yang andal dan aman.

Bab V: Transaksi elektronik

Bagian ini mengatur pelaksanaan transaksi elektronik dalam lingkup publik maupun privat serta penggunaan agen elektronik.

Bab VI: Nama domain, hak kekayaan intelektual, dan perlindungan hak pribadi

Bagian ini mengatur penggunaan nama domain, perlindungan terhadap karya intelektual dalam sistem elektronik, dan penggunaan data yang berkaitan dengan hak pribadi.

Bab VII: Perbuatan yang dilarang

Bagian ini mengatur konten yang dilarang, akses tanpa hak, intersepsi ilegal, manipulasi data, gangguan sistem, dan berbagai bentuk pelanggaran lainnya.

Bab VIII: Penyelesaian sengketa

Bagian ini mengatur gugatan perdata, penyelesaian sengketa melalui arbitrase, serta alternatif penyelesaian sengketa lainnya.

Bab IX: Peran pemerintah dan peran masyarakat

Bagian ini mengatur tanggung jawab pemerintah dalam memfasilitasi pemanfaatan teknologi informasi serta partisipasi masyarakat dalam penyelenggaraan sistem elektronik.

Bab X: Penyidikan

Bagian ini mengatur kewenangan penyidik dalam menangani tindak pidana di bidang teknologi informasi dan transaksi elektronik.

Bab XI: Ketentuan pidana

Bagian ini memuat ancaman pidana terhadap pelanggaran atas perbuatan-perbuatan yang dilarang dalam UU ITE.

Bab XII dan Bab XIII: Ketentuan peralihan dan ketentuan penutup

Bagian ini mengatur masa peralihan dan mulai berlakunya UU ITE.

Meskipun memberikan dasar hukum yang penting, penerapan UU ITE menimbulkan berbagai kritik. Kritik terutama diarahkan pada beberapa ketentuan pidana yang dinilai memiliki rumusan luas dan berpotensi menimbulkan perbedaan penafsiran. Ketentuan mengenai pencemaran nama baik, kesusilaan, ancaman, dan penyebaran informasi yang menimbulkan kebencian menjadi bagian yang paling sering diperdebatkan.

Sejumlah kasus menunjukkan bahwa UU ITE tidak hanya digunakan untuk menangani serangan terhadap sistem elektronik, tetapi juga digunakan dalam perselisihan antarpengguna media digital. Kondisi tersebut memunculkan

kekhawatiran bahwa ketentuan pidana dapat digunakan secara berlebihan dan berdampak terhadap kebebasan berekspresi.

Keadaan tersebut menunjukkan bahwa perkembangan hukum siber tidak cukup dilakukan melalui pembentukan undang-undang. Regulasi juga perlu dirumuskan secara jelas, diterapkan secara proporsional, dan didukung oleh pemahaman penegak hukum terhadap karakter teknologi digital. Perbandingan dengan negara lain menunjukkan bahwa keseimbangan antara keamanan siber, kepastian hukum, dan perlindungan hak warga merupakan salah satu tantangan utama regulasi teknologi (Hardjaloka, 2015).

2.4.3 Perkembangan Regulasi Pasca-UU ITE

Setelah UU ITE disahkan, ekosistem regulasi teknologi informasi di Indonesia berkembang melalui pembentukan undang-undang, peraturan pemerintah, peraturan presiden, dan berbagai peraturan teknis. Perkembangan tersebut mencerminkan semakin luasnya penggunaan sistem elektronik dalam pelayanan publik, perdagangan, komunikasi, perbankan, dan pengelolaan data.

Salah satu regulasi pelaksana awal UU ITE adalah Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan tersebut mengatur kewajiban penyelenggara sistem elektronik, tata kelola sistem, keamanan informasi, sertifikasi elektronik, dan pelaksanaan transaksi elektronik.

Pada tahun 2019, Peraturan Pemerintah Nomor 82 Tahun 2012 dicabut dan digantikan oleh Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan baru tersebut memperbarui klasifikasi penyelenggara sistem elektronik serta ketentuan mengenai pengelolaan, penempatan, dan perlindungan data dalam penyelenggaraan sistem elektronik.

Perubahan pertama terhadap UU ITE dilakukan melalui Undang-Undang Nomor 19 Tahun 2016. Perubahan tersebut dilakukan untuk memperjelas sejumlah ketentuan, menyesuaikan ancaman pidana, memperkuat perlindungan hak pribadi, serta memberikan dasar bagi penghapusan informasi elektronik tertentu berdasarkan penetapan pengadilan (Republik Indonesia, 2016b).

Undang-Undang Nomor 19 Tahun 2016 juga memperjelas bahwa ketentuan pencemaran nama baik merupakan delik aduan. Selain itu, undang-undang tersebut mengubah beberapa ancaman pidana dan memperkuat kewenangan pemerintah dalam mencegah penyebarluasan informasi elektronik yang memiliki muatan terlarang.

Meskipun telah dilakukan perubahan, perdebatan mengenai penerapan UU ITE tetap berlangsung. Sejumlah ketentuan masih dinilai dapat menimbulkan multitafsir dan ketidakpastian hukum. Kondisi tersebut mendorong penyusunan pedoman implementasi dan perubahan lebih lanjut terhadap UU ITE.

Dalam bidang keamanan siber, pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 53 Tahun 2017. Peraturan tersebut kemudian diubah melalui Peraturan Presiden Nomor 133 Tahun 2017. Pembentukan BSSN mengintegrasikan fungsi persandian, keamanan informasi, dan penanganan keamanan siber dalam suatu lembaga pemerintah (Republik Indonesia, 2017).

Kedudukan, tugas, fungsi, serta struktur organisasi BSSN kemudian diatur kembali melalui Peraturan Presiden Nomor 28 Tahun 2021. Berdasarkan peraturan tersebut, BSSN berkedudukan di bawah dan bertanggung jawab kepada Presiden serta memiliki tugas melaksanakan urusan pemerintahan di bidang keamanan siber dan sandi (Republik Indonesia, 2021).

Pembentukan BSSN menunjukkan bahwa keamanan siber telah berkembang menjadi bagian dari kebijakan keamanan nasional. Ancaman terhadap sistem pemerintahan, layanan publik, perbankan, transportasi, energi, dan infrastruktur informasi vital tidak lagi dipandang hanya sebagai persoalan teknis, tetapi juga sebagai risiko terhadap kepentingan negara.

Perkembangan penting berikutnya adalah pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi atau UU PDP. Undang-undang tersebut membentuk kerangka hukum nasional yang lebih komprehensif mengenai pemrosesan dan pelindungan data pribadi (Republik Indonesia, 2022b).

UU PDP mengatur jenis data pribadi, dasar pemrosesan data, hak subjek data, kewajiban pengendali dan prosesor data pribadi, transfer data, penyelesaian sengketa, sanksi administratif, serta ketentuan pidana. Pengaturan tersebut menunjukkan pergeseran pendekatan hukum dari

perlindungan data yang tersebar dalam berbagai regulasi sektoral menuju suatu kerangka hukum nasional.

Hak-hak subjek data pribadi dalam UU PDP antara lain meliputi hak memperoleh informasi, mengakses data, memperbaiki data, mengakhiri pemrosesan, menghapus atau memusnahkan data, menarik persetujuan, mengajukan keberatan terhadap keputusan otomatis, dan mengajukan gugatan atas pelanggaran pemrosesan data.

UU PDP juga mengatur kewajiban untuk menunjuk pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi dalam kondisi tertentu. Kewajiban tersebut berlaku, antara lain, apabila pemrosesan data dilakukan untuk kepentingan pelayanan publik, pemantauan sistematis dalam skala besar, atau pemrosesan data pribadi yang bersifat spesifik dalam skala besar.

Perubahan kedua terhadap UU ITE dilakukan melalui Undang-Undang Nomor 1 Tahun 2024. Perubahan tersebut bertujuan memperbaiki sejumlah ketentuan yang masih menimbulkan multitafsir, meningkatkan kepastian hukum, memperkuat perlindungan anak dalam penyelenggaraan sistem elektronik, serta menyesuaikan tanggung jawab penyelenggara sistem elektronik dengan perkembangan platform digital (Republik Indonesia, 2024b).

Perubahan kedua tersebut juga menata kembali ketentuan mengenai konten yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan, pengancaman, pemberitahuan bohong, dan informasi yang menimbulkan kebencian atau permusuhan. Penyesuaian ini menunjukkan bahwa regulasi teknologi informasi di Indonesia terus berkembang sebagai respons terhadap perubahan teknologi dan praktik penerapan hukum.

Tabel 2.3: Tonggak Perkembangan Regulasi Teknologi Informasi di Indonesia

Tahun	Peristiwa atau Regulasi	Keterangan
Awal 1990-an	Perkembangan jaringan internet akademik	Internet mulai digunakan oleh komunitas akademik dan kelompok pengguna teknologi di Indonesia.
1994	Perkembangan akses internet komersial	Penyedia jasa internet komersial mulai berkembang dan memperluas akses masyarakat terhadap internet.

Tahun	Peristiwa atau Regulasi	Keterangan
2008	Undang-Undang Nomor 11 Tahun 2008	Menjadi landasan hukum utama informasi dan transaksi elektronik di Indonesia.
2012	Peraturan Pemerintah Nomor 82 Tahun 2012	Mengatur penyelenggaraan sistem dan transaksi elektronik sebagai pelaksanaan UU ITE.
2016	Undang-Undang Nomor 19 Tahun 2016	Menjadi perubahan pertama atas UU ITE dan menyempurnakan sejumlah ketentuan pidana serta perlindungan hak pribadi.
2017	Peraturan Presiden Nomor 53 Tahun 2017	Menjadi dasar pembentukan Badan Siber dan Sandi Negara.
2019	Peraturan Pemerintah Nomor 71 Tahun 2019	Menggantikan PP Nomor 82 Tahun 2012 dan memperbarui ketentuan penyelenggaraan sistem elektronik.
2021	Peraturan Presiden Nomor 28 Tahun 2021	Mengatur kembali kedudukan, tugas, fungsi, dan organisasi BSSN.
2022	Undang-Undang Nomor 27 Tahun 2022	Membentuk kerangka nasional mengenai pelindungan data pribadi.
2024	Undang-Undang Nomor 1 Tahun 2024	Menjadi perubahan kedua atas UU ITE dan menyesuaikan pengaturan dengan perkembangan platform digital.

2.5 Transformasi Regulasi dari Era Komputer ke Era Internet

Perkembangan teknologi telah mengubah orientasi regulasi dari perlindungan perangkat dan data yang tersimpan secara lokal menuju pengaturan arus informasi, transaksi lintas negara, serta tanggung jawab para pelaku dalam ekosistem digital. Perubahan tersebut tidak berlangsung secara terputus, melainkan melalui proses adaptasi hukum yang mengikuti perkembangan komputer, internet, dan platform digital.

2.5.1 Era Komputer: Regulasi Pemrosesan Data

Era komputer yang berlangsung sekitar dekade 1950-an hingga akhir 1980-an ditandai oleh penggunaan komputer dalam lingkungan yang relatif terbatas dan terkontrol, seperti pusat data perusahaan, lembaga pemerintah, universitas, dan laboratorium penelitian. Pada masa tersebut, komputer masih merupakan perangkat yang mahal dan kompleks serta hanya dapat dioperasikan oleh personel yang memiliki keahlian khusus.

Konektivitas antarkomputer pada era tersebut masih sangat terbatas. Sebagian besar sistem beroperasi secara mandiri atau hanya terhubung melalui jaringan lokal dan sambungan *dial-up* dengan kecepatan rendah. Oleh karena itu, risiko hukum yang muncul lebih banyak berkaitan dengan pengelolaan perangkat, pemrosesan data internal, dan akses fisik terhadap sistem komputer.

Regulasi pada era komputer berfokus pada perlindungan data yang tersimpan dalam basis data dan pengamanan sistem dari akses tanpa hak. Kemampuan komputer untuk menyimpan, menggabungkan, dan menganalisis informasi dalam jumlah besar memunculkan kekhawatiran bahwa pemerintah atau perusahaan dapat membangun profil individu secara terperinci tanpa sepengetahuan orang yang bersangkutan (Bainbridge, 2008).

Ancaman utama yang menjadi perhatian pembentuk hukum pada era komputer meliputi tiga hal. Pertama, penggunaan komputer oleh pemerintah atau perusahaan untuk mengumpulkan dan memproses data pribadi dalam jumlah besar yang dapat mengarah pada terbentuknya negara pengawasan (*surveillance state*). Kedua, akses tanpa hak oleh peretas (*hacker*) yang didorong oleh rasa ingin tahu, keuntungan ekonomi, atau kepentingan politik. Ketiga, tindakan sabotase terhadap sistem komputer yang digunakan untuk menjalankan fungsi penting.

Undang-undang yang lahir pada periode tersebut pada umumnya memandang komputer sebagai aset yang memerlukan perlindungan fisik dan hukum. Konsep akses tanpa hak (*unauthorized access*) sering dirumuskan dengan menggunakan analogi tindak pidana memasuki suatu tempat tanpa izin (*breaking and entering*). Namun, analogi tersebut tidak selalu memadai karena akses terhadap sistem komputer dapat dilakukan dari

jarak jauh tanpa memasuki lokasi fisik tempat perangkat berada (Koops, 2010).

Data juga cenderung dipandang sebagai properti milik organisasi yang mengumpulkan dan menyimpannya. Kepentingan individu sebagai subjek data belum memperoleh perhatian sebesar perlindungan terhadap kepemilikan dan keamanan sistem. Perkembangan hukum perlindungan data kemudian mengubah pandangan tersebut dengan menempatkan individu sebagai pihak yang memiliki hak atas cara data pribadinya dikumpulkan, digunakan, dan disebarluaskan.

2.5.2 Era Internet: Regulasi Jaringan Global

Komersialisasi internet pada awal dekade 1990-an mengubah lanskap regulasi teknologi secara mendasar. Peluncuran *World Wide Web* oleh Tim Berners-Lee pada tahun 1991 dan berkembangnya peramban grafis (*graphical browser*), seperti Mosaic pada tahun 1993, mempermudah masyarakat dalam mengakses serta menyebarluaskan informasi melalui jaringan global.

Internet menghadirkan konektivitas yang memungkinkan individu, perusahaan, dan pemerintah berkomunikasi serta bertransaksi melintasi batas negara secara cepat dan relatif murah. Kondisi tersebut menciptakan hubungan hukum yang lebih kompleks daripada era komputer karena suatu aktivitas digital dapat melibatkan pelaku, korban, penyedia layanan, peladen, dan data yang berada di beberapa negara sekaligus.

Salah satu tantangan regulasi yang paling mendasar pada era internet adalah penentuan yurisdiksi. Sebagai contoh, seseorang di Indonesia dapat mengakses situs web yang datanya disimpan pada peladen di Amerika Serikat, menggunakan konten yang dibuat di negara lain, dan melakukan transaksi yang menimbulkan kerugian bagi warga negara Australia. Dalam keadaan tersebut, muncul persoalan mengenai hukum negara yang berlaku, pengadilan yang berwenang, dan mekanisme pelaksanaan putusan.

Karakter internet yang lintas batas menyebabkan yurisdiksi tidak lagi dapat ditentukan hanya berdasarkan lokasi fisik pelaku atau korban. Negara dapat menggunakan beberapa dasar untuk menetapkan kewenangan hukumnya, seperti lokasi pelaku, tempat timbulnya kerugian, kewarganegaraan korban, lokasi sistem elektronik, atau sasaran dari aktivitas digital. Perbedaan dasar

tersebut dapat menimbulkan tumpang tindih kewenangan dan konflik hukum antarnegara (Murray, 2019).

Era internet juga memunculkan persoalan mengenai tanggung jawab perantara digital (*intermediary liability*). Sebelum internet berkembang, tanggung jawab atas konten relatif lebih mudah ditentukan. Penerbit surat kabar bertanggung jawab atas artikel yang diterbitkan, sedangkan lembaga penyiaran bertanggung jawab atas program yang disiarkan.

Dalam lingkungan internet, muncul berbagai pihak yang memfasilitasi komunikasi tanpa selalu membuat atau mengendalikan konten secara langsung. Pihak tersebut mencakup penyedia jasa internet (*Internet Service Provider* atau ISP), penyedia layanan penyimpanan, mesin pencari, platform media sosial, dan lokapasar daring (*online marketplace*).

Persoalan hukumnya adalah menentukan sejauh mana perantara digital harus bertanggung jawab atas konten atau aktivitas yang dilakukan oleh penggunanya. Tanggung jawab yang terlalu luas dapat mendorong penyedia layanan menghapus konten secara berlebihan dan menghambat kebebasan berekspresi. Sebaliknya, perlindungan yang terlalu luas dapat menyebabkan platform mengabaikan konten ilegal dan aktivitas yang merugikan pengguna.

Pendekatan regulasi kemudian berkembang melalui mekanisme pembatasan tanggung jawab atau *safe harbour*. Berdasarkan pendekatan tersebut, penyedia layanan tidak serta-merta bertanggung jawab atas setiap konten pengguna selama memenuhi persyaratan tertentu, seperti tidak mengetahui keberadaan konten ilegal, menyediakan mekanisme pengaduan, dan mengambil tindakan setelah memperoleh pemberitahuan yang sah.

Perubahan paradigma regulasi dari era komputer menuju era internet dapat dirangkum sebagai berikut.

- **Objek pengaturan:** era komputer berfokus pada perlindungan perangkat dan data yang tersimpan, sedangkan era internet berfokus pada arus data, komunikasi, dan konten digital.
- **Lingkup regulasi:** era komputer lebih banyak menggunakan regulasi lokal dan nasional, sedangkan era internet membutuhkan koordinasi dan kerja sama internasional.

- **Subjek hukum:** era komputer didominasi oleh lembaga pemerintah dan organisasi besar, sedangkan era internet melibatkan individu, platform, ISP, pengembang, dan penyedia infrastruktur.
- **Karakter ancaman:** era komputer menghadapi ancaman fisik serta akses lokal, sedangkan era internet menghadapi serangan virtual dan akses jarak jauh.
- **Konsep privasi:** era komputer menekankan keamanan basis data, sedangkan era internet menekankan hak individu untuk mengendalikan pemrosesan data pribadinya.
- **Penentuan yurisdiksi:** era komputer relatif mudah dikaitkan dengan lokasi fisik sistem, sedangkan era internet melibatkan banyak yurisdiksi dan berpotensi menimbulkan konflik hukum.
- **Tanggung jawab konten:** era komputer menempatkan tanggung jawab pada pembuat atau penerbit, sedangkan era internet memunculkan persoalan mengenai tanggung jawab perantara dan platform.

Transformasi tersebut menunjukkan bahwa arsitektur teknologi turut memengaruhi perilaku pengguna dan efektivitas regulasi. Hukum tidak hanya berinteraksi dengan norma sosial dan mekanisme pasar, tetapi juga dengan kode serta desain teknis yang menentukan tindakan yang dapat dilakukan dalam suatu sistem digital (Lessig, 2006).

2.5.3 Era Platform Digital: Regulasi Ekosistem Digital

Memasuki dekade 2010-an, internet mengalami transformasi lebih lanjut melalui berkembangnya ekosistem platform digital. Platform tidak hanya menyediakan ruang komunikasi, tetapi juga mengatur interaksi antara pengguna, pelaku usaha, pemasang iklan, pengembang aplikasi, penyedia jasa, dan berbagai pihak lainnya.

Sejumlah perusahaan teknologi memiliki posisi dominan dalam ekosistem digital. Google menguasai sebagian besar layanan pencarian dan periklanan digital, Meta memiliki pengaruh besar dalam media sosial, Amazon berperan penting dalam perdagangan elektronik dan komputasi awan (*cloud computing*), sedangkan Apple dan Google mengendalikan distribusi aplikasi melalui *App Store* dan *Play Store*.

Dominasi tersebut menimbulkan bentuk kekuatan pasar yang berbeda dari pasar konvensional. Nilai suatu platform cenderung meningkat seiring

dengan bertambahnya jumlah pengguna. Fenomena ini dikenal sebagai efek jaringan (*network effect*). Semakin banyak pengguna yang bergabung, semakin sulit bagi platform baru untuk bersaing karena harus membangun basis pengguna, data, infrastruktur, dan ekosistem secara bersamaan.

Platform juga mengumpulkan data dalam jumlah besar yang dapat digunakan untuk mengembangkan layanan, mengarahkan iklan, menentukan rekomendasi, dan memperkuat posisi pasar. Penguasaan data tersebut dapat menciptakan hambatan bagi pesaing serta menimbulkan persoalan mengenai privasi, diskriminasi algoritmik, dan transparansi penggunaan data.

Regulasi pada era platform digital berfokus pada beberapa isu berikut.

1. **Kekuatan pasar dan monopoli digital**

   Platform yang memiliki posisi dominan dapat menentukan syarat perdagangan, membatasi akses pesaing, mengutamakan produknya sendiri, atau mengendalikan akses pelaku usaha terhadap konsumen. Praktik tersebut menuntut penyesuaian hukum persaingan usaha agar mampu menangani karakter pasar digital.

2. **Tanggung jawab terhadap konten**

   Platform media sosial dan layanan berbagi konten memengaruhi informasi yang dilihat pengguna melalui sistem rekomendasi. Oleh karena itu, tanggung jawab platform tidak hanya berkaitan dengan penghapusan konten ilegal, tetapi juga dengan transparansi algoritma, mekanisme pengaduan, dan pencegahan penyebaran konten yang membahayakan.

3. **Pelindungan data pribadi**

   Model bisnis platform digital banyak bergantung pada pengumpulan dan analisis data pengguna. Regulasi diperlukan untuk memastikan bahwa pengumpulan data dilakukan secara sah, transparan, terbatas pada tujuan tertentu, dan disertai langkah keamanan yang memadai.

4. **Perlindungan pekerja dalam ekonomi gig**

   Platform transportasi, pengantaran, dan jasa digital melahirkan ekonomi gig (*gig economy*) yang mempertemukan penyedia jasa dengan konsumen. Status hukum pekerja platform menimbulkan perdebatan

karena mereka dapat dikategorikan sebagai mitra independen, tetapi dalam praktiknya sering berada di bawah kendali algoritma platform.

5. **Perpajakan perusahaan digital**

   Perusahaan digital dapat memberikan layanan dan memperoleh pendapatan dari suatu negara tanpa memiliki kehadiran fisik yang signifikan. Kondisi tersebut menimbulkan tantangan bagi sistem perpajakan yang secara tradisional didasarkan pada lokasi perusahaan dan bentuk usaha tetap.

6. **Keamanan nasional dan kedaulatan data**

   Kepemilikan asing terhadap platform yang mengelola data dalam jumlah besar dapat menimbulkan kekhawatiran mengenai akses pemerintah asing, pemindahan data lintas negara, manipulasi informasi, dan ketergantungan terhadap infrastruktur digital tertentu.

Salah satu respons regulasi paling komprehensif terhadap dominasi platform digital adalah pengesahan *Digital Markets Act* (DMA) dan *Digital Services Act* (DSA) oleh Uni Eropa pada tahun 2022 (European Parliament and Council of the European Union, 2022c, 2022b).

DMA berfokus pada platform besar yang berkedudukan sebagai penjaga gerbang (*gatekeeper*) dalam pasar digital. Platform yang ditetapkan sebagai *gatekeeper* harus mematuhi sejumlah kewajiban, seperti memberikan kesempatan yang adil kepada pelaku usaha, mendukung interoperabilitas dalam kondisi tertentu, dan tidak mengutamakan layanan miliknya secara tidak adil.

DSA berfokus pada keamanan dan tanggung jawab layanan digital. Regulasi tersebut mewajibkan platform menyediakan mekanisme pelaporan konten ilegal, menjelaskan keputusan moderasi, meningkatkan transparansi iklan, dan mengelola risiko sistemik yang ditimbulkan oleh layanan mereka.

Platform yang sangat besar juga diwajibkan melakukan penilaian terhadap risiko penyebaran konten ilegal, manipulasi layanan, ancaman terhadap proses demokrasi, dan dampak terhadap hak fundamental. Kewajiban tersebut menunjukkan pergeseran dari pendekatan reaktif menuju tata kelola risiko yang lebih preventif.

DMA dan DSA menggambarkan perubahan paradigma regulasi teknologi. Pemerintah tidak lagi hanya bertindak setelah terjadi pelanggaran, tetapi juga

menetapkan kewajiban khusus berdasarkan ukuran, fungsi, dan pengaruh sistemik suatu platform. Pendekatan tersebut menempatkan akuntabilitas, transparansi, dan manajemen risiko sebagai unsur utama dalam tata kelola ekosistem digital.

2.6 Arah Perkembangan Hukum Teknologi pada Masa Depan

Perkembangan kecerdasan buatan, *blockchain*, komputasi kuantum, dan teknologi berbasis data akan terus mengubah hubungan hukum antara individu, perusahaan, platform, dan negara. Hukum teknologi pada masa depan tidak hanya berfungsi untuk menindak pelanggaran setelah terjadi, tetapi juga diarahkan pada pencegahan risiko, pengawasan sistem, transparansi teknologi, dan penetapan tanggung jawab sejak tahap perancangan.

2.6.1 Hukum dan Kecerdasan Buatan

Kecerdasan buatan (*Artificial Intelligence* atau AI) menjadi salah satu tantangan utama dalam perkembangan hukum teknologi. Berbeda dengan perangkat lunak konvensional yang menjalankan instruksi secara relatif tetap, sistem AI dapat menghasilkan prediksi, rekomendasi, keputusan, teks, gambar, suara, atau kode berdasarkan pola yang dipelajari dari data.

Kemampuan tersebut tidak berarti bahwa AI telah menjadi subjek hukum yang berdiri sendiri. Tanggung jawab hukum pada umumnya tetap dilekatkan kepada manusia atau organisasi yang mengembangkan, menyediakan, mengoperasikan, dan menggunakan sistem tersebut. Namun, pembagian tanggung jawab menjadi lebih kompleks ketika suatu sistem melibatkan pengembang model, penyedia data, penyedia layanan, pengelola platform, dan pengguna yang berbeda.

Permasalahan pertama berkaitan dengan tanggung jawab atas kerugian yang dihasilkan oleh sistem AI. Apabila kendaraan otonom menyebabkan kecelakaan atau sistem pendukung keputusan medis memberikan rekomendasi yang keliru, perlu ditentukan pihak yang bertanggung jawab. Pihak tersebut dapat mencakup produsen perangkat, pengembang model, penyedia sistem, operator, institusi pengguna, atau pengguna akhir.

Penentuan tanggung jawab memerlukan pemeriksaan terhadap beberapa unsur, seperti tingkat kendali manusia, tujuan penggunaan sistem, kualitas data, kepatuhan terhadap standar keselamatan, kemampuan sistem untuk diprediksi, dan tindakan yang dilakukan setelah risiko diketahui. Pendekatan tanggung jawab juga dapat berbeda berdasarkan bidang penggunaan, misalnya kesehatan, transportasi, keuangan, pendidikan, dan pelayanan publik.

Permasalahan kedua berkaitan dengan bias dan diskriminasi algoritmik. Sistem AI belajar dari data historis yang dapat mengandung ketimpangan, prasangka, atau kesalahan. Apabila data tersebut digunakan tanpa evaluasi yang memadai, sistem AI dapat menghasilkan keputusan yang merugikan kelompok tertentu dalam penerimaan kerja, pemberian kredit, pelayanan kesehatan, pendidikan, atau penegakan hukum.

Dalam konteks tersebut, hukum perlu mengatur kualitas data, pengujian sistem, dokumentasi proses pengembangan, audit algoritma, dan mekanisme keberatan bagi pihak yang dirugikan. Penggunaan sistem AI tidak dapat dijadikan alasan untuk menghilangkan tanggung jawab organisasi atas keputusan yang diambil dengan bantuan teknologi.

Permasalahan ketiga adalah transparansi dan kemampuan menjelaskan keputusan AI. Sebagian sistem AI, terutama model yang kompleks, dapat menghasilkan keputusan tanpa memberikan penjelasan yang mudah dipahami. Kondisi ini dikenal sebagai persoalan kotak hitam atau *black box*. Persoalan tersebut menjadi penting apabila AI digunakan untuk membuat keputusan yang memengaruhi hak, kesempatan, atau kewajiban seseorang.

Transparansi tidak selalu mengharuskan penyedia membuka seluruh kode sumber atau rahasia dagang. Namun, individu yang terdampak perlu memperoleh informasi yang memadai mengenai penggunaan AI, tujuan pemrosesan, faktor utama yang memengaruhi keputusan, dan mekanisme untuk meminta peninjauan oleh manusia.

Permasalahan keempat berkaitan dengan hak kekayaan intelektual. Sistem AI generatif dilatih menggunakan data dalam jumlah besar yang dapat mencakup karya yang dilindungi hak cipta. Kondisi tersebut menimbulkan perdebatan mengenai dasar hukum penggunaan data pelatihan, batas penggunaan yang wajar, kewajiban lisensi, dan hak pemegang karya.

Karya yang dihasilkan dengan bantuan AI juga menimbulkan persoalan mengenai kepengarangan dan kepemilikan. Tingkat keterlibatan manusia menjadi unsur penting dalam menentukan apakah suatu karya dapat memperoleh perlindungan hak cipta. Penggunaan perintah atau *prompt*, proses seleksi, penyuntingan, dan pengembangan lebih lanjut terhadap keluaran AI dapat menunjukkan kontribusi manusia, tetapi penilaiannya perlu dilakukan berdasarkan karakter setiap karya.

Permasalahan kelima adalah pelindungan data pribadi. Sistem AI memerlukan data untuk pelatihan, pengujian, dan pengoperasian. Data tersebut dapat mencakup identitas, perilaku, lokasi, kondisi ekonomi, kesehatan, rekaman wajah, dan bentuk data pribadi lainnya. Oleh karena itu, penggunaan AI harus memperhatikan dasar pemrosesan, pembatasan tujuan, minimalisasi data, keamanan, dan hak subjek data.

Permasalahan keenam berkaitan dengan penggunaan AI dalam pemerintahan dan sistem peradilan. AI dapat membantu analisis dokumen, penelusuran perkara, prediksi risiko, dan penyusunan rekomendasi. Namun, penerapannya harus disertai pengawasan manusia karena keputusan pemerintahan dan peradilan menyangkut hak individu serta legitimasi kekuasaan negara.

Penggunaan AI untuk pengenalan wajah, pengawasan massal, penilaian risiko kejahatan, atau penentuan hukuman juga berpotensi mengganggu privasi dan prinsip praduga tidak bersalah. Oleh karena itu, sistem AI yang digunakan oleh negara memerlukan dasar hukum yang jelas, tujuan yang sah, pembatasan kewenangan, dan mekanisme pengawasan yang independen.

Uni Eropa mengambil langkah penting melalui Regulasi (EU) 2024/1689 atau *Artificial Intelligence Act*. Regulasi tersebut diundangkan pada 2024 dan mulai berlaku pada 1 Agustus 2024 dengan penerapan ketentuan secara bertahap. Larangan terhadap praktik AI tertentu dan kewajiban literasi AI mulai diterapkan pada 2 Februari 2025, sedangkan sebagian besar ketentuan lainnya dijadwalkan berlaku mulai 2 Agustus 2026.

EU AI Act menggunakan pendekatan berbasis risiko. Regulasi tersebut tidak semata-mata mengelompokkan seluruh teknologi AI berdasarkan nama atau jenis algoritmanya, tetapi menilai tujuan penggunaan dan tingkat risiko yang ditimbulkan. Pendekatan tersebut meliputi larangan terhadap praktik

tertentu, kewajiban ketat bagi sistem berisiko tinggi, kewajiban transparansi bagi sistem tertentu, serta pengaturan terhadap model AI untuk tujuan umum atau *general-purpose AI* (European Parliament and Council of the European Union, 2024).

Sistem AI berisiko tinggi dapat mencakup penggunaan dalam infrastruktur kritis, pendidikan, ketenagakerjaan, layanan penting, penegakan hukum, migrasi, dan administrasi peradilan. Penyedianya diwajibkan menerapkan manajemen risiko, tata kelola data, dokumentasi teknis, pencatatan aktivitas, pengawasan manusia, akurasi, ketahanan, dan keamanan siber.

Isu hukum utama yang berkaitan dengan kecerdasan buatan dapat dirangkum sebagai berikut.

1. **Tanggung jawab AI:** penentuan pihak yang bertanggung jawab atas kerugian yang dihasilkan oleh sistem AI.
2. **Bias algoritmik:** pencegahan diskriminasi yang berasal dari data, desain model, atau proses penerapan sistem.
3. **Transparansi AI:** kewajiban memberikan informasi dan penjelasan kepada pihak yang dipengaruhi oleh keputusan AI.
4. **Hak kekayaan intelektual:** pengaturan data pelatihan, kepengarangan, kepemilikan, dan penggunaan karya yang dilindungi.
5. **Pelindungan data pribadi:** pembatasan pemrosesan data dalam pengembangan dan pengoperasian AI.
6. **Pengawasan manusia:** jaminan bahwa keputusan penting tetap dapat ditinjau, diperbaiki, atau dibatalkan oleh manusia.
7. **Keamanan AI:** perlindungan sistem dari manipulasi, serangan, kebocoran data, dan penggunaan yang menyimpang.
8. **AI dalam pemerintahan dan peradilan:** pembatasan penggunaan AI yang dapat memengaruhi hak dan kebebasan individu.
9. **Senjata otonom:** penentuan tanggung jawab dan batas penggunaan AI dalam konflik bersenjata.
10. **Literasi AI:** peningkatan kemampuan pengguna dan organisasi untuk memahami manfaat, keterbatasan, serta risiko sistem AI.

Perkembangan regulasi AI menunjukkan bahwa hukum tidak diarahkan untuk melarang seluruh inovasi. Regulasi lebih menekankan pada penerapan kewajiban yang proporsional dengan tingkat risiko. Sistem yang memiliki

potensi dampak besar terhadap keselamatan dan hak fundamental akan menghadapi kewajiban lebih ketat daripada aplikasi yang berisiko rendah.

2.6.2 Hukum dan Teknologi Blockchain

Teknologi *blockchain* menghadirkan bentuk pencatatan digital yang terdistribusi. Data transaksi disimpan dalam rangkaian blok dan diverifikasi berdasarkan mekanisme konsensus tertentu. Setelah tervalidasi, data menjadi sulit diubah tanpa terdeteksi karena perubahan akan memengaruhi hubungan antarblok dalam jaringan.

Meskipun sering disebut tidak dapat diubah, sifat *blockchain* tidak bersifat mutlak. Perubahan masih dapat terjadi melalui mekanisme tertentu, seperti percabangan jaringan, penguasaan mayoritas konsensus, perubahan protokol, atau kesepakatan para pengelola jaringan. Oleh karena itu, istilah "sulit diubah" lebih tepat daripada menyatakan bahwa data dalam *blockchain* sama sekali tidak dapat diubah.

Teknologi tersebut menantang asumsi hukum tradisional mengenai kepercayaan, otoritas, pencatatan, dan penggunaan perantara. Dalam sistem konvensional, pencatatan transaksi biasanya dilakukan oleh lembaga terpusat, seperti bank, pemerintah, bursa, atau notaris. Dalam jaringan *blockchain*, sebagian fungsi tersebut dapat dijalankan melalui protokol dan konsensus antaranggota jaringan.

Salah satu penerapan penting *blockchain* adalah kontrak pintar atau *smart contract*. Istilah tersebut merujuk pada kode komputer yang menjalankan tindakan secara otomatis ketika kondisi tertentu terpenuhi. Sebagai contoh, sistem dapat mengirimkan aset digital secara otomatis setelah pembayaran atau kondisi lain terverifikasi.

Smart contract tidak selalu sama dengan kontrak hukum. Sebuah program dapat menjalankan transaksi secara otomatis, tetapi belum tentu memenuhi seluruh syarat sah perjanjian, seperti kesepakatan, kecakapan para pihak, objek tertentu, dan sebab yang tidak bertentangan dengan hukum. Kode juga tidak selalu mampu menggambarkan seluruh konteks, maksud, dan kewajiban para pihak.

Persoalan muncul ketika kode mengandung kesalahan atau menghasilkan tindakan yang tidak sesuai dengan kehendak para pihak. Pelaksanaan

otomatis dapat menyebabkan aset berpindah sebelum sengketa diperiksa. Dalam kondisi tersebut, hukum perlu menentukan apakah transaksi dapat dibatalkan, siapa yang bertanggung jawab atas kesalahan kode, dan lembaga yang berwenang menyelesaikan sengketa.

Pada 2024, Komisi Perserikatan Bangsa-Bangsa untuk Hukum Perdagangan Internasional atau UNCITRAL mengadopsi *Model Law on Automated Contracting*. Instrumen tersebut memberikan kerangka bagi negara untuk mengakui penggunaan otomatisasi dan AI dalam pembentukan serta pelaksanaan kontrak. Namun, pengakuan terhadap proses otomatis tidak berarti bahwa setiap kode komputer otomatis menjadi kontrak yang sah atau tidak dapat dibatalkan.

Teknologi *blockchain* juga digunakan dalam penerbitan mata uang kripto, token, dan aset digital. Klasifikasi hukum terhadap aset tersebut berbeda antarnegara. Suatu aset dapat dikategorikan sebagai komoditas, efek, instrumen pembayaran, aset investasi, atau bentuk kekayaan digital lainnya. Perbedaan klasifikasi memengaruhi kewajiban perizinan, perpajakan, perlindungan konsumen, dan pengawasan pasar.

Uni Eropa membentuk kerangka yang lebih seragam melalui Regulasi (EU) 2023/1114 tentang pasar aset kripto atau *Markets in Crypto-Assets Regulation* (MiCA). Regulasi tersebut menetapkan ketentuan bagi penerbit aset kripto, pihak yang menawarkan aset kepada masyarakat, dan penyedia layanan aset kripto.

Aset virtual juga memiliki risiko digunakan untuk pencucian uang, pendanaan terorisme, penipuan, dan pemindahan dana lintas negara secara ilegal. *Financial Action Task Force* (FATF) mendorong negara menerapkan pendekatan berbasis risiko terhadap aset virtual dan penyedia layanan aset virtual, termasuk kewajiban perizinan atau pendaftaran, identifikasi pengguna, pemantauan transaksi, dan pelaporan aktivitas mencurigakan.

Persoalan hukum utama dalam penerapan *blockchain* meliputi hal-hal berikut.

1. Status hukum aset digital

Hukum perlu menentukan apakah suatu token merupakan alat pembayaran, komoditas, efek, bukti kepemilikan, atau jenis aset lainnya.

Penentuan tersebut berpengaruh terhadap kewenangan lembaga pengawas dan kewajiban pelaku usaha.

2. Keabsahan kontrak pintar

Pelaksanaan otomatis perlu tetap memenuhi syarat sah perjanjian, perlindungan konsumen, dan ketentuan hukum yang bersifat memaksa.

3. Kesalahan kode

Kesalahan pada kode dapat menimbulkan kerugian dalam skala besar. Pembagian tanggung jawab antara pengembang, pengelola jaringan, auditor, dan pengguna perlu ditentukan secara jelas.

4. Yurisdiksi

Jaringan *blockchain* dapat melibatkan simpul atau *node* yang tersebar di banyak negara. Keadaan tersebut menyulitkan penentuan hukum yang berlaku dan pengadilan yang berwenang.

5. Identitas para pihak

Penggunaan alamat digital dan nama samaran dapat menyulitkan proses identifikasi, verifikasi, perpajakan, dan penegakan hukum.

6. Pelindungan data pribadi

Penyimpanan data dalam jaringan yang sulit diubah dapat bertentangan dengan kewajiban koreksi atau penghapusan data pribadi. Oleh karena itu, data pribadi sebaiknya tidak selalu disimpan secara langsung pada rantai blok.

7. Perlindungan konsumen

Konsumen dapat menghadapi risiko volatilitas harga, informasi yang menyesatkan, kehilangan kunci akses, peretasan, dan kegagalan penyedia layanan.

8. Organisasi otonom terdesentralisasi

Organisasi otonom terdesentralisasi atau *decentralized autonomous organization* (DAO) menimbulkan persoalan mengenai status badan hukum, kepemilikan aset, tanggung jawab anggota, dan pihak yang dapat mewakili organisasi.

9. **Pencegahan pencucian uang**

   Penyedia layanan aset digital perlu menjalankan identifikasi pengguna dan pemantauan transaksi tanpa menghilangkan karakter inovatif teknologi.

10. **Penyelesaian sengketa**

    Sistem otomatis tetap membutuhkan mekanisme untuk menangani kesalahan, penipuan, keadaan memaksa, dan perbedaan penafsiran antarpara pihak.

Perkembangan hukum *blockchain* menunjukkan bahwa desentralisasi teknologi tidak menghilangkan kebutuhan terhadap hukum. Sebaliknya, sistem yang tidak memiliki pengelola terpusat memerlukan aturan yang lebih jelas mengenai tanggung jawab, identitas, perlindungan pengguna, dan penyelesaian sengketa.

2.6.3 Tren Global Regulasi Teknologi

Perkembangan hukum teknologi pada masa depan akan ditandai oleh regulasi yang semakin komprehensif dan berbasis risiko. Pemerintah tidak lagi hanya merespons pelanggaran setelah kerugian terjadi, tetapi mulai mewajibkan organisasi mengidentifikasi, mencegah, mendokumentasikan, dan mengurangi risiko sejak tahap perancangan teknologi.

Pertama, pendekatan regulasi akan semakin disesuaikan dengan tingkat risiko. Teknologi yang digunakan untuk hiburan atau kegiatan administratif sederhana tidak akan selalu diatur dengan cara yang sama seperti teknologi yang digunakan dalam kesehatan, transportasi, infrastruktur kritis, penegakan hukum, atau pelayanan publik.

Kedua, tanggung jawab penyedia teknologi akan semakin diperluas. Pengembang, penyedia model, platform, dan operator tidak hanya diwajibkan menjaga keamanan teknis, tetapi juga memastikan kualitas data, transparansi, perlindungan pengguna, mekanisme pengaduan, dan pengawasan manusia.

Ketiga, kedaulatan data akan semakin menonjol. Negara akan berusaha memastikan bahwa data penting warga dan institusinya tidak digunakan tanpa kontrol yang memadai. Kebijakan tersebut dapat berbentuk lokalisasi

data, pembatasan transfer lintas negara, penilaian kecukupan perlindungan, atau kewajiban menyediakan akses kepada otoritas yang berwenang.

Namun, kebijakan kedaulatan data yang terlalu ketat dapat menghambat perdagangan digital, penelitian internasional, dan penggunaan layanan global. Tantangan hukum utamanya adalah menyeimbangkan kepentingan keamanan nasional dengan kebutuhan pertukaran data yang sah dan bermanfaat.

Keempat, hak digital akan semakin dipandang sebagai bagian dari hak fundamental. Hak tersebut mencakup privasi, keamanan, akses informasi, kebebasan berekspresi, perlindungan dari diskriminasi algoritmik, dan hak untuk memperoleh peninjauan manusia terhadap keputusan otomatis.

Kelima, tanggung jawab platform akan berkembang dari kewajiban menghapus konten ilegal menuju kewajiban mengelola risiko sistemik. Platform dapat diwajibkan menjelaskan sistem rekomendasi, memberikan transparansi iklan, melindungi anak, mencegah manipulasi layanan, dan menyediakan mekanisme keberatan terhadap keputusan moderasi.

Keenam, regulasi aset digital dan teknologi keuangan akan semakin jelas. Pengaturan akan mencakup perizinan penyedia layanan, cadangan aset, keterbukaan informasi, perlindungan konsumen, keamanan penyimpanan, perpajakan, serta pencegahan pencucian uang dan pendanaan terorisme.

Ketujuh, keamanan siber akan semakin terintegrasi dengan kebijakan keamanan nasional. Serangan terhadap sistem pemerintahan, energi, kesehatan, transportasi, dan keuangan dapat menimbulkan dampak yang setara dengan gangguan terhadap infrastruktur fisik.

Kerja sama internasional dalam penanganan kejahatan siber juga terus berkembang. Majelis Umum Perserikatan Bangsa-Bangsa mengadopsi *United Nations Convention against Cybercrime* pada 24 Desember 2024. Konvensi tersebut dibuka untuk penandatanganan pada 25 Oktober 2025 dan ditujukan untuk memperkuat pencegahan, penyidikan, pertukaran bukti elektronik, bantuan teknis, dan kerja sama internasional.

Kedelapan, regulasi teknologi akan semakin memperhatikan dampak lingkungan. Pusat data, pelatihan model AI, jaringan komputasi, dan mekanisme konsensus tertentu membutuhkan energi serta sumber daya dalam jumlah besar. Perusahaan teknologi dapat menghadapi kewajiban

pelaporan penggunaan energi, emisi karbon, konsumsi air, dan pengelolaan limbah elektronik.

Kesembilan, kolaborasi antara pakar hukum dan pakar teknologi akan menjadi semakin penting. Regulasi yang efektif tidak dapat disusun hanya berdasarkan konsep hukum tanpa memahami cara kerja teknologi. Sebaliknya, teknologi tidak dapat dikembangkan hanya berdasarkan pertimbangan teknis tanpa memperhatikan keadilan, hak asasi manusia, dan kepentingan publik.

Bidang seperti teknologi hukum (*LegalTech*), hukum komputasional (*computational law*), audit algoritma, dan akuntabilitas algoritmik akan terus berkembang. Bidang-bidang tersebut berupaya menerjemahkan norma hukum ke dalam desain sistem sekaligus menilai apakah teknologi telah bekerja sesuai dengan kewajiban hukum.

Kesepuluh, kesenjangan digital akan menjadi persoalan hukum dan etika yang semakin penting. Perbedaan akses terhadap jaringan, perangkat, keterampilan, data, dan teknologi AI dapat memperbesar ketimpangan antara kelompok masyarakat serta antara negara maju dan negara berkembang.

Arah utama perkembangan hukum teknologi pada periode 2025–2035 dapat dirangkum sebagai berikut.

1. **Regulasi AI berbasis risiko:** penerapan kewajiban yang berbeda berdasarkan tujuan dan dampak sistem AI.
2. **Penguatan kedaulatan data:** peningkatan kontrol negara terhadap data strategis dan arus data lintas negara.
3. **Perlindungan hak digital:** penguatan privasi, kebebasan berekspresi, keamanan, dan perlindungan dari keputusan otomatis yang merugikan.
4. **Akuntabilitas platform:** perluasan tanggung jawab terhadap algoritma, iklan, moderasi konten, dan risiko sistemik.
5. **Regulasi aset digital:** pembentukan kerangka yang lebih jelas bagi aset kripto, tokenisasi, dan keuangan terdesentralisasi.
6. **Keamanan infrastruktur kritis:** penguatan kewajiban keamanan siber bagi sektor pemerintahan, energi, transportasi, kesehatan, dan keuangan.
7. **Diplomasi dan kerja sama siber:** peningkatan perjanjian dan mekanisme internasional untuk penyidikan, pertukaran bukti, dan penanganan serangan siber.

8. **Regulasi teknologi berkelanjutan:** pengawasan terhadap penggunaan energi, emisi, konsumsi sumber daya, dan limbah elektronik.
9. **Pengawasan teknologi kuantum:** persiapan hukum menghadapi perubahan keamanan enkripsi akibat perkembangan komputasi kuantum.
10. **Pemerataan akses digital:** penguatan kebijakan untuk mengurangi kesenjangan teknologi, keterampilan, dan akses informasi.

Bagi Indonesia, tantangan utama bukan sekadar mengikuti model regulasi negara lain, melainkan membentuk kerangka yang sesuai dengan kondisi sosial, ekonomi, budaya, dan kapasitas kelembagaan nasional. Regulasi perlu memberikan perlindungan yang efektif terhadap masyarakat tanpa menciptakan hambatan yang tidak proporsional bagi penelitian, inovasi, dan pertumbuhan ekonomi digital.

Arah perkembangan hukum teknologi pada akhirnya akan ditentukan oleh kemampuan negara menyeimbangkan inovasi, keamanan, kepastian hukum, dan perlindungan hak. Hukum yang terlalu lambat dapat gagal melindungi masyarakat, sedangkan regulasi yang terlalu kaku dapat menghambat manfaat teknologi. Oleh karena itu, diperlukan regulasi yang adaptif, berbasis bukti, terbuka terhadap evaluasi, dan disusun melalui kolaborasi antardisiplin.

Bab 3
Konsep dan Prinsip Hukum Siber

3.1 Pengertian dan Karakteristik Hukum Siber

Perkembangan internet telah menciptakan ruang interaksi baru yang dikenal sebagai ruang siber atau *cyberspace*. Ruang ini terbentuk melalui keterhubungan perangkat komputer, jaringan komunikasi, sistem elektronik, aplikasi, dan data digital. Di dalamnya, individu maupun organisasi dapat melakukan berbagai aktivitas, seperti berkomunikasi, membuat perjanjian, melakukan pembayaran, menyimpan data, menawarkan barang dan jasa, serta menyampaikan informasi kepada masyarakat. Meskipun berlangsung melalui perangkat dan jaringan digital, aktivitas tersebut tetap dapat menimbulkan hak, kewajiban, kerugian, dan pertanggungjawaban hukum.

Hukum siber atau *cyber law* dapat dipahami sebagai seperangkat norma hukum yang mengatur penggunaan teknologi informasi, internet, jaringan komputer, sistem elektronik, dan berbagai hubungan hukum yang timbul di dalam ruang siber. Hukum siber tidak hanya berkaitan dengan kejahatan yang dilakukan melalui komputer, tetapi juga meliputi transaksi elektronik, pelindungan data pribadi, privasi digital, hak kekayaan intelektual, perlindungan konsumen, keamanan sistem elektronik, kebebasan berekspresi, dan pembuktian elektronik (Ramli, 2004; Situmeang, 2020).

Dalam pengertian tersebut, hukum siber memiliki cakupan yang lebih luas daripada hukum kejahatan siber. Kejahatan siber merupakan salah satu bagian yang membahas perbuatan terlarang, unsur tindak pidana, pertanggungjawaban pelaku, dan sanksi pidana. Sementara itu, hukum siber juga mencakup hubungan hukum yang bersifat perdata dan administratif, seperti kontrak elektronik, tanggung jawab penyelenggara platform, pemrosesan data pribadi, perizinan sistem elektronik, serta penyelesaian sengketa digital. Oleh karena itu, hukum siber merupakan bidang hukum yang bersifat multidimensional karena mempertemukan hukum, teknologi, ekonomi, keamanan, dan kepentingan masyarakat.

Objek pengaturan hukum siber bukan hanya perangkat keras atau perangkat lunak, tetapi juga perilaku manusia dan organisasi yang menggunakan

teknologi tersebut. Pengguna, perusahaan teknologi, penyelenggara sistem elektronik, pemerintah, dan penyedia infrastruktur digital dapat menjadi subjek yang memiliki hak dan kewajiban hukum. Selain itu, data, informasi elektronik, dokumen elektronik, akun digital, identitas elektronik, nama domain, program komputer, dan aset digital dapat menjadi objek hubungan hukum.

Dalam konteks Indonesia, pengaturan utama mengenai informasi dan transaksi elektronik terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir melalui Undang-Undang Nomor 1 Tahun 2024. Ketentuan pelaksanaannya antara lain diatur melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Hukum siber mempunyai sejumlah karakteristik yang membedakannya dari pengaturan aktivitas konvensional.

Pertama, aktivitas siber bersifat virtual, tetapi menimbulkan akibat hukum yang nyata. Komunikasi atau transaksi dapat dilakukan tanpa pertemuan fisik, tetapi tetap dapat menghasilkan perjanjian, pembayaran, pemindahan hak, kerugian ekonomi, maupun pelanggaran hukum. Dengan demikian, sifat virtual dari ruang siber tidak menghapus keberadaan hubungan hukum di antara para pihak.

Kedua, aktivitas siber dapat melampaui batas wilayah negara. Pengguna, server, penyedia platform, sistem pembayaran, dan pihak yang dirugikan dapat berada di negara yang berbeda. Kondisi ini menimbulkan persoalan mengenai hukum negara mana yang berlaku, lembaga mana yang berwenang, dan bagaimana putusan hukum dapat dilaksanakan. Karakter lintas batas tersebut menjadikan yurisdiksi sebagai salah satu persoalan utama dalam hukum siber (Reed, 2012).

Ketiga, hukum siber sangat dipengaruhi oleh perkembangan teknologi. Perubahan teknologi berlangsung lebih cepat daripada proses pembentukan peraturan perundang-undangan. Kehadiran kecerdasan buatan, komputasi awan, teknologi blockchain, Internet of Things, dan platform digital dapat menghasilkan bentuk hubungan hukum dan risiko baru. Karena itu, hukum siber harus mampu beradaptasi tanpa kehilangan prinsip kepastian, keadilan, dan pelindungan hak.

Keempat, perilaku dalam ruang siber tidak hanya diatur oleh peraturan negara. Desain perangkat lunak, algoritma, kode program, standar teknis, dan kebijakan platform juga dapat menentukan tindakan yang dapat atau tidak dapat dilakukan oleh pengguna. Lessig (2006) menjelaskan bahwa arsitektur atau kode dalam ruang digital dapat berfungsi sebagai sarana pengaturan perilaku. Sebagai contoh, sistem dapat membatasi akses, menghapus konten, menolak transaksi, atau menangguhkan akun secara otomatis.

Kelima, identitas dan tindakan pengguna tidak selalu mudah dikenali secara langsung. Pengguna dapat menggunakan nama samaran, akun palsu, jaringan perantara, atau identitas milik pihak lain. Namun, aktivitas digital juga dapat meninggalkan jejak berupa alamat jaringan, catatan akses, waktu transaksi, metadata, dan rekaman sistem. Oleh sebab itu, ruang siber memiliki karakter yang tampak anonim, tetapi pada kondisi tertentu tetap dapat ditelusuri melalui pemeriksaan teknis dan forensik digital.

Keenam, pengaturan ruang siber melibatkan banyak pihak. Negara bukan satu-satunya pihak yang menentukan tata kelola ruang digital. Perusahaan teknologi, penyedia layanan internet, pengelola platform, organisasi internasional, komunitas teknis, dan pengguna turut berperan dalam pembentukan standar dan praktik digital. Hukum siber karenanya menuntut pendekatan kolaboratif yang menggabungkan regulasi negara, tata kelola organisasi, standar teknis, serta kesadaran pengguna (Murray, 2019; Rahmawati et al., 2024).

Tabel 3.1: Karakteristik Utama Hukum Siber

Karakteristik	Penjelasan
Bersifat virtual	Aktivitas dilakukan melalui sistem elektronik tanpa mensyaratkan pertemuan fisik, tetapi tetap menghasilkan akibat hukum.
Lintas batas wilayah	Pelaku, korban, data, server, dan penyedia layanan dapat berada dalam yurisdiksi yang berbeda.
Dinamis dan adaptif	Perkembangan objek pengaturan mengikuti perubahan teknologi yang berlangsung cepat.
Dipengaruhi arsitektur teknologi	Kode program, algoritma, dan desain platform dapat mengatur atau membatasi perilaku pengguna.

Karakteristik	Penjelasan
Berbasis data dan jejak digital	Aktivitas menghasilkan data elektronik yang dapat digunakan untuk identifikasi, pengawasan, dan pembuktian.
Melibatkan banyak pemangku kepentingan	Tata kelola ruang siber melibatkan pemerintah, perusahaan, komunitas teknis, organisasi internasional, dan pengguna.

Berdasarkan karakteristik tersebut, hukum siber tidak dapat dipahami hanya sebagai kumpulan larangan terhadap penyalahgunaan komputer. Hukum siber merupakan kerangka hukum untuk memastikan agar pemanfaatan teknologi berlangsung secara aman, adil, bertanggung jawab, dan memberikan kepastian bagi para pihak. Pemahaman mengenai karakteristik ini menjadi dasar untuk membahas yurisdiksi, keamanan, kebebasan informasi, dan pertanggungjawaban dalam aktivitas siber pada subbab berikutnya.

3.2 Prinsip Yurisdiksi dalam Ruang Siber

Yurisdiksi merupakan kewenangan suatu negara untuk membentuk dan memberlakukan hukum, mengadili suatu perkara, serta melaksanakan tindakan penegakan hukum. Dalam perkara konvensional, yurisdiksi umumnya ditentukan berdasarkan wilayah tempat perbuatan dilakukan. Penentuan tersebut menjadi lebih kompleks dalam ruang siber karena pelaku, korban, perangkat, server, data, penyedia layanan, dan akibat suatu perbuatan dapat berada di beberapa negara yang berbeda. Akibatnya, satu aktivitas siber dapat menimbulkan hubungan hukum dengan lebih dari satu sistem hukum pada waktu yang bersamaan (Reed, 2012; UNODC, 2013).

Sebagai contoh, seseorang yang berada di negara A dapat mengakses secara tidak sah sistem elektronik milik perusahaan di Indonesia. Sistem tersebut menggunakan layanan komputasi awan dengan pusat data di negara B, sedangkan data pelanggan yang disalahgunakan berasal dari beberapa negara. Dalam keadaan demikian, muncul pertanyaan mengenai negara yang berwenang melakukan penyidikan, hukum yang dapat diterapkan, pengadilan yang berwenang memeriksa perkara, serta mekanisme untuk memperoleh barang bukti yang berada di luar wilayah negara.

Yurisdiksi dalam hukum siber perlu dipahami dalam tiga bentuk kewenangan. Pertama, **yurisdiksi legislatif**, yaitu kewenangan negara untuk menetapkan norma hukum yang mengatur suatu perbuatan. Kedua, **yurisdiksi yudisial**, yaitu kewenangan pengadilan untuk memeriksa dan memutus perkara. Ketiga, **yurisdiksi eksekutif atau penegakan hukum**, yaitu kewenangan aparat negara untuk melakukan penyelidikan, penyidikan, penyitaan, penangkapan, atau pelaksanaan putusan. Suatu negara dapat memiliki dasar untuk menerapkan hukumnya terhadap suatu perkara, tetapi tidak selalu dapat melaksanakan tindakan penegakan hukum secara langsung di wilayah negara lain. Tindakan tersebut pada umumnya memerlukan persetujuan, bantuan hukum timbal balik, ekstradisi, atau bentuk kerja sama internasional lainnya.

Penentuan yurisdiksi dalam ruang siber dapat didasarkan pada beberapa prinsip berikut.

1. Prinsip teritorialitas

Prinsip teritorialitas memberikan kewenangan kepada negara terhadap perbuatan yang dilakukan di wilayahnya. Dalam perkara siber, wilayah terjadinya perbuatan tidak selalu mudah ditentukan. Lokasi pelaku, perangkat yang digunakan, sistem yang diserang, penyimpanan data, dan tempat timbulnya akibat dapat berbeda. Karena itu, hubungan teritorial dapat ditentukan berdasarkan tempat dilakukannya bagian penting dari perbuatan atau tempat terjadinya akibat yang substansial.

Prinsip ini tetap menjadi dasar utama yurisdiksi karena berkaitan dengan kedaulatan negara. Namun, penerapannya perlu mempertimbangkan bahwa lalu lintas data tidak selalu mengikuti batas geografis dan data dapat dipindahkan secara otomatis dari satu pusat data ke pusat data lainnya (UNODC, 2013).

2. Prinsip kewarganegaraan aktif

Berdasarkan prinsip kewarganegaraan aktif, negara dapat menerapkan hukumnya terhadap warga negaranya yang melakukan perbuatan tertentu di luar wilayah negara. Dalam konteks siber, prinsip ini dapat digunakan ketika warga negara Indonesia melakukan akses ilegal, penipuan digital, atau perbuatan siber lainnya dari luar negeri. Penerapannya tetap harus memperhatikan ketentuan hukum nasional,

hukum negara tempat perbuatan dilakukan, serta kemungkinan adanya persyaratan kriminalitas ganda.

3. Prinsip kewarganegaraan pasif

Prinsip kewarganegaraan pasif didasarkan pada kewarganegaraan korban. Negara dapat mengklaim yurisdiksi apabila warga negaranya menjadi korban perbuatan yang dilakukan dari luar wilayah negara. Dalam ruang siber, prinsip ini relevan ketika serangan, pencurian data, penipuan, atau pelecehan digital yang dilakukan dari luar negeri secara khusus ditujukan kepada warga negara suatu negara. Meskipun demikian, prinsip ini biasanya memerlukan hubungan yang cukup kuat antara perbuatan, korban, dan kepentingan negara yang mengklaim yurisdiksi.

4. Prinsip perlindungan

Prinsip perlindungan memberikan kewenangan kepada negara untuk menangani perbuatan yang dilakukan di luar wilayahnya apabila perbuatan tersebut mengancam keamanan, kedaulatan, atau kepentingan vital negara. Penerapannya dalam ruang siber dapat mencakup serangan terhadap infrastruktur informasi vital, sistem pertahanan, layanan pemerintahan, sistem keuangan nasional, atau jaringan strategis lainnya.

Prinsip ini tidak semata-mata didasarkan pada lokasi pelaku atau kewarganegaraan korban, tetapi pada kepentingan negara yang terdampak. Oleh karena itu, serangan yang dilakukan dari luar negeri tetap dapat menjadi perhatian hukum suatu negara apabila menimbulkan ancaman serius terhadap fungsi pemerintahan atau keamanan nasional.

5. Prinsip akibat

Prinsip akibat atau *effects doctrine* memungkinkan suatu negara mengklaim yurisdiksi terhadap perbuatan yang dilakukan di luar wilayahnya ketika perbuatan tersebut menimbulkan akibat yang nyata dan substansial di dalam wilayah negara tersebut. Prinsip ini penting dalam perkara siber karena serangan atau penyebaran konten dapat dilakukan dari jarak jauh.

Penerapannya harus dilakukan secara hati-hati. Keberadaan situs web atau konten yang dapat diakses dari suatu negara tidak secara otomatis cukup untuk membentuk yurisdiksi. Perlu dinilai apakah perbuatan tersebut secara sengaja diarahkan kepada wilayah tertentu, menargetkan

pengguna atau sistem di wilayah tersebut, atau menghasilkan kerugian yang dapat diperkirakan secara wajar.

6. Prinsip universalitas

Prinsip universalitas memungkinkan suatu negara menjalankan yurisdiksi terhadap kejahatan tertentu yang dipandang sebagai kejahatan serius terhadap masyarakat internasional. Prinsip ini secara tradisional diterapkan secara terbatas terhadap kejahatan internasional yang berat. Oleh karena itu, prinsip universalitas tidak dapat secara otomatis diterapkan terhadap seluruh pelanggaran atau kejahatan siber. Penerapannya bergantung pada sifat kejahatan, hukum nasional, dan ketentuan hukum internasional yang relevan.

Tabel 3.2: Prinsip-Prinsip Yurisdiksi dalam Ruang Siber

Prinsip yurisdiksi	Dasar penentuan	Contoh penerapan dalam ruang siber
Teritorialitas	Tempat perbuatan atau akibat terjadi	Sistem elektronik yang berada di Indonesia diserang dari dalam atau luar negeri.
Kewarganegaraan aktif	Kewarganegaraan pelaku	Warga negara Indonesia melakukan kejahatan siber dari luar negeri.
Kewarganegaraan pasif	Kewarganegaraan korban	Warga negara Indonesia menjadi sasaran penipuan digital lintas negara.
Perlindungan	Ancaman terhadap keamanan atau kepentingan vital negara	Serangan terhadap sistem pemerintahan atau infrastruktur informasi vital.
Akibat	Timbulnya akibat nyata dan substansial dalam wilayah negara	Serangan dari luar negeri menyebabkan kerugian terhadap perusahaan atau masyarakat di Indonesia.
Universalitas	Sifat kejahatan yang menjadi perhatian masyarakat internasional	Perbuatan siber yang menjadi bagian dari kejahatan internasional yang sangat serius.

Dalam konteks Indonesia, jangkauan yurisdiksi hukum teknologi informasi antara lain terlihat dalam Pasal 2 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ketentuan tersebut pada prinsipnya memungkinkan penerapan UU ITE terhadap perbuatan yang dilakukan di dalam maupun di luar wilayah Indonesia apabila perbuatan tersebut mempunyai akibat hukum di Indonesia atau merugikan kepentingan Indonesia (Republik Indonesia, 2008). Undang-undang tersebut selanjutnya mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024.

Jangkauan ekstrateritorial tersebut diperlukan karena lokasi fisik pelaku tidak selalu sama dengan lokasi terjadinya kerugian. Meskipun demikian, keberadaan dasar yurisdiksi tidak secara otomatis menjamin bahwa penegakan hukum dapat dilakukan dengan mudah. Aparat Indonesia dapat menghadapi kendala apabila pelaku, penyedia layanan, server, atau bukti elektronik berada di negara lain. Dalam kondisi tersebut, penanganan perkara memerlukan kerja sama antarlembaga dan antarnegara.

Convention on Cybercrime atau *Budapest Convention* memberikan salah satu kerangka mengenai yurisdiksi kejahatan siber. Pasal 22 konvensi tersebut mengakui yurisdiksi berdasarkan wilayah, kapal yang mengibarkan bendera suatu negara, pesawat yang terdaftar berdasarkan hukum negara tersebut, dan kewarganegaraan pelaku dalam kondisi tertentu. Apabila lebih dari satu negara mengklaim yurisdiksi atas perkara yang sama, negara-negara terkait diarahkan untuk berkonsultasi guna menentukan yurisdiksi yang paling tepat untuk melakukan penuntutan (Council of Europe, 2001).

Penentuan yurisdiksi yang paling tepat dapat mempertimbangkan lokasi sebagian besar perbuatan dilakukan, tempat timbulnya kerugian utama, lokasi pelaku, kewarganegaraan para pihak, keberadaan bukti elektronik, perlindungan korban, dan efektivitas pelaksanaan putusan. Pertimbangan tersebut diperlukan untuk mencegah konflik kewenangan, duplikasi proses hukum, atau keadaan ketika tidak ada negara yang bersedia menangani perkara.

> Prinsip yurisdiksi dalam ruang siber berfungsi menghubungkan aktivitas digital yang tidak mengenal batas geografis dengan kewenangan hukum negara yang masih didasarkan pada wilayah dan kedaulatan. Efektivitas penerapannya tidak hanya bergantung pada

```
luasnya ketentuan hukum nasional, tetapi juga pada koordinasi,
harmonisasi peraturan, pertukaran bukti elektronik, ekstradisi,
dan bantuan hukum timbal balik antarnegara.
```

3.3 Prinsip Keamanan, Kepastian, dan Perlindungan Hukum

Aktivitas dalam ruang siber menghadirkan berbagai kemudahan, tetapi sekaligus menimbulkan risiko terhadap sistem elektronik, data, transaksi, dan hak pengguna. Gangguan sistem, akses tanpa hak, kebocoran data, manipulasi informasi, pencurian identitas, dan kegagalan transaksi dapat menyebabkan kerugian yang luas. Oleh karena itu, penyelenggaraan aktivitas digital harus didasarkan pada prinsip keamanan, kepastian hukum, dan perlindungan hukum.

Ketiga prinsip tersebut saling berhubungan dan tidak dapat diterapkan secara terpisah. Keamanan dibutuhkan untuk menjaga sistem dan data dari gangguan. Kepastian hukum diperlukan agar para pihak mengetahui hak, kewajiban, larangan, dan akibat hukum dari tindakannya. Sementara itu, perlindungan hukum memastikan bahwa pihak yang dirugikan memiliki hak untuk memperoleh pencegahan, pemulihan, dan penyelesaian sengketa.

3.3.1 Prinsip Keamanan dalam Aktivitas Siber

Prinsip keamanan mengharuskan setiap aktivitas digital dilaksanakan dengan langkah yang memadai untuk menjaga sistem elektronik, jaringan, perangkat, dan data dari ancaman. Keamanan tidak hanya berkaitan dengan penggunaan perangkat teknis, tetapi juga mencakup tata kelola, prosedur organisasi, kompetensi sumber daya manusia, dan kepatuhan terhadap ketentuan hukum.

Keamanan siber pada dasarnya bertujuan menjaga tiga unsur utama, yaitu kerahasiaan, integritas, dan ketersediaan informasi. Kerahasiaan berarti informasi hanya dapat diakses oleh pihak yang berwenang. Integritas berarti informasi tetap lengkap, benar, dan tidak mengalami perubahan tanpa izin. Ketersediaan berarti sistem dan informasi dapat digunakan pada saat dibutuhkan oleh pihak yang berhak.

Selain ketiga unsur tersebut, keamanan sistem elektronik juga berkaitan dengan autentikasi dan akuntabilitas. Autentikasi digunakan untuk memastikan bahwa pengguna, perangkat, atau layanan yang mengakses sistem memiliki identitas yang sah. Akuntabilitas memastikan bahwa setiap aktivitas dalam sistem dapat dicatat, ditelusuri, dan dipertanggungjawabkan.

Prinsip keamanan dapat diwujudkan melalui beberapa tindakan, antara lain penggunaan autentikasi yang kuat, pembatasan hak akses, enkripsi data, pencadangan, pemantauan sistem, pencatatan aktivitas, pembaruan perangkat lunak, pengujian keamanan, dan penanganan insiden. Organisasi juga perlu menetapkan pembagian tanggung jawab yang jelas agar penanganan risiko tidak hanya dibebankan kepada bagian teknologi informasi.

Kerangka keamanan siber modern menempatkan tata kelola sebagai bagian penting dari pengelolaan risiko. Organisasi harus mengidentifikasi aset dan ancaman, menerapkan langkah perlindungan, mendeteksi gangguan, merespons insiden, dan memulihkan layanan setelah insiden terjadi. Pendekatan ini menunjukkan bahwa keamanan bukan tindakan sesaat, melainkan proses yang dilakukan secara berkelanjutan (NIST, 2024).

Dalam sistem hukum Indonesia, kewajiban menjaga keamanan sistem elektronik antara lain berkaitan dengan ketentuan mengenai penyelenggaraan sistem dan transaksi elektronik. Penyelenggara sistem elektronik pada dasarnya dituntut menyelenggarakan sistem secara andal, aman, dan bertanggung jawab terhadap beroperasinya sistem tersebut. Ketentuan ini menunjukkan bahwa keamanan merupakan kewajiban hukum, bukan sekadar pilihan teknis penyelenggara (Republik Indonesia, 2019).

Prinsip keamanan juga berhubungan dengan prinsip kehati-hatian. Penyelenggara layanan digital harus mengidentifikasi kemungkinan kerugian sebelum layanan digunakan secara luas. Tindakan pencegahan tersebut penting karena kebocoran atau gangguan sistem dapat merugikan pengguna, menghambat pelayanan publik, dan menurunkan kepercayaan masyarakat terhadap teknologi digital (Mantili & Dewi, 2020).

3.3.2 Prinsip Kepastian Hukum

Prinsip kepastian hukum menghendaki adanya aturan yang jelas, dapat diketahui, dapat dipahami, dan dapat diterapkan secara konsisten. Dalam ruang siber, kepastian hukum diperlukan karena hubungan antara para pihak sering berlangsung tanpa pertemuan langsung dan bergantung pada sistem elektronik.

Kepastian hukum membantu menentukan kedudukan informasi elektronik, keabsahan perjanjian elektronik, hak dan kewajiban pengguna, tanggung jawab penyelenggara platform, serta akibat hukum dari pelanggaran. Tanpa aturan yang jelas, para pihak akan mengalami kesulitan menentukan apakah suatu tindakan diperbolehkan, dilarang, atau menimbulkan tanggung jawab tertentu.

Prinsip ini juga menuntut agar aturan hukum mampu mengikuti perkembangan teknologi. Meskipun demikian, pembentukan aturan yang terlalu terperinci dapat menimbulkan masalah karena teknologi berubah dengan cepat. Karena itu, hukum siber perlu menggabungkan ketentuan yang jelas dengan prinsip yang cukup fleksibel untuk diterapkan pada perkembangan teknologi baru.

Kepastian hukum dalam aktivitas digital sekurang-kurangnya mencakup beberapa aspek. Pertama, kepastian mengenai identitas dan kedudukan para pihak. Kedua, kepastian mengenai keabsahan tindakan dan dokumen elektronik. Ketiga, kepastian mengenai tanggung jawab apabila terjadi kerugian. Keempat, kepastian mengenai lembaga dan prosedur penyelesaian sengketa. Kelima, kepastian mengenai sanksi terhadap pelanggaran.

Di Indonesia, kepastian hukum dalam aktivitas digital didukung oleh Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, serta peraturan sektoral lainnya. Kehadiran peraturan tersebut memberikan dasar bagi pengakuan informasi elektronik, transaksi elektronik, kewajiban penyelenggara sistem, pelindungan data pribadi, dan penegakan hukum terhadap pelanggaran digital.

Namun, kepastian hukum tidak hanya ditentukan oleh keberadaan peraturan tertulis. Penerapan yang konsisten, penafsiran yang proporsional, kapasitas

aparat penegak hukum, dan kesesuaian antarperaturan juga sangat menentukan. Aturan yang tersedia dapat kehilangan efektivitas apabila diterapkan secara berbeda-beda atau tidak didukung mekanisme penegakan yang memadai.

Kepastian hukum juga perlu diseimbangkan dengan keadilan. Penerapan aturan secara kaku tanpa memperhatikan konteks dapat menimbulkan hasil yang tidak adil. Oleh sebab itu, penegakan hukum siber harus mempertimbangkan tujuan aturan, tingkat kesalahan, kerugian yang ditimbulkan, posisi para pihak, dan kepentingan masyarakat.

3.3.3 Prinsip Perlindungan Hukum

Prinsip perlindungan hukum bertujuan menjaga hak dan kepentingan pihak yang terlibat dalam aktivitas digital. Pihak yang perlu memperoleh perlindungan tidak hanya pengguna individu, tetapi juga pelaku usaha, penyelenggara sistem elektronik, pemilik karya digital, konsumen, anak, kelompok rentan, dan masyarakat secara umum.

Perlindungan hukum dapat bersifat preventif dan represif. Perlindungan preventif dilakukan sebelum terjadi pelanggaran, misalnya melalui pengaturan standar keamanan, persetujuan pemrosesan data, transparansi layanan, pembatasan akses, kebijakan privasi, mekanisme keberatan, dan edukasi pengguna. Tujuannya adalah mengurangi kemungkinan terjadinya kerugian.

Perlindungan represif diberikan setelah terjadi pelanggaran. Bentuknya dapat berupa penghentian tindakan, penghapusan konten, pemulihan akun, pengembalian kerugian, ganti rugi, sanksi administratif, tuntutan perdata, atau penjatuhan pidana sesuai dengan karakter pelanggarannya. Perlindungan represif juga mencakup akses terhadap mekanisme pengaduan dan penyelesaian sengketa.

Dalam konteks data pribadi, perlindungan hukum mengharuskan pemrosesan data dilakukan secara sah, terbatas, transparan, dan sesuai tujuan. Pengendali dan prosesor data tidak boleh memperlakukan data pribadi sebagai sumber daya yang dapat digunakan tanpa batas. Data berkaitan dengan identitas, privasi, kebebasan, dan keamanan individu sehingga penggunaannya harus disertai tanggung jawab hukum.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar hukum yang lebih khusus mengenai hak subjek data, kewajiban pengendali dan prosesor data, pemrosesan data pribadi, serta tanggung jawab ketika terjadi kegagalan pelindungan data. Keberadaan aturan tersebut memperkuat posisi individu dalam hubungan digital yang sebelumnya sering tidak seimbang dengan organisasi pengelola data (Republik Indonesia, 2022).

Perlindungan hukum juga penting dalam hubungan antara pengguna dan platform digital. Platform umumnya memiliki kendali terhadap desain layanan, ketentuan penggunaan, pengumpulan data, moderasi konten, dan penangguhan akun. Sementara itu, pengguna sering hanya memiliki pilihan untuk menyetujui ketentuan yang telah ditetapkan. Ketimpangan posisi tersebut menuntut transparansi, keadilan prosedural, dan mekanisme keberatan yang dapat digunakan secara efektif.

Tabel 3.3: Penerapan Prinsip Keamanan, Kepastian, dan Perlindungan Hukum

Prinsip	**Tujuan utama**	**Bentuk penerapan**
Keamanan	Menjaga sistem, layanan, dan data dari ancaman atau gangguan	Pengendalian akses, enkripsi, pencadangan, pencatatan aktivitas, pemantauan, dan respons insiden
Kepastian hukum	Memastikan kejelasan hak, kewajiban, larangan, tanggung jawab, dan prosedur hukum	Pengakuan transaksi elektronik, kejelasan kontrak, pembagian tanggung jawab, dan mekanisme penyelesaian sengketa
Perlindungan hukum	Mencegah kerugian serta memulihkan hak pihak yang dirugikan	Transparansi layanan, pelindungan data pribadi, mekanisme pengaduan, ganti rugi, dan pemberian sanksi

Sebagai contoh, pada layanan perdagangan elektronik, prinsip keamanan diwujudkan melalui perlindungan akun, pengamanan pembayaran, dan penyimpanan data secara aman. Prinsip kepastian hukum diwujudkan melalui informasi mengenai identitas pelaku usaha, harga, ketentuan transaksi, kebijakan pengembalian barang, dan pembagian tanggung jawab. Adapun prinsip perlindungan hukum diwujudkan melalui hak konsumen

untuk mengajukan pengaduan, memperoleh pengembalian dana, meminta ganti rugi, atau menempuh penyelesaian sengketa.

Keamanan yang baik belum tentu memberikan perlindungan hukum apabila penyelenggara tidak transparan mengenai penggunaan data. Sebaliknya, aturan yang jelas tidak akan efektif apabila sistem tidak memiliki pengamanan yang memadai. Perlindungan hukum juga sulit diwujudkan apabila pengguna tidak dapat membuktikan kerugian atau tidak memiliki akses terhadap mekanisme pengaduan.

> Keamanan, kepastian, dan perlindungan hukum merupakan prinsip dasar dalam tata kelola ruang siber. Ketiganya memastikan bahwa perkembangan teknologi tidak hanya menghasilkan efisiensi dan inovasi, tetapi juga menghormati hak, mencegah kerugian, dan menyediakan mekanisme pertanggungjawaban. Penerapan ketiga prinsip tersebut menjadi dasar terbentuknya ekosistem digital yang aman, dapat dipercaya, dan berkeadilan.

3.4 Prinsip Kebebasan Informasi dan Batasannya

Kebebasan informasi merupakan salah satu prinsip penting dalam masyarakat digital. Internet memungkinkan setiap orang memperoleh, menyimpan, mengolah, menyampaikan, dan menyebarkan informasi dengan cepat tanpa dibatasi oleh jarak geografis. Melalui ruang siber, individu dapat menyampaikan pendapat, mengakses pengetahuan, mengikuti kegiatan pendidikan, menjalankan usaha, dan berpartisipasi dalam kehidupan sosial maupun pemerintahan.

Dalam perspektif hukum siber, kebebasan informasi tidak hanya berkaitan dengan hak untuk menerima informasi, tetapi juga hak untuk mencari, memproduksi, dan menyampaikan informasi melalui sistem elektronik. Kebebasan tersebut mendukung keterbukaan, inovasi, pengembangan ilmu pengetahuan, pengawasan terhadap kekuasaan, dan partisipasi masyarakat. Teknologi informasi telah memperluas ruang publik karena komunikasi tidak lagi hanya bergantung pada media konvensional atau lembaga tertentu.

Kebebasan informasi juga memberikan kesempatan kepada masyarakat untuk menyampaikan pengalaman, kritik, dan gagasan secara langsung. Pengguna dapat berperan sebagai penerima sekaligus pembuat informasi. Perubahan ini menyebabkan distribusi informasi menjadi lebih terbuka,

tetapi sekaligus menghadirkan persoalan mengenai kebenaran, tanggung jawab, privasi, dan dampak penyebaran informasi.

Meskipun penting, kebebasan informasi bukanlah hak yang bersifat mutlak. Penggunaannya harus mempertimbangkan hak orang lain, kepentingan umum, keamanan, dan ketertiban masyarakat. Informasi yang disebarkan melalui ruang siber dapat menimbulkan akibat yang luas karena mudah disalin, disimpan, dimodifikasi, dan didistribusikan kembali. Informasi yang telah tersebar juga sulit dihapus sepenuhnya karena dapat tersimpan pada berbagai perangkat atau platform.

Batasan terhadap kebebasan informasi diperlukan agar penggunaan hak tersebut tidak merugikan pihak lain. Batasan tersebut sekurang-kurangnya berkaitan dengan beberapa kepentingan berikut.

1. Pelindungan privasi dan data pribadi

Kebebasan menyampaikan informasi tidak memberikan hak kepada seseorang untuk menyebarkan data pribadi milik orang lain tanpa dasar yang sah. Data mengenai identitas, alamat, nomor telepon, kondisi keuangan, komunikasi pribadi, atau informasi sensitif lainnya harus dilindungi dari penggunaan dan penyebaran tanpa izin.

Privasi memberikan ruang kepada individu untuk mengendalikan informasi mengenai dirinya. Dalam lingkungan digital, kemampuan organisasi dan platform untuk mengumpulkan, menghubungkan, dan menganalisis data menyebabkan perlindungan privasi menjadi semakin penting (Solove, 2021). Oleh sebab itu, kebebasan informasi harus dibedakan dari tindakan membuka data pribadi atau kehidupan privat seseorang kepada publik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur hak subjek data serta kewajiban pihak yang memproses data pribadi. Pemrosesan dan penyebaran data harus mempunyai dasar yang sah, tujuan yang jelas, serta dilakukan secara terbatas dan bertanggung jawab (Republik Indonesia, 2022).

2. Pelindungan kehormatan dan hak orang lain

Informasi yang disampaikan di ruang siber tidak boleh merusak kehormatan, reputasi, atau hak pihak lain secara melawan hukum. Kritik terhadap individu, organisasi, atau pemerintah merupakan bagian dari

kebebasan berekspresi. Namun, kritik perlu dibedakan dari penyebaran tuduhan yang tidak didukung fakta, penghinaan, intimidasi, dan serangan terhadap pribadi.

Penentuan batas antara kritik dan pelanggaran hak harus dilakukan secara hati-hati. Pembatasan yang terlalu luas dapat menghambat kebebasan berpendapat, sedangkan pembatasan yang terlalu lemah dapat menyebabkan hak korban tidak terlindungi. Penegakan hukum harus mempertimbangkan isi pernyataan, konteks, tujuan, bukti, dampak, serta kepentingan publik yang terkait.

3. Pencegahan informasi palsu dan menyesatkan

Ruang digital memungkinkan informasi palsu atau menyesatkan menyebar secara cepat. Informasi tersebut dapat memengaruhi keputusan masyarakat, merusak reputasi, menimbulkan kepanikan, atau menyebabkan kerugian ekonomi. Algoritma platform dapat memperluas penyebaran konten karena informasi yang menarik perhatian sering memperoleh interaksi lebih tinggi.

Namun, tidak setiap kekeliruan informasi harus diperlakukan sebagai pelanggaran hukum. Perlu dibedakan antara kesalahan yang tidak disengaja, pendapat, satire, informasi yang belum terverifikasi, dan penyebaran informasi palsu yang dilakukan dengan sengaja untuk menimbulkan kerugian. Pembatasan harus diterapkan secara proporsional agar tidak menjadi alasan untuk membungkam perbedaan pendapat.

4. Pelindungan keamanan dan ketertiban umum

Informasi tertentu dapat dibatasi apabila penyebarannya menimbulkan ancaman nyata terhadap keamanan, keselamatan, atau ketertiban umum. Contohnya adalah penyebaran instruksi untuk melakukan serangan terhadap sistem elektronik, pengungkapan kredensial keamanan, atau penyebaran data yang dapat membahayakan infrastruktur penting.

Pembatasan atas dasar keamanan tidak boleh diterapkan secara sewenang-wenang. Harus terdapat hubungan yang jelas antara informasi yang dibatasi dan ancaman yang hendak dicegah. Pembatasan juga harus didasarkan pada hukum, mempunyai tujuan yang sah, dan tidak melebihi kebutuhan untuk melindungi kepentingan tersebut.

5. Pelindungan hak kekayaan intelektual

Kebebasan memperoleh dan menyebarkan informasi tidak menghapus hak pencipta atau pemegang hak atas karya digital. Buku elektronik, musik, video, fotografi, program komputer, dan karya lainnya tidak boleh digandakan atau disebarkan tanpa memperhatikan ketentuan hak cipta.

Pada saat yang sama, perlindungan hak kekayaan intelektual tidak boleh menghilangkan penggunaan yang diizinkan oleh hukum, seperti pemanfaatan untuk pendidikan, penelitian, kritik, atau kepentingan tertentu sesuai ketentuan yang berlaku. Keseimbangan diperlukan agar pencipta memperoleh perlindungan tanpa menghambat akses masyarakat terhadap pengetahuan.

Selain pembatasan oleh negara, kebebasan informasi juga dipengaruhi oleh kebijakan platform digital. Platform dapat menetapkan standar komunitas, melakukan moderasi konten, membatasi jangkauan informasi, atau menangguhkan akun. Gillespie (2018) menjelaskan bahwa platform mempunyai kekuasaan besar dalam menentukan konten yang dapat dilihat, diprioritaskan, atau dihapus.

Kebijakan moderasi diperlukan untuk menangani konten berbahaya, tetapi pelaksanaannya harus transparan dan dapat dipertanggungjawabkan. Pengguna perlu memperoleh penjelasan mengenai alasan penghapusan konten atau pembatasan akun serta diberikan kesempatan untuk mengajukan keberatan. Tanpa mekanisme tersebut, keputusan platform dapat membatasi kebebasan informasi secara tidak adil.

> Prinsip kebebasan informasi menuntut keseimbangan antara keterbukaan dan perlindungan hak. Informasi harus dapat diakses dan disampaikan secara bebas, tetapi kebebasan tersebut harus digunakan secara bertanggung jawab. Pembatasan hanya dapat dibenarkan apabila mempunyai dasar hukum, tujuan yang sah, diperlukan untuk mencegah kerugian, dan diterapkan secara proporsional. Pendekatan tersebut penting agar ruang siber tetap menjadi sarana pertukaran informasi yang terbuka tanpa mengabaikan privasi, keamanan, kehormatan, dan hak pihak lain.

3.5 Prinsip Tanggung Jawab dalam Aktivitas Siber

Setiap aktivitas dalam ruang siber dapat menimbulkan akibat hukum. Pengunggahan konten, pengumpulan data, penyelenggaraan platform, pelaksanaan transaksi, pengelolaan sistem, dan penggunaan algoritma dapat memberikan manfaat, tetapi juga dapat menyebabkan kerugian. Oleh karena itu, setiap pihak yang beraktivitas dalam ruang siber harus bertanggung jawab atas tindakan, keputusan, dan sistem yang berada dalam penguasaannya.

Prinsip tanggung jawab menegaskan bahwa ruang siber bukanlah wilayah yang bebas dari hukum. Sifat virtual, otomatis, dan lintas batas tidak menghapus kewajiban para pihak untuk menghormati hak orang lain. Pengguna maupun penyelenggara sistem tidak dapat melepaskan diri dari tanggung jawab hanya karena tindakan dilakukan melalui perangkat digital atau diproses oleh sistem otomatis.

Tanggung jawab dalam aktivitas siber sekurang-kurangnya mencakup tanggung jawab pengguna, penyelenggara sistem elektronik, platform digital, korporasi, dan pemerintah.

3.5.1 Tanggung Jawab Pengguna

Pengguna bertanggung jawab atas tindakan yang dilakukan melalui akun, perangkat, atau identitas digitalnya. Pengguna harus menjaga kredensial, menggunakan sistem secara sah, menghormati privasi, mematuhi hak kekayaan intelektual, dan tidak menyebarkan konten yang melanggar hukum.

Tanggung jawab pengguna tidak hanya berkaitan dengan perbuatan yang disengaja. Kelalaian juga dapat menimbulkan akibat hukum, misalnya penggunaan kata sandi yang diserahkan kepada pihak lain, penyebaran data tanpa pemeriksaan yang memadai, atau pengabaian terhadap peringatan keamanan. Namun, penilaian terhadap tanggung jawab tetap harus mempertimbangkan tingkat pengetahuan, kemampuan, kesalahan, dan hubungan pengguna dengan kerugian yang terjadi.

Pengguna juga perlu memahami bahwa penggunaan akun milik orang lain atau identitas palsu tidak otomatis menghilangkan tanggung jawab. Aktivitas

digital dapat meninggalkan catatan sistem, metadata, riwayat akses, dan jejak transaksi yang dapat digunakan untuk mengidentifikasi tindakan tertentu.

3.5.2 Tanggung Jawab Penyelenggara Sistem Elektronik

Penyelenggara sistem elektronik bertanggung jawab memastikan sistem yang dikelolanya berfungsi secara andal, aman, dan sesuai dengan ketentuan hukum. Tanggung jawab tersebut mencakup pengelolaan risiko, pengamanan data, pengendalian akses, pencatatan aktivitas, pemeliharaan sistem, dan penanganan insiden.

Peraturan Pemerintah Nomor 71 Tahun 2019 menempatkan keandalan dan keamanan sebagai kewajiban penting dalam penyelenggaraan sistem elektronik. Penyelenggara harus memiliki tata kelola dan prosedur yang memungkinkan sistem beroperasi secara bertanggung jawab (Republik Indonesia, 2019).

Ketika terjadi gangguan atau kebocoran data, penyelenggara tidak cukup hanya menyatakan bahwa insiden dilakukan oleh pihak luar. Perlu dinilai apakah penyelenggara telah menerapkan langkah pencegahan yang layak, melakukan pemantauan, memberikan pemberitahuan, dan mengambil tindakan pemulihan. Kegagalan menerapkan standar yang seharusnya dapat menjadi dasar pertanggungjawaban hukum (Amelia, 2025).

3.5.3 Tanggung Jawab Platform Digital

Platform digital mempunyai kedudukan yang berbeda dari pengguna biasa karena platform mengendalikan desain layanan, algoritma, aturan penggunaan, dan moderasi konten. Platform juga dapat mengumpulkan data dalam jumlah besar serta menentukan cara informasi ditampilkan kepada pengguna.

Tanggung jawab platform tidak selalu berarti bahwa platform harus menanggung seluruh perbuatan pengguna. Namun, platform perlu bertindak apabila mengetahui adanya pelanggaran, risiko keamanan, atau penyalahgunaan layanan. Tanggung jawab dapat meningkat ketika platform secara aktif memperoleh manfaat, mengendalikan transaksi, menentukan distribusi konten, atau mengabaikan laporan yang didukung bukti.

Dalam kasus kebocoran data, platform dapat dimintai tanggung jawab apabila tidak menerapkan perlindungan yang memadai atau tidak memenuhi kewajiban setelah insiden terjadi. Analisis terhadap tanggung jawab platform perlu mempertimbangkan tingkat kendali, kewajiban hukum, tindakan pencegahan, dan respons terhadap kerugian pengguna (Anindya & Subiyanto, 2025).

3.5.4 Tanggung Jawab Korporasi dan Organisasi

Aktivitas digital organisasi biasanya melibatkan pimpinan, pegawai, kontraktor, dan penyedia layanan. Karena itu, tanggung jawab tidak selalu berhenti pada individu yang melakukan tindakan teknis. Korporasi dapat dimintai pertanggungjawaban apabila pelanggaran dilakukan untuk kepentingannya, terjadi karena kebijakan organisasi, atau disebabkan oleh kegagalan pengawasan.

Organisasi perlu menetapkan pembagian tugas, kebijakan keamanan, prosedur pemrosesan data, pelatihan pegawai, dan mekanisme audit. Tanggung jawab organisasi juga mencakup pemilihan penyedia layanan pihak ketiga. Penyerahan pengelolaan data kepada vendor tidak dengan sendirinya menghapus kewajiban organisasi terhadap data pengguna.

3.5.5 Tanggung Jawab Pemerintah

Pemerintah bertanggung jawab membentuk regulasi, melakukan pengawasan, menyediakan mekanisme pengaduan, serta menegakkan hukum secara adil. Pemerintah juga bertanggung jawab melindungi sistem elektronik publik dan data warga yang dikelola oleh lembaga negara.

Dalam menjalankan pengawasan, pemerintah harus menghormati hak asasi, privasi, dan kebebasan informasi. Upaya keamanan tidak boleh menjadi dasar bagi pengawasan yang tidak terbatas. Setiap pembatasan atau akses terhadap data harus memiliki dasar hukum, tujuan yang sah, serta mekanisme pengawasan yang memadai.

Tanggung jawab hukum dalam aktivitas siber dapat berbentuk tanggung jawab perdata, pidana, atau administratif. Tanggung jawab perdata umumnya berkaitan dengan kewajiban mengganti kerugian atau memenuhi perjanjian. Tanggung jawab pidana muncul apabila perbuatan memenuhi unsur tindak pidana dan terdapat kesalahan pelaku. Adapun tanggung jawab

administratif dapat berupa teguran, penghentian layanan, denda administratif, pencabutan izin, atau tindakan lain oleh lembaga yang berwenang.

Penentuan tanggung jawab harus mempertimbangkan beberapa unsur, yaitu adanya kewajiban hukum, perbuatan atau kelalaian, kesalahan, kerugian, serta hubungan sebab akibat. Dalam sistem digital yang kompleks, kerugian dapat melibatkan beberapa pihak. Sebagai contoh, kebocoran data dapat disebabkan oleh kelemahan sistem, kesalahan pegawai, kelalaian vendor, dan tindakan penyerang. Karena itu, pembagian tanggung jawab perlu didasarkan pada peran, kendali, pengetahuan, dan kontribusi setiap pihak terhadap terjadinya kerugian.

Perkembangan sistem otomatis dan kecerdasan buatan juga menimbulkan persoalan baru. Keputusan yang dihasilkan algoritma dapat memengaruhi akses pengguna terhadap layanan, pekerjaan, kredit, atau informasi. Meskipun keputusan diproses secara otomatis, tanggung jawab tetap harus dapat ditelusuri kepada pihak yang merancang, menyediakan, menggunakan, atau mengendalikan sistem. Teknologi tidak dapat diposisikan sebagai alasan untuk menghilangkan akuntabilitas manusia dan organisasi.

> Prinsip tanggung jawab dalam aktivitas siber menuntut setiap pihak bertindak sesuai peran dan tingkat kendalinya. Semakin besar kemampuan suatu pihak untuk mengendalikan sistem, data, atau perilaku pengguna, semakin besar pula kewajiban yang harus dipenuhi. Penerapan prinsip ini diperlukan agar kerugian digital tidak dibebankan sepenuhnya kepada korban dan agar setiap pelanggaran dapat ditelusuri kepada pihak yang secara hukum wajib mempertanggungjawabkannya.

3.6 Hubungan Cyber Law dengan Bidang Hukum Lainnya

Cyber law bukan merupakan bidang hukum yang berdiri sepenuhnya terpisah dari sistem hukum yang telah ada. Hukum siber berkembang sebagai respons terhadap penggunaan teknologi informasi dalam berbagai aktivitas manusia yang sebelumnya telah diatur oleh hukum pidana, perdata, administrasi negara, perlindungan konsumen, kekayaan intelektual, hukum

internasional, dan hukum acara. Perbedaan utamanya terletak pada media, objek, cara pelaksanaan, serta karakter aktivitas yang berlangsung melalui sistem elektronik dan jaringan internet.

Hubungan tersebut menunjukkan bahwa hukum siber memiliki sifat interdisipliner. Suatu peristiwa digital dapat sekaligus menimbulkan persoalan dalam beberapa bidang hukum. Kebocoran data pada platform perdagangan elektronik, misalnya, dapat berkaitan dengan pelindungan data pribadi, tanggung jawab perdata, perlindungan konsumen, kewajiban administratif penyelenggara sistem elektronik, dan kemungkinan tindak pidana apabila terdapat akses tanpa hak. Oleh sebab itu, penyelesaian perkara siber sering memerlukan penggunaan beberapa ketentuan hukum secara bersamaan.

3.6.1 Hubungan dengan Hukum Pidana

Hukum pidana berhubungan dengan *cyber law* ketika teknologi informasi digunakan sebagai sarana, sasaran, atau lingkungan terjadinya tindak pidana. Komputer dapat menjadi sarana untuk melakukan penipuan, pemerasan, pencurian identitas, penyebaran konten ilegal, atau pelanggaran hak cipta. Sistem elektronik juga dapat menjadi sasaran perbuatan, seperti akses ilegal, gangguan sistem, manipulasi data, penyebaran perangkat berbahaya, dan perusakan informasi elektronik.

Tidak seluruh kejahatan siber merupakan bentuk kejahatan yang sepenuhnya baru. Sejumlah tindak pidana konvensional tetap dapat dilakukan melalui media digital. Penipuan, misalnya, telah dikenal dalam hukum pidana, tetapi pelaksanaannya melalui situs palsu, pesan elektronik, media sosial, atau aplikasi percakapan menimbulkan persoalan baru dalam identifikasi pelaku, penentuan tempat terjadinya perbuatan, dan pengumpulan bukti.

Hubungan hukum pidana dengan hukum siber juga terlihat dalam penentuan unsur perbuatan, kesalahan, hubungan sebab akibat, dan pertanggungjawaban pelaku. Sifat otomatis dan anonim dari teknologi tidak menghapus keharusan untuk membuktikan adanya perbuatan serta kesalahan. Dalam perkara yang melibatkan organisasi, penegak hukum juga perlu menentukan kemungkinan pertanggungjawaban korporasi, pimpinan, pegawai, atau penyedia layanan yang terlibat.

3.6.2 Hubungan dengan Hukum Perdata

Hukum perdata mengatur hubungan hukum antara individu, perusahaan, dan pihak lain dalam aktivitas digital. Hubungan tersebut dapat timbul melalui perjanjian elektronik, jual beli daring, layanan berlangganan, lisensi perangkat lunak, penyimpanan data, layanan komputasi awan, dan penggunaan platform digital.

Perjanjian yang dibuat melalui sistem elektronik pada dasarnya tetap harus memenuhi syarat sah perjanjian. Penggunaan media elektronik mengubah cara persetujuan diberikan dan dibuktikan, tetapi tidak menghilangkan prinsip kesepakatan, kecakapan para pihak, objek tertentu, dan sebab yang tidak bertentangan dengan hukum. Persetujuan dapat diberikan melalui tanda tangan elektronik, pemilihan menu persetujuan, penggunaan kode autentikasi, atau tindakan digital lain yang menunjukkan kehendak para pihak.

Hukum perdata juga menjadi dasar tuntutan ganti rugi apabila suatu pihak melakukan wanprestasi atau perbuatan melawan hukum. Penyelenggara layanan dapat dimintai pertanggungjawaban apabila tidak memenuhi kewajiban kontraktual, mengabaikan standar keamanan, atau menyebabkan kerugian karena kelalaiannya. Dalam menentukan tanggung jawab, perlu diperiksa adanya kewajiban, pelanggaran, kerugian, kesalahan, dan hubungan sebab akibat (Khasanah et al., 2023).

3.6.3 Hubungan dengan Hukum Administrasi Negara

Hubungan *cyber law* dengan hukum administrasi negara terlihat dalam peran pemerintah sebagai pembentuk regulasi, pemberi perizinan, pengawas, pengelola layanan publik, dan penegak sanksi administratif. Penyelenggara sistem elektronik dapat diwajibkan memenuhi persyaratan pendaftaran, tata kelola, keamanan sistem, pelindungan data, pelaporan insiden, dan penyimpanan informasi tertentu.

Pemerintah juga menggunakan sistem elektronik dalam pelayanan administrasi, perpajakan, kependudukan, kesehatan, pendidikan, dan perizinan. Penggunaan teknologi dalam pelayanan publik harus tetap memenuhi prinsip legalitas, transparansi, akuntabilitas, kepastian hukum, dan perlindungan hak masyarakat.

Apabila penyelenggara sistem elektronik melanggar kewajiban administratif, sanksi dapat diberikan dalam bentuk teguran, penghentian sementara, pemutusan akses, denda administratif, pencabutan izin, atau tindakan lain sesuai dengan peraturan yang berlaku. Sanksi administratif dapat diterapkan secara tersendiri atau bersama dengan tanggung jawab perdata dan pidana, bergantung pada sifat pelanggarannya.

3.6.4 Hubungan dengan Hukum Perlindungan Konsumen

Aktivitas perdagangan digital mempertemukan konsumen dengan penjual, marketplace, penyedia pembayaran, perusahaan logistik, dan penyedia layanan teknologi. Hubungan yang kompleks tersebut dapat menimbulkan persoalan mengenai kejelasan informasi, keamanan pembayaran, kesesuaian barang, iklan menyesatkan, pengembalian dana, dan penyalahgunaan data konsumen.

Hukum perlindungan konsumen memberikan hak kepada konsumen untuk memperoleh informasi yang benar, keamanan, kenyamanan, pilihan, mekanisme pengaduan, dan ganti rugi. Dalam transaksi elektronik, hak tersebut harus diwujudkan melalui informasi yang mudah dipahami mengenai identitas pelaku usaha, karakteristik produk, harga, biaya tambahan, prosedur pembayaran, pengiriman, pembatalan, dan pengembalian barang.

Pelindungan konsumen digital juga memerlukan pembagian tanggung jawab yang jelas antara penjual dan platform. Platform tidak selalu dapat diperlakukan hanya sebagai penyedia tempat karena dalam praktiknya platform dapat mengendalikan sistem pembayaran, promosi, peringkat penjual, distribusi informasi, dan mekanisme penyelesaian keluhan.

3.6.5 Hubungan dengan Hukum Kekayaan Intelektual

Teknologi digital memudahkan penciptaan, penyimpanan, penggandaan, perubahan, dan distribusi karya. Kemudahan tersebut mendukung inovasi, tetapi juga meningkatkan risiko pelanggaran hak cipta, merek, paten, rahasia dagang, dan hak kekayaan intelektual lainnya.

Hubungan *cyber law* dengan hukum kekayaan intelektual terlihat pada perlindungan program komputer, karya audiovisual, buku elektronik, desain digital, basis data, nama domain, dan konten media sosial. Penggunaan karya

digital tetap harus memperhatikan hak ekonomi dan hak moral pencipta. Penggandaan atau penyebaran konten tanpa izin dapat menimbulkan tanggung jawab hukum, meskipun dilakukan dengan mudah melalui fitur salin, unggah, atau bagikan.

Nama domain juga dapat menimbulkan sengketa apabila didaftarkan atau digunakan dengan memanfaatkan merek milik pihak lain. Karena itu, penyelesaian sengketa digital tidak hanya bergantung pada hukum nasional, tetapi dapat pula melibatkan kebijakan dan mekanisme yang dibentuk oleh lembaga pengelola nama domain. Hubungan antara hukum siber dan kekayaan intelektual diperlukan untuk menyeimbangkan perlindungan pencipta, kepentingan pengguna, dan perkembangan inovasi (Febriharini, 2016).

3.6.6 Hubungan dengan Hukum Pelindungan Data Pribadi

Data pribadi merupakan salah satu objek utama dalam ekosistem digital. Hampir seluruh layanan elektronik mengumpulkan data identitas, lokasi, komunikasi, kebiasaan, transaksi, atau preferensi pengguna. Oleh sebab itu, hukum siber sangat berkaitan dengan ketentuan mengenai dasar pemrosesan, persetujuan, keamanan, pembatasan tujuan, penyimpanan, penghapusan, dan pemindahan data.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur hak subjek data serta kewajiban pengendali dan prosesor data. Pelanggaran terhadap ketentuan tersebut dapat menimbulkan konsekuensi administratif, perdata, atau pidana sesuai dengan karakter perbuatannya. Hubungan ini menunjukkan bahwa keamanan informasi tidak hanya merupakan persoalan teknis, tetapi juga kewajiban hukum untuk melindungi hak individu.

3.6.7 Hubungan dengan Hukum Internasional

Karakter ruang siber yang melampaui batas negara menyebabkan *cyber law* berkaitan erat dengan hukum internasional. Serangan siber, penyimpanan data, penyediaan layanan, dan transaksi digital dapat melibatkan beberapa yurisdiksi. Keadaan ini menimbulkan kebutuhan terhadap kerja sama dalam penyidikan, pertukaran bukti, ekstradisi, bantuan hukum timbal balik, dan penanganan insiden lintas negara.

Hukum internasional juga berperan dalam pembentukan standar mengenai kejahatan siber, keamanan jaringan, pelindungan data, hak asasi manusia, dan tanggung jawab negara. Namun, perbedaan sistem hukum serta kepentingan nasional sering menyebabkan kesulitan dalam harmonisasi. Suatu perbuatan dapat dilarang di satu negara, tetapi tidak diatur atau diperlakukan berbeda di negara lain.

3.6.8 Hubungan dengan Hukum Acara dan Pembuktian

Hukum acara menentukan cara hak dan kewajiban hukum ditegakkan melalui proses peradilan. Dalam perkara siber, hukum acara berkaitan dengan keabsahan informasi elektronik sebagai alat bukti, penyitaan perangkat, pengumpulan data, pemeriksaan saksi ahli, dan pemeliharaan integritas bukti digital.

Bukti digital memiliki karakter yang mudah disalin, diubah, dipindahkan, dan dihapus. Oleh karena itu, proses penanganannya harus menjaga keaslian, integritas, dan rantai penguasaan bukti. Aparat penegak hukum harus dapat menjelaskan cara bukti diperoleh, disimpan, dianalisis, dan disajikan di pengadilan.

Permasalahan juga muncul ketika data berada pada penyedia layanan di luar negeri. Meskipun pengadilan memiliki kewenangan memeriksa perkara, akses terhadap data dapat memerlukan kerja sama internasional atau permintaan resmi kepada penyedia layanan. Kondisi tersebut memperlihatkan keterkaitan antara hukum acara, yurisdiksi, forensik digital, dan hukum internasional.

> Cyber law merupakan bidang hukum yang menghubungkan berbagai cabang hukum dalam menghadapi perubahan akibat teknologi informasi. Hukum pidana mengatur perbuatan terlarang dan pertanggungjawaban pelaku, hukum perdata mengatur hubungan para pihak dan ganti rugi, hukum administrasi mengatur tata kelola dan pengawasan, sedangkan bidang hukum lainnya memberikan perlindungan terhadap konsumen, data pribadi, karya intelektual, dan kepentingan lintas negara. Pemahaman lintas bidang tersebut diperlukan karena satu peristiwa siber hampir selalu mempunyai lebih dari satu dimensi hukum.

Bab 4
Sistem Hukum Informasi dan Transaksi Elektronik

4.1 Konsep Sistem Hukum dalam Lingkungan Digital

Seiring dengan pesatnya perkembangan teknologi informasi, transformasi digital telah menjadi fenomena yang tidak terpisahkan dari dunia bisnis modern. Konsep ini menunjukkan adanya perubahan menyeluruh dalam cara organisasi mengelola operasional, strategi, serta interaksi dengan berbagai pemangku kepentingan. Di era digital saat ini, transformasi digital telah menjadi bagian penting dari strategi bisnis organisasi. Penerapan teknologi digital tidak hanya mengubah cara organisasi menjalankan aktivitas operasional, tetapi juga mendorong terciptanya proses kerja yang lebih efektif, efisien, dan responsif terhadap perubahan (Fahmi, 2024).

Perubahan tersebut tidak hanya meningkatkan efisiensi dan mendorong inovasi, tetapi juga menciptakan peluang ekonomi baru melalui berkembangnya berbagai aktivitas bisnis berbasis digital. Era digital tidak hanya memberikan kemudahan dalam berbagai aspek kehidupan manusia, tetapi juga menghadirkan ruang yang lebih luas bagi masyarakat dan pelaku usaha untuk memperoleh manfaat ekonomi melalui pemanfaatan teknologi digital dalam kegiatan bisnis (Kaffah & Badriyah, 2024). Di sisi lain, aktivitas bisnis yang semakin bergantung pada teknologi digital turut memunculkan berbagai persoalan hukum yang sebelumnya belum dikenal dalam sistem hukum konvensional, seperti pelindungan data pribadi, keamanan siber, transaksi elektronik, keabsahan dokumen digital, tanggung jawab penyelenggara sistem elektronik, hingga penyelesaian sengketa yang melibatkan ruang siber. Oleh karena itu, perkembangan teknologi digital perlu diimbangi dengan sistem hukum yang mampu memberikan kepastian hukum, perlindungan hak, dan keadilan bagi seluruh pihak yang terlibat.

Sistem hukum dalam lingkungan digital adalah keseluruhan norma, lembaga, mekanisme penegakan, dan prinsip hukum yang mengatur aktivitas manusia di ruang digital. Sistem ini bertujuan memberikan kepastian hukum, perlindungan hak, keadilan, serta menjaga ketertiban

dalam berbagai aktivitas yang dilakukan melalui teknologi informasi dan internet. Berbeda dengan sistem hukum konvensional yang berorientasi pada ruang fisik, sistem hukum digital harus mampu mengakomodasi karakteristik dunia digital yang bersifat lintas batas (*borderless*), cepat, dinamis, dan berbasis data.

Perkembangan lingkungan digital tersebut menunjukkan bahwa hukum tidak lagi dipahami hanya sebagai seperangkat norma yang mengatur hubungan hukum dalam ruang fisik, melainkan juga sebagai instrumen yang mampu mengakomodasi hubungan hukum yang berlangsung melalui media elektronik. Dalam konteks ini, sistem hukum dituntut untuk beradaptasi terhadap perubahan karakter aktivitas masyarakat yang semakin terdigitalisasi, baik dalam bidang perdagangan, jasa keuangan, pemerintahan, maupun komunikasi. Adaptasi tersebut diperlukan agar hukum tetap mampu menjalankan fungsinya sebagai sarana menciptakan ketertiban, memberikan perlindungan terhadap hak-hak para pihak, serta menjamin kepastian hukum di tengah perkembangan teknologi yang berlangsung sangat cepat.

Perkembangan teknologi digital yang berlangsung secara masif menunjukkan bahwa hukum tidak dapat bersifat statis, melainkan harus mampu beradaptasi dengan perubahan sosial yang terjadi di masyarakat. Dalam perspektif Roscoe Pound, hukum dipandang sebagai *law as a tool of social engineering*, yaitu hukum berfungsi sebagai sarana rekayasa sosial untuk mengarahkan perubahan masyarakat menuju kondisi yang lebih tertib, adil, dan seimbang. Konsep *law as a tool of social engineering* memandang hukum sebagai instrumen yang secara aktif digunakan untuk mengarahkan perubahan sosial. Dalam perspektif ini, hukum tidak hanya berfungsi mencerminkan kondisi masyarakat yang telah ada, tetapi juga menjadi sarana untuk membentuk, memengaruhi, dan mengarahkan perkembangan masyarakat menuju tujuan yang diharapkan (Surachman et al., 2026).

Konsep ini menempatkan hukum tidak hanya sebagai instrumen yang mengendalikan perilaku masyarakat, tetapi juga sebagai mekanisme yang mampu mendorong terciptanya perubahan sosial sesuai dengan kebutuhan dan perkembangan zaman. Oleh karena itu, ketika teknologi digital mengubah pola interaksi, komunikasi, dan aktivitas bisnis masyarakat, hukum dituntut untuk menyesuaikan diri melalui pembentukan norma-norma baru yang mampu mengakomodasi perkembangan tersebut.

Secara konseptual, sistem hukum dalam lingkungan digital tidak hanya berkaitan dengan pembentukan peraturan perundang-undangan yang mengatur teknologi informasi, tetapi juga mencakup keseluruhan elemen yang mendukung berjalannya sistem hukum secara efektif. Hal ini meliputi keberadaan regulasi yang responsif terhadap perkembangan teknologi, kelembagaan yang memiliki kewenangan dalam penyelenggaraan dan pengawasan sistem elektronik, mekanisme penegakan hukum yang mampu menangani berbagai pelanggaran di ruang siber, serta budaya hukum masyarakat yang mendorong pemanfaatan teknologi secara bertanggung jawab. Dengan demikian, sistem hukum digital merupakan suatu ekosistem hukum yang dibangun untuk mengatur interaksi antara manusia, teknologi, data, dan penyelenggara sistem elektronik secara terpadu.

Konsep tersebut sejalan dengan teori sistem hukum yang dikemukakan oleh Lawrence M. Friedman yang menyatakan bahwa efektivitas suatu sistem hukum ditentukan oleh keterpaduan tiga unsur utama, yaitu substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*). Struktur hukum tidak dapat dipisahkan dari substansi hukum karena lembaga dan aparat penegak hukum merupakan pihak yang membentuk, menerapkan, dan mengembangkan berbagai produk hukum. Dengan demikian, segala bentuk norma yang digunakan sebagai dasar penyelenggaraan hukum, baik yang dituangkan dalam peraturan perundang-undangan maupun yang hidup dalam praktik sebagai hukum tidak tertulis, merupakan bagian dari substansi hukum (Al Kautsar & Muhammad, 2022). Budaya hukum merupakan salah satu unsur penting dalam penyelenggaraan sistem hukum nasional di Indonesia. Meskipun demikian, aspek ini memiliki karakter yang kompleks karena dipengaruhi oleh nilai, sikap, dan perilaku masyarakat terhadap hukum (Al Kautsar & Muhammad, 2022).

Meskipun teori ini dikembangkan dalam konteks sistem hukum secara umum, ketiga unsur tersebut tetap relevan dalam menjelaskan bagaimana hukum bekerja di lingkungan digital. Substansi hukum menyediakan norma yang mengatur aktivitas digital, struktur hukum berfungsi melaksanakan dan menegakkan ketentuan tersebut, sedangkan budaya hukum mencerminkan tingkat kesadaran serta kepatuhan masyarakat dalam menggunakan teknologi secara bertanggung jawab. Ketiga unsur tersebut harus berjalan secara harmonis agar penyelenggaraan sistem elektronik mampu mewujudkan kepastian hukum, keadilan, dan kemanfaatan.

Dalam perspektif substansi hukum, perkembangan teknologi digital telah melahirkan berbagai norma hukum baru yang sebelumnya belum dikenal dalam sistem hukum konvensional. Pengaturan mengenai informasi elektronik, dokumen elektronik, tanda tangan elektronik, kontrak elektronik, pelindungan data pribadi, keamanan siber, hingga kecerdasan buatan merupakan bentuk respons hukum terhadap dinamika masyarakat digital. Kehadiran berbagai instrumen hukum tersebut menunjukkan bahwa hukum memiliki sifat dinamis dan senantiasa berkembang mengikuti perubahan sosial sebagaimana dikemukakan oleh Roscoe Pound melalui konsep *law as a tool of social engineering*. Dengan kata lain, hukum tidak hanya berfungsi mengendalikan perubahan sosial akibat perkembangan teknologi, tetapi juga mengarahkan pemanfaatan teknologi agar memberikan manfaat sebesar-besarnya bagi masyarakat tanpa mengabaikan perlindungan terhadap hak-hak individu.

Berdasarkan uraian tersebut, dapat dipahami bahwa sistem hukum dalam lingkungan digital merupakan suatu sistem yang bersifat adaptif dan integratif dalam merespons perkembangan teknologi informasi. Efektivitasnya tidak hanya ditentukan oleh keberadaan regulasi yang memadai, tetapi juga oleh sinergi antara substansi hukum, struktur hukum, dan budaya hukum dalam menjamin kepastian hukum, keadilan, serta perlindungan terhadap hak-hak para pihak di ruang digital. Pemahaman mengenai konsep ini menjadi landasan penting untuk mengkaji lebih lanjut dasar hukum yang mengatur informasi dan transaksi elektronik sebagai instrumen utama penyelenggaraan aktivitas digital di Indonesia.

4.2 Dasar Hukum Informasi dan Transaksi Elektronik di Indonesia

Transformasi digital yang berlangsung secara masif telah mengubah pola interaksi masyarakat dalam berbagai bidang kehidupan, termasuk aktivitas ekonomi, pemerintahan, pendidikan, pelayanan publik, dan komunikasi. Berbagai aktivitas yang sebelumnya dilakukan secara konvensional kini beralih ke media elektronik melalui pemanfaatan teknologi informasi dan internet. Perubahan tersebut tidak hanya menciptakan efisiensi dan inovasi, tetapi juga melahirkan hubungan hukum baru yang memerlukan pengaturan secara komprehensif. Dalam konteks tersebut, hukum dituntut mampu mengikuti perkembangan teknologi agar dapat memberikan kepastian

hukum, perlindungan hak, serta menjaga keseimbangan antara kepentingan masyarakat, pelaku usaha, dan negara.

Di Indonesia, pembentukan kerangka hukum di bidang informasi dan transaksi elektronik dilakukan secara bertahap seiring dengan perkembangan teknologi digital dan meningkatnya kompleksitas aktivitas di ruang siber. Regulasi yang dibentuk tidak hanya mengatur keabsahan transaksi elektronik, tetapi juga mencakup berbagai aspek lain, seperti penyelenggaraan sistem elektronik, keamanan informasi, pelindungan data pribadi, perdagangan melalui sistem elektronik, serta penegakan hukum terhadap berbagai bentuk kejahatan siber. Hal ini menunjukkan bahwa sistem hukum digital di Indonesia berkembang secara dinamis untuk menjawab tantangan yang muncul akibat pesatnya digitalisasi di berbagai sektor.

Perkembangan regulasi tersebut mencerminkan adanya perubahan paradigma dalam pembentukan hukum nasional. Jika pada tahap awal regulasi lebih difokuskan pada pemberian pengakuan hukum terhadap informasi dan transaksi elektronik, maka pada tahap berikutnya orientasi kebijakan bergeser ke arah penguatan tata kelola ruang digital, peningkatan perlindungan hak masyarakat, serta penciptaan ekosistem digital yang aman, terpercaya, dan berkeadilan. Oleh karena itu, pemahaman terhadap perkembangan dasar hukum informasi dan transaksi elektronik menjadi penting untuk melihat bagaimana sistem hukum Indonesia beradaptasi dengan dinamika transformasi digital.

Untuk memberikan gambaran yang sistematis mengenai perkembangan tersebut, Gambar 4.1 menyajikan roadmap dasar hukum informasi dan transaksi elektronik di Indonesia. Roadmap ini menunjukkan evolusi regulasi mulai dari pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai fondasi hukum utama, berbagai perubahan terhadap undang-undang tersebut, hingga lahirnya berbagai peraturan pelaksana yang memperkuat tata kelola sistem elektronik, perdagangan digital, dan pelindungan data pribadi. Perkembangan hukum digital di Indonesia tidak berlangsung secara parsial, melainkan membentuk suatu kerangka regulasi yang saling melengkapi dalam mewujudkan kepastian hukum dan mendukung transformasi digital yang berkelanjutan.

Gambar 4.1: Roadmap Dasar Hukum Informasi Dan Transaksi Elektronik Di Indonesia

Dasar hukum informasi dan transaksi elektronik di Indonesia sebagaimana ditunjukkan pada Gambar 4.1 menggambarkan perkembangan regulasi yang berlangsung secara bertahap dan berkesinambungan. Perkembangan tersebut menunjukkan bahwa sistem hukum Indonesia terus beradaptasi dengan dinamika teknologi informasi yang berkembang sangat cepat. Regulasi yang dibentuk tidak hanya bertujuan mengatur penggunaan teknologi, tetapi juga menciptakan keseimbangan antara kepentingan inovasi digital, perlindungan hak masyarakat, kepastian hukum, keamanan siber, dan pertumbuhan ekonomi digital.

Tahap pertama dalam *roadmap* tersebut diawali dengan lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kehadiran undang-undang ini merupakan tonggak penting dalam sejarah hukum Indonesia karena untuk pertama kalinya negara mengakui informasi elektronik, dokumen elektronik, dan transaksi elektronik sebagai objek yang memiliki konsekuensi hukum. Sebelum UU ITE diberlakukan, berbagai aktivitas yang dilakukan melalui media elektronik belum memiliki dasar hukum yang memadai sehingga sering menimbulkan ketidakpastian ketika terjadi sengketa atau tindak pidana. Oleh karena itu, UU ITE hadir untuk memberikan legitimasi terhadap aktivitas digital sekaligus menjadi landasan bagi berkembangnya ekonomi digital nasional.

Salah satu substansi penting dalam UU Nomor 11 Tahun 2008 adalah pengakuan bahwa informasi elektronik dan dokumen elektronik memiliki kekuatan hukum yang sah sebagai alat bukti, sepanjang memenuhi persyaratan yang ditentukan oleh peraturan perundang-undangan. Ketentuan ini membawa perubahan yang sangat signifikan dalam sistem pembuktian hukum di Indonesia karena memperluas alat bukti yang sebelumnya lebih berorientasi pada dokumen fisik. Selain itu, UU ITE juga mengatur mengenai tanda tangan elektronik, penyelenggaraan sistem elektronik, transaksi elektronik, nama domain, serta berbagai bentuk tindak pidana yang dilakukan melalui media elektronik (*cybercrime*), seperti akses ilegal terhadap sistem elektronik, manipulasi data elektronik, gangguan terhadap sistem elektronik, hingga penyebaran informasi yang melanggar hukum.

Perkembangan teknologi digital yang sangat cepat menyebabkan beberapa ketentuan dalam UU ITE dinilai tidak lagi sepenuhnya mampu menjawab dinamika masyarakat digital. Sejumlah pasal bahkan menimbulkan perdebatan karena dianggap memiliki rumusan yang multitafsir dan berpotensi membatasi kebebasan berekspresi. Selain itu, meningkatnya penggunaan media sosial, perdagangan elektronik, layanan komputasi awan (*cloud computing*), serta berkembangnya ekonomi berbasis platform digital menuntut adanya penyempurnaan regulasi agar tetap relevan dengan kebutuhan masyarakat.

Sebagai respons terhadap berbagai perkembangan tersebut, pemerintah dan DPR melakukan perubahan pertama terhadap UU ITE melalui Undang-Undang Nomor 19 Tahun 2016. Perubahan ini tidak menggantikan keseluruhan substansi UU ITE, melainkan menyempurnakan beberapa ketentuan yang dinilai memerlukan penyesuaian. Salah satu perubahan yang paling dikenal adalah pengaturan mengenai hak untuk dilupakan (*right to be forgotten*), yaitu hak seseorang untuk mengajukan penghapusan informasi elektronik tertentu melalui mekanisme yang diatur berdasarkan putusan pengadilan. Ketentuan ini menunjukkan bahwa sistem hukum Indonesia mulai mengakomodasi perlindungan hak privasi individu dalam ruang digital sebagaimana berkembang di berbagai negara.

Selain itu, perubahan melalui UU Nomor 19 Tahun 2016 juga bertujuan memberikan perlindungan hukum yang lebih proporsional terhadap masyarakat. Beberapa ketentuan pidana diperjelas agar tidak menimbulkan penafsiran yang terlalu luas, sementara mekanisme penegakan hukum

terhadap pelanggaran di ruang digital diupayakan menjadi lebih akuntabel. Dengan demikian, perubahan pertama terhadap UU ITE mencerminkan upaya negara untuk menjaga keseimbangan antara kepentingan penegakan hukum, perlindungan hak asasi manusia, dan kebebasan berekspresi di ruang digital.

Tahap berikutnya ditandai dengan lahirnya Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas UU ITE. Perubahan ini merupakan respons terhadap semakin kompleksnya ekosistem digital Indonesia yang dipengaruhi oleh perkembangan teknologi seperti kecerdasan buatan (*artificial intelligence*), layanan digital berbasis *platform*, ekonomi digital, serta meningkatnya aktivitas masyarakat dalam ruang siber. Pembaruan regulasi tersebut sekaligus memperkuat kepastian hukum dalam penyelenggaraan informasi dan transaksi elektronik dengan menghadirkan pengaturan yang lebih jelas, adaptif, dan sesuai dengan perkembangan teknologi digital (Azi et al., 2024). Regulasi ini diarahkan untuk memperkuat kepastian hukum terhadap berbagai aktivitas digital yang sebelumnya belum diatur secara memadai atau masih menimbulkan berbagai penafsiran.

Perubahan kedua tersebut juga memperkuat perlindungan terhadap hak pengguna sistem elektronik, memperjelas beberapa norma pidana agar tidak menimbulkan kriminalisasi yang berlebihan, serta meningkatkan tanggung jawab penyelenggara sistem elektronik dalam menjaga keamanan dan keandalan layanan digital. Dengan demikian, arah pembentukan UU Nomor 1 Tahun 2024 menunjukkan pergeseran paradigma dari sekadar mengatur aktivitas elektronik menuju pembentukan tata kelola ruang digital yang lebih adaptif, inklusif, dan berorientasi pada perlindungan masyarakat.

Salah satu regulasi yang memiliki peranan penting adalah Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Peraturan ini menggantikan PP Nomor 82 Tahun 2012 dengan tujuan menyesuaikan perkembangan teknologi informasi dan kebutuhan masyarakat. PP PSTE mengatur berbagai aspek penyelenggaraan sistem elektronik, mulai dari kewajiban penyelenggara sistem elektronik, standar keamanan informasi, pengelolaan pusat data, pelindungan data elektronik, hingga tanggung jawab penyelenggara dalam menjaga keandalan sistem.

Keberadaan PP PSTE menjadi sangat penting karena sebagian besar aktivitas digital saat ini bergantung pada sistem elektronik yang dikelola oleh

pemerintah maupun sektor swasta. Oleh karena itu, regulasi ini menegaskan bahwa setiap penyelenggara sistem elektronik memiliki kewajiban untuk menjamin kerahasiaan, integritas, dan ketersediaan data yang dikelolanya. Ketentuan tersebut sekaligus memperkuat prinsip akuntabilitas dalam penyelenggaraan layanan digital di Indonesia.

Peraturan penting lainnya adalah Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE). Regulasi ini menjadi dasar hukum bagi penyelenggaraan perdagangan elektronik (*e-commerce*) yang berkembang sangat pesat dalam beberapa tahun terakhir. PP PMSE mengatur hak dan kewajiban pelaku usaha, penyelenggara platform digital, konsumen, serta mekanisme transaksi elektronik. Kehadiran peraturan ini memberikan kepastian hukum bagi seluruh pihak yang terlibat dalam aktivitas perdagangan digital sekaligus meningkatkan kepercayaan masyarakat terhadap transaksi elektronik.

Di samping itu, pemerintah juga menerbitkan berbagai Peraturan Menteri Komunikasi dan Digital yang mengatur aspek teknis penyelenggaraan sistem elektronik, sertifikasi elektronik, tata kelola platform digital, keamanan informasi, serta kewajiban penyelenggara sistem elektronik. Regulasi teknis tersebut diperlukan karena perkembangan teknologi digital berlangsung jauh lebih cepat dibandingkan proses pembentukan undang-undang. Oleh sebab itu, peraturan menteri berfungsi sebagai instrumen hukum yang lebih fleksibel dalam merespons perkembangan teknologi. *Roadmap* pada gambar 4.2 tersebut kemudian semakin lengkap dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi (UU PDP). Lahirnya UU PDP merupakan tonggak penting dalam pembangunan sistem hukum digital Indonesia karena untuk pertama kalinya Indonesia memiliki regulasi khusus yang mengatur pelindungan data pribadi secara komprehensif. Sebelumnya, ketentuan mengenai data pribadi tersebar dalam berbagai regulasi sektoral sehingga sering menimbulkan ketidakpastian hukum. Urgensi pembentukan UU PDP semakin menguat seiring pesatnya perkembangan teknologi informasi yang telah mempermudah proses pengumpulan, pengelolaan, dan pemrosesan data melalui sistem elektronik. Di sisi lain, perkembangan tersebut juga meningkatkan risiko terjadinya pelanggaran terhadap privasi serta penyalahgunaan data pribadi, sehingga diperlukan landasan hukum yang

mampu memberikan perlindungan yang lebih efektif bagi pemilik data (Ramadhani & Wiraguna, 2025).

UU PDP menetapkan berbagai prinsip pengolahan data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, mekanisme persetujuan, hingga sanksi administratif maupun pidana terhadap pelanggaran. Kehadiran undang-undang ini menunjukkan bahwa pelindungan data pribadi telah menjadi bagian integral dari pembangunan sistem hukum digital nasional, mengingat data merupakan aset strategis dalam ekonomi digital.

4.3 Subjek dan Objek Hukum dalam Transaksi Elektronik

Perkembangan teknologi informasi telah mengubah cara masyarakat melakukan berbagai aktivitas hukum, khususnya dalam bidang perdagangan, jasa, layanan keuangan, maupun pelayanan publik. Berbagai bentuk perjanjian dan hubungan hukum yang sebelumnya dilakukan secara tatap muka kini dapat dilaksanakan melalui sistem elektronik tanpa dibatasi oleh ruang dan waktu. Kondisi tersebut melahirkan bentuk-bentuk hubungan hukum baru yang tetap memiliki akibat hukum sebagaimana transaksi konvensional. Oleh karena itu, setiap transaksi elektronik harus memenuhi prinsip-prinsip hukum yang menjamin adanya kepastian hukum, keadilan, perlindungan hukum, serta keseimbangan hak dan kewajiban para pihak.

Dalam perspektif hukum perdata, suatu transaksi elektronik pada hakikatnya merupakan hubungan hukum yang melibatkan subjek hukum sebagai pelaku dan objek hukum sebagai sasaran dari hubungan hukum tersebut. Subjek hukum merupakan pihak yang memiliki hak dan kewajiban untuk melakukan tindakan hukum, sedangkan objek hukum adalah segala sesuatu yang menjadi tujuan atau sasaran dari hubungan hukum sehingga dapat menimbulkan hak dan kewajiban bagi para pihak. Meskipun transaksi dilakukan melalui media elektronik, keberadaan subjek dan objek hukum tetap menjadi unsur fundamental yang menentukan sah atau tidaknya suatu hubungan hukum.

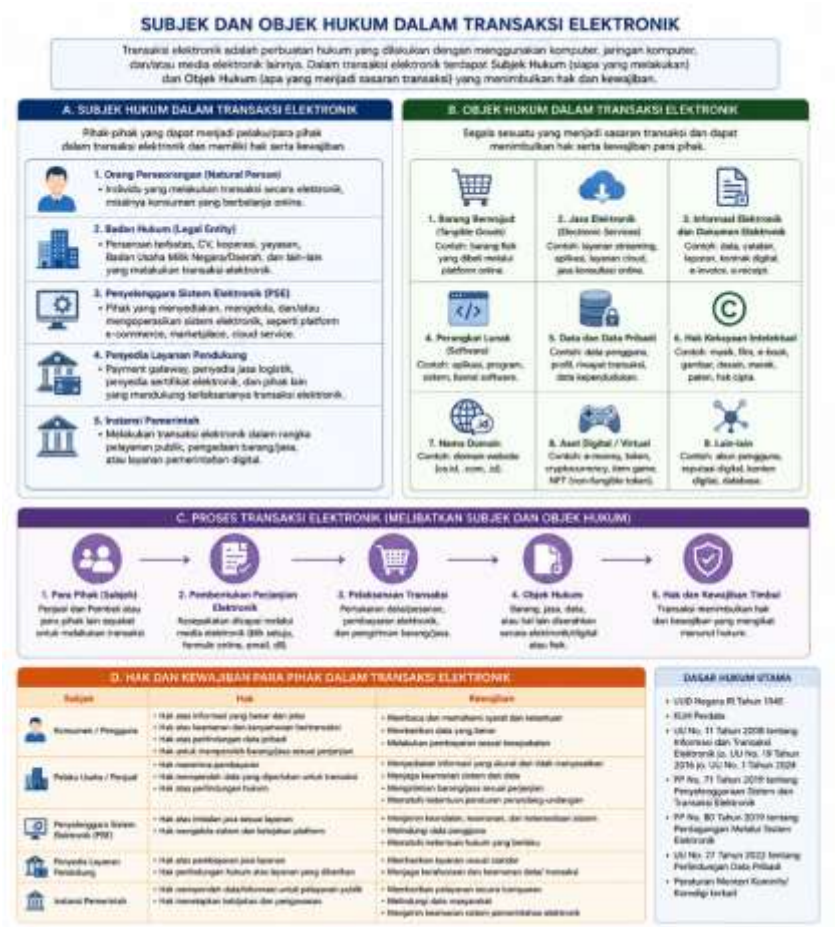
Subjek hukum merupakan istilah yang berasal dari bahasa Belanda *rechtssubject*, yaitu setiap pihak yang oleh hukum diakui sebagai pemegang hak dan sekaligus pembawa kewajiban sehingga memiliki kewenangan untuk melakukan tindakan hukum (*rechtsbevoegdheid*). Dalam ranah

hukum perdata, subjek hukum dibedakan menjadi dua kategori utama, yaitu orang perseorangan (*natuurlijk persoon*) dan badan hukum (*rechtspersoon*) (Suadi, 2021).

Berbeda dengan transaksi konvensional, transaksi elektronik memiliki karakteristik yang lebih kompleks karena melibatkan berbagai pihak yang tidak selalu berinteraksi secara langsung. Selain penjual dan pembeli, transaksi elektronik juga melibatkan penyelenggara sistem elektronik, penyedia platform digital, penyedia layanan pembayaran, penyedia sertifikat elektronik, hingga penyelenggara jaringan komunikasi. Di sisi lain, objek hukum dalam transaksi elektronik juga mengalami perkembangan yang signifikan. Objek transaksi tidak lagi terbatas pada barang berwujud, tetapi juga mencakup jasa digital, data elektronik, perangkat lunak, dokumen elektronik, hak kekayaan intelektual, hingga berbagai aset digital yang memiliki nilai ekonomi.

Kompleksitas hubungan hukum tersebut menunjukkan bahwa perkembangan teknologi informasi telah memperluas ruang lingkup hukum perdata ke dalam ekosistem digital. Oleh sebab itu, pemahaman mengenai subjek dan objek hukum dalam transaksi elektronik menjadi sangat penting untuk menentukan kedudukan hukum masing-masing pihak, ruang lingkup hak dan kewajibannya, serta bentuk perlindungan hukum yang diberikan apabila terjadi sengketa. Gambar 4.2 memberikan gambaran mengenai keterkaitan antara subjek hukum, objek hukum, proses transaksi elektronik, serta hak dan kewajiban yang timbul dalam penyelenggaraan transaksi elektronik berdasarkan kerangka hukum teknologi informasi di Indonesia.

Gambar 4.2 memperlihatkan bahwa transaksi elektronik pada dasarnya merupakan suatu hubungan hukum yang terbentuk melalui interaksi antara subjek hukum dan objek hukum yang difasilitasi oleh sistem elektronik. Hubungan hukum tersebut tidak hanya melibatkan para pihak yang melakukan transaksi, tetapi juga berbagai penyelenggara layanan digital yang mendukung terlaksananya transaksi secara elektronik. Dengan demikian, transaksi elektronik merupakan suatu sistem yang terdiri atas berbagai komponen yang saling berkaitan, mulai dari para pelaku transaksi, objek yang diperdagangkan, mekanisme pembentukan perjanjian elektronik, hingga hak dan kewajiban yang timbul sebagai akibat hukum dari transaksi tersebut.



Gambar 4.2: Subjek dan Objek Hukum Dalam Transaksi Elektronik

Pada sisi subjek hukum, gambar menunjukkan bahwa pihak-pihak yang dapat terlibat dalam transaksi elektronik tidak hanya terbatas pada individu sebagai penjual dan pembeli, tetapi juga mencakup badan hukum, penyelenggara sistem elektronik, penyedia layanan pembayaran digital, penyelenggara sertifikasi elektronik, *platform marketplace*, serta instansi pemerintah yang menyelenggarakan layanan berbasis elektronik. Setiap subjek hukum tersebut memiliki kewenangan, hak, dan tanggung jawab yang berbeda sesuai dengan kedudukannya dalam hubungan hukum. Oleh karena itu, apabila terjadi pelanggaran hukum atau sengketa dalam transaksi

elektronik, penentuan pihak yang bertanggung jawab harus didasarkan pada fungsi dan peran masing-masing subjek dalam penyelenggaraan transaksi.

Sementara itu, objek hukum dalam transaksi elektronik mengalami perkembangan yang jauh lebih luas dibandingkan objek hukum dalam transaksi konvensional. Selain barang berwujud (*tangible goods*), objek transaksi juga mencakup barang tidak berwujud (*intangible goods*), jasa digital, informasi elektronik, dokumen elektronik, perangkat lunak (*software*), data pribadi, hak kekayaan intelektual, aset digital, hingga berbagai bentuk layanan berbasis internet. Perkembangan tersebut menunjukkan bahwa digitalisasi telah memperluas cakupan objek hukum yang memiliki nilai ekonomi sekaligus memerlukan perlindungan hukum yang memadai.

Hubungan antara subjek dan objek hukum diwujudkan melalui pembentukan perjanjian elektronik sebagai dasar lahirnya hak dan kewajiban para pihak. Perjanjian elektronik dapat dilakukan melalui berbagai mekanisme, seperti persetujuan secara daring (*click-wrap agreement*), persetujuan penggunaan layanan (*terms and conditions*), maupun kontrak elektronik yang ditandatangani menggunakan tanda tangan elektronik tersertifikasi. Meskipun dilakukan secara digital, perjanjian tersebut tetap harus memenuhi syarat sah perjanjian sebagaimana diatur dalam ketentuan hukum perdata Indonesia agar mempunyai kekuatan mengikat bagi para pihak.

Selanjutnya, gambar juga menggambarkan bahwa setiap transaksi elektronik menimbulkan konsekuensi hukum berupa hak dan kewajiban yang harus dipenuhi oleh masing-masing pihak. Konsumen berhak memperoleh informasi yang benar, pelindungan data pribadi, keamanan transaksi, serta barang atau jasa yang sesuai dengan perjanjian. Sebaliknya, pelaku usaha berkewajiban memberikan informasi yang jujur, menjaga keamanan sistem, memenuhi prestasi sesuai perjanjian, dan bertanggung jawab atas layanan yang diberikan. Penyelenggara sistem elektronik juga memiliki kewajiban untuk menjamin keandalan sistem, menjaga kerahasiaan data pengguna, serta menerapkan standar keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan.

Secara keseluruhan, uraian tersebut menunjukkan bahwa transaksi elektronik tidak hanya merupakan aktivitas ekonomi berbasis teknologi,

tetapi juga merupakan hubungan hukum yang melibatkan berbagai subjek, objek, hak, dan kewajiban yang saling berkaitan dalam suatu ekosistem digital. Oleh karena itu, keberhasilan penyelenggaraan transaksi elektronik tidak hanya bergantung pada kecanggihan teknologi yang digunakan, tetapi juga pada kepatuhan seluruh pihak terhadap prinsip-prinsip hukum, seperti kepastian hukum, itikad baik, perlindungan konsumen, keamanan informasi, serta pelindungan data pribadi.

4.4 Hak dan Kewajiban Para Pihak dalam Sistem Elektronik

Perkembangan teknologi informasi telah mengubah pola hubungan hukum dalam berbagai aktivitas masyarakat, khususnya dalam penyelenggaraan sistem elektronik dan transaksi elektronik. Interaksi yang sebelumnya dilakukan secara langsung kini beralih ke platform digital yang memungkinkan para pihak melakukan komunikasi, pertukaran data, hingga pembentukan hubungan hukum tanpa harus bertatap muka. Perubahan tersebut memberikan kemudahan dalam berbagai aspek, tetapi pada saat yang sama juga melahirkan konsekuensi hukum berupa hak dan kewajiban yang harus dipenuhi oleh setiap pihak yang terlibat dalam penyelenggaraan sistem elektronik.

Dalam perspektif hukum perdata, setiap hubungan hukum pada dasarnya melahirkan hubungan timbal balik (*reciprocal rights and obligations*) antara para pihak. Prinsip tersebut tetap berlaku dalam penyelenggaraan sistem elektronik, meskipun hubungan hukumnya berlangsung melalui media digital. Perbedaannya terletak pada karakteristik ruang siber yang bersifat *borderless*, berbasis teknologi, melibatkan pemrosesan data elektronik, serta mempertemukan berbagai aktor dalam satu ekosistem digital. Oleh karena itu, pengaturan hak dan kewajiban dalam sistem elektronik tidak cukup hanya mengacu pada ketentuan umum hukum perdata, tetapi juga harus memperhatikan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta berbagai regulasi sektoral lainnya.

Pengaturan mengenai hak dan kewajiban para pihak merupakan manifestasi dari asas kepastian hukum, itikad baik (*good faith*), akuntabilitas, dan perlindungan hukum. Asas-asas tersebut diperlukan untuk menciptakan keseimbangan antara kepentingan pengguna sistem elektronik, pelaku usaha, penyelenggara sistem elektronik, maupun negara sebagai regulator. Tanpa adanya pembagian hak dan kewajiban yang proporsional, penyelenggaraan sistem elektronik berpotensi menimbulkan ketidakpastian hukum, penyalahgunaan data pribadi, pelanggaran hak konsumen, hingga sengketa akibat kegagalan sistem elektronik.

Dalam praktiknya, hubungan hukum dalam sistem elektronik setidaknya melibatkan empat aktor utama, yaitu pengguna sistem elektronik, pelaku usaha digital, Penyelenggara Sistem Elektronik (PSE), dan pemerintah. Masing-masing memiliki kedudukan hukum yang berbeda sehingga hak dan kewajibannya pun tidak dapat disamakan. Pengguna sistem elektronik berhak memperoleh layanan yang aman, informasi yang benar, perlindungan terhadap data pribadinya, serta mekanisme penyelesaian sengketa apabila mengalami kerugian. Di sisi lain, pengguna juga berkewajiban menggunakan sistem elektronik secara bertanggung jawab, memberikan data yang benar, mematuhi syarat dan ketentuan penggunaan layanan (*terms and conditions*), dan tidak melakukan penyalahgunaan sistem elektronik.

Pelaku usaha digital memiliki hak untuk memperoleh pembayaran atas barang atau jasa yang diperdagangkan serta mendapatkan perlindungan hukum terhadap tindakan konsumen yang dilakukan dengan itikad tidak baik. Sebaliknya, pelaku usaha berkewajiban memberikan informasi yang benar, jelas, dan jujur mengenai produk yang diperdagangkan, menjamin keamanan transaksi elektronik, memenuhi prestasi sesuai perjanjian, serta bertanggung jawab atas kerugian yang timbul akibat kesalahan atau kelalaiannya. Dalam konteks transaksi elektronik, kewajiban tersebut tidak hanya didasarkan pada hukum perjanjian, tetapi juga diperkuat oleh prinsip perlindungan konsumen dan tata kelola perdagangan melalui sistem elektronik. Penelitian Rizkia et al. (2024) menunjukkan bahwa efektivitas perlindungan konsumen dalam transaksi elektronik sangat dipengaruhi oleh kepatuhan pelaku usaha terhadap kewajiban hukum, kualitas penegakan hukum, kesadaran konsumen terhadap hak-haknya, serta tersedianya mekanisme penyelesaian sengketa yang efektif.

Di samping pelaku usaha, Penyelenggara Sistem Elektronik memiliki posisi strategis karena menyediakan infrastruktur digital yang memungkinkan berlangsungnya transaksi elektronik. Peraturan Pemerintah Nomor 71 Tahun 2019 mewajibkan PSE untuk menjamin keandalan, keamanan, dan keberlangsungan sistem elektronik yang diselenggarakannya. Selain itu, PSE wajib melindungi kerahasiaan, integritas, dan ketersediaan data elektronik, menerapkan manajemen risiko keamanan informasi, serta bertanggung jawab atas penyelenggaraan sistem elektronik sesuai dengan standar yang ditentukan oleh peraturan perundang-undangan. Kewajiban tersebut menunjukkan bahwa tanggung jawab PSE tidak hanya bersifat teknis, tetapi juga memiliki dimensi hukum karena berkaitan langsung dengan perlindungan hak pengguna sistem elektronik.

Perkembangan ekonomi digital juga memperluas dimensi tanggung jawab penyelenggara sistem elektronik, terutama terkait pelindungan data pribadi. Setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, PSE yang bertindak sebagai pengendali data wajib memproses data secara sah, transparan, dan terbatas pada tujuan tertentu, serta menerapkan langkah-langkah teknis dan organisatoris untuk mencegah kebocoran data. Apabila terjadi pelanggaran keamanan data pribadi, penyelenggara wajib memberitahukan kepada pemilik data serta dapat dikenai sanksi administratif maupun tanggung jawab keperdataan apabila kelalaiannya menimbulkan kerugian. Hasil penelitian (Salim et al., 2024) menunjukkan bahwa perlindungan data konsumen dalam praktik *e-commerce* tidak lagi dipandang sebagai kewajiban etis semata, melainkan telah menjadi kewajiban hukum yang dapat menimbulkan konsekuensi administratif, perdata, maupun pidana apabila dilanggar.

Negara juga memiliki hak dan kewajiban dalam penyelenggaraan sistem elektronik. Sebagai regulator, pemerintah berwenang membentuk regulasi, melakukan pengawasan, menetapkan standar keamanan sistem elektronik, serta menjatuhkan sanksi terhadap pelanggaran yang dilakukan oleh penyelenggara sistem elektronik maupun pelaku usaha digital. Di sisi lain, pemerintah berkewajiban menciptakan ekosistem digital yang aman, menjamin kepastian hukum, melindungi hak-hak masyarakat, serta mendorong berkembangnya inovasi teknologi yang bertanggung jawab. Dengan demikian, fungsi negara tidak hanya bersifat represif melalui

penegakan hukum, tetapi juga preventif melalui pembentukan kebijakan yang adaptif terhadap perkembangan teknologi digital.

Berdasarkan uraian tersebut, dapat dipahami bahwa hak dan kewajiban para pihak dalam sistem elektronik merupakan konsekuensi hukum yang melekat pada setiap hubungan hukum digital. Keseimbangan antara hak dan kewajiban tersebut menjadi fondasi penting dalam mewujudkan penyelenggaraan sistem elektronik yang akuntabel, aman, dan berkeadilan. Oleh karena itu, kepatuhan seluruh pihak terhadap kewajiban hukumnya sekaligus penghormatan terhadap hak pihak lain merupakan prasyarat utama bagi terciptanya kepercayaan (*digital trust*) yang menjadi dasar berkembangnya ekonomi digital dan transformasi digital di Indonesia.

4.5 Peran Penyelenggara Sistem Elektronik

Secara normatif, kedudukan Penyelenggara Sistem Elektronik di Indonesia diatur dalam perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Peraturan Pemerintah Nomor 71 Tahun 2019. Peraturan tersebut mendefinisikan Penyelenggara Sistem Elektronik sebagai setiap orang, badan usaha, penyelenggara negara, maupun masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik bagi kepentingannya sendiri maupun kepentingan pihak lain. Pengaturan tersebut menunjukkan bahwa ruang lingkup PSE sangat luas, mulai dari instansi pemerintah, perbankan digital, *marketplace*, penyedia komputasi awan (*cloud computing*), media sosial, hingga berbagai platform digital yang saat ini menjadi bagian dari kehidupan masyarakat. Ketentuan tersebut sekaligus menegaskan bahwa penyelenggaraan sistem elektronik tidak hanya dipandang sebagai aktivitas teknis, melainkan juga sebagai aktivitas hukum yang harus memenuhi prinsip keamanan, keandalan, akuntabilitas, dan perlindungan terhadap hak-hak pengguna (Republik Indonesia, 2019b).

Dalam perspektif hukum teknologi informasi, PSE memiliki fungsi strategis karena menjadi penghubung antara teknologi dengan hubungan hukum yang terjadi di ruang digital. Sistem elektronik yang diselenggarakan tidak hanya berfungsi sebagai sarana komunikasi atau transaksi, tetapi juga menjadi media lahirnya hak, kewajiban, serta tanggung jawab hukum para pihak. Oleh sebab itu, penyelenggaraan sistem elektronik harus mampu menjamin

bahwa informasi elektronik, dokumen elektronik, maupun transaksi elektronik dapat berlangsung secara aman, utuh, autentik, serta dapat dipertanggungjawabkan secara hukum. Dengan kata lain, kualitas penyelenggaraan sistem elektronik akan menentukan tingkat kepercayaan masyarakat (*digital trust*) terhadap berbagai layanan digital yang berkembang di Indonesia.

4.5.1 Penyedia Infrastruktur Digital

Peran pertama Penyelenggara Sistem Elektronik adalah menyediakan infrastruktur digital yang memungkinkan berlangsungnya berbagai aktivitas elektronik. Infrastruktur tersebut meliputi perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komunikasi, pusat data (*data center*), layanan komputasi awan, hingga berbagai aplikasi yang menjadi media penyelenggaraan layanan digital. Tanpa keberadaan infrastruktur tersebut, berbagai transaksi elektronik seperti perdagangan elektronik (*e-commerce*), layanan perbankan digital, pemerintahan berbasis elektronik (*e-government*), maupun layanan kesehatan digital tidak akan dapat berjalan secara optimal.

Dalam konteks ini, PSE tidak hanya dituntut menyediakan sistem yang berfungsi secara teknis, tetapi juga menjamin bahwa sistem tersebut memiliki tingkat keandalan (*reliability*), interoperabilitas, serta keberlangsungan layanan (*business continuity*) yang memadai. Peraturan Pemerintah Nomor 71 Tahun 2019 mengharuskan setiap penyelenggara menjamin sistem elektronik tetap berfungsi sesuai dengan tujuan penyelenggaraannya, memiliki mekanisme pemulihan ketika terjadi gangguan, serta menyediakan rekam jejak audit (*audit trail*) yang dapat digunakan dalam proses pengawasan maupun penyelesaian sengketa.

4.5.2 Menjamin Keamanan Sistem Elektronik

Selain menyediakan infrastruktur digital, Penyelenggara Sistem Elektronik juga berperan sebagai pihak yang bertanggung jawab menjaga keamanan sistem elektronik. Keamanan tersebut mencakup perlindungan terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi elektronik. Ketiga prinsip tersebut dikenal sebagai CIA (*Confidentiality, Integrity, dan Availability)* Triad yang hingga saat ini menjadi standar internasional dalam tata kelola keamanan informasi.

Peraturan Pemerintah Nomor 71 Tahun 2019 mewajibkan setiap PSE melakukan pengamanan terhadap seluruh komponen sistem elektronik, menyediakan prosedur pencegahan dan penanggulangan gangguan, menjaga kerahasiaan informasi elektronik, serta menjamin keberlangsungan layanan apabila terjadi gangguan sistem. Bahkan apabila terjadi serangan siber yang menimbulkan dampak serius, PSE berkewajiban mengamankan informasi elektronik dan segera melaporkannya kepada aparat penegak hukum maupun instansi pemerintah yang berwenang.

Menurut Mantili & Dewi (2020) kewajiban tersebut merupakan implementasi asas kehati-hatian (*prudential principle*) dalam penyelenggaraan sistem elektronik. Penyelenggara sistem elektronik tidak cukup hanya menyediakan teknologi, tetapi juga wajib menerapkan tata kelola sistem elektronik yang baik (*good electronic system governance*), melakukan pengamanan terhadap seluruh komponen sistem, serta melindungi pengguna dari kerugian yang mungkin timbul akibat penyelenggaraan sistem elektronik. Oleh karena itu, tanggung jawab PSE bersifat preventif sekaligus represif karena mencakup upaya pencegahan maupun penanganan apabila terjadi gangguan terhadap sistem elektronik.

4.5.3 Melindungi Data Pribadi Pengguna

Perkembangan ekonomi digital menyebabkan data pribadi menjadi salah satu aset yang paling bernilai dalam penyelenggaraan layanan elektronik. Hampir seluruh aktivitas digital, mulai dari penggunaan media sosial, perdagangan elektronik, layanan kesehatan, pendidikan, hingga layanan keuangan digital, melibatkan pemrosesan data pribadi pengguna. Oleh karena itu, pelindungan data pribadi telah menjadi salah satu tanggung jawab utama Penyelenggara Sistem Elektronik.

Setelah berlakunya Undang-Undang Nomor 27 Tahun 2022, setiap PSE yang bertindak sebagai pengendali data wajib memastikan bahwa pemrosesan data dilakukan secara sah, transparan, terbatas pada tujuan tertentu, serta dilengkapi dengan langkah-langkah teknis dan organisatoris untuk mencegah penyalahgunaan maupun kebocoran data. Penelitian Maharani & Prakoso (2024) menjelaskan bahwa pelindungan data pribadi merupakan bentuk tanggung jawab hukum yang melekat pada Penyelenggara Sistem Elektronik. Kewajiban tersebut tidak hanya berkaitan

dengan penyimpanan data secara aman, tetapi juga meliputi transparansi penggunaan data, pemberian informasi kepada pengguna, pembatasan akses terhadap data pribadi, serta kewajiban melakukan pemberitahuan apabila terjadi insiden kebocoran data. Menurut penelitian tersebut, keberhasilan pelindungan data pribadi sangat dipengaruhi oleh kepatuhan PSE dalam menerapkan prinsip akuntabilitas, transparansi, dan keamanan informasi.

Urgensi pelindungan data pribadi semakin meningkat seiring bertambahnya kasus kebocoran data di Indonesia. Penelitian Amelia (2025) menunjukkan bahwa meningkatnya penggunaan layanan digital juga meningkatkan risiko kebocoran data akibat serangan siber maupun kelalaian internal penyelenggara sistem elektronik. Oleh karena itu, tanggung jawab hukum PSE tidak hanya terbatas pada pemenuhan kewajiban administratif, tetapi juga dapat melahirkan tanggung jawab perdata, administratif, maupun pidana apabila terbukti lalai dalam menjaga keamanan data pribadi pengguna.

4.5.4 Mendukung Penegakan Hukum dan Penyelesaian Sengketa

Peran penting lainnya adalah mendukung proses penegakan hukum di ruang digital. Sistem elektronik yang diselenggarakan oleh PSE harus mampu menyediakan rekam jejak audit (*audit trail*), menyimpan log aktivitas pengguna, menjaga integritas dokumen elektronik, serta menyediakan bukti elektronik yang dapat digunakan dalam proses pembuktian di pengadilan. Fungsi tersebut menjadi sangat penting mengingat bukti elektronik telah diakui sebagai alat bukti yang sah dalam sistem hukum Indonesia.

Peraturan Pemerintah Nomor 71 Tahun 2019 juga mengatur bahwa Penyelenggara Sistem Elektronik lingkup privat wajib memberikan akses terhadap sistem elektronik maupun data elektronik dalam rangka pengawasan dan penegakan hukum sesuai dengan ketentuan peraturan perundang-undangan. Di sisi lain, kewajiban tersebut tetap harus memperhatikan prinsip pelindungan data pribadi serta hak atas privasi sehingga tidak menimbulkan penyalahgunaan kewenangan oleh pihak tertentu. Peran Penyelenggara Sistem Elektronik dalam mendukung penegakan hukum juga semakin penting seiring dengan meningkatnya kompleksitas tindak pidana siber dan sengketa yang melibatkan transaksi elektronik. Dalam praktiknya, bukti elektronik yang tersimpan dalam sistem

elektronik sering kali menjadi alat bukti utama untuk mengungkap peristiwa hukum, baik dalam perkara perdata, pidana, maupun administrasi. Oleh karena itu, PSE dituntut untuk menerapkan tata kelola informasi yang mampu menjamin keaslian (*authenticity*), keutuhan (*integrity*), dan keterlacakan (*traceability*) setiap data elektronik yang dikelolanya. Tanggung jawab PSE tidak berhenti pada penyediaan layanan elektronik, tetapi juga mencakup kewajiban untuk memastikan bahwa sistem yang diselenggarakan mampu menghasilkan dan menyimpan informasi elektronik yang dapat dipertanggungjawabkan sebagai alat bukti apabila terjadi sengketa hukum (Mantili & Dewi, 2020).

4.6 Permasalahan Hukum dalam Implementasi Sistem Elektronik

Transformasi digital telah mengubah sistem penyelenggaraan berbagai aktivitas masyarakat dari mekanisme konvensional menuju mekanisme elektronik yang semakin terintegrasi. Sistem elektronik saat ini tidak lagi hanya berfungsi sebagai instrumen pendukung administrasi, tetapi telah berkembang menjadi infrastruktur utama dalam penyelenggaraan pemerintahan, perdagangan, pelayanan kesehatan, pendidikan, jasa keuangan, hingga penegakan hukum. Ketergantungan yang semakin tinggi terhadap sistem elektronik menunjukkan bahwa keberhasilan pembangunan ekonomi digital tidak hanya ditentukan oleh kemajuan teknologi, melainkan juga oleh kemampuan sistem hukum dalam mengatur, mengawasi, dan menjamin kepastian hukum terhadap seluruh aktivitas yang berlangsung di ruang digital.

Meskipun Indonesia telah memiliki berbagai instrumen hukum, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, keberadaan regulasi tersebut belum sepenuhnya mampu menghilangkan berbagai persoalan hukum dalam praktik penyelenggaraan sistem elektronik. Perkembangan teknologi berlangsung jauh lebih cepat dibandingkan proses pembentukan maupun pembaruan regulasi, sehingga hukum sering kali berada pada posisi mengejar (*law lags*

behind technology). Akibatnya, muncul berbagai persoalan baru yang tidak selalu dapat diselesaikan hanya dengan pendekatan hukum konvensional. Kondisi ini menunjukkan bahwa tantangan utama hukum teknologi informasi bukan lagi sekadar membentuk regulasi baru, melainkan memastikan bahwa regulasi yang ada mampu diimplementasikan secara efektif, adaptif, dan responsif terhadap perubahan teknologi (Setyananda & Israhadi, 2025).

Persoalan hukum pertama adalah masih adanya fragmentasi regulasi yang mengatur penyelenggaraan sistem elektronik. Saat ini pengaturan tersebar dalam berbagai peraturan, antara lain Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, dan berbagai peraturan sektoral lainnya. Banyaknya regulasi tersebut memang menunjukkan perhatian negara terhadap perkembangan teknologi informasi, tetapi di sisi lain juga menimbulkan persoalan berupa tumpang tindih kewenangan, inkonsistensi norma, serta potensi perbedaan penafsiran dalam implementasi.

Misalnya, pengaturan mengenai pelindungan data pribadi tidak hanya terdapat dalam Undngag-Undang Pelindungan Data Pribadi, tetapi juga tersebar dalam Undang-Undang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah Nomor 71 Tahun 2019. Akibatnya, ketika terjadi pelanggaran berupa kebocoran data pribadi, sering muncul pertanyaan mengenai regulasi mana yang menjadi dasar utama pertanggungjawaban hukum serta instansi mana yang memiliki kewenangan pengawasan. Kondisi tersebut berpotensi mengurangi kepastian hukum bagi masyarakat maupun pelaku usaha. Koswara (2022) mengemukakan bahwa persoalan utama pelindungan data pribadi di Indonesia bukan semata-mata terletak pada ketersediaan regulasi, melainkan pada belum terintegrasinya berbagai ketentuan yang mengatur isu tersebut. Akibatnya, implementasi pelindungan hukum sering menghadapi kendala berupa perbedaan penafsiran norma dan pembagian kewenangan antarinstansi, sehingga harmonisasi regulasi menjadi kebutuhan yang tidak dapat dihindari.

Persoalan hukum kedua yang masih dihadapi dalam penyelenggaraan sistem elektronik adalah belum meratanya tingkat kepatuhan Penyelenggara Sistem Elektronik (PSE) terhadap kewajiban hukum yang telah ditetapkan dalam

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Padahal, regulasi tersebut mewajibkan setiap PSE untuk memastikan sistem elektronik yang dikelolanya memenuhi prinsip keandalan, keamanan, dan akuntabilitas. Selain itu, penyelenggara juga diwajibkan menerapkan manajemen risiko, menjaga perlindungan terhadap informasi dan data elektronik, serta menyediakan prosedur pemulihan (*recovery mechanism*) guna menjamin keberlangsungan layanan apabila terjadi gangguan atau kegagalan sistem.

Namun, dalam praktiknya masih ditemukan berbagai kasus gangguan sistem, kegagalan layanan, hingga kebocoran data yang menunjukkan bahwa standar keamanan informasi belum diterapkan secara optimal. Permasalahan tersebut memperlihatkan adanya kesenjangan antara norma hukum (*das sollen*) dengan praktik penyelenggaraan sistem elektronik (*das sein*). Akibatnya, perlindungan hukum terhadap pengguna belum sepenuhnya terjamin, sementara mekanisme pengawasan terhadap kepatuhan PSE juga masih belum berjalan secara efektif.

Persoalan hukum yang paling banyak mendapat perhatian dalam beberapa tahun terakhir adalah meningkatnya kasus kebocoran data pribadi. Dalam perspektif hukum, kebocoran data tidak hanya merupakan persoalan keamanan informasi (*cybersecurity*), tetapi juga merupakan bentuk pelanggaran terhadap hak konstitusional warga negara atas pelindungan data pribadi.

Walaupun Undang-Undang Nomor 27 Tahun 2022 telah menetapkan kewajiban pengendali data untuk melindungi data pribadi, implementasinya masih menghadapi berbagai kendala, terutama dalam menentukan bentuk pertanggungjawaban hukum PSE apabila kebocoran terjadi akibat kelalaian (negligence), kegagalan sistem, maupun serangan siber oleh pihak ketiga. Di samping itu, pembuktian hubungan kausal antara kelalaian penyelenggara dan kerugian yang dialami pengguna juga masih menjadi tantangan dalam praktik penyelesaian sengketa. Kajian yang dilakukan oleh (Maharani & Prakoso, 2024) menunjukkan bahwa implementasi pelindungan data pribadi dalam transaksi digital masih menghadapi berbagai hambatan. Hambatan tersebut terutama berkaitan dengan belum optimalnya penerapan prinsip-prinsip tata kelola oleh Penyelenggara Sistem Elektronik, khususnya dalam aspek akuntabilitas, transparansi, dan pengamanan data. Kondisi tersebut mengindikasikan perlunya pengawasan yang lebih efektif serta mekanisme

penegakan hukum yang mampu memastikan kepatuhan penyelenggara terhadap ketentuan peraturan perundang-undangan.

Permasalahan hukum ketiga berkaitan dengan pembuktian apabila terjadi sengketa yang melibatkan sistem elektronik. Secara normatif, informasi elektronik dan dokumen elektronik telah diakui sebagai alat bukti yang sah. Akan tetapi, dalam praktik masih sering muncul persoalan mengenai autentisitas, integritas, serta keandalan bukti elektronik. Pembuktian menjadi semakin kompleks apabila data elektronik telah mengalami perubahan, kerusakan, atau tersimpan pada server yang berada di luar wilayah Indonesia. Selain itu, belum semua aparat penegak hukum memiliki kemampuan teknis yang memadai dalam melakukan pemeriksaan terhadap bukti elektronik maupun audit forensik digital. Akibatnya, proses pembuktian sering berlangsung lebih lama dibandingkan perkara konvensional sehingga berpengaruh terhadap efektivitas penyelesaian sengketa.

Karakteristik internet yang bersifat lintas negara juga menimbulkan persoalan mengenai yurisdiksi hukum. Banyak penyelenggara platform digital berkedudukan di luar Indonesia, sementara pengguna dan kerugian yang ditimbulkan berada di wilayah Indonesia. Kondisi tersebut memunculkan pertanyaan mengenai hukum mana yang berlaku, pengadilan mana yang berwenang mengadili, serta bagaimana pelaksanaan putusan apabila pelaku berada di negara lain. Persoalan ini menunjukkan bahwa implementasi sistem elektronik tidak lagi dapat diselesaikan hanya melalui pendekatan hukum nasional, tetapi memerlukan harmonisasi hukum internasional serta kerja sama lintas negara dalam bidang penegakan hukum siber.

Persoalan terakhir adalah efektivitas pengawasan terhadap penyelenggara sistem elektronik. Peraturan Pemerintah Nomor 71 Tahun 2019 memang memberikan kewenangan kepada pemerintah untuk melakukan pengawasan dan menjatuhkan sanksi administratif kepada PSE yang melanggar ketentuan. Akan tetapi, dalam praktik pemberian sanksi masih dinilai belum memberikan efek jera, terutama terhadap pelanggaran berupa kebocoran data pribadi maupun kelalaian dalam menjaga keamanan sistem.

Attidhira & Permana (2022) menilai bahwa salah satu persoalan dalam implementasi Peraturan Pemerintah Nomor 71 Tahun 2019 terletak pada belum komprehensifnya pengaturan mengenai penanganan insiden

kebocoran data pribadi. Regulasi tersebut belum memberikan parameter yang jelas terkait kategori pelanggaran maupun batas waktu yang wajib dipenuhi oleh Penyelenggara Sistem Elektronik untuk menyampaikan pemberitahuan kepada pemilik data apabila terjadi kebocoran. Ketidakjelasan tersebut berpotensi menimbulkan perbedaan penafsiran dalam penerapan sanksi administratif dan mengurangi efektivitas proses penegakan hukum.

Persoalan terbesar implementasi sistem elektronik di Indonesia bukan lagi kekurangan regulasi, melainkan rendahnya efektivitas implementasi regulasi. Indonesia sebenarnya telah memiliki perangkat hukum yang relatif lengkap, tetapi masih menghadapi tiga persoalan mendasar, yaitu:

11. Normative gap, berupa disharmoni dan tumpang tindih antarregulasi.
12. Enforcement gap, berupa lemahnya pengawasan dan penegakan hukum terhadap penyelenggara sistem elektronik.
13. Compliance gap, berupa belum optimalnya kepatuhan PSE terhadap kewajiban hukum, khususnya dalam pelindungan data pribadi dan keamanan sistem.

Ketiga persoalan tersebut saling berkaitan sehingga penyelesaiannya memerlukan pendekatan yang tidak hanya berorientasi pada pembentukan regulasi baru, tetapi juga pada penguatan kelembagaan, peningkatan kapasitas aparat penegak hukum, pengawasan yang efektif, dan pembangunan budaya kepatuhan hukum di kalangan penyelenggara sistem elektronik maupun pengguna layanan digital. Dengan demikian, sistem elektronik tidak hanya mampu mendorong transformasi digital nasional, tetapi juga memberikan kepastian hukum, perlindungan hak, dan keadilan bagi seluruh pihak yang terlibat.

Bab 5
Aspek Hukum Informasi dan Dokumen Elektronik

5.1 Pengertian Informasi Elektronik dan Dokumen Elektronik

Perkembangan teknologi informasi telah mengubah cara manusia menciptakan, menyimpan, mengirimkan, dan menggunakan informasi. Informasi yang sebelumnya banyak diwujudkan dalam bentuk fisik, seperti surat, formulir, kuitansi, kontrak, arsip kertas, atau dokumen tertulis lainnya, kini dapat dibuat dan dikelola dalam bentuk elektronik. Perubahan ini menunjukkan bahwa informasi tidak lagi hanya dipahami sebagai sesuatu yang melekat pada media kertas, tetapi juga sebagai data yang diproses, disimpan, dan ditransmisikan melalui sistem elektronik. Dalam konteks hukum teknologi informasi, perubahan bentuk informasi tersebut memiliki konsekuensi penting karena informasi elektronik dapat menimbulkan akibat hukum, digunakan dalam transaksi, serta menjadi dasar pembuktian dalam penyelesaian sengketa (Edrisy, 2019; Murray, 2019).

Dalam sistem hukum Indonesia, pengertian informasi elektronik merujuk pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah, termasuk melalui Undang-Undang Nomor 1 Tahun 2024. Secara normatif, informasi elektronik dapat dipahami sebagai satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, pertukaran data elektronik, surat elektronik, telegram, teleks, telekopi, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah dan memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya (Republik Indonesia, 2008, 2024b). Berdasarkan pengertian tersebut, informasi elektronik memiliki cakupan yang sangat luas karena tidak hanya meliputi teks tertulis, tetapi juga berbagai bentuk data digital yang dapat diproses oleh sistem elektronik.

Dokumen elektronik merupakan bentuk lebih spesifik dari informasi elektronik. Dokumen elektronik dapat dipahami sebagai setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau bentuk sejenis lainnya, yang dapat dilihat, ditampilkan, atau didengar melalui komputer atau sistem elektronik. Dengan demikian, dokumen elektronik tidak hanya menunjuk pada file digital dalam format tertentu, tetapi juga mencakup berbagai bentuk informasi yang tersimpan dan dapat diakses kembali melalui perangkat elektronik, seperti dokumen kontrak digital, surat elektronik, bukti pembayaran elektronik, rekaman transaksi, formulir daring, arsip administrasi digital, serta dokumen yang ditandatangani secara elektronik (Republik Indonesia, 2008, 2019b).

Perbedaan utama antara informasi elektronik dan dokumen elektronik terletak pada karakter dan fungsinya. Informasi elektronik lebih menekankan pada data atau muatan informasi yang memiliki arti, sedangkan dokumen elektronik menekankan pada bentuk, media, dan keberadaan informasi tersebut sebagai dokumen yang dapat disimpan, ditampilkan, dikirimkan, atau digunakan kembali. Dengan kata lain, setiap dokumen elektronik pada dasarnya mengandung informasi elektronik, tetapi tidak semua informasi elektronik selalu diposisikan sebagai dokumen elektronik. Misalnya, kode akses, data lokasi, atau metadata dapat dikategorikan sebagai informasi elektronik, sedangkan kontrak digital, kuitansi elektronik, dan surat elektronik yang tersimpan dalam sistem dapat dikategorikan sebagai dokumen elektronik apabila memenuhi karakter sebagai dokumen yang dapat ditampilkan dan digunakan kembali.

Dalam praktik transaksi elektronik, informasi elektronik dan dokumen elektronik memiliki peran yang sangat penting. Keduanya menjadi dasar terbentuknya hubungan hukum dalam berbagai aktivitas digital, seperti perdagangan elektronik (*e-commerce*), layanan keuangan digital, administrasi pemerintahan elektronik, pendidikan daring, layanan kesehatan digital, dan komunikasi bisnis berbasis platform. Dalam transaksi elektronik, dokumen seperti konfirmasi pesanan, bukti pembayaran, syarat dan ketentuan layanan, perjanjian elektronik, serta tanda terima digital dapat menjadi bukti adanya hubungan hukum antara para pihak. Oleh karena itu, informasi elektronik dan dokumen elektronik tidak dapat dipandang semata-mata sebagai data teknis, tetapi harus dipahami sebagai objek hukum yang

dapat menimbulkan hak, kewajiban, dan tanggung jawab hukum (Brownsword & Goodwin, 2012; Rahmawati et al., 2024).

Pengakuan terhadap informasi elektronik dan dokumen elektronik juga berkaitan erat dengan kebutuhan kepastian hukum dalam masyarakat digital. Tanpa pengakuan hukum terhadap informasi dan dokumen elektronik, aktivitas digital akan menghadapi kesulitan dalam pembuktian, pertanggungjawaban, dan penyelesaian sengketa. Oleh karena itu, hukum memberikan legitimasi terhadap informasi elektronik dan dokumen elektronik agar dapat digunakan dalam hubungan hukum sepanjang memenuhi persyaratan yang ditentukan oleh peraturan perundang-undangan. Persyaratan tersebut terutama berkaitan dengan keutuhan, keaslian, keteraksesan, dan kemampuan dokumen untuk dipertanggungjawabkan melalui sistem elektronik yang andal dan aman (Casey, 2011; Republik Indonesia, 2019b).

Dengan demikian, informasi elektronik dan dokumen elektronik merupakan fondasi penting dalam penyelenggaraan aktivitas hukum di lingkungan digital. Informasi elektronik menunjukkan adanya data yang memiliki arti dan dapat dipahami, sedangkan dokumen elektronik menunjukkan bentuk informasi yang dibuat, disimpan, dikirimkan, diterima, atau digunakan melalui sistem elektronik. Keduanya menjadi elemen utama dalam transaksi elektronik, pembuktian hukum, penyelenggaraan layanan digital, serta pengelolaan data dalam berbagai sektor. Pemahaman yang tepat mengenai kedua konsep ini menjadi dasar penting sebelum membahas kedudukan hukum dokumen elektronik, keabsahannya sebagai alat bukti, serta penggunaan tanda tangan elektronik dan sertifikat elektronik dalam transaksi digital.

5.2 Kedudukan Hukum Dokumen Elektronik

Dokumen elektronik memiliki kedudukan penting dalam sistem hukum digital karena menjadi salah satu bentuk utama dari informasi yang digunakan dalam hubungan hukum berbasis teknologi. Dalam aktivitas masyarakat modern, berbagai dokumen yang sebelumnya dibuat dalam bentuk fisik kini banyak dialihkan ke dalam bentuk elektronik, seperti perjanjian digital, bukti pembayaran, surat elektronik, formulir daring, arsip administrasi, dokumen transaksi, rekam jejak sistem, hingga dokumen yang

ditandatangani secara elektronik. Perubahan bentuk dokumen dari fisik ke elektronik tidak menghilangkan nilai hukumnya, sepanjang dokumen tersebut memenuhi persyaratan yang ditentukan oleh peraturan perundang-undangan (Republik Indonesia, 2008).

Secara normatif, hukum Indonesia telah mengakui dokumen elektronik sebagai bagian dari sistem hukum informasi dan transaksi elektronik. Pengakuan tersebut menunjukkan bahwa dokumen elektronik tidak hanya dipandang sebagai data teknis yang tersimpan dalam sistem komputer, tetapi juga sebagai objek hukum yang dapat digunakan untuk membuktikan adanya hubungan hukum, peristiwa hukum, hak, kewajiban, maupun tanggung jawab para pihak. Dengan demikian, dokumen elektronik dapat memiliki fungsi yang setara dengan dokumen tertulis dalam banyak aktivitas hukum, terutama dalam transaksi elektronik, administrasi digital, layanan publik berbasis elektronik, dan kegiatan bisnis digital (Edrisy, 2019; Rahmawati et al., 2024).

Kedudukan hukum dokumen elektronik semakin kuat karena Undang-Undang Informasi dan Transaksi Elektronik mengakui informasi elektronik, dokumen elektronik, dan hasil cetaknya sebagai alat bukti hukum yang sah. Pengakuan ini menjadi dasar penting bagi penyelenggaraan aktivitas digital karena para pihak tidak lagi harus selalu bergantung pada dokumen kertas untuk membuktikan adanya suatu transaksi atau komunikasi hukum. Meskipun demikian, pengakuan tersebut tidak bersifat mutlak. Dokumen elektronik harus memenuhi persyaratan agar informasi yang terdapat di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan (Republik Indonesia, 2008, 2019b).

Dalam praktiknya, kedudukan hukum dokumen elektronik bergantung pada keandalan sistem elektronik yang digunakan untuk membuat, mengirim, menerima, menyimpan, atau mengelola dokumen tersebut. Dokumen elektronik yang dibuat melalui sistem yang tidak aman, mudah diubah, tidak memiliki rekam jejak, atau tidak dapat diverifikasi keasliannya akan lebih sulit dipertanggungjawabkan secara hukum. Oleh karena itu, aspek keutuhan (*integrity*), keaslian (*authenticity*), keteraksesan (*accessibility*), dan keterlacakan (*traceability*) menjadi unsur penting dalam menentukan kekuatan hukum dokumen elektronik (Casey, 2011; Republik Indonesia, 2019b).

Selain itu, dokumen elektronik juga memiliki kedudukan penting dalam pembentukan hubungan hukum antarpara pihak. Dalam transaksi elektronik, dokumen seperti syarat dan ketentuan layanan, konfirmasi pesanan, bukti pembayaran, kontrak elektronik, faktur digital, dan persetujuan pengguna dapat menunjukkan adanya kehendak, persetujuan, dan pelaksanaan kewajiban. Oleh karena itu, dokumen elektronik tidak hanya berfungsi sebagai arsip, tetapi juga sebagai bukti adanya kesepakatan dan pelaksanaan hubungan hukum dalam ruang digital (Brownsword & Goodwin, 2012; Murray, 2019).

Namun, tidak semua dokumen dapat sepenuhnya digantikan oleh dokumen elektronik. Dalam ketentuan hukum Indonesia, terdapat jenis dokumen tertentu yang tetap harus dibuat dalam bentuk tertulis atau dalam bentuk akta autentik sesuai dengan ketentuan peraturan perundang-undangan. Misalnya, dokumen yang menurut hukum harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta tertentu tidak dapat begitu saja digantikan oleh dokumen elektronik biasa. Ketentuan ini menunjukkan bahwa kedudukan hukum dokumen elektronik tetap harus memperhatikan jenis dokumen, tujuan penggunaannya, serta syarat formal yang ditentukan oleh hukum (Republik Indonesia, 2008, 2024b) [republikindonesia2008ite; republikindonesia2024ite].

Dalam konteks penyelenggaraan sistem elektronik, dokumen elektronik juga harus dikelola secara aman dan bertanggung jawab. Penyelenggara sistem elektronik memiliki kewajiban untuk memastikan bahwa dokumen dan data elektronik yang dikelolanya tetap terjaga kerahasiaan, keutuhan, ketersediaan, dan keandalannya. Hal ini penting karena dokumen elektronik sering kali memuat informasi yang bernilai hukum, ekonomi, dan pribadi. Apabila dokumen elektronik mengalami perubahan tanpa izin, kehilangan data, kebocoran, atau manipulasi, maka kedudukan hukumnya dapat dipersoalkan dan dapat menimbulkan kerugian bagi para pihak (Republik Indonesia, 2019b, 2022a).

Dengan demikian, kedudukan hukum dokumen elektronik dalam sistem hukum Indonesia telah memperoleh pengakuan yang kuat, terutama dalam konteks informasi dan transaksi elektronik. Dokumen elektronik dapat digunakan sebagai dasar hubungan hukum, alat administrasi, bukti transaksi, dan alat pembuktian sepanjang memenuhi syarat keandalan, keutuhan, keaslian, dan keteraksesan. Namun, pengakuan tersebut tetap memiliki

batasan, terutama terhadap dokumen yang menurut undang-undang wajib dibuat dalam bentuk tertentu. Oleh karena itu, pemanfaatan dokumen elektronik harus selalu memperhatikan ketentuan hukum, keandalan sistem elektronik, serta prinsip keamanan dan pertanggungjawaban dalam pengelolaan data digital.

5.3 Keabsahan Informasi Elektronik sebagai Alat Bukti

Keabsahan informasi elektronik sebagai alat bukti merupakan salah satu aspek penting dalam sistem hukum digital. Dalam aktivitas masyarakat modern, banyak peristiwa hukum tidak lagi meninggalkan jejak dalam bentuk dokumen fisik, tetapi dalam bentuk data elektronik, pesan digital, rekaman transaksi, log sistem, surat elektronik, tangkapan layar, dokumen digital, maupun rekam jejak aktivitas pada suatu platform. Perubahan tersebut menuntut sistem hukum untuk mengakui bahwa pembuktian tidak hanya dapat dilakukan melalui dokumen tertulis konvensional, tetapi juga melalui informasi elektronik yang dihasilkan, dikirimkan, diterima, atau disimpan melalui sistem elektronik (Casey, 2011; Murray, 2019).

Gambar 5.1: Alur Kedudukan Hukum Informasi dan Dokumen Elektronik

Dalam hukum Indonesia, pengakuan terhadap informasi elektronik sebagai alat bukti didasarkan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah, termasuk

melalui Undang-Undang Nomor 1 Tahun 2024. Undang-Undang ITE mengakui bahwa informasi elektronik, dokumen elektronik, dan hasil cetaknya merupakan alat bukti hukum yang sah. Pengakuan ini memperluas sistem pembuktian hukum karena informasi yang tersimpan atau dikirim melalui media elektronik dapat digunakan untuk membuktikan adanya perbuatan hukum, hubungan hukum, transaksi, komunikasi, maupun peristiwa hukum tertentu (Republik Indonesia, 2008, 2024b).

Meskipun demikian, keabsahan informasi elektronik sebagai alat bukti tidak hanya ditentukan oleh keberadaannya dalam bentuk digital. Informasi elektronik harus memenuhi persyaratan tertentu agar dapat diterima dan dipertanggungjawabkan secara hukum. Syarat utama yang harus diperhatikan adalah informasi tersebut dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan. Dengan kata lain, informasi elektronik harus dapat menunjukkan bahwa data yang digunakan sebagai bukti tidak mengalami perubahan yang tidak sah, berasal dari sumber yang dapat ditelusuri, dan dapat diperiksa kembali apabila diperlukan dalam proses pembuktian (Republik Indonesia, 2008, *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*; Republik Indonesia, 2019, *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*).

Aspek keutuhan (*integrity*) menjadi unsur penting dalam menentukan kekuatan pembuktian informasi elektronik. Suatu informasi elektronik akan lebih kuat kedudukannya sebagai alat bukti apabila dapat dibuktikan bahwa isinya tidak berubah sejak pertama kali dibuat, dikirim, diterima, atau disimpan. Keutuhan ini dapat dijaga melalui mekanisme teknis seperti pengamanan sistem, penggunaan tanda tangan elektronik, pencatatan waktu, rekam jejak sistem, enkripsi, dan pengendalian akses. Jika suatu informasi elektronik dapat dengan mudah diubah tanpa rekam jejak yang jelas, maka nilai pembuktiannya dapat dipersoalkan karena tidak ada jaminan bahwa informasi tersebut masih sesuai dengan kondisi aslinya (Casey, 2011; Republik Indonesia, 2019b).

Selain keutuhan, aspek keaslian (*authenticity*) juga menjadi syarat penting. Keaslian berkaitan dengan kemampuan untuk membuktikan bahwa informasi elektronik benar-benar berasal dari pihak, sistem, perangkat, atau akun tertentu. Dalam perkara hukum, keaslian diperlukan untuk memastikan bahwa suatu pesan, dokumen, atau data benar-benar dibuat atau dikirim oleh

pihak yang dikaitkan dengan informasi tersebut. Oleh karena itu, autentikasi melalui tanda tangan elektronik, sertifikat elektronik, metadata, alamat internet protokol, rekam aktivitas, atau bukti teknis lain menjadi penting dalam menilai hubungan antara informasi elektronik dan pihak yang diduga membuat atau menggunakannya (Casey, 2011; Rahmawati et al., 2024).

Keteraksesan (*accessibility*) juga menentukan apakah informasi elektronik dapat digunakan secara efektif dalam proses pembuktian. Informasi elektronik yang tidak dapat dibuka, tidak dapat ditampilkan, rusak, terenkripsi tanpa kunci yang sah, atau tersimpan dalam sistem yang tidak dapat diperiksa akan sulit digunakan sebagai alat bukti. Oleh karena itu, penyimpanan dan pengelolaan informasi elektronik harus dilakukan dengan cara yang memungkinkan informasi tersebut dapat ditemukan, ditampilkan, dibaca, dan diverifikasi kembali. Dalam konteks ini, keandalan sistem elektronik menjadi faktor penting karena sistem yang andal mampu menjaga agar informasi tetap tersedia, utuh, dan dapat digunakan ketika diperlukan (Republik Indonesia, 2019b).

Dalam praktik pembuktian, informasi elektronik juga perlu dinilai berdasarkan relevansi dan keterkaitannya dengan peristiwa hukum yang dibuktikan. Tidak semua data elektronik otomatis memiliki nilai pembuktian yang kuat. Informasi elektronik harus memiliki hubungan yang jelas dengan perkara, menunjukkan fakta yang relevan, dan diperoleh melalui cara yang sah. Misalnya, bukti pembayaran elektronik dapat digunakan untuk menunjukkan adanya transaksi, rekam percakapan dapat menunjukkan adanya komunikasi, log sistem dapat menunjukkan aktivitas akses, dan surat elektronik dapat menunjukkan adanya kesepakatan atau pemberitahuan. Namun, setiap bukti tersebut tetap harus diuji dari sisi keaslian, keutuhan, dan cara memperolehnya (Aini & Lubis, 2024; Casey, 2011).

Keabsahan informasi elektronik juga berkaitan dengan prinsip kehati-hatian dalam penyelenggaraan sistem elektronik. Penyelenggara sistem elektronik memiliki tanggung jawab untuk memastikan bahwa sistem yang digunakan mampu menghasilkan, menyimpan, dan menampilkan informasi elektronik secara andal. Apabila sistem elektronik tidak memiliki prosedur pengamanan, tidak menyimpan rekam jejak, atau tidak mampu menunjukkan proses terbentuknya suatu data, maka informasi yang dihasilkan dari sistem tersebut dapat dipersoalkan dalam pembuktian. Oleh karena itu, tanggung jawab penyelenggara sistem elektronik tidak hanya

bersifat teknis, tetapi juga memiliki konsekuensi hukum karena berkaitan dengan keabsahan dan kekuatan pembuktian informasi elektronik (Mantili & Dewi, 2020; Republik Indonesia, 2019b).

Dalam konteks perkara perdata, informasi elektronik dapat digunakan untuk membuktikan adanya perjanjian, transaksi, pembayaran, persetujuan, wanprestasi, maupun kerugian. Dalam perkara pidana, informasi elektronik dapat digunakan untuk membuktikan adanya akses tanpa hak, manipulasi data, penipuan daring, pencemaran nama baik, penyebaran dokumen elektronik, atau tindak pidana lain yang dilakukan melalui sistem elektronik. Sementara itu, dalam perkara administrasi, informasi elektronik dapat digunakan untuk membuktikan kepatuhan atau pelanggaran terhadap kewajiban administratif dalam penyelenggaraan sistem elektronik. Hal ini menunjukkan bahwa informasi elektronik memiliki kedudukan lintas bidang hukum karena dapat digunakan dalam berbagai jenis perkara sepanjang memenuhi persyaratan pembuktian yang sah (Edrisy, 2019; Rahmawati et al., 2024).

Namun, penggunaan informasi elektronik sebagai alat bukti juga menghadapi berbagai tantangan. Tantangan tersebut antara lain manipulasi data, pemalsuan dokumen elektronik, penghapusan jejak digital, penggunaan identitas palsu, penyimpanan data pada server luar negeri, serta keterbatasan kemampuan teknis dalam memeriksa bukti elektronik. Selain itu, proses pembuktian juga dapat menjadi kompleks apabila bukti elektronik diperoleh dari platform digital yang berada di yurisdiksi berbeda. Kondisi ini menunjukkan bahwa pembuktian elektronik memerlukan kombinasi antara pemahaman hukum, kemampuan forensik digital, keandalan sistem, dan prosedur pengambilan bukti yang benar (Aini & Lubis, 2024; Casey, 2011).

Dengan demikian, informasi elektronik dapat memiliki keabsahan sebagai alat bukti apabila memenuhi persyaratan hukum dan teknis yang menjamin keaslian, keutuhan, keteraksesan, relevansi, serta dapat dipertanggungjawabkan. Pengakuan hukum terhadap informasi elektronik merupakan respons terhadap perkembangan masyarakat digital yang semakin bergantung pada sistem elektronik. Akan tetapi, nilai pembuktiannya tetap harus diuji secara cermat agar informasi elektronik yang digunakan benar-benar dapat dipercaya dan tidak merugikan hak para pihak. Oleh karena itu, pembuktian elektronik membutuhkan regulasi yang

jelas, sistem elektronik yang andal, serta kemampuan aparat dan para pihak dalam memahami karakteristik bukti digital.

5.4 Tanda Tangan Elektronik dan Sertifikat Elektronik

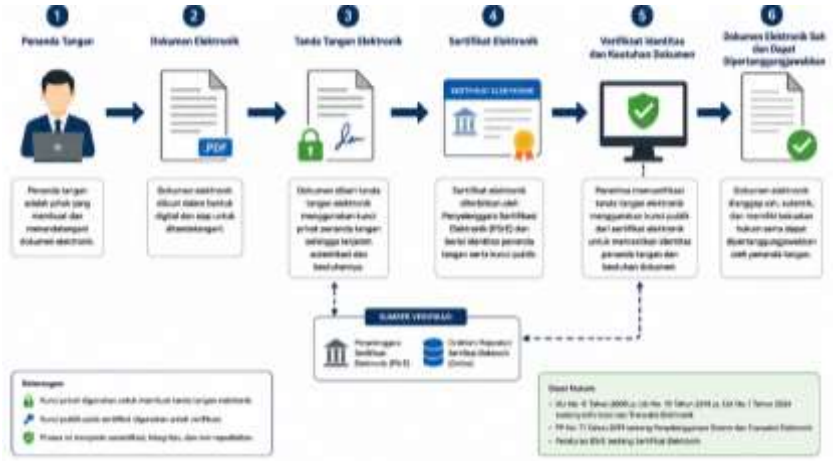
Perkembangan transaksi elektronik menuntut adanya mekanisme hukum dan teknologi yang mampu memastikan identitas para pihak, keutuhan dokumen, serta persetujuan yang diberikan dalam suatu hubungan hukum digital. Dalam transaksi konvensional, tanda tangan basah pada dokumen tertulis berfungsi sebagai tanda persetujuan, identitas, dan tanggung jawab pihak yang menandatangani. Namun, dalam transaksi elektronik, fungsi tersebut tidak dapat sepenuhnya bergantung pada tanda tangan fisik karena dokumen dibuat, dikirim, diterima, dan disimpan melalui sistem elektronik. Oleh karena itu, tanda tangan elektronik hadir sebagai instrumen penting untuk menjamin keabsahan dokumen elektronik dan memberikan kepastian hukum bagi para pihak yang melakukan transaksi secara digital (Republik Indonesia, 2008, *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*; Murray, 2019, *Information Technology Law: The Law and Society*).

5.4.1 Konsep dan Fungsi Tanda Tangan Elektronik

Tanda tangan elektronik pada dasarnya merupakan tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Pengertian ini menunjukkan bahwa tanda tangan elektronik tidak hanya dipahami sebagai gambar tanda tangan yang ditempelkan pada dokumen digital, tetapi juga mencakup mekanisme elektronik yang dapat menghubungkan identitas penanda tangan dengan dokumen yang ditandatangani. Dengan demikian, tanda tangan elektronik memiliki fungsi utama untuk menunjukkan identitas penanda tangan, membuktikan adanya persetujuan, serta menjaga keutuhan dokumen elektronik setelah ditandatangani (Republik Indonesia, 2008, 2019b).

Dalam praktiknya, tanda tangan elektronik dapat digunakan pada berbagai bentuk dokumen digital, seperti perjanjian elektronik, persetujuan layanan, dokumen administrasi pemerintahan, dokumen perbankan digital, kontrak bisnis, faktur elektronik, surat kuasa elektronik, dan dokumen layanan publik. Fungsi tanda tangan elektronik menjadi penting karena transaksi

digital sering dilakukan tanpa pertemuan langsung antara para pihak. Oleh karena itu, tanda tangan elektronik berperan sebagai instrumen autentikasi untuk memastikan bahwa pihak yang memberikan persetujuan benar-benar dapat dikaitkan dengan identitas tertentu dan dokumen tertentu (Edrisy, 2019; Rahmawati et al., 2024).



Gambar 5.2: Mekanisme Tanda Tangan Elektronik dan Sertifikat Elektronik

5.4.2 Syarat Keabsahan Tanda Tangan Elektronik

Tanda tangan elektronik dapat memiliki kekuatan hukum apabila memenuhi persyaratan yang ditentukan oleh peraturan perundang-undangan. Syarat tersebut pada prinsipnya berkaitan dengan kemampuan tanda tangan elektronik untuk mengidentifikasi penanda tangan, menunjukkan persetujuan penanda tangan terhadap informasi elektronik, serta menjamin bahwa perubahan terhadap tanda tangan atau dokumen setelah proses penandatanganan dapat diketahui. Dengan demikian, tanda tangan elektronik yang sah harus mampu menjaga hubungan antara penanda tangan, dokumen elektronik, dan tindakan persetujuan yang diberikan (Republik Indonesia, 2008, 2024b).

Keabsahan tanda tangan elektronik juga bergantung pada keandalan sistem elektronik yang digunakan. Sistem elektronik harus mampu menjaga kerahasiaan, keutuhan, dan ketersediaan data yang berkaitan dengan proses penandatanganan. Apabila suatu tanda tangan elektronik dibuat melalui sistem yang tidak aman, tidak memiliki mekanisme autentikasi, atau tidak

dapat menunjukkan rekam jejak perubahan dokumen, maka kekuatan pembuktiannya dapat dipersoalkan. Oleh karena itu, aspek teknis seperti enkripsi, autentikasi berlapis, pencatatan waktu, rekam jejak sistem, dan pengendalian akses menjadi bagian penting dalam menjamin keabsahan tanda tangan elektronik (Casey, 2011; Republik Indonesia, 2019b).

Tanda tangan elektronik juga perlu dibedakan dari tanda tangan hasil pindai atau gambar tanda tangan yang ditempelkan pada dokumen digital. Gambar tanda tangan yang ditempelkan pada dokumen elektronik belum tentu memenuhi syarat sebagai tanda tangan elektronik yang kuat secara hukum apabila tidak dilengkapi dengan mekanisme autentikasi dan verifikasi yang memadai. Sebaliknya, tanda tangan elektronik yang menggunakan teknologi kriptografi dan didukung oleh sertifikat elektronik memiliki tingkat keandalan yang lebih tinggi karena dapat menghubungkan identitas penanda tangan dengan dokumen secara lebih aman dan dapat diverifikasi (Casey, 2011; Murray, 2019).

5.4.3 Sertifikat Elektronik dan Penyelenggara Sertifikasi Elektronik

Sertifikat elektronik merupakan sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik. Sertifikat elektronik berfungsi sebagai instrumen untuk memastikan bahwa tanda tangan elektronik yang digunakan benar-benar terhubung dengan identitas subjek hukum tertentu. Dengan adanya sertifikat elektronik, proses verifikasi tanda tangan elektronik dapat dilakukan secara lebih andal karena identitas penanda tangan tidak hanya diklaim secara sepihak, tetapi diverifikasi melalui mekanisme sertifikasi elektronik (Republik Indonesia, 2008, 2019b).

Penyelenggara Sertifikasi Elektronik berperan sebagai pihak yang menerbitkan, mengelola, dan memverifikasi sertifikat elektronik. Peran ini penting karena kepercayaan terhadap tanda tangan elektronik sangat bergantung pada keandalan pihak yang menerbitkan sertifikat tersebut. Dalam ekosistem transaksi elektronik, Penyelenggara Sertifikasi Elektronik membantu memastikan bahwa identitas digital pihak yang menandatangani dokumen dapat diverifikasi, dokumen yang ditandatangani tidak berubah setelah proses penandatanganan, dan hubungan antara identitas penanda

tangan dengan tanda tangan elektronik dapat dipertanggungjawabkan (Brownsword & Goodwin, 2012; Republik Indonesia, 2019b).

Secara teknis, sertifikat elektronik biasanya berkaitan dengan penggunaan kriptografi kunci publik, yaitu mekanisme yang memungkinkan proses verifikasi identitas dan keutuhan dokumen dilakukan secara elektronik. Melalui mekanisme ini, tanda tangan elektronik tidak hanya berfungsi sebagai simbol persetujuan, tetapi juga sebagai alat untuk mendeteksi apakah dokumen telah berubah setelah ditandatangani. Hal ini menjadikan sertifikat elektronik sangat penting dalam transaksi yang membutuhkan tingkat kepercayaan tinggi, seperti kontrak bisnis, layanan keuangan digital, administrasi pemerintahan, dan dokumen hukum elektronik (Casey, 2011; Fairuzabadi et al., 2023).

5.4.4 Tanda Tangan Elektronik Tersertifikasi dan Tidak Tersertifikasi

Dalam praktik hukum Indonesia, tanda tangan elektronik dapat dibedakan menjadi tanda tangan elektronik tersertifikasi dan tanda tangan elektronik tidak tersertifikasi. Tanda tangan elektronik tersertifikasi adalah tanda tangan elektronik yang dibuat dengan menggunakan jasa Penyelenggara Sertifikasi Elektronik dan didukung oleh sertifikat elektronik. Jenis tanda tangan ini memiliki tingkat keandalan yang lebih kuat karena identitas penanda tangan diverifikasi oleh pihak penyelenggara sertifikasi. Sementara itu, tanda tangan elektronik tidak tersertifikasi tetap dapat digunakan, tetapi kekuatan pembuktiannya sangat bergantung pada kemampuan para pihak untuk membuktikan keaslian, keutuhan, dan hubungan tanda tangan tersebut dengan penanda tangan (Republik Indonesia, 2019b).

Perbedaan antara tanda tangan elektronik tersertifikasi dan tidak tersertifikasi penting dipahami agar para pihak dapat memilih bentuk tanda tangan yang sesuai dengan tingkat risiko transaksi. Untuk transaksi sederhana, tanda tangan elektronik tidak tersertifikasi mungkin masih dapat digunakan sepanjang para pihak menyepakati dan dapat membuktikan keabsahannya. Namun, untuk transaksi bernilai tinggi, dokumen hukum penting, layanan publik, kontrak bisnis, atau dokumen yang berpotensi menjadi objek sengketa, penggunaan tanda tangan elektronik tersertifikasi lebih dianjurkan

karena memiliki dukungan autentikasi dan verifikasi yang lebih kuat (Edrisy, 2019; Rahmawati et al., 2024)

Tabel berikut dapat digunakan untuk memperjelas perbedaan antara tanda tangan elektronik tersertifikasi dan tidak tersertifikasi.

Tabel 5.1: Perbandingan Tanda Tangan Elektronik Tersertifikasi dan Tidak Tersertifikasi

Aspek	Tanda Tangan Elektronik Tersertifikasi	Tanda Tangan Elektronik Tidak Tersertifikasi
Dasar penggunaan	Menggunakan sertifikat elektronik dari Penyelenggara Sertifikasi Elektronik	Tidak selalu menggunakan sertifikat elektronik
Verifikasi identitas	Identitas penanda tangan diverifikasi oleh penyelenggara sertifikasi	Verifikasi identitas bergantung pada mekanisme yang digunakan para pihak
Tingkat keandalan	Lebih tinggi karena didukung sistem sertifikasi elektronik	Lebih bergantung pada bukti pendukung dan kesepakatan para pihak
Kekuatan pembuktian	Lebih kuat apabila memenuhi persyaratan hukum dan teknis	Tetap dapat digunakan, tetapi lebih mudah dipersoalkan apabila terjadi sengketa
Contoh penggunaan	Kontrak bisnis penting, dokumen pemerintahan, layanan keuangan, dokumen hukum elektronik	Persetujuan internal, formulir digital sederhana, komunikasi bisnis tertentu
Risiko hukum	Relatif lebih rendah karena identitas dan keutuhan dokumen lebih mudah diverifikasi	Relatif lebih tinggi jika tidak didukung rekam jejak dan autentikasi yang memadai

5.4.5 Peran Tanda Tangan Elektronik dalam Kepastian Hukum Digital

Tanda tangan elektronik dan sertifikat elektronik memiliki peran strategis dalam menciptakan kepastian hukum di ruang digital. Keduanya memungkinkan dokumen elektronik digunakan secara lebih aman, autentik, dan dapat dipertanggungjawabkan. Tanpa mekanisme tanda tangan elektronik yang andal, para pihak akan kesulitan membuktikan siapa yang memberikan persetujuan, kapan persetujuan diberikan, dan apakah dokumen mengalami perubahan setelah ditandatangani. Oleh karena itu, tanda tangan elektronik menjadi instrumen penting dalam membangun kepercayaan

digital (*digital trust*) dalam transaksi elektronik (Brownsword & Goodwin, 2012; Murray, 2019).

Dalam penyelenggaraan pemerintahan elektronik, tanda tangan elektronik juga mendukung efisiensi administrasi dan pelayanan publik. Dokumen yang sebelumnya memerlukan tanda tangan fisik dapat diproses secara elektronik sehingga pelayanan menjadi lebih cepat dan terdokumentasi dengan baik. Namun, efisiensi tersebut harus tetap diimbangi dengan keamanan sistem, perlindungan data pribadi, dan kepatuhan terhadap ketentuan hukum. Jika tanda tangan elektronik digunakan tanpa prosedur pengamanan yang memadai, maka risiko penyalahgunaan identitas, pemalsuan dokumen, dan manipulasi persetujuan tetap dapat terjadi (Republik Indonesia, 2019b, 2022a).

Tanda tangan elektronik dan sertifikat elektronik merupakan instrumen hukum dan teknologi yang saling berkaitan dalam menjamin keabsahan dokumen elektronik. Tanda tangan elektronik berfungsi sebagai alat autentikasi dan verifikasi, sedangkan sertifikat elektronik berfungsi memperkuat kepercayaan terhadap identitas penanda tangan dan keutuhan dokumen. Penggunaan keduanya menjadi semakin penting dalam ekosistem digital karena transaksi, administrasi, dan layanan publik semakin bergantung pada dokumen elektronik. Oleh karena itu, pemanfaatan tanda tangan elektronik harus dilakukan secara hati-hati, sesuai dengan ketentuan hukum, dan didukung oleh sistem elektronik yang andal agar mampu memberikan kepastian hukum bagi para pihak.

5.5 Penyimpanan, Pengelolaan, dan Keamanan Dokumen Elektronik

Penyimpanan, pengelolaan, dan keamanan dokumen elektronik merupakan aspek penting dalam penyelenggaraan sistem hukum digital. Dokumen elektronik tidak hanya berfungsi sebagai arsip administratif, tetapi juga dapat menjadi dasar hubungan hukum, bukti transaksi, alat pembuktian, dan sumber pertanggungjawaban hukum. Oleh karena itu, dokumen elektronik harus disimpan dan dikelola dengan cara yang menjamin keutuhan, keteraksesan, keaslian, dan keamanan informasinya. Apabila dokumen elektronik tidak dikelola secara baik, maka dokumen tersebut dapat

kehilangan nilai pembuktiannya, menimbulkan sengketa, atau bahkan menyebabkan kerugian bagi para pihak yang berkepentingan (Casey, 2011).

5.5.1 Penyimpanan Dokumen Elektronik

Penyimpanan dokumen elektronik berbeda dengan penyimpanan dokumen fisik. Dokumen fisik biasanya disimpan dalam bentuk kertas dan arsip, sedangkan dokumen elektronik disimpan dalam media digital seperti server, pusat data, perangkat penyimpanan lokal, layanan komputasi awan, atau sistem manajemen dokumen elektronik. Perbedaan media penyimpanan ini membawa konsekuensi hukum dan teknis karena dokumen elektronik harus tetap dapat diakses, ditampilkan, dan diverifikasi kembali apabila dibutuhkan. Oleh karena itu, sistem penyimpanan dokumen elektronik harus dirancang agar mampu menjaga ketersediaan dan keutuhan dokumen dalam jangka waktu tertentu sesuai kebutuhan hukum, administrasi, dan bisnis.

Dalam praktiknya, penyimpanan dokumen elektronik harus memperhatikan prinsip keteraksesan (*accessibility*) dan keterbacaan (*readability*). Dokumen elektronik yang disimpan harus dapat dibuka dan ditampilkan kembali dalam format yang dapat dipahami. Masalah dapat muncul apabila dokumen tersimpan dalam format yang sudah tidak didukung oleh perangkat lunak tertentu, rusak karena kegagalan sistem, atau tidak memiliki mekanisme pencadangan. Oleh karena itu, organisasi perlu memastikan bahwa dokumen elektronik disimpan dalam format yang sesuai, memiliki cadangan, dan dapat dimigrasikan apabila terjadi perubahan teknologi penyimpanan (NIST, 2024b).

Selain itu, penyimpanan dokumen elektronik juga harus memperhatikan masa retensi atau jangka waktu penyimpanan. Tidak semua dokumen elektronik perlu disimpan selamanya. Beberapa dokumen harus disimpan dalam jangka waktu tertentu karena memiliki nilai hukum, nilai administrasi, nilai ekonomi, atau nilai pembuktian. Sebaliknya, dokumen yang tidak lagi diperlukan sebaiknya dimusnahkan secara aman agar tidak menimbulkan risiko kebocoran data atau penyalahgunaan informasi. Dalam konteks pelindungan data pribadi, penyimpanan data dan dokumen elektronik harus dilakukan secara terbatas sesuai tujuan pemrosesan dan tidak boleh melebihi kebutuhan yang sah (Republik Indonesia, 2022a).

5.5.2 Pengelolaan Dokumen Elektronik

Pengelolaan dokumen elektronik mencakup seluruh proses sejak dokumen dibuat, diterima, dikirim, digunakan, disimpan, diarsipkan, hingga dimusnahkan. Proses ini sering disebut sebagai siklus hidup dokumen elektronik. Setiap tahap dalam siklus hidup tersebut harus dikelola secara tertib agar dokumen tetap memiliki nilai hukum dan dapat dipertanggungjawabkan. Dokumen elektronik yang tidak memiliki mekanisme pengelolaan yang jelas akan lebih mudah hilang, berubah, digandakan tanpa izin, atau digunakan di luar tujuan semula (Brownsword & Goodwin, 2012; Murray, 2019).

Dalam pengelolaan dokumen elektronik, organisasi perlu menerapkan klasifikasi dokumen. Klasifikasi ini bertujuan membedakan dokumen berdasarkan tingkat kerahasiaan, nilai hukum, fungsi administrasi, dan tingkat risikonya. Misalnya, dokumen kontrak, dokumen keuangan, data pribadi, dokumen layanan publik, dan rekam transaksi perlu dikelola dengan standar keamanan yang lebih tinggi dibandingkan dokumen umum. Klasifikasi tersebut membantu organisasi menentukan siapa yang berhak mengakses dokumen, bagaimana dokumen disimpan, berapa lama dokumen dipertahankan, dan bagaimana dokumen dimusnahkan secara aman (NIST, 2024b; Republik Indonesia, 2022a)

Pengelolaan dokumen elektronik juga memerlukan pencatatan aktivitas atau rekam jejak sistem (*audit trail*). Rekam jejak tersebut berfungsi untuk mencatat siapa yang membuat, mengakses, mengubah, mengirim, menghapus, atau memindahkan dokumen elektronik. Keberadaan *audit trail* sangat penting karena dapat membantu proses pengawasan internal, pemeriksaan keamanan, dan pembuktian apabila terjadi sengketa. Tanpa rekam jejak yang memadai, sulit untuk menentukan apakah dokumen telah diubah, siapa yang melakukan perubahan, dan kapan perubahan tersebut terjadi.

5.5.3 Keamanan Dokumen Elektronik

Keamanan dokumen elektronik bertujuan melindungi dokumen dari akses tanpa hak, perubahan tanpa izin, kehilangan, kerusakan, kebocoran, dan penyalahgunaan. Dalam tata kelola keamanan informasi, perlindungan dokumen elektronik umumnya didasarkan pada prinsip kerahasiaan

(*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Kerahasiaan berarti dokumen hanya dapat diakses oleh pihak yang berwenang. Keutuhan berarti isi dokumen tidak berubah tanpa izin. Ketersediaan berarti dokumen dapat diakses ketika diperlukan oleh pihak yang berwenang (Fairuzabadi et al., 2023).

Untuk menjaga kerahasiaan dokumen elektronik, organisasi perlu menerapkan pembatasan akses berdasarkan tugas dan kewenangan. Tidak semua pengguna sistem elektronik boleh memiliki akses yang sama terhadap seluruh dokumen. Dokumen yang memuat data pribadi, rahasia perusahaan, informasi keuangan, atau dokumen hukum penting harus dibatasi aksesnya. Pengendalian akses dapat dilakukan melalui penggunaan kata sandi yang kuat, autentikasi berlapis, manajemen hak akses, enkripsi, dan pemantauan aktivitas pengguna. Pengendalian akses yang lemah dapat membuka peluang terjadinya pencurian data, pemalsuan dokumen, dan penyebaran informasi tanpa izin (CISA, 2022).

Keutuhan dokumen elektronik dapat dijaga melalui penggunaan mekanisme teknis seperti *hashing*, tanda tangan elektronik, sertifikat elektronik, pencatatan waktu, serta sistem penyimpanan yang memiliki kontrol perubahan. Mekanisme tersebut membantu memastikan bahwa setiap perubahan terhadap dokumen dapat diketahui dan ditelusuri. Dalam konteks hukum, keutuhan dokumen sangat penting karena dokumen elektronik yang telah berubah tanpa penjelasan yang dapat dipertanggungjawabkan dapat dipersoalkan nilai pembuktiannya. Oleh karena itu, keamanan dokumen elektronik tidak hanya penting dari sisi teknologi, tetapi juga dari sisi hukum pembuktian.

Sementara itu, ketersediaan dokumen elektronik perlu dijaga melalui sistem pencadangan, pemulihan bencana, dan rencana keberlanjutan layanan. Gangguan sistem, serangan *ransomware*, kerusakan perangkat, atau kesalahan manusia dapat menyebabkan dokumen elektronik tidak dapat diakses. Oleh sebab itu, organisasi harus memiliki mekanisme *backup* yang teratur, pengujian pemulihan data, dan prosedur penanganan insiden. Dalam konteks penyelenggaraan sistem elektronik, ketersediaan dokumen menjadi bagian dari kewajiban untuk menjaga keandalan dan keberlangsungan sistem elektronik (BSSN, 2024; CISA, 2025).

5.5.4 Tanggung Jawab Penyelenggara Sistem Elektronik

Penyelenggara Sistem Elektronik memiliki tanggung jawab penting dalam penyimpanan, pengelolaan, dan keamanan dokumen elektronik. Tanggung jawab tersebut mencakup kewajiban untuk menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab. Penyelenggara juga wajib memastikan bahwa sistem yang digunakan mampu melindungi informasi elektronik dan dokumen elektronik dari gangguan, penyalahgunaan, dan akses tanpa hak. Dengan demikian, tanggung jawab Penyelenggara Sistem Elektronik tidak hanya berkaitan dengan penyediaan layanan teknis, tetapi juga mencakup tanggung jawab hukum terhadap dokumen dan data yang dikelolanya (Mantili & Dewi, 2020).

Tanggung jawab tersebut semakin penting apabila dokumen elektronik memuat data pribadi. Dalam hal ini, pengendali data wajib memastikan bahwa pemrosesan data pribadi dilakukan secara sah, terbatas, transparan, dan aman. Dokumen elektronik yang memuat data pribadi tidak boleh disimpan atau digunakan di luar tujuan yang sah. Selain itu, apabila terjadi kebocoran atau kegagalan pelindungan data pribadi, penyelenggara dapat dimintai pertanggungjawaban sesuai ketentuan peraturan perundang-undangan. Hal ini menunjukkan bahwa pengelolaan dokumen elektronik tidak dapat dipisahkan dari prinsip pelindungan data pribadi (Maharani & Prakoso, 2024).

Dalam praktik organisasi, tanggung jawab pengelolaan dokumen elektronik perlu diwujudkan melalui kebijakan internal yang jelas. Kebijakan tersebut dapat mencakup prosedur pembuatan dokumen, klasifikasi dokumen, pengendalian akses, pencadangan, retensi dokumen, pemusnahan dokumen, penanganan insiden, serta audit keamanan informasi. Kebijakan ini penting agar setiap pengguna sistem memahami hak dan kewajibannya dalam mengelola dokumen elektronik. Tanpa kebijakan yang jelas, keamanan dokumen elektronik sering bergantung pada kebiasaan masing-masing pengguna sehingga lebih rentan terhadap kesalahan manusia dan pelanggaran keamanan (BSSN, 2024; NIST, 2024a).

Tabel berikut dapat digunakan untuk memperjelas hubungan antara aspek pengelolaan dokumen elektronik dan tujuan hukumnya.

Tabel 5.2: Aspek Pengelolaan dan Keamanan Dokumen Elektronik

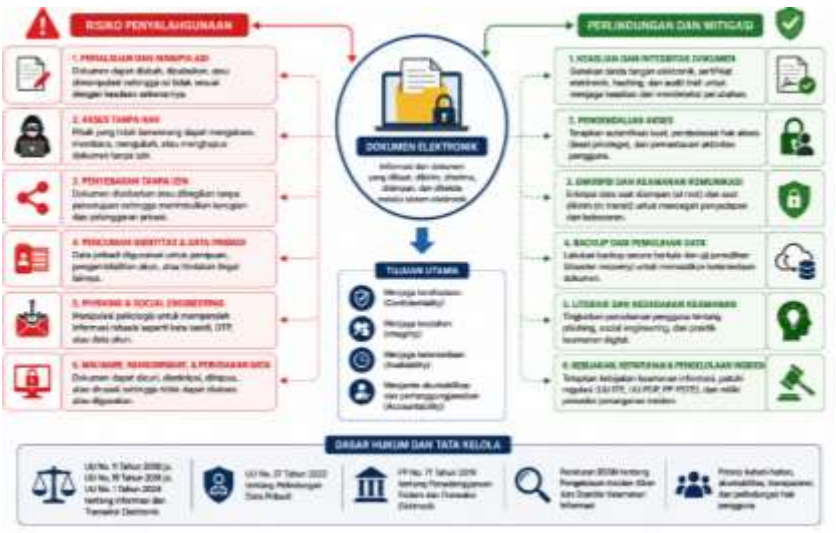
Aspek	Tujuan	Contoh Penerapan	Risiko Jika Diabaikan
Penyimpanan	Menjamin dokumen tetap tersedia dan dapat digunakan kembali	Server, pusat data, *cloud storage*, arsip digital	Dokumen hilang, rusak, atau tidak dapat diakses
Klasifikasi dokumen	Menentukan tingkat kerahasiaan dan perlakuan terhadap dokumen	Dokumen publik, internal, rahasia, data pribadi	Akses tidak sesuai kewenangan
Pengendalian akses	Membatasi akses hanya kepada pihak yang berwenang	Kata sandi, autentikasi berlapis, hak akses berbasis peran	Kebocoran data dan penyalahgunaan dokumen
Rekam jejak sistem	Menelusuri aktivitas terhadap dokumen	*Audit trail*, log akses, pencatatan perubahan	Sulit membuktikan siapa yang mengubah atau mengakses dokumen
Pencadangan	Menjamin pemulihan apabila terjadi gangguan	*Backup* berkala dan uji pemulihan data	Kehilangan dokumen akibat serangan atau kerusakan sistem
Keamanan dokumen	Menjaga kerahasiaan, keutuhan, dan ketersediaan	Enkripsi, tanda tangan elektronik, pemantauan sistem	Manipulasi, pemalsuan, atau perubahan tanpa izin
Pemusnahan aman	Menghapus dokumen yang tidak lagi diperlukan secara terkendali	Penghapusan permanen dan pencatatan pemusnahan	Data lama disalahgunakan atau bocor

Dengan demikian, penyimpanan, pengelolaan, dan keamanan dokumen elektronik merupakan bagian penting dari tata kelola hukum digital. Dokumen elektronik hanya dapat berfungsi secara optimal apabila disimpan dalam sistem yang andal, dikelola berdasarkan prosedur yang jelas, dan dilindungi dengan mekanisme keamanan yang memadai. Keamanan dokumen elektronik tidak hanya berkaitan dengan perlindungan teknis, tetapi juga berhubungan langsung dengan kepastian hukum, pelindungan data pribadi, pembuktian, dan tanggung jawab penyelenggara sistem elektronik. Oleh karena itu, setiap pihak yang mengelola dokumen

elektronik perlu menerapkan prinsip kehati-hatian, akuntabilitas, dan keamanan informasi agar dokumen elektronik tetap memiliki nilai hukum dan dapat dipertanggungjawabkan.

5.6 Risiko Penyalahgunaan Informasi dan Dokumen Elektronik

Informasi elektronik dan dokumen elektronik memiliki peran penting dalam kehidupan digital karena digunakan dalam transaksi, administrasi, komunikasi, layanan publik, kegiatan bisnis, dan pembuktian hukum. Namun, kemudahan dalam membuat, menggandakan, mengirim, menyimpan, dan mengubah dokumen elektronik juga menimbulkan berbagai risiko penyalahgunaan. Berbeda dengan dokumen fisik yang biasanya meninggalkan jejak perubahan secara kasatmata, dokumen elektronik dapat dimanipulasi secara cepat, disebarluaskan secara luas, atau dihapus tanpa mudah diketahui apabila tidak dikelola melalui sistem yang aman. Oleh karena itu, penggunaan informasi dan dokumen elektronik harus disertai dengan mekanisme hukum dan teknologi yang mampu mencegah penyalahgunaan serta menjamin pertanggungjawaban para pihak (Casey, 2011).



Gambar 5.3: Risiko dan Perlindungan Dokumen Elektronik

5.6.1 Pemalsuan dan Manipulasi Dokumen Elektronik

Salah satu risiko utama dalam penggunaan dokumen elektronik adalah pemalsuan dan manipulasi dokumen. Dokumen elektronik dapat diubah pada bagian tertentu, seperti isi perjanjian, tanggal transaksi, identitas pihak, nilai pembayaran, tanda tangan, atau lampiran dokumen. Manipulasi tersebut dapat dilakukan dengan menggunakan perangkat lunak pengolah dokumen, pengubahan metadata, pengeditan gambar, atau penyisipan informasi palsu pada file elektronik. Apabila tidak terdapat mekanisme pengamanan seperti tanda tangan elektronik, rekam jejak sistem, atau pembatasan akses, maka perubahan terhadap dokumen elektronik dapat sulit dibedakan dari dokumen asli (Fairuzabadi et al., 2023).

Pemalsuan dokumen elektronik dapat menimbulkan akibat hukum yang serius. Dalam transaksi elektronik, dokumen yang telah dimanipulasi dapat digunakan untuk menipu pihak lain, mengklaim hak yang tidak sah, menghindari kewajiban, atau menciptakan bukti palsu. Risiko ini menjadi semakin besar apabila para pihak hanya mengandalkan salinan dokumen tanpa memeriksa keaslian, sumber, dan rekam jejak dokumen tersebut. Oleh karena itu, setiap dokumen elektronik yang memiliki nilai hukum perlu dilengkapi dengan mekanisme verifikasi, seperti tanda tangan elektronik, sertifikat elektronik, pencatatan waktu, dan sistem penyimpanan yang mampu menjaga keutuhan dokumen (Republik Indonesia, 2019b).

5.6.2 Akses Tanpa Hak dan Penyebaran Dokumen Tanpa Izin

Risiko berikutnya adalah akses tanpa hak terhadap informasi dan dokumen elektronik. Akses tanpa hak terjadi ketika seseorang masuk, mengambil, melihat, mengunduh, mengubah, atau menyebarkan dokumen elektronik tanpa kewenangan. Bentuk penyalahgunaan ini dapat terjadi karena lemahnya pengamanan akun, penggunaan kata sandi yang mudah ditebak, tidak adanya autentikasi berlapis, kelalaian pengguna, atau adanya celah keamanan pada sistem elektronik. Dalam konteks hukum siber, akses tanpa hak merupakan salah satu bentuk pelanggaran yang dapat menimbulkan tanggung jawab pidana maupun perdata apabila mengakibatkan kerugian bagi pihak lain (Republik Indonesia, 2008, 2024b)

Penyebaran dokumen elektronik tanpa izin juga menjadi persoalan yang sering terjadi dalam ruang digital. Dokumen yang berisi data pribadi, rahasia

bisnis, informasi keuangan, rekam medis, dokumen akademik, atau dokumen hukum dapat disebarluaskan melalui media sosial, aplikasi percakapan, surat elektronik, atau platform penyimpanan daring tanpa persetujuan pemiliknya. Penyebaran semacam ini dapat menimbulkan kerugian reputasi, kerugian ekonomi, pelanggaran privasi, bahkan penyalahgunaan identitas. Jika dokumen tersebut memuat data pribadi, maka penyebarannya harus memperhatikan prinsip pelindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Republik Indonesia, 2022b; Solove & Schwartz, 2020)

5.6.3 Pencurian Identitas dan Penyalahgunaan Data Pribadi

Informasi elektronik sering kali memuat data pribadi yang dapat digunakan untuk mengidentifikasi seseorang, seperti nama, nomor identitas, alamat, nomor telepon, alamat surat elektronik, data keuangan, data biometrik, riwayat transaksi, atau akun digital. Apabila informasi tersebut jatuh ke tangan pihak yang tidak berwenang, data pribadi dapat digunakan untuk pencurian identitas, pembuatan akun palsu, penipuan transaksi, pengajuan pinjaman tanpa izin, pengambilalihan akun, atau tindakan lain yang merugikan pemilik data. Risiko ini menunjukkan bahwa dokumen elektronik yang memuat data pribadi harus dikelola dengan standar keamanan yang lebih tinggi (Solove & Schwartz, 2020).

Penyalahgunaan data pribadi juga dapat terjadi karena kelalaian penyelenggara sistem elektronik dalam mengamankan data yang dikelolanya. Kebocoran data dapat disebabkan oleh serangan siber, konfigurasi sistem yang lemah, akses internal yang tidak terkendali, atau tidak adanya kebijakan pengelolaan data yang memadai. Dalam konteks ini, pelindungan data pribadi bukan hanya tanggung jawab teknis, melainkan juga tanggung jawab hukum. Penyelenggara sistem elektronik yang bertindak sebagai pengendali atau prosesor data wajib memastikan bahwa pemrosesan data dilakukan secara sah, terbatas, transparan, aman, dan sesuai dengan tujuan yang telah ditentukan (Amelia, 2025; Maharani & Prakoso, 2024).

5.6.4 Penipuan Digital, Phishing, dan Social Engineering

Penyalahgunaan informasi elektronik juga sering dilakukan melalui penipuan digital. Salah satu bentuk yang banyak terjadi adalah *phishing*, yaitu upaya memperoleh informasi rahasia seperti kata sandi, kode OTP, nomor kartu, atau data akun melalui penyamaran sebagai pihak terpercaya. Pelaku biasanya menggunakan pesan elektronik, tautan palsu, situs tiruan, atau komunikasi yang seolah-olah berasal dari lembaga resmi. Jika korban memberikan informasi tersebut, pelaku dapat mengakses akun, mengambil data, atau melakukan transaksi tanpa izin (Gharibi, 2012).

Selain *phishing*, penyalahgunaan informasi juga dapat dilakukan melalui *social engineering*, yaitu teknik manipulasi psikologis untuk membuat korban menyerahkan informasi atau melakukan tindakan tertentu. Pelaku tidak selalu menyerang sistem secara teknis, tetapi memanfaatkan kelengahan, rasa takut, kepercayaan, atau ketidaktahuan korban. Misalnya, pelaku berpura-pura sebagai petugas bank, admin platform, aparat, atau pihak layanan pelanggan untuk meminta kode rahasia. Risiko ini menunjukkan bahwa keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan kehati-hatian pengguna (Kementerian Kominfo RI, 2020; Nurse, 2018).

5.6.5 Malware, Ransomware, dan Perusakan Dokumen Elektronik

Dokumen elektronik juga rentan terhadap serangan perangkat lunak berbahaya seperti *malware* dan *ransomware*. *Malware* dapat merusak, mencuri, atau memodifikasi dokumen elektronik tanpa izin. Sementara itu, *ransomware* dapat mengenkripsi dokumen sehingga tidak dapat diakses oleh pemiliknya, kemudian pelaku meminta tebusan agar dokumen dapat dibuka kembali. Serangan semacam ini dapat mengganggu layanan organisasi, menghilangkan arsip penting, merusak kepercayaan pengguna, dan menimbulkan kerugian ekonomi yang besar (CISA, 2025, 2026).

Risiko *malware* dan *ransomware* semakin berbahaya apabila organisasi tidak memiliki pencadangan data, sistem pemulihan, pembaruan keamanan, dan prosedur penanganan insiden. Dokumen elektronik yang hanya disimpan pada satu sistem tanpa *backup* akan sangat rentan hilang atau tidak dapat digunakan ketika terjadi serangan. Oleh karena itu, organisasi perlu

menerapkan sistem pencadangan berkala, enkripsi, autentikasi berlapis, pembaruan perangkat lunak, pelatihan keamanan bagi pengguna, serta prosedur pelaporan insiden siber (BSSN, 2024; NIST, 2024a).

5.6.6 Risiko Pembuktian dan Pertanggungjawaban Hukum

Penyalahgunaan informasi dan dokumen elektronik juga menimbulkan risiko dalam proses pembuktian. Dokumen elektronik yang telah diubah, dipalsukan, dihapus, atau disebarkan tanpa izin dapat menyulitkan penegak hukum maupun para pihak dalam menentukan kebenaran suatu peristiwa hukum. Dalam perkara yang melibatkan bukti elektronik, isu penting yang harus diperiksa meliputi keaslian, keutuhan, sumber, waktu pembuatan, pihak yang mengakses, serta cara memperoleh dokumen tersebut. Apabila aspek-aspek tersebut tidak dapat dibuktikan secara memadai, nilai pembuktian dokumen elektronik dapat menjadi lemah (Aini & Lubis, 2024).

Pertanggungjawaban hukum atas penyalahgunaan dokumen elektronik dapat melibatkan berbagai pihak, tergantung pada bentuk pelanggaran dan akibat yang ditimbulkan. Pelaku yang secara sengaja mengakses, mengubah, menyebarkan, atau menggunakan dokumen elektronik tanpa hak dapat dimintai pertanggungjawaban sesuai ketentuan hukum yang berlaku. Penyelenggara sistem elektronik juga dapat dimintai pertanggungjawaban apabila terbukti lalai dalam menjaga keamanan sistem, tidak menerapkan pengamanan yang layak, atau tidak memenuhi kewajiban pelindungan data pribadi. Dengan demikian, risiko penyalahgunaan informasi dan dokumen elektronik tidak hanya berkaitan dengan pelaku langsung, tetapi juga berkaitan dengan tata kelola sistem elektronik secara keseluruhan (Mantili & Dewi, 2020; Republik Indonesia, 2019b).

Tabel 5.3: Risiko Penyalahgunaan Informasi dan Dokumen Elektronik

Bentuk Risiko	**Contoh Bentuk Penyalahgunaan**	**Dampak Hukum/Praktis**	**Upaya Pencegahan**
Pemalsuan dokumen elektronik	Mengubah isi kontrak, tanggal, identitas, atau nilai transaksi	Sengketa, kerugian ekonomi, bukti dipersoalkan	Tanda tangan elektronik, sertifikat elektronik, *audit trail*

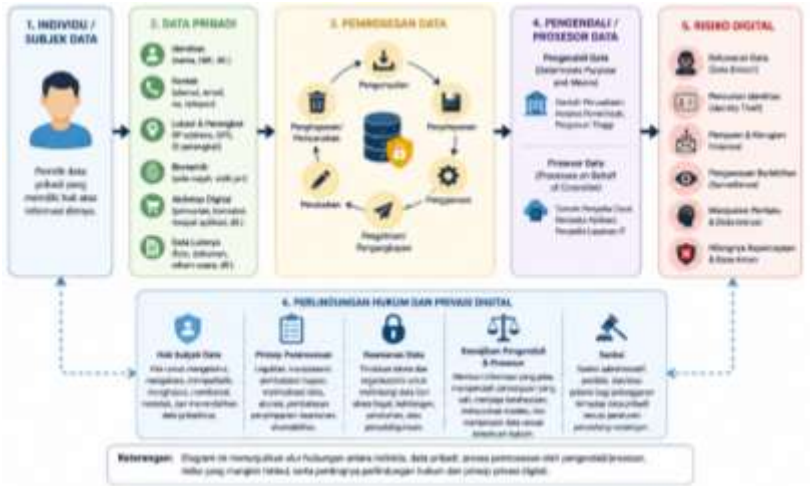
Bentuk Risiko	Contoh Bentuk Penyalahgunaan	Dampak Hukum/Praktis	Upaya Pencegahan
Akses tanpa hak	Mengakses dokumen, akun, atau sistem tanpa izin	Pelanggaran hukum, kebocoran data, kerugian pihak lain	Autentikasi berlapis, pembatasan akses, pemantauan sistem
Penyebaran dokumen tanpa izin	Membagikan dokumen pribadi, rahasia bisnis, atau data pelanggan	Pelanggaran privasi, kerugian reputasi, tuntutan hukum	Kebijakan kerahasiaan, klasifikasi dokumen, edukasi pengguna
Pencurian identitas	Menggunakan data pribadi untuk membuat akun atau transaksi palsu	Kerugian finansial dan penyalahgunaan identitas	Pelindungan data pribadi, verifikasi identitas, edukasi keamanan
Phishing dan *social engineering*	Meminta OTP, kata sandi, atau data akun melalui penyamaran	Pengambilalihan akun dan transaksi ilegal	Literasi keamanan, verifikasi sumber pesan, MFA
Malware dan *ransomware*	Merusak, mencuri, atau mengenkripsi dokumen elektronik	Hilangnya data dan gangguan layanan	*Backup*, pembaruan sistem, antivirus, penanganan insiden
Penghapusan jejak digital	Menghapus log, metadata, atau bukti elektronik	Sulitnya pembuktian dan penegakan hukum	Rekam jejak sistem, penyimpanan log, audit keamanan

Risiko penyalahgunaan informasi dan dokumen elektronik merupakan konsekuensi dari semakin luasnya penggunaan teknologi digital dalam kehidupan hukum, bisnis, dan administrasi. Risiko tersebut dapat berupa pemalsuan dokumen, akses tanpa hak, penyebaran dokumen tanpa izin, pencurian identitas, penipuan digital, serangan *malware*, hingga kesulitan pembuktian. Oleh karena itu, perlindungan terhadap informasi dan dokumen elektronik harus dilakukan melalui kombinasi antara regulasi yang jelas, sistem elektronik yang andal, keamanan teknis yang memadai, pengawasan internal, dan literasi digital pengguna. Semakin tinggi nilai hukum dan ekonomi suatu dokumen elektronik, semakin tinggi pula standar pengamanan dan pertanggungjawaban yang harus diterapkan.

Bab 6
Pelindungan data pribadi dan Privasi Digital

6.1 Konsep Data Pribadi dan Privasi Digital

Perkembangan teknologi informasi telah mengubah cara manusia berinteraksi, bertransaksi, belajar, bekerja, dan mengakses layanan publik. Hampir setiap aktivitas digital meninggalkan jejak data, baik berupa nama, alamat, nomor telepon, alamat surel, nomor identitas, lokasi, rekam transaksi, riwayat pencarian, hingga pola perilaku pengguna di internet. Data tersebut tidak lagi hanya berfungsi sebagai informasi administratif, tetapi juga menjadi aset penting bagi organisasi, perusahaan, penyelenggara sistem elektronik, dan pemerintah. Oleh karena itu, pemahaman tentang data pribadi dan privasi digital menjadi bagian penting dalam hukum teknologi informasi.



Gambar 6.1: Konsep Data Pribadi dan Privasi Digital

Secara hukum, data pribadi dapat dipahami sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik atau nonelektronik. Pengertian ini menunjukkan bahwa data pribadi tidak terbatas pada informasi yang secara jelas menyebut identitas seseorang, seperti nama

atau nomor induk kependudukan, tetapi juga mencakup data yang jika digabungkan dengan data lain dapat mengarah pada identitas seseorang (Republik Indonesia, 2022b). Dengan demikian, alamat IP, lokasi perangkat, rekam aktivitas digital, atau pola transaksi dapat menjadi data pribadi apabila dapat digunakan untuk mengenali seseorang.

Privasi digital memiliki cakupan yang lebih luas daripada data pribadi. Data pribadi berkaitan dengan informasi yang melekat pada individu, sedangkan privasi digital berkaitan dengan hak, kontrol, dan batasan atas penggunaan informasi tersebut dalam ruang digital. Privasi digital mencakup hak seseorang untuk mengetahui data apa yang dikumpulkan, untuk tujuan apa data digunakan, siapa yang dapat mengakses data tersebut, berapa lama data disimpan, serta bagaimana data dilindungi dari penyalahgunaan. Dalam konteks ini, privasi bukan hanya persoalan "rahasia", tetapi juga persoalan kendali individu atas informasi tentang dirinya (Solove, 2021).

Dalam praktiknya, data pribadi sering diproses melalui berbagai kegiatan, seperti pengumpulan, perekaman, penyimpanan, pengubahan, penggunaan, pengungkapan, pengiriman, penghapusan, dan pemusnahan data. Proses ini dapat terjadi ketika seseorang membuat akun media sosial, mendaftar aplikasi e-commerce, menggunakan layanan transportasi daring, mengakses layanan perbankan digital, atau mengisi formulir akademik secara online. Setiap proses tersebut harus dilakukan berdasarkan prinsip kehati-hatian, transparansi, keamanan, dan tujuan yang sah agar tidak merugikan pemilik data.

Pelindungan data pribadi menjadi penting karena penyalahgunaan data dapat menimbulkan berbagai risiko. Risiko tersebut dapat berbentuk kerugian ekonomi, seperti penipuan, pengambilalihan akun, pinjaman online ilegal, atau transaksi tanpa izin. Selain itu, penyalahgunaan data juga dapat menimbulkan kerugian non-ekonomi, seperti pencemaran nama baik, diskriminasi, pengawasan berlebihan, manipulasi perilaku, dan hilangnya rasa aman dalam menggunakan layanan digital. Dalam era ekonomi digital, data bahkan sering disebut sebagai sumber daya strategis karena dapat dipakai untuk membaca kebiasaan, preferensi, dan kecenderungan seseorang.

Secara konseptual, terdapat beberapa unsur penting dalam pelindungan data pribadi dan privasi digital.

1. **Subjek data pribadi**, yaitu individu yang memiliki data pribadi. Subjek data memiliki kepentingan langsung terhadap bagaimana datanya dikumpulkan, digunakan, disimpan, dan dibagikan.
2. **Pengendali data pribadi**, yaitu pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan data pribadi. Pengendali data dapat berupa lembaga pemerintah, perusahaan, perguruan tinggi, rumah sakit, platform digital, atau organisasi lain.
3. **Prosesor data pribadi**, yaitu pihak yang memproses data pribadi atas nama pengendali data. Misalnya, penyedia layanan cloud, penyedia aplikasi, atau penyedia jasa pengolahan data.
4. **Pemrosesan data pribadi**, yaitu seluruh kegiatan terhadap data pribadi, mulai dari memperoleh data sampai menghapus atau memusnahkannya.
5. **Persetujuan dan dasar pemrosesan**, yaitu dasar hukum atau alasan sah yang memungkinkan data pribadi diproses. Persetujuan harus diberikan secara sadar, jelas, dan tidak menyesatkan.
6. **Keamanan data**, yaitu tindakan teknis dan organisatoris untuk mencegah kebocoran, kehilangan, perubahan, akses ilegal, atau penyalahgunaan data.

Tabel berikut dapat digunakan untuk membedakan data pribadi dan privasi digital.

Tabel 6.1: Perbandingan Antara Data Pribadi Dan Privasi Digital

Aspek	Data Pribadi	Privasi Digital
Fokus utama	Informasi tentang individu	Kendali individu atas informasi dan aktivitas digitalnya
Bentuk	Nama, NIK, alamat, nomor telepon, biometrik, lokasi, akun digital	Hak untuk mengetahui, membatasi, menyetujui, menolak, dan mengontrol penggunaan data
Objek perlindungan	Data yang dapat mengidentifikasi seseorang	Ruang pribadi, pilihan, perilaku, komunikasi, dan keamanan individu di dunia digital
Risiko utama	Kebocoran data, pencurian identitas, penyalahgunaan akun	Pengawasan berlebihan, manipulasi perilaku, hilangnya kontrol, pelanggaran martabat pribadi
Contoh kasus	Data pelanggan bocor dari sistem aplikasi	Aplikasi mengakses lokasi dan kontak tanpa penjelasan yang jelas

Pelindungan data pribadi juga berkaitan dengan prinsip-prinsip umum yang dikenal dalam praktik internasional. OECD merumuskan prinsip dasar

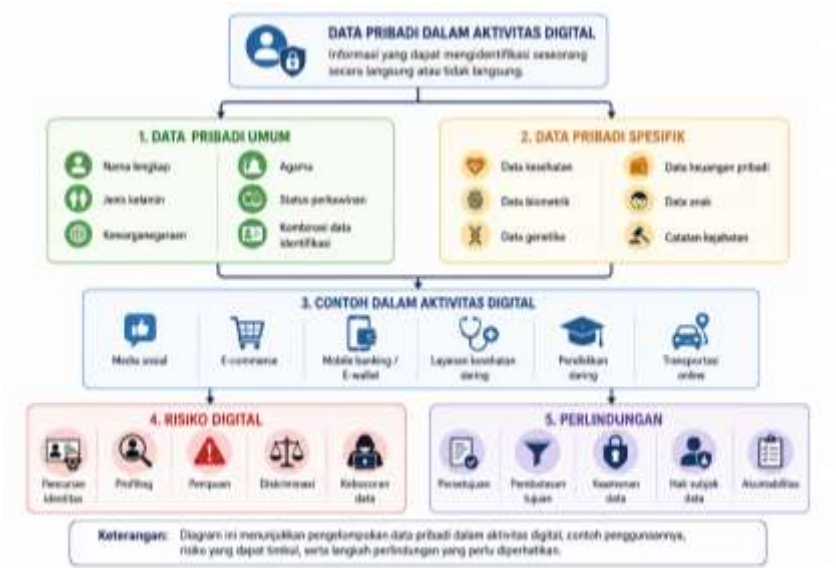
seperti pembatasan pengumpulan data, kualitas data, pembatasan tujuan, pembatasan penggunaan, keamanan, keterbukaan, partisipasi individu, dan akuntabilitas (OECD, 2013). Prinsip-prinsip tersebut juga sejalan dengan pendekatan General Data Protection Regulation atau GDPR di Uni Eropa yang menekankan perlindungan individu dalam pemrosesan data pribadi serta pentingnya dasar hukum, transparansi, dan akuntabilitas dalam pemrosesan data (European Parliament and Council of the European Union, 2016b).

Dalam konteks Indonesia, pelindungan data pribadi semakin kuat setelah lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang ini menjadi dasar penting karena mengatur jenis data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, transfer data pribadi, sanksi administratif, penyelesaian sengketa, serta ketentuan pidana. Kehadiran aturan ini menunjukkan bahwa data pribadi bukan sekadar urusan teknis, tetapi merupakan bagian dari perlindungan hak warga negara dalam masyarakat digital (Republik Indonesia, 2022).

Selain itu, pelindungan data pribadi juga berhubungan dengan hukum informasi dan transaksi elektronik. Aktivitas digital yang dilakukan melalui sistem elektronik harus memperhatikan keamanan, keandalan, dan tanggung jawab penyelenggara sistem elektronik. Penggunaan data pribadi tanpa dasar yang sah dapat menimbulkan konsekuensi hukum, terutama jika menimbulkan kerugian bagi pemilik data. Oleh karena itu, penyelenggara sistem elektronik perlu membangun tata kelola data yang bertanggung jawab, mulai dari tahap pengumpulan data, penyimpanan, penggunaan, pembagian, hingga penghapusan data.

6.2 Jenis-Jenis Data Pribadi dalam Aktivitas Digital

Dalam aktivitas digital, data pribadi muncul hampir di setiap interaksi pengguna dengan sistem elektronik. Ketika seseorang membuat akun media sosial, mendaftar aplikasi e-commerce, menggunakan dompet digital, mengakses layanan kesehatan daring, membuka rekening digital, mengisi formulir akademik, atau menggunakan aplikasi transportasi daring, sistem akan meminta, merekam, menyimpan, dan memproses data tertentu. Data tersebut dapat terlihat sederhana, seperti nama dan nomor telepon, tetapi dapat menjadi sangat sensitif apabila dikombinasikan dengan data lain seperti lokasi, riwayat transaksi, perilaku pencarian, atau data biometrik.



Gambar 6.2: Jenis-Jenis Data Pribadi dalam Aktivitas Digital

Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, data pribadi dibedakan menjadi dua kelompok besar, yaitu **data pribadi yang bersifat umum** dan **data pribadi yang bersifat spesifik**. Data pribadi umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Sementara itu, data pribadi spesifik meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai ketentuan peraturan perundang-undangan (Republik Indonesia, 2022).

Pembedaan tersebut penting karena tidak semua data memiliki tingkat risiko yang sama. Data seperti nama, jenis kelamin, atau kewarganegaraan dapat terlihat umum, tetapi tetap harus dilindungi karena dapat digunakan untuk mengenali seseorang. Sementara itu, data kesehatan, biometrik, genetika, keuangan, dan data anak memerlukan perlindungan lebih kuat karena penyalahgunaannya dapat menimbulkan dampak serius, seperti diskriminasi, pencurian identitas, pemerasan, penipuan finansial, atau kerugian psikologis. Dalam praktik internasional, GDPR juga menempatkan beberapa data seperti kesehatan, biometrik, dan genetika sebagai kategori

data yang membutuhkan perlindungan khusus (European Parliament and Council of the European Union, 2016).

Secara praktis, jenis-jenis data pribadi dalam aktivitas digital dapat dijelaskan sebagai berikut.

1. Data Identitas Dasar

Data identitas dasar adalah data yang paling sering digunakan untuk mengenali seseorang dalam layanan digital. Contohnya adalah nama lengkap, tempat dan tanggal lahir, jenis kelamin, kewarganegaraan, agama, status perkawinan, nomor induk kependudukan, nomor kartu mahasiswa, atau nomor keanggotaan tertentu. Data ini banyak digunakan dalam pendaftaran akun, verifikasi pengguna, administrasi pendidikan, layanan publik, dan transaksi digital.

2. Data Kontak

Data kontak meliputi nomor telepon, alamat rumah, alamat surel, kontak darurat, dan akun media sosial. Data ini sering digunakan untuk komunikasi, autentikasi, pengiriman kode OTP, pemberitahuan transaksi, pemulihan akun, dan layanan pelanggan. Risiko penyalahgunaan data kontak antara lain spam, phishing, penipuan, doxing, dan pengambilalihan akun.

3. Data Akun dan Kredensial Digital

Data akun dan kredensial digital mencakup username, password, PIN, kode OTP, token autentikasi, pertanyaan keamanan, dan data login. Jenis data ini sangat penting karena menjadi pintu masuk menuju akun pribadi pengguna. Apabila password, PIN, atau OTP bocor, akun media sosial, e-commerce, e-wallet, atau mobile banking dapat diambil alih oleh pihak lain.

4. Data Lokasi dan Perangkat

Aktivitas digital sering menghasilkan data lokasi, seperti koordinat GPS, alamat IP, lokasi Wi-Fi, metadata foto, dan riwayat perjalanan. Selain itu, sistem digital juga dapat merekam data perangkat, seperti jenis perangkat, sistem operasi, browser, nomor IMEI, ID perangkat, dan cookie. Data ini dapat membantu meningkatkan layanan, tetapi juga dapat digunakan untuk pelacakan, profiling, atau pengawasan berlebihan apabila tidak dikelola secara benar.

5. Data Aktivitas dan Perilaku Digital

Data aktivitas digital muncul dari kebiasaan pengguna saat menggunakan internet. Contohnya adalah riwayat pencarian, riwayat belanja, video yang ditonton, artikel yang dibaca, komentar, unggahan, klik, durasi penggunaan aplikasi, dan pola interaksi. Data perilaku digital sering digunakan untuk personalisasi layanan, rekomendasi konten, iklan tertarget, dan analisis preferensi pengguna. Namun, jika digunakan tanpa batas yang jelas, data ini dapat menimbulkan risiko manipulasi perilaku, profiling berlebihan, dan pelanggaran privasi digital (Solove, 2008).

6. Data Keuangan Pribadi

Data keuangan pribadi mencakup nomor rekening, nomor kartu debit atau kartu kredit, saldo, riwayat transaksi, tagihan, pinjaman, skor kredit, slip gaji, pajak, dan data pembayaran digital. Dalam aktivitas digital, data ini banyak muncul pada layanan mobile banking, dompet digital, fintech, e-commerce, paylater, dan aplikasi investasi. Data keuangan pribadi termasuk data pribadi spesifik sehingga harus memperoleh perlindungan lebih kuat (Republik Indonesia, 2022).

7. Data Kesehatan

Data kesehatan meliputi rekam medis, hasil laboratorium, riwayat penyakit, informasi konsultasi dokter, resep elektronik, data asuransi kesehatan, dan data dari aplikasi kebugaran. Data ini tergolong sensitif karena dapat memengaruhi perlakuan sosial, pekerjaan, asuransi, dan akses layanan tertentu. Penyalahgunaan data kesehatan dapat menyebabkan diskriminasi, pemerasan, atau pelanggaran martabat pribadi.

8. Data Biometrik dan Genetika

Data biometrik adalah data yang berkaitan dengan ciri fisik atau perilaku unik seseorang, seperti sidik jari, wajah, retina mata, suara, dan pola tanda tangan. Data genetika berkaitan dengan karakteristik genetik seseorang. Data ini banyak digunakan untuk absensi digital, penguncian perangkat, verifikasi identitas, sistem perbankan, layanan imigrasi, dan keamanan aplikasi. Risiko data biometrik lebih tinggi daripada password karena sidik jari, wajah, atau retina tidak mudah diganti ketika bocor.

9. Data Anak

Data anak termasuk data pribadi spesifik. Data ini dapat muncul dalam sistem sekolah, aplikasi pembelajaran daring, layanan kesehatan anak, media sosial, gim online, dan platform hiburan. Perlindungan data anak penting karena anak belum sepenuhnya mampu memahami risiko hukum, sosial, dan ekonomi dari penggunaan data digital. Karena itu, pemrosesan data anak perlu memperhatikan persetujuan, kepentingan terbaik anak, serta pembatasan penggunaan data.

10. Data Catatan Kejahatan atau Riwayat Hukum

Data ini mencakup catatan pidana, status hukum seseorang, riwayat perkara, atau informasi lain yang berkaitan dengan proses hukum. Dalam UU PDP, catatan kejahatan termasuk data pribadi spesifik (Republik Indonesia, 2022). Penyalahgunaan data ini dapat menimbulkan stigma, diskriminasi, dan pelanggaran hak individu, terutama jika dipublikasikan tanpa dasar hukum yang sah.

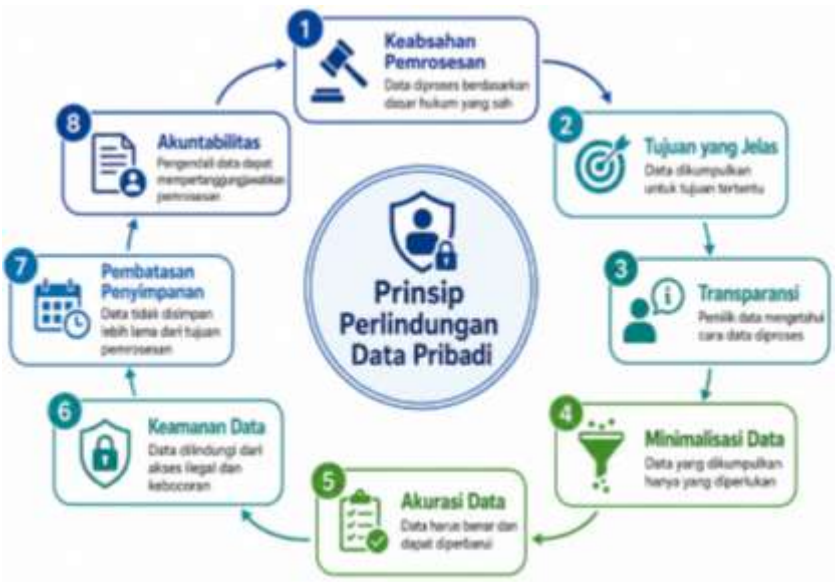
6.3 Prinsip Pelindungan data pribadi

Prinsip pelindungan data pribadi merupakan dasar yang digunakan untuk memastikan bahwa data seseorang tidak dikumpulkan, digunakan, disimpan, atau dibagikan secara sembarangan. Dalam aktivitas digital, data pribadi sering berpindah dari pengguna kepada aplikasi, platform, lembaga pendidikan, rumah sakit, bank, marketplace, penyedia layanan keuangan digital, hingga instansi pemerintah. Perpindahan data tersebut tidak selalu terlihat oleh pengguna. Karena itu, diperlukan prinsip yang dapat menjadi pedoman agar pemrosesan data berlangsung secara sah, aman, transparan, dan bertanggung jawab.

Pelindungan data pribadi tidak hanya berbicara tentang keamanan sistem. Banyak orang mengira perlindungan data cukup dilakukan dengan password, firewall, antivirus, atau enkripsi. Padahal, pelindungan data pribadi juga berkaitan dengan pertanyaan hukum dan etika: apakah data dikumpulkan dengan alasan yang sah, apakah pengguna mengetahui tujuan pemrosesan, apakah data yang diminta benar-benar diperlukan, apakah data disimpan terlalu lama, dan apakah pengendali data dapat mempertanggungjawabkan penggunaan data tersebut. Artinya, pelindungan

data pribadi harus dimulai sejak data pertama kali dikumpulkan, bukan hanya setelah terjadi kebocoran.

Dalam praktik internasional, prinsip pelindungan data pribadi telah lama dikenal melalui OECD Privacy Framework. OECD menekankan beberapa prinsip utama, seperti pembatasan pengumpulan data, kualitas data, pembatasan tujuan, pembatasan penggunaan, perlindungan keamanan, keterbukaan, partisipasi individu, dan akuntabilitas (OECD, 2013). Prinsip tersebut juga sejalan dengan General Data Protection Regulation atau GDPR di Uni Eropa yang mengatur bahwa data pribadi harus diproses secara sah, adil, transparan, terbatas pada tujuan tertentu, sesuai kebutuhan, akurat, aman, dan dapat dipertanggungjawabkan (European Parliament and Council of the European Union, 2016). Di Indonesia, prinsip serupa tercermin dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang mengatur pemrosesan data pribadi, hak subjek data, kewajiban pengendali data, kewajiban prosesor data, serta sanksi atas pelanggaran data pribadi (Republik Indonesia, 2022).



Gambar 6.3: Prinsip Pelindungan data pribadi

Prinsip pelindungan data pribadi dapat dipahami melalui beberapa aspek utama yang menjadi pedoman dalam mengumpulkan, menggunakan,

menyimpan, melindungi, dan mempertanggungjawabkan pemrosesan data pribadi.

1. **Keabsahan Pemrosesan**

   Data pribadi hanya boleh diproses apabila memiliki dasar yang sah. Dasar tersebut dapat berupa persetujuan pemilik data, pelaksanaan perjanjian, pemenuhan kewajiban hukum, perlindungan kepentingan vital, pelaksanaan tugas untuk kepentingan umum, atau dasar lain yang diakui oleh peraturan perundang-undangan. Tanpa dasar yang sah, pemrosesan data pribadi dapat menjadi tindakan yang melanggar hukum.

2. **Tujuan yang Jelas**

   Setiap pengumpulan data harus memiliki tujuan tertentu yang dapat dijelaskan kepada pemilik data. Data tidak boleh dikumpulkan hanya karena mungkin berguna di masa depan. Misalnya, marketplace dapat meminta nama, nomor telepon, dan alamat karena data tersebut diperlukan untuk pengiriman barang. Namun, apabila aplikasi meminta akses mikrofon, galeri, atau kontak tanpa alasan yang jelas, maka permintaan tersebut perlu dipertanyakan.

3. **Transparansi**

   Pemilik data perlu mengetahui data apa yang dikumpulkan, untuk apa data digunakan, siapa yang mengelola data, apakah data dibagikan kepada pihak ketiga, dan berapa lama data disimpan. Informasi mengenai pemrosesan data harus disampaikan dengan jelas, ringkas, dan mudah diakses agar pengguna dapat memahami risiko sebelum memberikan persetujuan.

4. **Minimalisasi Data**

   Data yang dikumpulkan seharusnya hanya data yang benar-benar diperlukan. Semakin banyak data yang dikumpulkan, semakin besar pula risiko jika terjadi kebocoran. Misalnya, layanan pengiriman barang membutuhkan alamat penerima, tetapi tidak selalu membutuhkan data biometrik. Prinsip ini membantu mengurangi risiko pencurian identitas, profiling berlebihan, penipuan, dan penyalahgunaan data.

5. Akurasi Data

Data pribadi yang diproses harus benar, lengkap, dan sesuai dengan kondisi terbaru. Data yang tidak akurat dapat menimbulkan kerugian bagi pemilik data, seperti kesalahan verifikasi, pengiriman barang, administrasi akademik, atau transaksi keuangan. Karena itu, pengendali data perlu menyediakan mekanisme agar pemilik data dapat memperbaiki atau memperbarui data yang keliru.

6. Keamanan dan Kerahasiaan Data

Data pribadi harus dilindungi dari akses tidak sah, kehilangan, perubahan, pengungkapan, perusakan, dan penyalahgunaan. Perlindungan dapat dilakukan melalui langkah teknis seperti enkripsi, autentikasi multifaktor, kontrol akses, pencadangan data, pemantauan log, dan pembaruan sistem. Selain itu, organisasi juga perlu menerapkan kebijakan internal, pembatasan akses pegawai, pelatihan keamanan data, audit, dan prosedur penanganan insiden.

7. Pembatasan Penyimpanan

Data pribadi tidak seharusnya disimpan tanpa batas waktu. Apabila tujuan pemrosesan telah selesai, data perlu dihapus, dimusnahkan, dianonimkan, atau disimpan berdasarkan dasar hukum lain yang sah. Pengendali data perlu memiliki kebijakan retensi data yang menjelaskan berapa lama data disimpan dan kapan data harus dihapus.

8. Akuntabilitas

Pihak yang mengelola data pribadi harus dapat mempertanggungjawabkan seluruh proses pemrosesan data. Akuntabilitas berarti pengendali data tidak hanya mengaku patuh, tetapi juga mampu membuktikan kepatuhannya melalui kebijakan, dokumentasi, prosedur, audit, pengamanan sistem, serta mekanisme penanganan keluhan. Dalam layanan digital modern, hubungan dengan pihak ketiga seperti penyedia cloud, penyedia pembayaran, jasa pengiriman, atau penyedia analitik juga harus dikelola agar data pribadi tidak disalahgunakan.

6.4 Hak Pemilik Data dan Kewajiban Pengendali Data

Hak pemilik data dan kewajiban pengendali data merupakan bagian penting dalam pelindungan data pribadi. Pemilik data atau subjek data pribadi adalah orang perseorangan yang datanya dikumpulkan, digunakan, disimpan, dikirim, diungkapkan, atau diproses oleh pihak lain. Pengendali data pribadi adalah pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan data pribadi.

Gambar 6.4: Hak Pemilik Data dan Kewajiban Pengendali Data

Dalam praktik digital, pengendali data dapat berupa lembaga pemerintah, perusahaan, perguruan tinggi, rumah sakit, bank, platform digital, marketplace, penyedia layanan keuangan digital, atau organisasi lain yang mengelola data pengguna. UU PDP mengatur hak subjek data pribadi serta kewajiban pengendali dan prosesor data pribadi dalam pemrosesan data pribadi (Republik Indonesia, 2022). Secara internasional, GDPR juga menempatkan hak subjek data dan kewajiban pengendali data sebagai bagian utama pelindungan data pribadi (European Parliament and Council of the European Union, 2016).

Hubungan antara pemilik data dan pengendali data harus berjalan seimbang. Organisasi membutuhkan data untuk memberikan layanan, memverifikasi identitas, menjalankan transaksi, dan meningkatkan kualitas sistem. Namun,

individu tetap memiliki hak untuk mengetahui, mengontrol, dan membatasi penggunaan informasi tentang dirinya. Privasi tidak hanya berkaitan dengan kerahasiaan, tetapi juga berkaitan dengan kendali individu terhadap informasi pribadi dan risiko penyalahgunaan data (Solove, 2008). OECD juga menekankan prinsip keterbukaan, partisipasi individu, dan akuntabilitas sebagai bagian penting dalam tata kelola data pribadi (OECD, 2013).

6.4.1 Hak Pemilik Data

Pemilik data memiliki beberapa hak penting agar tetap memiliki kendali atas data pribadinya. Hak-hak tersebut dapat dijelaskan sebagai berikut.

1. **Hak memperoleh informasi**

   Pemilik data berhak mengetahui jenis data yang dikumpulkan, tujuan pemrosesan, dasar hukum pemrosesan, pihak yang mengelola data, pihak yang menerima data, jangka waktu penyimpanan, serta risiko yang mungkin timbul. Informasi ini penting agar pemilik data dapat memberikan persetujuan secara sadar. GDPR menekankan bahwa informasi kepada subjek data harus diberikan secara ringkas, transparan, mudah dipahami, dan mudah diakses (European Parliament and Council of the European Union, 2016). Prinsip keterbukaan juga menjadi bagian dari OECD Privacy Framework karena individu perlu mengetahui praktik pengelolaan data yang dilakukan oleh organisasi (OECD, 2013).

2. **Hak mengakses data pribadi**

   Pemilik data berhak mengetahui apakah datanya sedang diproses dan data apa saja yang disimpan oleh pengendali data. Hak akses penting karena pengguna sering tidak mengetahui jumlah dan jenis data yang telah dikumpulkan oleh aplikasi, platform, lembaga pendidikan, bank, rumah sakit, atau layanan digital lainnya. Dalam GDPR, hak akses memberi ruang bagi subjek data untuk memperoleh konfirmasi mengenai pemrosesan data serta informasi mengenai tujuan, kategori data, penerima data, dan jangka waktu penyimpanan (European Parliament and Council of the European Union, 2016). Namun, pelaksanaan hak akses juga harus hati-hati karena penelitian Bufalieri et al. menunjukkan bahwa prosedur akses data yang lemah dapat menimbulkan risiko baru apabila identitas pemohon tidak diverifikasi dengan benar (Bufalieri et al., 2020).

3. Hak memperbaiki atau memperbarui data

Pemilik data berhak meminta perbaikan apabila data pribadinya salah, tidak lengkap, atau tidak sesuai dengan kondisi terbaru. Kesalahan data dapat menimbulkan kerugian, misalnya kesalahan alamat pengiriman, nomor telepon, data akademik, data kesehatan, atau data keuangan. Prinsip kualitas data dalam OECD Privacy Framework menekankan bahwa data pribadi harus relevan dengan tujuan penggunaan serta akurat, lengkap, dan mutakhir sesuai kebutuhan (OECD, 2013). GDPR juga mengatur hak pembetulan atau *right to rectification* terhadap data pribadi yang tidak akurat (European Parliament and Council of the European Union, 2016).

4. Hak menarik persetujuan

Persetujuan yang pernah diberikan tidak berarti data pribadi dapat digunakan selamanya. Pemilik data dapat menarik persetujuan terhadap pemrosesan tertentu, misalnya berhenti menerima promosi, menonaktifkan akses lokasi, mencabut izin akses kontak, atau menutup akun layanan. GDPR menyatakan bahwa subjek data memiliki hak untuk menarik persetujuan kapan saja, dan penarikan tersebut tidak memengaruhi keabsahan pemrosesan sebelum persetujuan ditarik (European Parliament and Council of the European Union, 2016). Dalam konteks Indonesia, UU PDP juga mengatur pemrosesan data pribadi berdasarkan dasar yang sah, termasuk persetujuan subjek data pribadi (Republik Indonesia, 2022).

5. Hak membatasi pemrosesan data

Pemilik data dapat meminta pembatasan pemrosesan apabila data diproses secara berlebihan, tidak sesuai tujuan, atau sedang disengketakan. Pembatasan ini dapat dilakukan dengan menghentikan penggunaan data untuk tujuan tertentu, seperti iklan tertarget atau pembagian kepada pihak ketiga. Prinsip pembatasan tujuan dan pembatasan penggunaan dalam OECD Privacy Framework menegaskan bahwa data pribadi tidak boleh digunakan di luar tujuan yang telah ditentukan kecuali berdasarkan persetujuan atau dasar hukum yang sah (OECD, 2013). GDPR juga mengatur pembatasan pemrosesan dalam kondisi tertentu, misalnya ketika akurasi data sedang dipersoalkan atau pemrosesan dianggap tidak sah (European Parliament and Council of the European Union, 2016).

6. Hak meminta penghapusan atau pemusnahan data

Pemilik data dapat meminta penghapusan data apabila tujuan pemrosesan telah selesai, data tidak lagi diperlukan, atau pemrosesan dilakukan tanpa dasar yang sah. Namun, hak ini tidak selalu mutlak karena data tertentu masih dapat disimpan untuk kewajiban hukum, pembuktian transaksi, audit, perpajakan, atau penyelesaian sengketa. GDPR mengenal hak penghapusan atau *right to erasure* dalam kondisi tertentu, seperti ketika data tidak lagi diperlukan untuk tujuan awal atau persetujuan telah ditarik (European Parliament and Council of the European Union, 2016). UU PDP juga mengatur hak subjek data dan kewajiban pengendali data dalam penghentian pemrosesan, penghapusan, atau pemusnahan data pribadi sesuai ketentuan hukum (Republik Indonesia, 2022).

7. Hak mengajukan keberatan, pengaduan, atau gugatan

Pemilik data berhak mengajukan keberatan apabila merasa data pribadinya diproses secara tidak sah, disebarkan tanpa izin, digunakan secara berlebihan, atau menyebabkan kerugian. Jika tidak memperoleh penyelesaian, pemilik data dapat menggunakan jalur pengaduan atau penyelesaian sengketa sesuai ketentuan hukum. UU PDP mengatur penyelesaian sengketa dan mekanisme hukum dalam pelindungan data pribadi (Republik Indonesia, 2022). GDPR juga memberikan hak kepada subjek data untuk mengajukan pengaduan kepada otoritas pengawas apabila pemrosesan data dianggap melanggar ketentuan perlindungan data (European Parliament and Council of the European Union, 2016).

6.4.2 Kewajiban Pengendali Data

Pengendali data memiliki kewajiban untuk memastikan bahwa pemrosesan data pribadi dilakukan secara sah, transparan, aman, terbatas, dan bertanggung jawab. Kewajiban tersebut dapat dijelaskan sebagai berikut.

1. Menentukan tujuan pemrosesan secara jelas

Pengendali data wajib menjelaskan alasan data dikumpulkan dan untuk apa data digunakan. Data tidak boleh dikumpulkan tanpa tujuan yang sah atau digunakan untuk tujuan lain yang tidak dijelaskan kepada pemilik data. Prinsip *purpose specification* dalam OECD Privacy

Framework menuntut tujuan pengumpulan data ditentukan paling lambat saat data dikumpulkan (OECD, 2013). GDPR juga menekankan bahwa data pribadi harus dikumpulkan untuk tujuan yang spesifik, eksplisit, dan sah (European Parliament and Council of the European Union, 2016).

2. Memastikan dasar hukum pemrosesan

Setiap pemrosesan data harus memiliki dasar yang sah, seperti persetujuan, pelaksanaan perjanjian, pemenuhan kewajiban hukum, kepentingan vital, kepentingan umum, atau dasar lain yang diakui oleh peraturan perundang-undangan. UU PDP mengatur bahwa pemrosesan data pribadi harus memiliki dasar pemrosesan yang sah (Republik Indonesia, 2022). GDPR juga mengatur dasar hukum pemrosesan data, termasuk persetujuan, pelaksanaan kontrak, kewajiban hukum, kepentingan vital, tugas publik, dan kepentingan sah tertentu (European Parliament and Council of the European Union, 2016).

3. Memberikan informasi yang transparan

Pengendali data wajib menyampaikan informasi tentang pemrosesan data dengan bahasa yang jelas, mudah dipahami, dan tidak menyesatkan. Informasi ini dapat disampaikan melalui kebijakan privasi, pemberitahuan penggunaan data, atau pengaturan persetujuan. Transparansi penting karena pengguna tidak dapat mengambil keputusan yang sadar jika informasi pemrosesan data tidak jelas. Solove menjelaskan bahwa masalah privasi sering muncul bukan hanya karena informasi bersifat rahasia, tetapi karena individu kehilangan kendali dan pemahaman atas penggunaan informasi tentang dirinya (Solove, 2008).

4. Menjaga akurasi data

Pengendali data wajib menjaga agar data yang diproses tetap benar, lengkap, dan mutakhir. Jika terdapat kesalahan, pengendali data perlu menyediakan mekanisme koreksi agar pemilik data dapat memperbarui data pribadinya. Kewajiban ini berkaitan dengan prinsip kualitas data dalam OECD Privacy Framework yang menekankan bahwa data harus relevan, akurat, lengkap, dan mutakhir sesuai tujuan penggunaannya (OECD, 2013). GDPR juga menegaskan bahwa data pribadi harus akurat dan, jika perlu, diperbarui (European Parliament and Council of the European Union, 2016).

5. Menjaga keamanan dan kerahasiaan data

Pengendali data wajib melindungi data pribadi dari akses ilegal, kebocoran, kehilangan, perubahan, pengungkapan, atau penyalahgunaan. Perlindungan dapat dilakukan melalui enkripsi, autentikasi multifaktor, kontrol akses, pencadangan data, pembaruan sistem, pelatihan pegawai, audit, dan prosedur respons insiden. OECD menempatkan perlindungan keamanan sebagai prinsip utama dalam pengelolaan data pribadi (OECD, 2013). GDPR juga menegaskan bahwa data pribadi harus diproses dengan keamanan yang sesuai, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum serta kehilangan, kerusakan, atau kerugian yang tidak disengaja (European Parliament and Council of the European Union, 2016).

6. Mengelola prosesor data secara bertanggung jawab

Jika pengendali data bekerja sama dengan pihak ketiga seperti penyedia cloud, penyedia pembayaran, jasa pengiriman, atau vendor teknologi, pengendali data harus memastikan bahwa pihak tersebut memproses data sesuai instruksi dan menerapkan keamanan yang memadai. GDPR membedakan peran controller dan processor, serta mewajibkan hubungan pemrosesan data diatur agar prosesor hanya bertindak berdasarkan instruksi pengendali data (European Parliament and Council of the European Union, 2016). Kewajiban serupa juga sejalan dengan UU PDP yang mengatur pengendali data pribadi dan prosesor data pribadi dalam pemrosesan data pribadi (Republik Indonesia, 2022).

7. Menyediakan mekanisme pengaduan

Pengendali data wajib menyediakan saluran pengaduan yang jelas dan mudah diakses. Mekanisme ini penting agar pemilik data dapat meminta informasi, koreksi, pembatasan, penghapusan, atau penyelesaian apabila terjadi penyalahgunaan data. UU PDP mengatur penyelesaian sengketa dan perlindungan hak subjek data pribadi (Republik Indonesia, 2022). GDPR juga menegaskan pentingnya mekanisme pelaksanaan hak subjek data, termasuk hak untuk mengajukan keluhan atas pemrosesan data yang melanggar hukum (European Parliament and Council of the European Union, 2016).

8. Menerapkan akuntabilitas

Pengendali data harus mampu mempertanggungjawabkan seluruh proses pemrosesan data. Akuntabilitas dapat diwujudkan melalui dokumentasi, kebijakan internal, SOP, audit, pencatatan aktivitas pemrosesan, dan pelaporan apabila terjadi insiden atau pelanggaran data. OECD menempatkan akuntabilitas sebagai salah satu prinsip utama dalam perlindungan privasi (OECD, 2013). GDPR juga menegaskan bahwa pengendali data bertanggung jawab atas kepatuhan terhadap prinsip pemrosesan data dan harus mampu membuktikan kepatuhan tersebut (European Parliament and Council of the European Union, 2016).

6.5 Risiko Kebocoran dan Penyalahgunaan Data Pribadi

Risiko kebocoran dan penyalahgunaan data pribadi semakin meningkat seiring dengan luasnya penggunaan layanan digital. Aktivitas seperti membuat akun, berbelanja online, menggunakan dompet digital, mengakses sistem akademik, memakai media sosial, atau menggunakan layanan kesehatan digital selalu melibatkan data pribadi. Data tersebut dapat berupa nama, nomor telepon, alamat, email, nomor identitas, lokasi, riwayat transaksi, data kesehatan, data biometrik, dan aktivitas pengguna di internet. Jika data tersebut tidak dikelola dengan baik, data pribadi dapat berubah menjadi sumber kerugian bagi pemiliknya.

Kebocoran data pribadi terjadi ketika data yang seharusnya dilindungi dapat diakses, disalin, disebarkan, atau digunakan oleh pihak yang tidak berwenang. Penyebabnya dapat berupa serangan siber, kelemahan sistem, kesalahan konfigurasi server, kelalaian pegawai, penggunaan password lemah, malware, atau lemahnya pengawasan terhadap pihak ketiga. Data yang bocor dapat digunakan secara langsung untuk kejahatan, atau digabungkan dengan data lain untuk membentuk profil korban. Persoalan privasi tidak hanya berkaitan dengan kerahasiaan, tetapi juga dengan kendali individu terhadap informasi tentang dirinya dan risiko penyalahgunaan informasi tersebut oleh pihak lain (Solove, 2008).

6.5.1 Bentuk Penyalahgunaan Data Pribadi

Penyalahgunaan data pribadi dapat terjadi dalam berbagai bentuk. Beberapa bentuk yang sering ditemukan dalam praktik layanan digital adalah sebagai berikut.

Gambar 6.5: Bentuk Penyalahgunaan Data Pribadi

1. **Pencurian identitas**

   Pencurian identitas terjadi ketika data pribadi seseorang digunakan oleh pihak lain untuk berpura-pura menjadi orang tersebut. Data seperti nama, NIK, nomor telepon, email, foto, atau alamat dapat digunakan untuk membuat akun palsu, melakukan transaksi, mendaftar layanan tertentu, atau mengajukan pinjaman. Korban dapat mengalami kerugian meskipun tidak pernah melakukan tindakan tersebut.

2. **Pengambilalihan akun digital**

   Akun digital dapat diambil alih apabila pelaku memperoleh username, password, PIN, OTP, token, atau tautan pemulihan akun. Setelah akun dikuasai, pelaku dapat mengubah password, melakukan transaksi, mencuri data tambahan, atau menyebarkan penipuan kepada kontak korban. Risiko ini menunjukkan bahwa data akun dan kredensial digital harus diperlakukan sebagai informasi yang sangat sensitif.

3. Penipuan finansial

Data pribadi yang bocor dapat digunakan untuk transaksi tidak sah, penyalahgunaan kartu, pembukaan akun palsu, atau pengajuan pinjaman online ilegal. Dalam layanan keuangan digital, risiko fraud dapat muncul melalui penyalahgunaan identitas, phishing, rekayasa sosial, dan serangan berbasis teknologi. OJK menekankan bahwa penyelenggara layanan keuangan digital perlu memperhatikan risiko fraud karena dapat merugikan konsumen dan merusak kepercayaan terhadap layanan keuangan digital (OJK, 2024).

4. Phishing dan rekayasa sosial

Data yang bocor sering digunakan untuk membuat pesan penipuan terlihat lebih meyakinkan. Misalnya, pelaku menyebut nama korban, alamat, nomor transaksi, atau informasi pribadi lain agar korban percaya bahwa pesan tersebut berasal dari pihak resmi. Dalam kondisi ini, kebocoran data menjadi bahan untuk memanipulasi kepercayaan korban.

5. Doxing dan penyebaran informasi pribadi

Doxing adalah tindakan menyebarkan informasi pribadi seseorang tanpa izin, seperti alamat rumah, nomor telepon, tempat kerja, foto keluarga, atau akun media sosial. Tindakan ini dapat menimbulkan intimidasi, pencemaran nama baik, gangguan psikologis, dan risiko keamanan fisik. Informasi yang sudah tersebar di internet juga sulit dihapus sepenuhnya karena dapat disalin dan disebarkan ulang oleh banyak pihak.

6. Profiling dan manipulasi perilaku

Data aktivitas digital, seperti riwayat pencarian, klik, belanja, tontonan, lokasi, dan interaksi media sosial, dapat digunakan untuk membentuk profil pengguna. Profil ini dapat dipakai untuk personalisasi layanan, tetapi juga berisiko digunakan untuk iklan invasif, diskriminasi harga, manipulasi pilihan, atau pengawasan berlebihan. OECD menekankan pentingnya pembatasan tujuan, pembatasan penggunaan, keterbukaan, dan akuntabilitas dalam pengelolaan data pribadi agar data tidak digunakan secara merugikan pemiliknya (OECD, 2013).

6.5.2 Dampak Kebocoran Data Pribadi

Kebocoran dan penyalahgunaan data pribadi dapat menimbulkan dampak yang luas. Dampak pertama adalah **kerugian ekonomi**, seperti kehilangan saldo, transaksi tidak sah, tagihan palsu, penipuan belanja online, atau pinjaman ilegal atas nama korban. Dampak kedua adalah **kerugian sosial**, seperti rusaknya reputasi, pencemaran nama baik, penyebaran informasi pribadi, atau hilangnya kepercayaan dari lingkungan sosial. Dampak ketiga adalah **kerugian psikologis**, seperti rasa takut, malu, cemas, tidak aman, atau tertekan setelah data pribadi tersebar.

Selain bagi individu, kebocoran data juga berdampak pada organisasi. Organisasi dapat kehilangan kepercayaan pengguna, mengalami kerusakan reputasi, menghadapi tuntutan hukum, menerima sanksi administratif, dan menanggung biaya pemulihan sistem. UU Pelindungan Data Pribadi menegaskan bahwa pemrosesan data pribadi harus dilakukan secara hati-hati karena pelanggaran terhadap data pribadi dapat menimbulkan konsekuensi hukum bagi pihak yang mengelola data (Republik Indonesia, 2022).

6.5.3 Faktor Penyebab Kebocoran Data

Kebocoran data tidak selalu terjadi karena serangan besar. Banyak kasus muncul akibat kelemahan sederhana dalam penggunaan teknologi dan tata kelola organisasi. Beberapa faktor penyebab yang umum antara lain:

- penggunaan password yang lemah atau sama pada banyak akun;
- tidak mengaktifkan autentikasi multifaktor;
- mengklik tautan palsu atau mengunduh file berbahaya;
- sistem tidak diperbarui sehingga memiliki celah keamanan;
- akses pegawai tidak dibatasi sesuai kebutuhan;
- penyimpanan data tanpa enkripsi;
- pengiriman data kepada pihak yang salah;
- lemahnya pengawasan terhadap vendor atau pihak ketiga.

Faktor-faktor tersebut menunjukkan bahwa pelindungan data pribadi tidak hanya bergantung pada teknologi, tetapi juga pada perilaku pengguna, kebijakan organisasi, dan pengawasan terhadap proses pemrosesan data. NIST Cybersecurity Framework 2.0 menekankan pentingnya pengelolaan

risiko melalui fungsi *govern*, *identify*, *protect*, *detect*, *respond*, dan *recover* agar organisasi mampu mencegah, mendeteksi, merespons, serta memulihkan diri dari insiden keamanan siber (National Institute of Standards and Technology, 2024).

6.6 Pelindungan data pribadi dalam Praktik Layanan Digital

Pelindungan data pribadi tidak hanya penting dalam teori, tetapi juga harus diterapkan dalam berbagai layanan digital. Media sosial, marketplace, dompet digital, mobile banking, sistem akademik, dan layanan kesehatan sama-sama memproses data pribadi pengguna. Data tersebut dapat berupa identitas, kontak, lokasi, riwayat transaksi, data kesehatan, maupun aktivitas pengguna di internet. Karena itu, setiap layanan digital perlu memastikan bahwa data diproses secara sah, aman, dan bertanggung jawab (Republik Indonesia, 2022).

Gambar 6.6: Pelindungan data pribadi dalam Praktik Layanan Digital

6.6.1 Penerapan pada Layanan Digital

Pelindungan data pribadi dapat diterapkan dalam berbagai layanan digital sebagai berikut:

- **Media sosial**: melindungi foto, lokasi, pesan, dan aktivitas pengguna melalui pengaturan privasi dan autentikasi dua faktor.
- **Marketplace**: melindungi data pembeli, alamat, dan transaksi melalui keamanan akun dan mekanisme pelaporan penipuan.
- **Dompet digital dan mobile banking**L melindungi identitas, PIN, OTP, dan riwayat transaksi melalui enkripsi, autentikasi multifaktor, dan pemantauan transaksi mencurigakan.
- **Sistem akademik** – melindungi data mahasiswa, nilai, dan dokumen akademik melalui pembatasan akses sesuai kewenangan.
- **Layanan kesehatan digital** – melindungi rekam medis dan data kesehatan melalui kontrol akses dan persetujuan pasien.

6.6.2 Peran Pengguna dalam Melindungi Data

Pengguna memiliki peran penting dalam menjaga keamanan data pribadi. Beberapa langkah yang dapat dilakukan antara lain:

- menggunakan password yang kuat dan berbeda untuk setiap akun;
- mengaktifkan autentikasi multifaktor;
- tidak membagikan PIN, OTP, atau password;
- memeriksa alamat situs sebelum login;
- menghindari tautan atau file yang mencurigakan;
- membatasi informasi pribadi yang dibagikan di media sosial;
- menggunakan aplikasi resmi dari sumber terpercaya.

6.6.3 Peran Organisasi dalam Melindungi Data

Organisasi memiliki peran penting dalam melindungi data pribadi karena menjadi pihak yang mengumpulkan, menyimpan, menggunakan, dan mengelola data pengguna. Perlindungan data tidak cukup hanya bergantung pada pengguna, tetapi juga harus didukung oleh kebijakan, sistem keamanan, dan prosedur kerja yang jelas. Organisasi yang mengelola data pribadi perlu melakukan beberapa langkah berikut.

1. **Menerapkan kebijakan privasi yang jelas**

   Kebijakan privasi perlu menjelaskan jenis data yang dikumpulkan,

tujuan penggunaan, pihak yang dapat mengakses, jangka waktu penyimpanan, dan hak pemilik data.

2. **Mengumpulkan data sesuai kebutuhan layanan**

   Data yang dikumpulkan harus sesuai dengan fungsi layanan dan tidak berlebihan. Misalnya, layanan pengiriman membutuhkan nama, alamat, dan nomor telepon, tetapi tidak selalu membutuhkan akses kontak atau galeri.

3. **Membatasi akses data berdasarkan kewenangan**

   Akses data hanya diberikan kepada pihak yang membutuhkan sesuai tugasnya. Pembatasan ini penting untuk mencegah penyalahgunaan data dari dalam organisasi.

4. **Menggunakan mekanisme keamanan yang memadai**

   Organisasi perlu menerapkan enkripsi, autentikasi multifaktor, kontrol akses, firewall, dan pemantauan sistem untuk mencegah kebocoran atau akses ilegal.

5. **Melakukan pencadangan data secara berkala**

   Backup diperlukan agar data dapat dipulihkan jika terjadi kerusakan sistem, serangan ransomware, kesalahan teknis, atau bencana.

6. **Menyediakan mekanisme pelaporan dan penanganan insiden**

   Organisasi perlu menyediakan saluran pelaporan serta prosedur respons apabila terjadi kebocoran data, akses tidak sah, atau penyalahgunaan data.

7. **Menghapus data yang tidak lagi diperlukan**

   Data yang sudah tidak dibutuhkan perlu dihapus, dimusnahkan, atau dianonimkan sesuai kebijakan retensi dan ketentuan hukum.

Melalui langkah-langkah tersebut, organisasi dapat mengurangi risiko kebocoran data, penyalahgunaan identitas, penipuan digital, dan kerugian bagi pengguna.

NIST Cybersecurity Framework 2.0 menempatkan fungsi *govern*, *identify*, *protect*, *detect*, *respond*, dan *recover* sebagai kerangka pengelolaan risiko keamanan siber organisasi (National Institute of Standards and Technology, 2024).

Bab 7
Hukum Perlindungan Konsumen di Era Digital

7.1 Konsep Perlindungan Konsumen Digital

Perlindungan konsumen digital merupakan bagian penting dari hukum teknologi informasi karena aktivitas konsumsi masyarakat semakin banyak dilakukan melalui media elektronik. Pada era digital, konsumen tidak hanya membeli barang secara langsung di toko fisik, tetapi juga melakukan transaksi melalui marketplace, aplikasi mobile, media sosial, website, layanan dompet digital, mobile banking, layanan streaming, transportasi online, hingga platform jasa berbasis aplikasi. Perubahan pola transaksi ini melahirkan hubungan hukum baru antara konsumen, pelaku usaha, penyelenggara sistem elektronik, dan platform digital.

Gambar 7.1: Konsep Perlindungan Konsumen Digital

Secara umum, perlindungan konsumen digital dapat dipahami sebagai upaya hukum untuk memberikan kepastian, keamanan, keadilan, dan perlindungan terhadap konsumen dalam menggunakan layanan digital. Perlindungan ini mencakup hak konsumen untuk memperoleh informasi yang benar, hak atas keamanan transaksi, hak atas pelindungan data pribadi, hak atas produk atau layanan yang sesuai dengan janji, hak untuk mengajukan komplain, serta hak

untuk memperoleh ganti rugi apabila mengalami kerugian. United Nations (2015) menekankan bahwa perlindungan konsumen perlu menjamin hak atas keamanan, informasi, pilihan, penyelesaian sengketa, serta perlakuan yang adil dalam kegiatan perdagangan.

Dalam transaksi konvensional, konsumen dan pelaku usaha biasanya dapat bertemu secara langsung. Konsumen dapat melihat barang, menilai kualitas, menawar harga, dan mengetahui identitas penjual. Namun, dalam transaksi digital, hubungan antara konsumen dan pelaku usaha sering berlangsung tanpa pertemuan fisik. Konsumen hanya melihat gambar, deskripsi produk, ulasan, rating, atau informasi yang ditampilkan melalui platform. Kondisi ini membuat konsumen digital lebih rentan terhadap informasi yang tidak benar, iklan menyesatkan, barang tidak sesuai, keterlambatan pengiriman, penyalahgunaan data pribadi, hingga penipuan online.

Perlindungan konsumen digital di Indonesia tidak dapat dilepaskan dari Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Undang-undang ini memberikan dasar bahwa konsumen berhak memperoleh kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa. Konsumen juga berhak memperoleh informasi yang benar, jelas, dan jujur mengenai kondisi barang dan/atau jasa. Meskipun undang-undang ini lahir sebelum perkembangan e-commerce sepesat saat ini, prinsip-prinsipnya tetap relevan untuk melindungi konsumen dalam ruang digital.

Selain itu, perlindungan konsumen digital juga berkaitan dengan Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE. UU ITE memberikan dasar hukum bagi transaksi elektronik, kontrak elektronik, dokumen elektronik, tanda tangan elektronik, serta tanggung jawab penyelenggara sistem elektronik. Dalam konteks ini, transaksi yang dilakukan melalui internet tetap memiliki akibat hukum. Artinya, kesepakatan yang dibuat secara digital tetap dapat mengikat para pihak selama memenuhi syarat hukum yang berlaku. Anami et al. (2025) menjelaskan bahwa kontrak digital memiliki kesamaan dengan kontrak konvensional dan tetap mengikat para pihak sepanjang memenuhi unsur sahnya perjanjian sebagaimana diatur dalam Pasal 1320 KUH Perdata.

Perlindungan konsumen digital juga berkaitan erat dengan hukum perdata. Dalam transaksi online, hubungan antara konsumen dan pelaku usaha pada dasarnya merupakan hubungan perjanjian. Konsumen berkewajiban

membayar harga, sedangkan pelaku usaha berkewajiban menyerahkan barang atau jasa sesuai dengan kesepakatan. Apabila salah satu pihak tidak memenuhi kewajibannya, maka dapat terjadi wanprestasi. Sugara dan Az-Zahra (2024) menjelaskan bahwa transaksi e-commerce merupakan bentuk perjanjian yang diatur dalam hukum perdata, tetapi pelaksanaannya sering menimbulkan masalah yang merugikan konsumen.

Dalam praktiknya, permasalahan konsumen digital sering muncul karena ketidakseimbangan posisi antara konsumen dan pelaku usaha. Konsumen biasanya berada pada posisi yang lebih lemah karena tidak dapat memeriksa barang secara langsung, tidak selalu mengetahui identitas pelaku usaha, dan sering harus menyetujui syarat layanan yang sudah disediakan sepihak oleh platform. Syarat dan ketentuan digital biasanya berbentuk kontrak baku, yaitu perjanjian yang isinya telah ditentukan terlebih dahulu oleh pelaku usaha atau platform. Konsumen hanya diberi pilihan untuk menyetujui atau tidak menggunakan layanan tersebut.

Ketidakseimbangan ini membuat konsep perlindungan konsumen digital menjadi penting. Perlindungan tidak hanya diberikan setelah terjadi sengketa, tetapi juga harus dilakukan sejak sebelum transaksi. Konsumen harus memperoleh informasi yang jelas mengenai harga, spesifikasi barang, biaya pengiriman, metode pembayaran, jaminan produk, kebijakan pengembalian barang, kebijakan refund, serta identitas pelaku usaha. Jika informasi tersebut tidak disampaikan secara jelas, maka konsumen berisiko mengambil keputusan transaksi berdasarkan informasi yang keliru. OECD (2016) menegaskan bahwa perlindungan konsumen dalam e-commerce harus menjamin transparansi informasi, praktik bisnis yang adil, mekanisme pembayaran yang aman, dan penyelesaian sengketa yang efektif.

Dalam konteks transaksi elektronik, kepercayaan menjadi unsur utama. Konsumen bersedia melakukan pembayaran karena percaya bahwa barang akan dikirim atau layanan akan diberikan. Pelaku usaha juga percaya bahwa konsumen akan memenuhi kewajiban pembayaran. Platform digital berperan sebagai perantara yang menyediakan sistem transaksi, sistem pembayaran, sistem ulasan, layanan pengaduan, dan mekanisme penyelesaian sengketa. Oleh karena itu, perlindungan konsumen digital tidak hanya bergantung pada penjual dan pembeli, tetapi juga pada tanggung jawab platform sebagai penyelenggara sistem elektronik.

Perlindungan konsumen digital juga mencakup perlindungan terhadap data pribadi. Dalam transaksi online, konsumen biasanya memberikan data seperti nama, alamat, nomor telepon, email, lokasi, riwayat transaksi, metode pembayaran, dan informasi identitas lainnya. Data tersebut diperlukan untuk memproses transaksi, tetapi juga dapat menimbulkan risiko apabila disalahgunakan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar bahwa pemrosesan data pribadi harus dilakukan secara sah, transparan, terbatas pada tujuan tertentu, dan disertai tanggung jawab pengendali data. Dengan demikian, perlindungan konsumen digital tidak hanya menyangkut barang atau jasa, tetapi juga keamanan data konsumen.

Pelindungan data pribadi dalam transaksi digital juga sejalan dengan prinsip internasional mengenai privasi. OECD (2013) menekankan pentingnya pembatasan pengumpulan data, kualitas data, pembatasan penggunaan, keamanan, keterbukaan, partisipasi individu, dan akuntabilitas. Sementara itu, Solove (2008) menjelaskan bahwa privasi tidak hanya berkaitan dengan kerahasiaan, tetapi juga dengan kontrol individu terhadap informasi tentang dirinya. Dengan demikian, konsumen digital harus memiliki kendali atas data pribadinya, termasuk mengetahui tujuan pengumpulan data, pihak yang mengelola data, dan risiko penggunaan data tersebut.

Kasus-kasus kebocoran data pada layanan digital menunjukkan bahwa perlindungan konsumen digital harus dipahami secara luas. Konsumen tidak hanya dapat dirugikan karena barang tidak dikirim, tetapi juga karena data pribadinya bocor, akunnya diambil alih, atau saldo digitalnya hilang. Anindya & Subiyanto (2025) menunjukkan bahwa kasus kebocoran data Tokopedia menimbulkan persoalan mengenai tanggung jawab platform dalam menjaga data pengguna. Hal ini menunjukkan bahwa platform digital yang mengelola data konsumen memiliki tanggung jawab hukum dan etik untuk menjaga keamanan sistemnya.

Perlindungan konsumen digital juga diperlukan dalam layanan keuangan digital, seperti dompet digital, mobile banking, dan pembayaran elektronik. Sengketa saldo digital, transaksi tidak dikenal, pencurian OTP, phishing, dan gagal refund merupakan contoh masalah yang dapat merugikan konsumen. Dalam kasus sengketa saldo DANA, Anami et al. (2025) menjelaskan bahwa meskipun regulasi mengenai kontrak digital telah tersedia, implementasi perlindungan hukum bagi para pihak masih membutuhkan

penguatan. Hal ini memperlihatkan pentingnya mekanisme pengaduan yang cepat, transparan, dan mudah diakses oleh konsumen.

Dalam perspektif e-commerce, hubungan antara konsumen, pelaku usaha, dan platform harus dipahami sebagai hubungan yang saling bergantung. Turban et al., (2015) menjelaskan bahwa e-commerce melibatkan proses pembelian, penjualan, pertukaran produk, layanan, dan informasi melalui jaringan komputer, terutama internet. Karena transaksi dilakukan melalui sistem elektronik, aspek kepercayaan, keamanan, reputasi penjual, dan kualitas informasi menjadi sangat penting. Jika salah satu aspek tersebut lemah, maka risiko kerugian konsumen meningkat.

Dari sisi hukum, perlindungan konsumen digital memiliki beberapa tujuan utama. Pertama, memberikan kepastian hukum bagi konsumen dan pelaku usaha. Kedua, menciptakan keadilan dalam transaksi digital. Ketiga, mencegah penyalahgunaan posisi dominan oleh pelaku usaha atau platform. Keempat, meningkatkan kepercayaan masyarakat terhadap ekosistem digital. Kelima, mendorong pertumbuhan ekonomi digital yang sehat dan bertanggung jawab.

Konsep perlindungan konsumen digital dapat dilihat melalui beberapa prinsip berikut.

1. **Prinsip informasi yang benar dan transparan**

   Konsumen berhak memperoleh informasi yang jelas mengenai produk, harga, biaya tambahan, kualitas barang, risiko layanan, garansi, dan kebijakan pengembalian. Informasi yang tidak jelas atau menyesatkan dapat merugikan konsumen.

2. **Prinsip keamanan transaksi**

   Sistem transaksi digital harus memberikan perlindungan terhadap pembayaran, data akun, riwayat transaksi, dan akses pengguna. Keamanan transaksi penting untuk mencegah pencurian akun, transaksi tidak sah, dan penipuan online.

3. **Prinsip pelindungan data pribadi**

   Data konsumen harus dikumpulkan dan digunakan secara sah, terbatas, dan bertanggung jawab. Pelaku usaha dan platform tidak boleh menggunakan data konsumen di luar tujuan yang telah disepakati.

4. **Prinsip tanggung jawab pelaku usaha**

   Pelaku usaha digital wajib menyerahkan barang atau jasa sesuai informasi yang diberikan. Jika terjadi kerugian karena kesalahan atau kelalaian pelaku usaha, konsumen berhak memperoleh penyelesaian.

5. **Prinsip akses terhadap pengaduan dan penyelesaian sengketa**

   Konsumen harus memiliki akses yang mudah untuk mengajukan komplain, meminta refund, mengajukan retur, atau menyelesaikan sengketa. Widjaja et al. (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun di luar pengadilan seperti mediasi, negosiasi, dan arbitrase.

6. **Prinsip keadilan dan keseimbangan para pihak**

   erlindungan konsumen digital tidak dimaksudkan untuk merugikan pelaku usaha, tetapi untuk menciptakan keseimbangan hak dan kewajiban. Rosid & Musadad (2025) menjelaskan bahwa penyelesaian sengketa e-commerce juga perlu memperhatikan perlindungan terhadap konsumen dan pelaku usaha.

7. **Prinsip akuntabilitas platform digital**

   Platform digital perlu bertanggung jawab dalam menyediakan sistem yang aman, kebijakan yang jelas, verifikasi pelaku usaha, serta mekanisme penanganan pengaduan. Platform tidak hanya menjadi tempat bertemunya penjual dan pembeli, tetapi juga bagian dari ekosistem perlindungan konsumen.

Tabel berikut menjelaskan unsur penting dalam konsep perlindungan konsumen digital.

Tabel 7.1: Unsur Perlindungan Konsumen Digital

Unsur Perlindungan	Penjelasan	Contoh dalam Transaksi Digital
Informasi yang benar	Konsumen memperoleh informasi jelas dan tidak menyesatkan	Deskripsi produk, harga, biaya pengiriman, garansi
Keamanan transaksi	Sistem melindungi pembayaran dan akses akun konsumen	OTP, autentikasi dua faktor, enkripsi pembayaran

Unsur Perlindungan	Penjelasan	Contoh dalam Transaksi Digital
Pelindungan data pribadi	Data konsumen digunakan secara sah dan terbatas	Nama, alamat, nomor telepon, riwayat transaksi
Tanggung jawab pelaku usaha	Pelaku usaha wajib memenuhi janji transaksi	Barang dikirim sesuai pesanan
Mekanisme pengaduan	Konsumen dapat menyampaikan keluhan	Fitur komplain, pusat bantuan, layanan pelanggan
Penyelesaian sengketa	Konsumen memiliki jalur penyelesaian kerugian	Refund, retur, mediasi, BPSK, gugatan perdata
Akuntabilitas platform	Platform menyediakan sistem yang aman dan adil	Verifikasi penjual, escrow, rating, moderasi toko

Perlindungan konsumen digital juga perlu memperhatikan karakteristik platform. Dalam marketplace, platform sering menjadi penghubung antara penjual dan pembeli. Dalam layanan dompet digital, platform menjadi penyimpan nilai uang elektronik. Dalam layanan transportasi online, platform menghubungkan konsumen dengan mitra pengemudi. Setiap jenis platform memiliki risiko dan bentuk perlindungan yang berbeda. Oleh karena itu, pengaturan perlindungan konsumen digital tidak dapat disamakan secara sederhana, tetapi harus melihat jenis layanan dan hubungan hukum yang terjadi.

Dalam e-commerce, misalnya, konsumen memerlukan perlindungan terhadap barang tidak sesuai, barang palsu, keterlambatan pengiriman, dan penjual yang tidak bertanggung jawab. Dalam dompet digital, konsumen memerlukan perlindungan terhadap saldo hilang, transaksi tidak sah, kegagalan sistem, dan pencurian akun. Dalam media sosial commerce, konsumen menghadapi risiko lebih besar karena transaksi sering dilakukan tanpa sistem perlindungan platform yang memadai. Dalam layanan digital berlangganan, konsumen perlu memperoleh kejelasan mengenai biaya, perpanjangan otomatis, pembatalan, dan penggunaan data.

Dengan demikian, konsep perlindungan konsumen digital harus dipahami sebagai perlindungan yang bersifat menyeluruh. Perlindungan ini mencakup

aspek informasi, transaksi, data pribadi, keamanan sistem, tanggung jawab pelaku usaha, akuntabilitas platform, serta penyelesaian sengketa. Perlindungan konsumen digital tidak hanya bertujuan menyelesaikan masalah setelah kerugian terjadi, tetapi juga mencegah terjadinya kerugian melalui transparansi, keamanan, literasi digital, dan tata kelola platform yang baik.

Pada akhirnya, perlindungan konsumen digital menjadi syarat penting bagi terbentuknya ekosistem ekonomi digital yang sehat. Jika konsumen merasa aman, percaya, dan terlindungi, maka transaksi digital akan berkembang dengan lebih baik. Sebaliknya, apabila konsumen sering dirugikan dan tidak memperoleh penyelesaian yang adil, maka kepercayaan terhadap layanan digital akan menurun. Oleh karena itu, perlindungan konsumen digital harus menjadi perhatian bersama antara pemerintah, pelaku usaha, platform digital, aparat penegak hukum, dan masyarakat.

7.2 Hak dan Kewajiban Konsumen dalam Transaksi Online

Transaksi online merupakan salah satu bentuk transaksi elektronik yang paling banyak dilakukan masyarakat pada era digital. Melalui transaksi online, konsumen dapat membeli barang, memesan jasa, membayar tagihan, menggunakan layanan transportasi, berlangganan aplikasi, membeli tiket, menggunakan dompet digital, hingga melakukan transaksi keuangan tanpa harus bertemu langsung dengan pelaku usaha. Kemudahan ini memberikan manfaat besar bagi konsumen, tetapi juga menimbulkan risiko hukum apabila hak dan kewajiban para pihak tidak dipahami dengan baik.

Dalam transaksi online, konsumen memiliki kedudukan sebagai pihak yang menggunakan barang atau jasa untuk kepentingan diri sendiri, keluarga, orang lain, atau makhluk hidup lain dan tidak untuk diperdagangkan kembali. Konsumen digital pada dasarnya tetap memiliki hak sebagaimana konsumen dalam transaksi konvensional. Perbedaannya terletak pada media transaksi, bentuk bukti, cara komunikasi, mekanisme pembayaran, dan peran platform digital sebagai perantara. Oleh karena itu, hak dan kewajiban konsumen dalam transaksi online perlu dipahami secara khusus agar konsumen dapat bertransaksi secara aman dan bertanggung jawab.

Gambar 7.2: Hak dan Kewajiban Konsumen dalam Transaksi Online

Hak konsumen dalam transaksi online berakar pada prinsip perlindungan konsumen. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menegaskan bahwa konsumen berhak memperoleh kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang dan/atau jasa. Konsumen juga berhak memperoleh informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa. Prinsip ini tetap berlaku dalam transaksi digital, baik transaksi dilakukan melalui marketplace, media sosial, website, maupun aplikasi mobile.

Hak pertama konsumen dalam transaksi online adalah hak atas informasi yang benar, jelas, dan jujur. Konsumen berhak mengetahui identitas pelaku usaha, deskripsi produk, harga, biaya tambahan, ongkos kirim, kondisi barang, garansi, kebijakan retur, kebijakan refund, dan waktu pengiriman. Informasi yang tidak jelas dapat menyebabkan konsumen salah mengambil keputusan. Misalnya, foto produk terlihat bagus, tetapi barang yang dikirim berbeda dari deskripsi. Dalam kondisi seperti ini, konsumen dapat menuntut penyelesaian karena informasi yang diberikan tidak sesuai dengan kenyataan.

Hak atas informasi juga mencakup informasi mengenai syarat dan ketentuan layanan. Dalam transaksi digital, konsumen sering diminta menyetujui terms and conditions sebelum menggunakan layanan. Syarat tersebut dapat mencakup aturan pembayaran, pembatalan transaksi, penggunaan data

pribadi, penyelesaian sengketa, serta batas tanggung jawab platform. Oleh karena itu, pelaku usaha dan platform digital harus menyusun syarat layanan secara jelas, mudah dipahami, dan tidak merugikan konsumen. OECD (2016) menekankan bahwa perlindungan konsumen dalam e-commerce harus mencakup transparansi informasi, praktik bisnis yang adil, dan penyelesaian sengketa yang efektif.

Hak kedua adalah hak atas keamanan dan keselamatan dalam transaksi. Konsumen berhak menggunakan sistem transaksi yang aman, terutama dalam pembayaran elektronik. Keamanan ini mencakup perlindungan terhadap pencurian akun, penyalahgunaan OTP, transaksi tidak sah, phishing, kebocoran data pembayaran, dan kegagalan sistem. Dalam transaksi online, keamanan tidak hanya berkaitan dengan barang yang dibeli, tetapi juga dengan sistem elektronik yang digunakan. Apabila sistem tidak aman dan menimbulkan kerugian, konsumen berhak meminta pertanggungjawaban sesuai hukum yang berlaku.

Hak ketiga adalah hak untuk menerima barang atau jasa sesuai dengan perjanjian. Dalam e-commerce, konsumen berhak menerima barang sesuai deskripsi, jumlah, kualitas, ukuran, warna, merek, dan kondisi yang dijanjikan. Jika barang tidak sesuai, cacat, rusak, atau tidak dikirim, konsumen berhak mengajukan komplain, meminta penggantian barang, refund, atau ganti rugi. Sugara dan Az-Zahra (2024) menjelaskan bahwa transaksi e-commerce merupakan bentuk perjanjian yang diatur dalam hukum perdata, sehingga pelaku usaha berkewajiban memenuhi prestasi sebagaimana telah disepakati dengan konsumen.

Hak keempat adalah hak atas pelindungan data pribadi. Dalam transaksi online, konsumen biasanya memberikan data seperti nama, alamat, nomor telepon, email, lokasi, nomor rekening, riwayat pembelian, dan data pembayaran. Data tersebut hanya boleh digunakan untuk tujuan yang sah dan sesuai dengan kebutuhan transaksi. Konsumen berhak mengetahui bagaimana datanya dikumpulkan, digunakan, disimpan, dan dibagikan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar bahwa pemrosesan data pribadi harus dilakukan secara sah, transparan, terbatas pada tujuan tertentu, dan disertai tanggung jawab pengendali data. OECD (2013) juga menekankan prinsip pembatasan pengumpulan data, pembatasan penggunaan, keamanan data, keterbukaan, dan akuntabilitas.

Hak kelima adalah hak untuk mengajukan pengaduan. Konsumen yang mengalami kerugian dalam transaksi online berhak menyampaikan keluhan kepada penjual, platform, penyedia layanan pembayaran, jasa ekspedisi, atau lembaga penyelesaian sengketa. Hak ini penting karena transaksi digital sering melibatkan lebih dari satu pihak. Misalnya, dalam transaksi marketplace, masalah dapat berasal dari penjual, sistem platform, jasa pengiriman, atau penyedia pembayaran. Oleh sebab itu, platform digital perlu menyediakan fitur pengaduan yang mudah diakses, transparan, dan memiliki batas waktu penyelesaian yang jelas.

Hak keenam adalah hak untuk memperoleh penyelesaian sengketa. Jika keluhan tidak selesai melalui komunikasi langsung atau fitur komplain platform, konsumen dapat menggunakan jalur penyelesaian sengketa. Penyelesaian dapat dilakukan melalui negosiasi, mediasi, Badan Penyelesaian Sengketa Konsumen, arbitrase, atau pengadilan. Widjaja et al. (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun melalui penyelesaian nonlitigasi seperti mediasi, negosiasi, dan arbitrase. Rosid & Musadad (2025) juga menekankan bahwa penyelesaian sengketa konsumen e-commerce di luar pengadilan penting untuk memberikan penyelesaian yang lebih cepat dan efisien.

Hak ketujuh adalah hak untuk memperoleh ganti rugi. Apabila konsumen mengalami kerugian karena barang tidak sesuai, layanan gagal, saldo hilang, transaksi tidak sah, atau kelalaian pelaku usaha, konsumen berhak menuntut ganti rugi. Bentuk ganti rugi dapat berupa pengembalian uang, penggantian barang, perbaikan layanan, kompensasi, atau pemulihan hak lainnya. Dalam transaksi digital, ganti rugi sering diberikan melalui refund, voucher, saldo pengganti, pengiriman ulang barang, atau pengembalian dana ke metode pembayaran awal.

Selain memiliki hak, konsumen dalam transaksi online juga memiliki kewajiban. Perlindungan konsumen tidak berarti konsumen bebas bertindak tanpa tanggung jawab. Konsumen tetap harus beritikad baik, membaca informasi produk, menggunakan sistem secara benar, membayar sesuai kesepakatan, dan tidak menyalahgunakan mekanisme pengaduan. Keseimbangan antara hak dan kewajiban diperlukan agar transaksi digital berjalan adil bagi semua pihak.

Kewajiban pertama konsumen adalah membaca dan memahami informasi produk atau layanan sebelum melakukan transaksi. Konsumen perlu memperhatikan deskripsi produk, harga, ukuran, warna, kondisi barang, ulasan, rating penjual, garansi, biaya pengiriman, estimasi waktu sampai, dan kebijakan retur. Banyak sengketa terjadi karena konsumen tidak membaca informasi secara cermat atau hanya melihat gambar tanpa memahami syarat transaksi. Oleh karena itu, konsumen wajib bersikap teliti sebelum menekan tombol beli atau setuju.

Kewajiban kedua adalah menggunakan data dan identitas secara benar. Konsumen harus memberikan informasi yang benar ketika melakukan transaksi, seperti nama, alamat pengiriman, nomor telepon, dan metode pembayaran. Kesalahan alamat atau nomor telepon dapat menyebabkan barang tidak sampai atau proses pengiriman terganggu. Konsumen juga tidak boleh menggunakan identitas palsu, akun orang lain tanpa izin, atau data pembayaran milik pihak lain. Dalam transaksi digital, keakuratan data sangat penting karena proses transaksi berjalan berdasarkan informasi elektronik.

Kewajiban ketiga adalah melakukan pembayaran sesuai kesepakatan. Jika konsumen telah melakukan pemesanan dan memilih metode pembayaran tertentu, maka konsumen wajib memenuhi pembayaran sesuai aturan yang berlaku. Dalam sistem cash on delivery, konsumen wajib membayar ketika barang diterima apabila barang sesuai dengan pesanan dan ketentuan transaksi. Sengketa COD sering muncul ketika konsumen menolak membayar tanpa alasan yang jelas atau melampiaskan ketidakpuasan kepada kurir. Padahal, kurir hanya bertugas mengantarkan barang dan bukan pihak yang membuat perjanjian jual beli dengan konsumen.

Kewajiban keempat adalah menggunakan layanan digital secara bertanggung jawab. Konsumen tidak boleh melakukan penyalahgunaan fitur platform, membuat komplain palsu, memanipulasi bukti transaksi, memberikan ulasan palsu, melakukan pembatalan sepihak secara merugikan, atau menyalahgunakan kebijakan refund. Jika konsumen melakukan tindakan tidak jujur, maka konsumen juga dapat dimintai pertanggungjawaban. Transaksi online harus dijalankan berdasarkan itikad baik dari kedua belah pihak.

Kewajiban kelima adalah menjaga keamanan akun pribadi. Konsumen wajib menjaga kerahasiaan password, PIN, OTP, kode verifikasi, dan akses

perangkat. Banyak kasus kerugian digital terjadi karena konsumen membagikan OTP kepada pihak lain, mengklik tautan palsu, menggunakan password lemah, atau melakukan transaksi di luar platform resmi. Meskipun pelaku usaha dan platform wajib menyediakan sistem yang aman, konsumen juga harus menjaga keamanan akunnya sendiri agar tidak disalahgunakan.

Kewajiban keenam adalah menyimpan bukti transaksi. Dalam transaksi online, bukti sangat penting apabila terjadi sengketa. Konsumen perlu menyimpan invoice, bukti pembayaran, nomor resi, tangkapan layar percakapan, deskripsi produk, email konfirmasi, dan riwayat transaksi. Bukti ini dapat digunakan untuk mengajukan komplain kepada platform atau sebagai alat bukti apabila sengketa dibawa ke lembaga penyelesaian sengketa. Anami et al. (2025) menjelaskan bahwa kontrak digital dan dokumen elektronik dapat menjadi dasar penting dalam melihat hubungan hukum para pihak.

Kewajiban ketujuh adalah mengikuti prosedur pengaduan yang tersedia. Konsumen yang mengalami kerugian sebaiknya tidak langsung menyebarkan tuduhan di media sosial tanpa bukti yang cukup. Langkah awal yang lebih tepat adalah menghubungi penjual, menggunakan fitur komplain platform, mengajukan permintaan refund atau retur, dan mengikuti prosedur resmi. Jika tidak selesai, konsumen dapat melanjutkan ke lembaga penyelesaian sengketa atau aparat hukum. Prosedur ini penting agar penyelesaian dilakukan secara tertib dan dapat dipertanggungjawabkan.

Tabel berikut merangkum hak dan kewajiban konsumen dalam transaksi online.

Tabel 7.2: Hak dan Kewajiban Konsumen dalam Transaksi Online

Hak Konsumen Digital	Kewajiban Konsumen Digital
Mendapatkan informasi yang benar, jelas, dan jujur	Membaca informasi produk dan syarat layanan secara teliti
Mendapatkan keamanan dalam transaksi online	Menjaga password, OTP, PIN, dan akses akun pribadi
Menerima barang atau jasa sesuai perjanjian	Memberikan data transaksi yang benar
Mendapat pelindungan data pribadi	Tidak menyalahgunakan data atau identitas pihak lain

Hak Konsumen Digital	Kewajiban Konsumen Digital
Mengajukan komplain atau pengaduan	Mengikuti prosedur pengaduan resmi
Memperoleh penyelesaian sengketa	Menyimpan bukti transaksi digital
Memperoleh ganti rugi jika dirugikan	Beritikad baik dalam melakukan transaksi

Hak dan kewajiban konsumen dalam transaksi online harus dilihat sebagai satu kesatuan. Konsumen yang memahami haknya akan lebih mampu melindungi diri dari penipuan, informasi menyesatkan, dan penyalahgunaan data. Sebaliknya, konsumen yang memahami kewajibannya akan lebih bertanggung jawab dalam menggunakan layanan digital. Dengan demikian, transaksi online tidak hanya bergantung pada regulasi, tetapi juga pada kesadaran hukum para pihak.

Dalam praktiknya, konsumen digital perlu menerapkan beberapa langkah kehati-hatian. Pertama, membeli barang melalui platform resmi atau penjual yang terpercaya. Kedua, memeriksa reputasi toko, ulasan pembeli, dan rating penjual. Ketiga, tidak mudah percaya pada harga yang terlalu murah atau promosi yang tidak masuk akal. Keempat, tidak memberikan OTP, password, atau PIN kepada siapa pun. Kelima, tidak melakukan pembayaran di luar sistem resmi platform jika berisiko. Keenam, menyimpan semua bukti transaksi. Ketujuh, segera melapor apabila terjadi transaksi mencurigakan.

Pelaku usaha dan platform digital juga perlu menghormati hak konsumen dengan menyediakan informasi yang benar, sistem pembayaran yang aman, kebijakan refund yang jelas, layanan pengaduan yang mudah diakses, serta pelindungan data pribadi. Perlindungan konsumen digital tidak akan berjalan efektif apabila hanya membebankan kehati-hatian kepada konsumen. Diperlukan tanggung jawab bersama antara konsumen, pelaku usaha, platform, pemerintah, dan aparat penegak hukum.

Dengan demikian, hak dan kewajiban konsumen dalam transaksi online merupakan dasar penting dalam menciptakan ekosistem digital yang aman dan adil. Konsumen berhak memperoleh informasi, keamanan, perlindungan data, penyelesaian sengketa, dan ganti rugi. Namun, konsumen juga wajib membaca informasi, memberikan data yang benar, membayar sesuai kesepakatan, menjaga keamanan akun, menyimpan bukti, dan

menggunakan layanan secara bertanggung jawab. Keseimbangan hak dan kewajiban ini menjadi fondasi utama perlindungan konsumen di era digital.

7.3 Tanggung Jawab Pelaku Usaha Digital

Pelaku usaha digital merupakan pihak yang menyediakan, menawarkan, menjual, atau mendistribusikan barang dan/atau jasa melalui media elektronik. Pelaku usaha digital dapat berupa penjual di marketplace, penyedia aplikasi, penyedia layanan dompet digital, penyedia layanan transportasi online, pengelola toko online, penyedia jasa digital, pengembang platform, maupun perusahaan yang menjalankan kegiatan usaha melalui sistem elektronik. Dalam era digital, pelaku usaha tidak hanya bertanggung jawab atas barang atau jasa yang ditawarkan, tetapi juga atas informasi, sistem transaksi, keamanan data, mekanisme pengaduan, dan perlindungan konsumen.

Tanggung jawab pelaku usaha digital menjadi penting karena hubungan antara konsumen dan pelaku usaha dalam transaksi online sering tidak berlangsung secara langsung. Konsumen tidak selalu dapat memeriksa kualitas barang, memastikan identitas penjual, atau menilai keandalan layanan sebelum melakukan transaksi. Oleh sebab itu, pelaku usaha digital harus memberikan informasi yang benar, jelas, jujur, dan tidak menyesatkan. Informasi tersebut meliputi identitas pelaku usaha, spesifikasi produk, harga, biaya tambahan, jaminan, garansi, metode pembayaran, waktu pengiriman, kebijakan retur, kebijakan refund, serta syarat penggunaan layanan.

Dalam hukum perlindungan konsumen, pelaku usaha memiliki kewajiban untuk beritikad baik dalam menjalankan kegiatan usahanya. Itikad baik berarti pelaku usaha tidak boleh menipu, menyembunyikan informasi penting, memanipulasi ulasan, menjual barang palsu, memberikan iklan menyesatkan, atau membuat syarat transaksi yang merugikan konsumen secara sepihak. Prinsip ini tetap berlaku dalam transaksi digital. Semakin kompleks sistem transaksi online, semakin besar pula kebutuhan terhadap tanggung jawab pelaku usaha agar konsumen tidak berada dalam posisi yang lemah.

Gambar 7.3: Tanggung Jawab Pelaku Usaha Digital

Tanggung jawab pertama pelaku usaha digital adalah memberikan informasi yang benar dan transparan. Informasi produk dalam transaksi online menjadi dasar bagi konsumen untuk mengambil keputusan. Apabila pelaku usaha menampilkan foto yang tidak sesuai, menyembunyikan cacat barang, memberikan deskripsi palsu, atau tidak menjelaskan risiko layanan, maka konsumen dapat dirugikan. OECD (2016) menegaskan bahwa perlindungan konsumen dalam e-commerce harus menjamin transparansi informasi, praktik bisnis yang adil, dan penyelesaian sengketa yang efektif. Dengan demikian, keterbukaan informasi merupakan syarat utama dalam transaksi digital.

Tanggung jawab kedua adalah menyerahkan barang atau jasa sesuai dengan perjanjian. Dalam transaksi online, pelaku usaha wajib mengirimkan barang sesuai pesanan konsumen, baik dari segi jenis, jumlah, kualitas, ukuran, warna, merek, maupun waktu pengiriman. Jika barang tidak dikirim, terlambat tanpa alasan jelas, cacat, palsu, atau berbeda dari deskripsi, maka pelaku usaha dapat dianggap melakukan wanprestasi. Sugara & Az-Zahra (2024) menjelaskan bahwa transaksi e-commerce merupakan bentuk perjanjian yang diatur dalam hukum perdata, sehingga pelaksanaannya dapat menimbulkan sengketa apabila salah satu pihak tidak memenuhi prestasi.

Tanggung jawab ketiga adalah menjamin keamanan transaksi. Pelaku usaha digital perlu memastikan bahwa proses transaksi dilakukan melalui sistem yang aman, terutama apabila pelaku usaha mengelola pembayaran, akun pengguna, data transaksi, atau informasi pembayaran. Keamanan transaksi

mencakup perlindungan terhadap akses tidak sah, pencurian akun, manipulasi pesanan, penyalahgunaan metode pembayaran, dan kegagalan sistem. Dalam layanan digital yang lebih kompleks, seperti dompet digital atau layanan keuangan berbasis aplikasi, tanggung jawab terhadap keamanan sistem menjadi semakin penting karena berhubungan langsung dengan dana konsumen.

Tanggung jawab keempat adalah melindungi data pribadi konsumen. Dalam transaksi digital, pelaku usaha biasanya mengumpulkan data seperti nama, alamat, nomor telepon, email, lokasi, riwayat pembelian, preferensi produk, dan informasi pembayaran. Data tersebut harus digunakan secara terbatas sesuai tujuan transaksi. Pelaku usaha tidak boleh menjual, menyebarkan, atau menggunakan data konsumen untuk kepentingan lain tanpa dasar yang sah. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan bahwa pemrosesan data pribadi harus dilakukan secara sah, transparan, terbatas, dan bertanggung jawab. OECD (2013) juga menekankan prinsip pembatasan pengumpulan data, pembatasan penggunaan, keamanan data, keterbukaan, dan akuntabilitas.

Tanggung jawab perlindungan data menjadi semakin penting karena banyak kasus kerugian digital berawal dari lemahnya keamanan sistem dan pengelolaan data. Kasus kebocoran data pengguna Tokopedia menunjukkan bahwa platform digital yang mengelola data konsumen memiliki tanggung jawab untuk menjaga keamanan data pengguna. Anindya & Subiyanto (2025) menjelaskan bahwa kebocoran data Tokopedia menimbulkan persoalan mengenai tanggung jawab platform berdasarkan Undang-Undang Pelindungan Data Pribadi. Hal ini menunjukkan bahwa pelaku usaha digital tidak cukup hanya menyediakan layanan, tetapi juga harus memastikan tata kelola data yang aman.

Tanggung jawab kelima adalah menyediakan mekanisme pengaduan. Pelaku usaha digital wajib memberikan akses kepada konsumen untuk menyampaikan keluhan apabila terjadi masalah dalam transaksi. Mekanisme pengaduan dapat berupa fitur komplain, layanan pelanggan, pusat bantuan, email resmi, call center, atau sistem tiket pengaduan. Mekanisme tersebut harus mudah digunakan, memiliki alur yang jelas, dan memberikan respons dalam waktu yang wajar. Jika pengaduan konsumen tidak ditangani secara baik, kepercayaan terhadap pelaku usaha dan platform digital dapat menurun.

Tanggung jawab keenam adalah memberikan penyelesaian apabila konsumen mengalami kerugian. Bentuk penyelesaian dapat berupa penggantian barang, perbaikan layanan, pengembalian dana, kompensasi, permintaan maaf, pemulihan akun, atau tindakan lain sesuai bentuk kerugian. Dalam e-commerce, penyelesaian yang umum diberikan adalah retur, refund, pengiriman ulang barang, atau pembatalan transaksi. Rosid & Musadad (2025) menjelaskan bahwa penyelesaian sengketa konsumen e-commerce di luar pengadilan penting karena dapat memberikan penyelesaian yang lebih cepat, sederhana, dan efisien.

Tanggung jawab ketujuh adalah tidak menyalahgunakan posisi dominan. Dalam platform digital, pelaku usaha atau penyedia platform sering memiliki posisi lebih kuat dibandingkan konsumen. Mereka menentukan syarat layanan, algoritma tampilan produk, sistem pembayaran, kebijakan refund, biaya layanan, dan akses akun. Posisi ini tidak boleh digunakan untuk merugikan konsumen. Kontrak baku digital yang dibuat sepihak harus tetap memperhatikan keadilan dan keseimbangan para pihak. United Nations (2015) menekankan bahwa perlindungan konsumen perlu menjamin perlakuan yang adil, akses informasi, penyelesaian sengketa, serta perlindungan terhadap praktik bisnis yang merugikan.

Tanggung jawab kedelapan adalah menjaga kejujuran dalam iklan dan promosi digital. Iklan digital memiliki pengaruh besar terhadap keputusan konsumen. Pelaku usaha tidak boleh menggunakan klaim palsu, testimoni fiktif, diskon menyesatkan, harga yang tidak transparan, foto produk yang tidak sesuai, atau promosi yang menyembunyikan syarat tertentu. Dalam transaksi online, konsumen sering bergantung pada iklan, ulasan, rating, dan rekomendasi platform. Oleh karena itu, pelaku usaha digital wajib memastikan bahwa promosi yang dibuat tidak menipu atau menyesatkan.

Tanggung jawab kesembilan adalah memastikan keaslian dan legalitas produk. Pelaku usaha digital tidak boleh menjual barang palsu, produk ilegal, produk bajakan, barang berbahaya, atau produk yang melanggar hak kekayaan intelektual. Dalam platform marketplace, penjual bertanggung jawab atas produk yang ditawarkan, sedangkan platform memiliki tanggung jawab untuk menyediakan mekanisme pengawasan, pelaporan, dan penghapusan produk yang melanggar hukum. Perlindungan konsumen digital juga berkaitan dengan perlindungan hak cipta, merek, keamanan produk, dan standar kualitas barang.

Tanggung jawab kesepuluh adalah melakukan edukasi kepada konsumen. Pelaku usaha digital dan platform perlu memberikan informasi edukatif mengenai cara bertransaksi aman, cara menggunakan fitur pengaduan, cara menjaga akun, risiko penipuan, pelindungan data pribadi, dan kebijakan layanan. Edukasi ini penting karena sebagian konsumen belum memahami risiko transaksi digital. Pelaku usaha yang bertanggung jawab tidak hanya mengejar keuntungan, tetapi juga membangun ekosistem transaksi yang aman dan dipercaya.

Dalam praktiknya, tanggung jawab pelaku usaha digital dapat dibedakan menjadi tanggung jawab kontraktual, tanggung jawab perdata, tanggung jawab administratif, tanggung jawab pidana, dan tanggung jawab etik. Tanggung jawab kontraktual muncul karena adanya perjanjian antara pelaku usaha dan konsumen. Tanggung jawab perdata muncul ketika konsumen mengalami kerugian akibat wanprestasi atau perbuatan melawan hukum. Tanggung jawab administratif dapat muncul apabila pelaku usaha melanggar ketentuan perizinan, perlindungan konsumen, atau penyelenggaraan sistem elektronik. Tanggung jawab pidana dapat muncul apabila terdapat penipuan, manipulasi sistem, penyalahgunaan data, atau tindakan melawan hukum lainnya. Sementara itu, tanggung jawab etik berkaitan dengan kejujuran, kepatutan, transparansi, dan penghormatan terhadap hak konsumen.

Tabel berikut merangkum bentuk tanggung jawab pelaku usaha digital.

Tabel 7.3: Bentuk Tanggung Jawab Pelaku Usaha Digital

Bentuk Tanggung Jawab	Penjelasan	Contoh Penerapan
Informasi produk	Memberikan informasi yang benar, jelas, dan tidak menyesatkan	Deskripsi barang, harga, garansi, biaya tambahan
Pemenuhan transaksi	Menyerahkan barang atau jasa sesuai perjanjian	Barang dikirim sesuai pesanan dan waktu yang dijanjikan
Keamanan transaksi	Menjaga sistem pembayaran dan akun konsumen	Autentikasi, enkripsi, pencegahan akses ilegal
Pelindungan data pribadi	Menggunakan data konsumen secara sah dan terbatas	Tidak menjual atau menyebarkan data tanpa dasar hukum

Bentuk Tanggung Jawab	Penjelasan	Contoh Penerapan
Pengaduan konsumen	Menyediakan saluran komplain yang mudah diakses	Pusat bantuan, call center, fitur pengaduan
Penyelesaian kerugian	Memberikan solusi apabila konsumen dirugikan	Refund, retur, kompensasi, pemulihan akun
Kejujuran promosi	Tidak membuat iklan menyesatkan	Diskon transparan, testimoni asli, klaim yang dapat dibuktikan
Legalitas produk	Tidak menjual barang ilegal atau palsu	Produk asli, tidak bajakan, sesuai standar keamanan

Dalam konteks marketplace, tanggung jawab pelaku usaha digital tidak hanya berada pada penjual, tetapi juga dapat melibatkan platform. Penjual bertanggung jawab atas kebenaran produk yang dijual, pengemasan, pengiriman, dan kesesuaian barang. Platform bertanggung jawab menyediakan sistem transaksi yang aman, fitur pengaduan, perlindungan pembayaran, verifikasi penjual, serta mekanisme penyelesaian sengketa. Oleh karena itu, tanggung jawab dalam ekosistem digital bersifat berlapis. Jika terjadi kerugian, perlu dianalisis apakah kerugian berasal dari kesalahan penjual, kelalaian platform, masalah jasa pengiriman, atau kesalahan konsumen.

Tanggung jawab pelaku usaha digital juga berkaitan dengan prinsip akuntabilitas. Akuntabilitas berarti pelaku usaha harus dapat menjelaskan dan mempertanggungjawabkan tindakannya. Misalnya, jika terjadi kegagalan transaksi, pelaku usaha harus mampu menunjukkan riwayat transaksi, status pesanan, bukti pengiriman, dan alasan penolakan refund. Jika terjadi insiden data, pelaku usaha harus mampu menjelaskan penyebab, dampak, langkah pemulihan, dan pemberitahuan kepada konsumen. Tanpa akuntabilitas, konsumen akan kesulitan memperoleh perlindungan.

Pelaku usaha digital yang bertanggung jawab akan memperkuat kepercayaan konsumen. Kepercayaan merupakan modal utama dalam transaksi digital karena konsumen sering melakukan pembayaran sebelum menerima barang atau layanan. Jika pelaku usaha sering mengabaikan komplain, menyembunyikan informasi, atau tidak bertanggung jawab atas kerugian, maka reputasinya akan menurun. Sebaliknya, pelaku usaha yang transparan, responsif, dan adil akan lebih dipercaya konsumen.

Dengan demikian, tanggung jawab pelaku usaha digital merupakan unsur utama dalam perlindungan konsumen di era digital. Pelaku usaha wajib memberikan informasi yang benar, memenuhi transaksi, menjaga keamanan sistem, melindungi data pribadi, menyediakan mekanisme pengaduan, menyelesaikan kerugian, menjaga kejujuran promosi, dan memastikan legalitas produk. Tanggung jawab tersebut tidak hanya bersumber dari hukum, tetapi juga dari etika bisnis digital. Semakin besar peran pelaku usaha dalam ekosistem digital, semakin besar pula tanggung jawabnya untuk menciptakan transaksi yang aman, adil, transparan, dan dapat dipercaya.

7.4 Iklan Digital, Promosi, dan Informasi Menyesatkan

Iklan digital dan promosi online merupakan bagian penting dari aktivitas bisnis di era digital. Pelaku usaha menggunakan berbagai media untuk memperkenalkan produk dan jasa kepada konsumen, seperti marketplace, media sosial, website, aplikasi mobile, mesin pencari, influencer, email marketing, video pendek, live shopping, dan iklan berbayar. Melalui iklan digital, informasi mengenai produk dapat tersebar dengan cepat, murah, luas, dan terarah kepada kelompok konsumen tertentu.

Namun, perkembangan iklan digital juga menimbulkan persoalan hukum baru. Tidak semua informasi yang disampaikan dalam iklan digital bersifat benar, jelas, dan jujur. Dalam praktiknya, masih banyak ditemukan iklan yang melebih-lebihkan manfaat produk, menyembunyikan risiko, menggunakan foto yang tidak sesuai, menampilkan harga yang tidak transparan, memakai testimoni palsu, atau membuat promosi yang seolah-olah menguntungkan padahal memiliki syarat tertentu yang merugikan konsumen. Kondisi ini menempatkan konsumen digital pada posisi rentan karena keputusan transaksi sering diambil berdasarkan informasi yang ditampilkan secara online.

Dalam hukum perlindungan konsumen, informasi merupakan unsur utama dalam transaksi. Konsumen hanya dapat mengambil keputusan secara tepat apabila memperoleh informasi yang benar. Oleh karena itu, iklan digital tidak boleh hanya dipahami sebagai alat pemasaran, tetapi juga sebagai bentuk komunikasi hukum antara pelaku usaha dan konsumen. Informasi yang disampaikan melalui iklan, promosi, deskripsi produk, ulasan, dan tampilan platform dapat memengaruhi hubungan hukum antara para pihak.

Gambar 7.4: Iklan Digital yang Jujur vs Iklan Digital Menyesatkan

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menegaskan bahwa konsumen berhak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa. Prinsip ini berlaku pula dalam iklan digital. Pelaku usaha tidak boleh menyampaikan informasi yang dapat menyesatkan konsumen mengenai kualitas, manfaat, harga, ukuran, komposisi, garansi, asal produk, ketersediaan barang, atau syarat promosi. OECD (2016) juga menekankan bahwa perlindungan konsumen dalam e-commerce harus mencakup praktik bisnis yang adil, transparansi informasi, serta perlindungan dari informasi yang menyesatkan.

7.4.1 Bentuk Iklan Digital yang Berpotensi Menyesatkan

Iklan digital dapat dikatakan menyesatkan apabila informasi yang disampaikan tidak sesuai dengan fakta, tidak lengkap, sulit dipahami, atau sengaja dirancang untuk memengaruhi konsumen secara tidak adil. Dalam transaksi online, informasi menyesatkan tidak selalu berbentuk kebohongan langsung. Kadang, informasi tersebut muncul karena pelaku usaha menyembunyikan fakta penting atau menampilkan informasi secara berlebihan.

Beberapa bentuk iklan digital yang berpotensi menyesatkan antara lain sebagai berikut.

1. **Foto produk tidak sesuai dengan barang asli**

   Pelaku usaha menampilkan foto produk yang terlihat lebih bagus daripada barang sebenarnya. Misalnya, warna, ukuran, bahan, atau kualitas produk berbeda jauh dari yang diterima konsumen.

2. **Deskripsi produk tidak lengkap atau tidak benar**

   Informasi mengenai bahan, ukuran, fungsi, kondisi barang, masa berlaku, atau kompatibilitas produk tidak dijelaskan dengan benar. Hal ini dapat membuat konsumen membeli barang yang tidak sesuai kebutuhan.

3. **Harga promosi tidak transparan**

   Iklan menampilkan harga murah, tetapi setelah konsumen melakukan transaksi muncul biaya tambahan, biaya layanan, pajak, ongkos kirim tinggi, atau syarat tertentu yang sebelumnya tidak dijelaskan.

4. **Diskon palsu atau manipulatif**

   Pelaku usaha menaikkan harga terlebih dahulu lalu memberikan diskon besar agar produk terlihat lebih murah. Praktik ini dapat menyesatkan konsumen karena harga promosi tidak mencerminkan pengurangan harga yang sebenarnya.

5. **Testimoni dan ulasan palsu**

   Pelaku usaha menggunakan ulasan buatan, komentar palsu, rating tidak asli, atau testimoni dari orang yang tidak pernah memakai produk. Hal ini dapat menciptakan kepercayaan palsu terhadap kualitas produk.

6. **Klaim manfaat yang berlebihan**

   Produk diklaim dapat memberikan hasil tertentu secara cepat, pasti, atau luar biasa tanpa bukti yang dapat dipertanggungjawabkan. Contohnya klaim "pasti sembuh", "langsung putih", "100% aman", atau "hasil permanen" tanpa dasar yang jelas.

7. **Promosi dengan syarat tersembunyi**

   Iklan menyatakan "gratis", "cashback", "beli satu gratis satu", atau "diskon besar", tetapi syaratnya tersembunyi, sulit ditemukan, atau baru diketahui setelah konsumen melakukan transaksi.

8. **Penggunaan influencer tanpa keterbukaan sponsor**

   Promosi dilakukan oleh influencer seolah-olah sebagai pengalaman pribadi, padahal merupakan kerja sama berbayar. Jika hubungan komersial tidak dijelaskan, konsumen dapat menganggap ulasan tersebut sebagai pendapat objektif.

9. **Iklan yang menyerupai informasi netral**

   Pelaku usaha membuat konten promosi seolah-olah berupa artikel edukasi, berita, rekomendasi ahli, atau ulasan independen. Praktik ini dapat mengaburkan batas antara informasi dan iklan.

10. **Informasi ketersediaan barang yang tidak benar**

    Platform atau penjual menampilkan keterangan "stok terbatas" atau "hampir habis" untuk mendorong konsumen segera membeli, padahal informasi tersebut tidak sesuai dengan kondisi sebenarnya.

Bentuk-bentuk iklan menyesatkan tersebut dapat menimbulkan kerugian bagi konsumen. Kerugian tidak hanya berupa kehilangan uang, tetapi juga dapat berupa kekecewaan, kerugian waktu, risiko kesehatan, risiko keamanan, serta hilangnya kepercayaan terhadap transaksi digital.

7.4.2 Hubungan Iklan Digital dengan Keputusan Konsumen

Dalam transaksi digital, konsumen sering tidak melihat barang secara langsung. Konsumen hanya bergantung pada informasi yang disediakan oleh pelaku usaha dan platform. Informasi tersebut dapat berupa foto, video, deskripsi, rating, ulasan, jumlah produk terjual, rekomendasi algoritma, dan promosi. Oleh karena itu, kualitas informasi sangat menentukan keputusan konsumen.

Jika informasi yang diberikan akurat, konsumen dapat memilih produk dengan lebih tepat. Sebaliknya, jika informasi tersebut salah atau menyesatkan, konsumen dapat mengambil keputusan yang merugikan dirinya. Misalnya, konsumen membeli produk elektronik karena iklan menyatakan produk tersebut memiliki kapasitas tertentu, tetapi setelah diterima spesifikasinya berbeda. Dalam situasi ini, konsumen dapat mengajukan komplain karena barang tidak sesuai informasi yang dijanjikan.

Sugara & Az-Zahra (2024) menjelaskan bahwa transaksi e-commerce merupakan bentuk perjanjian yang diatur dalam hukum perdata dan sering

menimbulkan masalah apabila pelaksanaannya merugikan konsumen. Dalam konteks iklan digital, informasi yang ditampilkan sebelum transaksi dapat menjadi bagian penting dari kesepakatan. Apabila pelaku usaha menjanjikan kualitas tertentu dalam iklan, maka pelaku usaha harus bertanggung jawab apabila barang atau jasa tidak sesuai dengan informasi tersebut.

Iklan digital juga dapat memanfaatkan psikologi konsumen. Contohnya, penggunaan kalimat "hanya hari ini", "stok tinggal satu", "promo berakhir dalam 10 menit", atau "ribuan orang sudah membeli" dapat mendorong konsumen mengambil keputusan secara cepat. Strategi tersebut tidak selalu melanggar hukum. Namun, apabila informasi yang digunakan tidak benar atau sengaja dimanipulasi, maka strategi tersebut dapat menjadi praktik yang menyesatkan.

7.4.3 Tanggung Jawab Pelaku Usaha dan Platform

Pelaku usaha digital bertanggung jawab memastikan bahwa semua iklan, promosi, dan informasi produk yang ditampilkan kepada konsumen bersifat benar, jelas, jujur, dan tidak menyesatkan. Tanggung jawab ini meliputi informasi yang dibuat sendiri oleh pelaku usaha maupun informasi yang disampaikan melalui pihak lain, seperti influencer, afiliasi, atau agen pemasaran.

Tanggung jawab pelaku usaha dalam iklan digital mencakup beberapa hal berikut.

1. **Memastikan kebenaran informasi produk**

   Semua klaim mengenai kualitas, fungsi, manfaat, bahan, ukuran, garansi, dan harga harus dapat dibuktikan.

2. **Menampilkan harga secara jelas**

   Harga produk, biaya layanan, pajak, ongkos kirim, dan biaya tambahan perlu dijelaskan agar konsumen tidak tertipu oleh harga awal yang tampak murah.

3. **Menjelaskan syarat promosi secara terbuka**

   Diskon, cashback, kupon, bundling, atau gratis ongkir harus disertai syarat dan ketentuan yang mudah ditemukan dan mudah dipahami.

4. **Tidak menggunakan testimoni palsu**

   Ulasan, rating, atau testimoni harus berasal dari pengalaman yang benar dan tidak dimanipulasi.

5. **Membedakan iklan dan konten biasa**

   Jika konten merupakan promosi berbayar, maka perlu diberi keterangan yang jelas agar konsumen tidak menganggapnya sebagai informasi netral.

6. **Memberikan mekanisme koreksi**

   Jika terdapat kesalahan informasi, pelaku usaha harus segera memperbaiki iklan, memberi pemberitahuan, dan menyelesaikan kerugian konsumen.

Platform digital juga memiliki peran penting. Dalam marketplace, platform sering menjadi tempat bertemunya konsumen dan penjual. Platform menyediakan ruang iklan, sistem pencarian, sistem rekomendasi, rating, ulasan, dan fitur promosi. Oleh karena itu, platform perlu memiliki kebijakan untuk mencegah iklan palsu, promosi menyesatkan, produk ilegal, dan ulasan palsu. Platform juga perlu menyediakan fitur pelaporan agar konsumen dapat melaporkan iklan atau produk yang mencurigakan.

Tanggung jawab platform tidak selalu sama dengan tanggung jawab penjual. Penjual bertanggung jawab atas kebenaran informasi produk yang ditawarkan, sedangkan platform bertanggung jawab atas sistem, kebijakan, moderasi, dan mekanisme pengaduan. Namun, apabila platform mengetahui adanya praktik menyesatkan tetapi membiarkannya, maka platform dapat dinilai tidak menjalankan tanggung jawabnya secara memadai.

7.4.4 Perlindungan Konsumen dari Informasi Menyesatkan

Perlindungan konsumen dari informasi menyesatkan dapat dilakukan melalui pendekatan preventif dan represif. Pendekatan preventif dilakukan sebelum kerugian terjadi, sedangkan pendekatan represif dilakukan setelah konsumen mengalami kerugian.

Pendekatan preventif dapat dilakukan melalui kewajiban transparansi informasi, pengawasan iklan, edukasi konsumen, verifikasi penjual, moderasi konten promosi, dan standar penayangan iklan. Pelaku usaha harus memastikan iklan yang dibuat tidak menimbulkan pemahaman keliru.

Platform juga harus menyediakan sistem pelaporan dan menindak iklan yang terbukti melanggar.

Pendekatan represif dilakukan apabila konsumen telah mengalami kerugian. Konsumen dapat mengajukan komplain kepada penjual atau platform, meminta refund, retur, penggantian barang, atau kompensasi. Jika tidak selesai, konsumen dapat menempuh penyelesaian melalui Badan Penyelesaian Sengketa Konsumen, mediasi, arbitrase, atau pengadilan. Widjaja et al. (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun di luar pengadilan seperti mediasi, negosiasi, dan arbitrase.

Dalam praktiknya, konsumen perlu menyimpan bukti iklan atau promosi yang menyesatkan. Bukti tersebut dapat berupa tangkapan layar iklan, deskripsi produk, harga promosi, syarat promosi, percakapan dengan penjual, invoice, bukti pembayaran, bukti penerimaan barang, dan rekaman halaman produk. Bukti ini penting karena iklan digital dapat berubah atau dihapus sewaktu-waktu.

Tabel berikut merangkum bentuk informasi menyesatkan dan contoh dampaknya bagi konsumen.

Tabel 7.4: Bentuk Informasi Menyesatkan dalam Iklan Digital

Bentuk Informasi Menyesatkan	Contoh Praktik	Dampak bagi Konsumen
Foto produk tidak sesuai	Foto terlihat premium, barang asli berkualitas rendah	Konsumen menerima barang tidak sesuai harapan
Diskon palsu	Harga dinaikkan dahulu lalu diberi diskon besar	Konsumen merasa mendapat harga murah padahal tidak
Syarat promosi tersembunyi	Cashback berlaku hanya dengan syarat tertentu yang tidak jelas	Konsumen gagal memperoleh manfaat promosi
Testimoni palsu	Ulasan dibuat oleh akun palsu atau buzzer	Konsumen percaya pada kualitas yang tidak nyata
Klaim manfaat berlebihan	Produk diklaim pasti berhasil tanpa bukti	Konsumen membeli berdasarkan harapan yang keliru
Harga tidak transparan	Biaya tambahan muncul setelah checkout	Konsumen membayar lebih dari perkiraan

Bentuk Informasi Menyesatkan	Contoh Praktik	Dampak bagi Konsumen
Iklan influencer tidak terbuka	Promosi berbayar tidak diberi keterangan sponsor	Konsumen mengira ulasan bersifat objektif
Stok terbatas palsu	Keterangan "hampir habis" tidak sesuai fakta	Konsumen terdorong membeli secara tergesa-gesa

Dari tabel tersebut dapat dilihat bahwa informasi menyesatkan tidak selalu berbentuk penipuan yang terang-terangan. Informasi yang tidak lengkap, tidak jelas, atau sengaja dibuat ambigu juga dapat merugikan konsumen. Oleh karena itu, pelaku usaha digital perlu berhati-hati dalam menyusun materi iklan.

Konsumen juga perlu memiliki sikap kritis terhadap iklan digital. Konsumen sebaiknya tidak langsung percaya pada klaim yang terlalu berlebihan, harga yang terlalu murah, promosi yang terlalu mendesak, atau testimoni yang tampak tidak wajar. Konsumen perlu membandingkan informasi dari beberapa sumber, membaca ulasan negatif, memeriksa reputasi toko, memahami syarat promosi, dan menyimpan bukti transaksi.

Dalam konteks hukum teknologi informasi, iklan digital dan informasi menyesatkan menunjukkan bahwa perlindungan konsumen tidak hanya berkaitan dengan proses setelah transaksi, tetapi juga sebelum transaksi. Informasi yang salah pada tahap awal dapat menjadi penyebab utama terjadinya sengketa. Oleh sebab itu, kejujuran informasi merupakan dasar penting dalam transaksi digital.

Dengan demikian, iklan digital, promosi, dan informasi menyesatkan merupakan isu penting dalam perlindungan konsumen di era digital. Pelaku usaha wajib memastikan iklan yang dibuat benar, jelas, jujur, dan dapat dipertanggungjawabkan. Platform digital perlu menyediakan sistem pengawasan, pelaporan, dan penanganan iklan yang merugikan konsumen. Konsumen juga perlu bersikap kritis dan menyimpan bukti apabila menemukan informasi yang tidak sesuai. Jika ketiga pihak tersebut menjalankan perannya, maka transaksi digital dapat berlangsung lebih aman, transparan, dan adil.

7.5 Penyelesaian Sengketa Konsumen Digital

Penyelesaian sengketa konsumen digital merupakan proses untuk menyelesaikan perselisihan yang terjadi antara konsumen, pelaku usaha, platform digital, penyedia layanan pembayaran, jasa pengiriman, atau penyelenggara sistem elektronik lainnya. Sengketa ini dapat muncul karena transaksi dilakukan melalui sistem elektronik, sehingga hubungan antara para pihak sering berlangsung tanpa pertemuan langsung. Konsumen membeli barang atau menggunakan layanan berdasarkan informasi digital, bukti elektronik, sistem pembayaran, dan mekanisme yang disediakan oleh platform.

Gambar 7.5: Alur Penyelesaian Sengketa Konsumen Digital

Dalam transaksi digital, sengketa dapat terjadi dalam berbagai bentuk, seperti barang tidak dikirim, barang tidak sesuai deskripsi, keterlambatan pengiriman, penolakan refund, saldo digital hilang, akun diblokir, transaksi tidak dikenal, penyalahgunaan data pribadi, layanan tidak sesuai janji, promosi menyesatkan, atau kegagalan sistem. Sengketa tersebut dapat menimbulkan kerugian finansial, kerugian waktu, hilangnya akses layanan, rusaknya reputasi, atau ketidaknyamanan bagi konsumen.

Penyelesaian sengketa konsumen digital penting karena kepercayaan merupakan dasar utama transaksi online. Konsumen bersedia melakukan pembayaran karena percaya bahwa barang atau jasa akan diterima sesuai perjanjian. Pelaku usaha juga percaya bahwa konsumen akan memenuhi

kewajibannya. Platform digital menyediakan sistem yang mempertemukan para pihak. Apabila sengketa tidak diselesaikan dengan baik, kepercayaan terhadap ekosistem digital dapat menurun.

Secara hukum, penyelesaian sengketa konsumen digital di Indonesia berkaitan dengan Undang-Undang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Perdata, serta aturan mengenai penyelenggaraan sistem dan transaksi elektronik. Widjaja et al. (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun di luar pengadilan, seperti mediasi, negosiasi, dan arbitrase. Dengan demikian, penyelesaian sengketa digital tidak selalu harus langsung dibawa ke pengadilan.

Penyelesaian sengketa konsumen digital perlu dilakukan secara bertahap. Langkah penyelesaian yang baik dimulai dari mekanisme yang paling sederhana, seperti komplain kepada penjual atau platform. Jika tidak selesai, konsumen dapat menggunakan jalur mediasi, Badan Penyelesaian Sengketa Konsumen, arbitrase, atau pengadilan. Dalam kondisi tertentu, apabila terdapat unsur penipuan, akses ilegal, penyalahgunaan data, atau tindak pidana lain, konsumen juga dapat membuat laporan kepada aparat penegak hukum.

7.5.1 Bentuk Sengketa Konsumen Digital

Sengketa konsumen digital dapat diklasifikasikan berdasarkan sumber masalahnya. Pengelompokan ini penting agar penyelesaian dapat diarahkan pada pihak yang tepat dan dasar hukum yang sesuai.

1. **Sengketa barang tidak sesuai pesanan**

   Sengketa ini terjadi ketika barang yang diterima konsumen berbeda dari deskripsi, foto, ukuran, warna, merek, spesifikasi, atau kondisi yang dijanjikan. Contohnya, konsumen membeli sepatu ukuran tertentu, tetapi barang yang dikirim berbeda ukuran atau kualitasnya tidak sesuai.

2. **Sengketa barang tidak dikirim**

   Sengketa ini terjadi ketika konsumen sudah melakukan pembayaran, tetapi pelaku usaha tidak mengirim barang. Kasus ini dapat berupa wanprestasi apabila penjual gagal memenuhi kewajibannya, atau dapat berkembang menjadi penipuan apabila sejak awal terdapat niat untuk merugikan konsumen.

3. Sengketa keterlambatan pengiriman

Sengketa ini terjadi ketika barang dikirim melewati waktu yang dijanjikan. Keterlambatan dapat berasal dari penjual, jasa pengiriman, sistem platform, atau keadaan tertentu di luar kendali para pihak. Analisis perlu melihat siapa yang bertanggung jawab atas keterlambatan tersebut.

4. Sengketa refund dan retur

Sengketa ini muncul ketika konsumen meminta pengembalian dana atau pengembalian barang, tetapi permintaan tersebut ditolak atau tidak diproses dengan jelas. Masalah refund sering terjadi karena perbedaan tafsir terhadap syarat dan ketentuan platform.

5. Sengketa pembayaran digital

Sengketa pembayaran digital dapat berupa saldo hilang, pembayaran gagal tetapi saldo terpotong, transaksi ganda, transaksi tidak dikenal, atau pengembalian dana yang tidak masuk ke akun konsumen. Anami et al. (2025) menunjukkan bahwa sengketa saldo DANA menggambarkan pentingnya perlindungan hukum dalam kontrak digital dan layanan pembayaran elektronik.

6. Sengketa cash on delivery

Transaksi COD dapat menimbulkan sengketa ketika konsumen menolak membayar, menolak menerima barang, atau menyalahkan kurir atas masalah yang sebenarnya berasal dari penjual atau platform. Rosid & Musadad (2025) menjelaskan bahwa sistem COD dalam e-commerce dapat menimbulkan sengketa dan membutuhkan penyelesaian yang memperhatikan konsumen maupun pelaku usaha.

7. Sengketa data pribadi konsumen

Sengketa ini muncul ketika data konsumen digunakan tanpa izin, disebarkan, dijual, atau bocor akibat lemahnya sistem keamanan. Dalam transaksi digital, data pribadi merupakan bagian penting dari perlindungan konsumen karena konsumen menyerahkan data untuk kebutuhan transaksi.

8. **Sengketa iklan dan informasi menyesatkan**

   Sengketa ini terjadi ketika konsumen membeli barang atau jasa karena terpengaruh iklan yang tidak benar, testimoni palsu, diskon manipulatif, klaim berlebihan, atau informasi produk yang tidak lengkap. Dalam kasus ini, bukti iklan dan deskripsi produk menjadi penting.

7.5.2 Tahapan Penyelesaian Sengketa Konsumen Digital

Penyelesaian sengketa konsumen digital sebaiknya dilakukan secara bertahap agar masalah dapat diselesaikan secara efektif, cepat, dan proporsional. Tahapan ini juga membantu konsumen menentukan langkah yang tepat sebelum membawa sengketa ke lembaga penyelesaian atau pengadilan.

1. **Mengidentifikasi masalah**

   Konsumen perlu memahami jenis masalah yang terjadi. Apakah barang tidak sesuai, pembayaran gagal, refund tidak diproses, saldo hilang, atau data pribadi disalahgunakan. Identifikasi ini penting untuk menentukan pihak yang harus dihubungi.

2. **Mengumpulkan bukti digital**

   Konsumen harus menyimpan bukti transaksi, seperti invoice, bukti pembayaran, nomor pesanan, resi pengiriman, tangkapan layar iklan, deskripsi produk, percakapan dengan penjual, email konfirmasi, dan riwayat transaksi. Bukti digital penting karena transaksi online sering tidak memiliki bukti fisik.

3. **Menghubungi penjual atau penyedia layanan**

   Langkah awal yang dapat dilakukan adalah menghubungi penjual, pelaku usaha, atau penyedia layanan secara langsung. Pada tahap ini, konsumen dapat meminta klarifikasi, penggantian barang, refund, atau solusi lain.

4. **Menggunakan fitur komplain platform**

   Jika transaksi dilakukan melalui marketplace atau aplikasi, konsumen sebaiknya menggunakan fitur pengaduan resmi. Fitur ini penting karena platform dapat menahan pembayaran, memediasi penjual dan pembeli, memeriksa bukti, atau memberikan keputusan berdasarkan kebijakan layanan.

5. **Melakukan negosiasi atau mediasi**

   Jika komplain belum selesai, para pihak dapat melakukan negosiasi atau mediasi. Negosiasi dilakukan langsung oleh para pihak, sedangkan mediasi melibatkan pihak ketiga sebagai penengah. Penyelesaian ini lebih cepat dan murah dibandingkan pengadilan.

6. **Mengajukan sengketa ke BPSK atau lembaga terkait**

   Konsumen dapat membawa sengketa ke Badan Penyelesaian Sengketa Konsumen apabila sengketa berkaitan dengan kerugian konsumen. Selain itu, sengketa tertentu dapat dilaporkan kepada lembaga pengawas sesuai sektor, misalnya layanan keuangan digital kepada otoritas yang berwenang.

7. **Menggunakan arbitrase atau penyelesaian alternatif lainnya**

   Dalam beberapa transaksi digital, syarat layanan dapat memuat klausul penyelesaian melalui arbitrase atau lembaga penyelesaian sengketa alternatif. Penyelesaian ini dapat digunakan apabila para pihak menyepakatinya.

8. **Mengajukan gugatan ke pengadilan**

   Apabila sengketa tidak dapat diselesaikan melalui jalur nonlitigasi, konsumen dapat mengajukan gugatan perdata ke pengadilan. Gugatan dapat didasarkan pada wanprestasi atau perbuatan melawan hukum.

9. **Melaporkan unsur pidana jika ada**

   Apabila terdapat indikasi penipuan, pemalsuan identitas, akses ilegal, pencurian data, atau tindak pidana siber, konsumen dapat membuat laporan kepada aparat penegak hukum. Namun, perlu dibedakan antara sengketa perdata biasa dan tindak pidana.

7.5.3 Jalur Penyelesaian Sengketa

Penyelesaian sengketa konsumen digital dapat dilakukan melalui dua jalur utama, yaitu nonlitigasi dan litigasi.

Penyelesaian nonlitigasi

Penyelesaian nonlitigasi adalah penyelesaian sengketa di luar pengadilan. Jalur ini biasanya lebih cepat, sederhana, dan hemat biaya. Bentuk penyelesaian nonlitigasi meliputi:

- negosiasi antara konsumen dan pelaku usaha;
- mediasi melalui platform atau pihak ketiga;
- konsiliasi;
- penyelesaian melalui Badan Penyelesaian Sengketa Konsumen;
- arbitrase;
- mekanisme pengaduan internal platform;
- penyelesaian melalui lembaga pengawas sektor terkait.

Rosid & Musadad (2025) menekankan bahwa penyelesaian sengketa e-commerce di luar pengadilan penting karena dapat memberikan penyelesaian yang lebih cepat dan efisien. Dalam transaksi digital yang bernilai kecil atau menengah, penyelesaian nonlitigasi sering lebih sesuai dibandingkan langsung membawa perkara ke pengadilan.

Penyelesaian litigasi

Penyelesaian litigasi dilakukan melalui pengadilan. Jalur ini biasanya digunakan apabila sengketa tidak selesai melalui mekanisme internal platform atau nonlitigasi. Konsumen dapat mengajukan gugatan perdata berdasarkan wanprestasi atau perbuatan melawan hukum. Jika kerugian dialami oleh banyak konsumen, dapat dipertimbangkan gugatan perwakilan kelompok sesuai ketentuan hukum acara yang berlaku.

Widjaja et al. (2018) menjelaskan bahwa Pasal 38 UU ITE memberikan ruang bagi setiap orang untuk mengajukan gugatan terhadap pihak yang menyelenggarakan sistem elektronik atau menggunakan teknologi informasi yang menimbulkan kerugian. Pasal 39 UU ITE juga membuka kemungkinan penyelesaian melalui arbitrase atau lembaga penyelesaian sengketa alternatif lainnya.

7.5.4 Peran Bukti Digital dalam Penyelesaian Sengketa

Bukti digital memiliki peran sangat penting dalam penyelesaian sengketa konsumen digital. Dalam transaksi online, banyak peristiwa hukum terjadi melalui sistem elektronik. Oleh karena itu, bukti yang digunakan juga banyak berbentuk elektronik.

Bukti digital yang perlu disimpan konsumen antara lain:

- invoice atau bukti pesanan;
- bukti pembayaran;
- nomor resi pengiriman;
- tangkapan layar iklan atau promosi;
- deskripsi produk;
- percakapan dengan penjual atau layanan pelanggan;
- email atau notifikasi transaksi;
- riwayat transaksi dalam aplikasi;
- bukti barang yang diterima;
- rekaman pengaduan atau nomor tiket komplain.

Bukti digital harus disimpan sejak awal karena informasi dalam platform dapat berubah, dihapus, atau tidak dapat diakses kembali. Misalnya, penjual dapat mengubah deskripsi produk setelah transaksi, menghapus iklan, atau menghapus percakapan. Oleh sebab itu, konsumen perlu segera mengambil tangkapan layar dan menyimpan dokumen transaksi.

Dalam penyelesaian sengketa, bukti digital membantu menjawab beberapa pertanyaan penting, yaitu:

- apakah transaksi benar terjadi;
- siapa para pihak yang terlibat;
- apa yang diperjanjikan;
- apakah barang atau jasa sesuai dengan informasi awal;
- apakah pembayaran telah dilakukan;
- apakah konsumen telah mengajukan komplain;
- apakah pelaku usaha telah merespons;
- apakah konsumen benar-benar mengalami kerugian.

7.5.5 Tanggung Jawab Para Pihak dalam Penyelesaian Sengketa

Penyelesaian sengketa konsumen digital tidak hanya menjadi tanggung jawab konsumen. Pelaku usaha, platform digital, jasa pengiriman, penyedia pembayaran, dan pemerintah juga memiliki peran masing-masing.

Konsumen

Konsumen bertanggung jawab menyampaikan keluhan secara jelas, menyimpan bukti transaksi, mengikuti prosedur pengaduan, dan tidak membuat tuduhan tanpa dasar.

Pelaku usaha

Pelaku usaha bertanggung jawab merespons pengaduan, memberikan penjelasan, memperbaiki kesalahan, serta memberikan refund, retur, atau ganti rugi apabila terbukti merugikan konsumen.

Platform digital

Platform bertanggung jawab menyediakan sistem pengaduan, memediasi penjual dan pembeli, menjaga keamanan transaksi, serta menindak pelaku usaha yang melanggar aturan.

Jasa pengiriman

Jasa pengiriman bertanggung jawab terhadap proses pengantaran barang, terutama apabila terjadi kehilangan, kerusakan, atau keterlambatan yang berasal dari proses pengiriman.

Penyedia pembayaran digital

Penyedia pembayaran bertanggung jawab terhadap keamanan pembayaran, kejelasan status transaksi, dan penanganan masalah seperti saldo terpotong, transaksi gagal, atau transaksi tidak dikenal.

Pemerintah dan lembaga pengawas

Pemerintah bertanggung jawab membentuk regulasi, melakukan pengawasan, menyediakan lembaga penyelesaian sengketa, dan menindak pelanggaran yang merugikan konsumen.

Tabel berikut merangkum jalur penyelesaian sengketa konsumen digital.

Tabel 7.5: Jalur Penyelesaian Sengketa Konsumen Digital

Jalur Penyelesaian	Contoh Penggunaan	Kelebihan	Keterbatasan
Komplain ke penjual	Barang tidak sesuai, keterlambatan, retur	Cepat dan langsung	Bergantung pada itikad baik penjual
Fitur pengaduan platform	Sengketa marketplace, refund, COD	Tersedia dalam aplikasi dan mudah diakses	Terikat kebijakan platform

Jalur Penyelesaian	Contoh Penggunaan	Kelebihan	Keterbatasan
Negosiasi	Kesepakatan penggantian barang atau refund	Fleksibel dan murah	Tidak selalu menghasilkan kesepakatan
Mediasi	Sengketa antara konsumen dan pelaku usaha	Ada pihak ketiga yang membantu	Hasil bergantung pada kesediaan para pihak
BPSK	Sengketa konsumen dengan pelaku usaha	Khusus perlindungan konsumen	Tidak semua sengketa digital mudah dibuktikan
Arbitrase	Sengketa dengan klausul arbitrase	Lebih cepat daripada pengadilan	Perlu kesepakatan para pihak
Gugatan perdata	Kerugian besar atau sengketa tidak selesai	Putusan memiliki kekuatan hukum	Membutuhkan waktu dan biaya
Laporan pidana	Penipuan online, pencurian data, akses ilegal	Menangani unsur kejahatan	Tidak otomatis memulihkan kerugian perdata

Penyelesaian sengketa konsumen digital yang baik harus memenuhi beberapa prinsip. Pertama, mudah diakses oleh konsumen. Kedua, cepat dan tidak berbelit-belit. Ketiga, transparan dalam proses dan hasil. Keempat, adil bagi konsumen dan pelaku usaha. Kelima, berbasis bukti digital. Keenam, mampu memberikan pemulihan yang nyata, seperti refund, retur, penggantian barang, kompensasi, atau pemulihan akun.

Dalam praktiknya, banyak sengketa digital dapat selesai pada tahap awal apabila pelaku usaha dan platform memiliki sistem pengaduan yang baik. Misalnya, marketplace dapat menyelesaikan sengketa dengan menahan dana pembayaran sampai barang diterima konsumen. Jika barang tidak sesuai, platform dapat memfasilitasi retur dan refund. Sistem seperti ini membantu mengurangi kebutuhan konsumen untuk membawa sengketa ke lembaga eksternal.

Namun, tidak semua sengketa dapat selesai melalui platform. Dalam kasus yang melibatkan nilai kerugian besar, data pribadi, sistem pembayaran, atau unsur pidana, konsumen mungkin perlu menggunakan jalur hukum lebih lanjut. Oleh karena itu, konsumen perlu memahami haknya, menyimpan bukti, dan memilih jalur penyelesaian yang sesuai dengan jenis sengketa.

Dengan demikian, penyelesaian sengketa konsumen digital merupakan bagian penting dari perlindungan konsumen di era digital. Sengketa dapat terjadi karena barang tidak sesuai, pembayaran gagal, saldo hilang, iklan menyesatkan, penyalahgunaan data, atau kegagalan layanan platform. Penyelesaian dapat dilakukan melalui komplain internal, negosiasi, mediasi, BPSK, arbitrase, pengadilan, atau laporan pidana apabila terdapat unsur kejahatan. Penyelesaian yang cepat, adil, transparan, dan berbasis bukti digital akan memperkuat kepercayaan masyarakat terhadap transaksi online dan ekosistem ekonomi digital.

7.6 Tantangan Perlindungan Konsumen pada Platform Digital

Platform digital telah menjadi bagian penting dalam kehidupan masyarakat modern. Melalui platform digital, konsumen dapat membeli barang, menggunakan layanan transportasi, memesan makanan, melakukan pembayaran, berinvestasi, belajar, bekerja, berkomunikasi, hingga memperoleh hiburan. Platform digital memberikan kemudahan karena transaksi dapat dilakukan secara cepat, praktis, dan tanpa batas ruang. Namun, di balik kemudahan tersebut, perlindungan konsumen menghadapi tantangan yang semakin kompleks.

Platform digital tidak hanya mempertemukan konsumen dan pelaku usaha, tetapi juga mengatur sistem transaksi, metode pembayaran, pengumpulan data, algoritma rekomendasi, iklan, ulasan, promosi, pengaduan, dan penyelesaian sengketa. Oleh karena itu, posisi platform digital sangat strategis. Platform dapat membantu melindungi konsumen, tetapi juga dapat menjadi sumber persoalan apabila sistemnya tidak transparan, tidak aman, atau tidak bertanggung jawab.

Tantangan perlindungan konsumen pada platform digital muncul karena hubungan hukum dalam ekosistem digital tidak selalu sederhana. Dalam transaksi konvensional, hubungan biasanya hanya terjadi antara konsumen dan penjual. Dalam transaksi platform digital, hubungan dapat melibatkan banyak pihak, seperti konsumen, penjual, platform, penyedia pembayaran, jasa pengiriman, penyedia iklan, influencer, penyedia data, dan pihak ketiga lainnya. Banyaknya pihak yang terlibat membuat tanggung jawab hukum sering menjadi tidak jelas.

Gambar 7.6: Tantangan Perlindungan Konsumen pada Platform Digital

7.6.1 Ketidakjelasan Tanggung Jawab Platform

Tantangan pertama adalah ketidakjelasan tanggung jawab platform. Dalam banyak kasus, platform menyatakan dirinya hanya sebagai perantara antara penjual dan pembeli. Akibatnya, ketika terjadi sengketa, konsumen sering diarahkan untuk menyelesaikan masalah langsung dengan penjual. Padahal, platform juga berperan menyediakan sistem transaksi, menampilkan produk, mengatur pembayaran, memfasilitasi komunikasi, dan membuat kebijakan pengembalian dana.

Ketidakjelasan ini dapat merugikan konsumen. Misalnya, konsumen membeli barang melalui marketplace, tetapi barang tidak dikirim atau tidak sesuai pesanan. Penjual sulit dihubungi, sedangkan platform menyatakan bahwa tanggung jawab utama berada pada penjual. Dalam kondisi seperti ini, konsumen membutuhkan kepastian mengenai siapa yang bertanggung jawab dan mekanisme apa yang dapat digunakan untuk memulihkan kerugiannya.

Anindya & Subiyanto (2025) menjelaskan bahwa kasus kebocoran data Tokopedia menunjukkan pentingnya tanggung jawab platform dalam menjaga data pengguna. Meskipun platform menyediakan layanan digital, platform tetap memiliki tanggung jawab terhadap keamanan sistem dan perlindungan konsumen. Dengan demikian, platform digital tidak dapat

sepenuhnya melepaskan diri dari tanggung jawab hanya dengan menyatakan dirinya sebagai perantara.

7.6.2 Ketimpangan Posisi antara Konsumen dan Platform

Tantangan kedua adalah ketimpangan posisi antara konsumen dan platform. Platform digital biasanya memiliki kendali atas syarat dan ketentuan layanan, sistem pembayaran, fitur pengaduan, kebijakan refund, algoritma pencarian, serta akses terhadap akun pengguna. Konsumen hanya memiliki pilihan untuk menyetujui syarat layanan atau tidak menggunakan platform tersebut.

Dalam praktiknya, syarat dan ketentuan digital sering berbentuk kontrak baku yang panjang, rumit, dan jarang dibaca oleh konsumen. Konsumen hanya menekan tombol "setuju" tanpa memahami seluruh konsekuensi hukum. Hal ini dapat menimbulkan masalah apabila terdapat klausul yang membatasi hak konsumen, mempersempit tanggung jawab platform, atau menyulitkan konsumen mengajukan sengketa. Anami et al., (2025) menjelaskan bahwa kontrak digital memang dapat mengikat para pihak, tetapi perlindungan hukum dalam praktiknya masih memerlukan penguatan.

Ketimpangan posisi juga terlihat ketika konsumen mengalami masalah akun, saldo, atau transaksi. Platform memiliki akses terhadap data dan sistem, sedangkan konsumen hanya memiliki bukti terbatas seperti tangkapan layar, invoice, atau riwayat transaksi. Jika platform tidak transparan, konsumen akan kesulitan membuktikan kerugian yang dialaminya.

7.6.3 Risiko Iklan dan Informasi Menyesatkan

Tantangan ketiga adalah maraknya iklan digital dan informasi menyesatkan. Platform digital menjadi ruang promosi yang sangat luas. Pelaku usaha dapat menampilkan foto produk, deskripsi, diskon, rating, ulasan, testimoni, video promosi, dan live shopping. Informasi tersebut sangat memengaruhi keputusan konsumen.

Masalah muncul ketika informasi yang ditampilkan tidak benar, tidak lengkap, atau sengaja dibuat menyesatkan. Konsumen dapat tertarik membeli barang karena foto produk terlihat menarik, diskon terlihat besar, atau testimoni tampak meyakinkan. Namun, barang yang diterima ternyata berbeda, kualitas rendah, atau tidak sesuai klaim. (OECD, 2016)

menekankan bahwa perlindungan konsumen dalam e-commerce harus mencakup transparansi informasi, praktik bisnis yang adil, dan pencegahan informasi menyesatkan.

Platform digital memiliki tantangan besar dalam mengawasi iklan dan promosi. Jumlah penjual dan produk yang sangat banyak membuat pengawasan sulit dilakukan secara manual. Selain itu, promosi dapat dilakukan melalui influencer, afiliasi, dan konten kreator yang tidak selalu secara jelas menyatakan bahwa konten tersebut adalah iklan berbayar. Akibatnya, konsumen dapat mengira promosi sebagai ulasan objektif.

7.6.4 Pelindungan data pribadi Konsumen

Tantangan keempat adalah pelindungan data pribadi. Platform digital mengumpulkan banyak data konsumen, seperti nama, alamat, nomor telepon, email, lokasi, riwayat transaksi, preferensi belanja, metode pembayaran, dan perilaku penggunaan aplikasi. Data tersebut digunakan untuk menjalankan layanan, memberikan rekomendasi, menargetkan iklan, meningkatkan sistem, dan menganalisis perilaku konsumen.

Pengumpulan data dalam jumlah besar menimbulkan risiko hukum dan etika. Data dapat disalahgunakan, dijual, bocor, atau digunakan untuk tujuan yang tidak diketahui konsumen. OECD (2013) menekankan pentingnya pembatasan pengumpulan data, pembatasan penggunaan, keamanan, keterbukaan, dan akuntabilitas dalam perlindungan privasi. Solove (2008) juga menjelaskan bahwa privasi berkaitan dengan kemampuan individu untuk mengendalikan informasi tentang dirinya.

Dalam konteks Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan dasar bahwa pemrosesan data pribadi harus dilakukan secara sah, transparan, terbatas pada tujuan tertentu, dan bertanggung jawab. Namun, tantangan utamanya adalah bagaimana memastikan platform benar-benar menerapkan prinsip tersebut dalam praktik. Konsumen sering tidak mengetahui data apa yang dikumpulkan, untuk tujuan apa data digunakan, berapa lama data disimpan, dan kepada siapa data dibagikan.

7.6.5 Keamanan Transaksi dan Risiko Kejahatan Siber

Tantangan kelima adalah keamanan transaksi. Platform digital menjadi target kejahatan siber karena menyimpan data, uang elektronik, akun pengguna, dan informasi transaksi. Risiko yang sering terjadi antara lain phishing, pencurian OTP, pengambilalihan akun, transaksi tidak sah, penipuan toko online, tautan palsu, dan penyalahgunaan metode pembayaran.

Habibi & Liviani (2020) menjelaskan bahwa kejahatan teknologi informasi memiliki karakter yang berbeda dari kejahatan konvensional karena dapat dilakukan secara cepat, lintas wilayah, dan menggunakan identitas anonim. Dalam transaksi platform digital, kejahatan tersebut dapat merugikan konsumen secara langsung. Misalnya, konsumen tertipu tautan palsu yang menyerupai halaman resmi platform, memasukkan OTP, lalu saldo atau akun diambil alih.

Keamanan transaksi tidak hanya menjadi tanggung jawab konsumen. Platform harus menyediakan sistem keamanan yang memadai, seperti autentikasi dua faktor, enkripsi, deteksi transaksi mencurigakan, notifikasi keamanan, pembatasan akses, dan edukasi pengguna. Jika platform lalai menjaga keamanan sistem, konsumen dapat mengalami kerugian yang sulit dipulihkan.

7.6.6 Kesulitan Pembuktian Digital

Tantangan keenam adalah kesulitan pembuktian digital. Dalam sengketa platform digital, bukti sering berbentuk elektronik, seperti tangkapan layar, invoice, riwayat transaksi, log akses, email, chat, notifikasi aplikasi, dan metadata. Bukti digital dapat berubah, terhapus, atau tidak mudah diakses kembali. Hal ini membuat konsumen perlu segera menyimpan bukti sejak awal.

Aini & Lubis (2024) menjelaskan bahwa pembuktian dalam kasus kejahatan siber menghadapi tantangan karena bukti digital bersifat mudah berubah, pelaku dapat anonim, dan proses pembuktian membutuhkan keahlian teknis. Dalam sengketa konsumen digital, tantangan serupa juga muncul. Konsumen sering hanya memiliki bukti tampilan aplikasi, sedangkan data teknis lengkap berada di tangan platform.

Kesulitan pembuktian juga terjadi ketika platform tidak memberikan transparansi mengenai log transaksi, alasan pemblokiran akun, status refund, atau hasil investigasi internal. Konsumen dapat merasa dirugikan, tetapi tidak memiliki akses terhadap data yang cukup untuk membuktikan klaimnya. Oleh karena itu, platform perlu menyediakan mekanisme pembuktian yang adil dan dapat diaudit.

7.6.7 Mekanisme Pengaduan yang Belum Efektif

Tantangan ketujuh adalah mekanisme pengaduan yang belum selalu efektif. Banyak platform memang menyediakan fitur pusat bantuan atau layanan pelanggan, tetapi prosesnya sering lambat, otomatis, sulit dipahami, atau tidak memberikan solusi yang jelas. Konsumen sering hanya menerima jawaban template tanpa penjelasan rinci mengenai penyelesaian masalah.

Mekanisme pengaduan yang tidak efektif dapat memperburuk kerugian konsumen. Misalnya, konsumen mengalami saldo hilang atau transaksi tidak dikenal, tetapi respons platform lambat. Dalam kasus lain, konsumen meminta refund karena barang tidak sesuai, tetapi pengaduannya ditutup tanpa pemeriksaan memadai. Kondisi ini menunjukkan bahwa perlindungan konsumen tidak cukup hanya menyediakan fitur pengaduan, tetapi juga membutuhkan prosedur yang adil, cepat, transparan, dan responsif.

Widjaja et al. (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun di luar pengadilan. Namun, dalam praktik platform digital, penyelesaian internal platform sering menjadi jalur pertama. Karena itu, mekanisme internal tersebut harus dirancang dengan baik agar tidak justru menjadi hambatan bagi konsumen.

7.6.8 Tantangan Lintas Wilayah dan Yurisdiksi

Tantangan kedelapan adalah sifat platform digital yang sering melampaui batas wilayah. Konsumen dapat membeli barang dari penjual di luar kota atau luar negeri. Platform juga dapat berbasis di negara lain, menggunakan server di luar wilayah Indonesia, atau melibatkan pihak ketiga dari berbagai yurisdiksi. Hal ini menimbulkan pertanyaan mengenai hukum mana yang berlaku dan lembaga mana yang berwenang menyelesaikan sengketa.

Junior et al. (2021) menjelaskan bahwa transaksi e-commerce dapat menimbulkan persoalan apabila melibatkan pihak dari negara berbeda,

sehingga perlu ditentukan aturan hukum yang digunakan untuk menyelesaikan masalah. Tantangan yurisdiksi ini penting karena konsumen sering tidak memahami bahwa transaksi digital dapat melibatkan hukum lintas wilayah.

Dalam transaksi lintas batas, konsumen dapat kesulitan mengajukan komplain, meminta refund, atau menuntut pelaku usaha. Perbedaan bahasa, mata uang, hukum, dan lokasi pelaku usaha dapat membuat penyelesaian sengketa menjadi lebih rumit. Oleh karena itu, perlindungan konsumen digital membutuhkan kerja sama antarnegara dan standar perlindungan yang lebih kuat.

7.6.9 Algoritma, Personalisasi, dan Risiko Manipulasi Konsumen

Tantangan kesembilan adalah penggunaan algoritma dan personalisasi. Platform digital menggunakan algoritma untuk menampilkan produk, menentukan rekomendasi, mengatur harga, menampilkan iklan, dan memengaruhi urutan pencarian. Algoritma dapat membantu konsumen menemukan produk yang relevan, tetapi juga dapat menimbulkan risiko manipulasi.

Konsumen mungkin tidak menyadari bahwa produk yang muncul di halaman utama bukan selalu produk terbaik, melainkan produk yang diprioritaskan karena iklan, popularitas, histori pencarian, atau kepentingan komersial platform. Personalisasi harga dan promosi juga dapat membuat konsumen melihat harga berbeda berdasarkan perilaku digitalnya. Jika tidak transparan, algoritma dapat memperlemah posisi konsumen.

Tantangan ini menunjukkan bahwa perlindungan konsumen digital tidak hanya berkaitan dengan penjual dan produk, tetapi juga dengan cara platform merancang sistem. Platform perlu memastikan bahwa algoritma tidak merugikan konsumen, tidak menyembunyikan informasi penting, dan tidak mendorong keputusan transaksi secara manipulatif.

7.6.10 Rendahnya Literasi Konsumen Digital

Tantangan kesepuluh adalah rendahnya literasi konsumen digital. Banyak konsumen belum memahami risiko transaksi online, cara memeriksa keaslian toko, bahaya tautan palsu, pentingnya menjaga OTP, cara membaca

syarat promosi, atau langkah menyimpan bukti transaksi. Rendahnya literasi membuat konsumen lebih mudah menjadi korban penipuan, iklan menyesatkan, atau penyalahgunaan data.

Literasi konsumen digital mencakup kemampuan memahami hak dan kewajiban, membaca informasi produk, memeriksa reputasi penjual, menjaga keamanan akun, memahami kebijakan refund, dan menggunakan jalur pengaduan. United Nations (2015) menekankan bahwa perlindungan konsumen tidak hanya membutuhkan regulasi, tetapi juga pendidikan konsumen agar masyarakat dapat mengambil keputusan secara sadar dan bertanggung jawab.

Tabel berikut merangkum tantangan perlindungan konsumen pada platform digital.

Tabel 7.6: Tantangan Perlindungan Konsumen pada Platform Digital

Tantangan	Bentuk Permasalahan	Dampak bagi Konsumen
Ketidakjelasan tanggung jawab platform	Platform mengaku hanya sebagai perantara	Konsumen sulit menentukan pihak yang bertanggung jawab
Kontrak baku digital	Syarat layanan panjang dan sulit dipahami	Konsumen menyetujui klausul tanpa memahami risikonya
Iklan menyesatkan	Diskon palsu, testimoni palsu, foto tidak sesuai	Konsumen membeli berdasarkan informasi keliru
Pelindungan data pribadi	Data dikumpulkan, digunakan, atau dibagikan tanpa transparansi	Risiko kebocoran data dan penyalahgunaan identitas
Keamanan transaksi	Phishing, pencurian OTP, transaksi tidak sah	Kerugian finansial dan kehilangan akses akun
Pembuktian digital	Bukti berubah, hilang, atau berada di tangan platform	Konsumen sulit membuktikan kerugian
Pengaduan tidak efektif	Respons lambat, otomatis, atau tidak jelas	Sengketa tidak segera selesai
Yurisdiksi lintas wilayah	Penjual atau platform berada di wilayah berbeda	Penyelesaian sengketa menjadi lebih rumit
Algoritma dan personalisasi	Rekomendasi atau harga tidak transparan	Konsumen dapat diarahkan secara manipulatif
Literasi digital rendah	Konsumen tidak memahami risiko dan prosedur	Konsumen lebih rentan menjadi korban

Untuk menghadapi tantangan tersebut, perlindungan konsumen pada platform digital perlu diperkuat melalui beberapa langkah. Pertama, memperjelas tanggung jawab platform dalam regulasi dan kebijakan

layanan. Kedua, mewajibkan transparansi informasi, iklan, algoritma, dan syarat promosi. Ketiga, memperkuat pelindungan data pribadi dan keamanan transaksi. Keempat, menyediakan mekanisme pengaduan yang cepat, adil, dan mudah diakses. Kelima, meningkatkan literasi konsumen digital melalui edukasi berkelanjutan.

Platform digital juga perlu menerapkan prinsip akuntabilitas. Artinya, platform harus dapat menjelaskan bagaimana sistem bekerja, bagaimana data diproses, bagaimana komplain ditangani, dan bagaimana keputusan terhadap sengketa dibuat. Akuntabilitas penting agar konsumen tidak merasa berhadapan dengan sistem yang tertutup dan tidak dapat dipertanyakan.

Pemerintah memiliki peran penting dalam pengawasan. Regulasi perlu memastikan bahwa platform tidak hanya mengejar pertumbuhan bisnis, tetapi juga melindungi konsumen. Pengawasan dapat dilakukan terhadap iklan menyesatkan, keamanan data, praktik penjualan ilegal, sistem pengaduan, dan klausul baku yang merugikan konsumen. Selain itu, kerja sama antara pemerintah, platform, pelaku usaha, lembaga konsumen, dan masyarakat diperlukan untuk membangun ekosistem digital yang sehat.

Konsumen juga perlu berperan aktif. Konsumen harus membaca informasi produk, memahami syarat layanan, menjaga data pribadi, tidak membagikan OTP, memeriksa reputasi penjual, menyimpan bukti transaksi, dan menggunakan jalur pengaduan resmi. Perlindungan hukum akan lebih efektif apabila konsumen memiliki kesadaran dan literasi yang memadai.

Dengan demikian, tantangan perlindungan konsumen pada platform digital bersifat multidimensi. Tantangan tersebut meliputi tanggung jawab platform, ketimpangan posisi konsumen, iklan menyesatkan, pelindungan data pribadi, keamanan transaksi, pembuktian digital, pengaduan, yurisdiksi lintas wilayah, algoritma, dan literasi digital. Perlindungan konsumen digital tidak cukup hanya dilakukan melalui aturan hukum, tetapi juga memerlukan tata kelola platform yang baik, penegakan hukum yang efektif, edukasi masyarakat, serta tanggung jawab bersama seluruh pihak dalam ekosistem digital.

Bab 8
Kejahatan Siber dan Aspek Hukumnya

8.1 Pengertian dan Karakteristik Kejahatan Siber

Perkembangan teknologi informasi telah mengubah cara manusia berkomunikasi, bekerja, belajar, bertransaksi, dan mengakses layanan publik. Internet, komputer, telepon pintar, sistem cloud, media sosial, dompet digital, marketplace, mobile banking, dan berbagai aplikasi digital telah menjadi bagian penting dalam kehidupan masyarakat modern. Namun, perkembangan tersebut tidak hanya membawa kemudahan, tetapi juga melahirkan bentuk-bentuk penyalahgunaan baru. Penyalahgunaan teknologi informasi inilah yang kemudian dikenal sebagai kejahatan siber atau *cybercrime*.

Gambar 8.1: Konsep dan Karakteristik Kejahatan Siber

8.1.1 Pengertian Kejahatan Siber

Kejahatan siber dapat dipahami sebagai setiap perbuatan melawan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, internet, sistem elektronik, atau perangkat digital, baik sebagai alat untuk

melakukan kejahatan maupun sebagai sasaran kejahatan. Dalam pengertian ini, teknologi dapat berperan dalam dua posisi. Pertama, teknologi menjadi objek atau sasaran kejahatan, misalnya peretasan sistem, pencurian data, penyebaran malware, serangan terhadap server, atau gangguan terhadap layanan digital. Kedua, teknologi menjadi sarana untuk melakukan kejahatan, misalnya penipuan online, pemerasan digital, pencemaran nama baik melalui media sosial, penyebaran konten ilegal, atau manipulasi transaksi elektronik (UNODC, 2013).

Kejahatan siber tidak dapat dipahami hanya sebagai tindakan merusak komputer. Kejahatan siber mencakup berbagai tindakan yang dilakukan melalui ruang digital dan menimbulkan kerugian bagi individu, organisasi, perusahaan, pemerintah, maupun masyarakat luas. Bentuk kerugian yang ditimbulkan dapat berupa kerugian ekonomi, kehilangan data, gangguan layanan, pencurian identitas, pelanggaran privasi, rusaknya reputasi, hingga ancaman terhadap keamanan nasional. Oleh karena itu, kejahatan siber perlu dipandang sebagai persoalan hukum, teknologi, ekonomi, sosial, dan keamanan secara sekaligus.

Secara internasional, Convention on Cybercrime atau Budapest Convention menempatkan beberapa tindakan sebagai tindak pidana yang berkaitan dengan sistem komputer, seperti akses ilegal, penyadapan ilegal, gangguan data, gangguan sistem, penyalahgunaan perangkat, pemalsuan berbasis komputer, dan penipuan berbasis komputer (Council of Europe, 2001). Kerangka tersebut menunjukkan bahwa kejahatan siber tidak hanya berkaitan dengan konten yang disebarkan di internet, tetapi juga berkaitan dengan serangan terhadap kerahasiaan, integritas, dan ketersediaan data serta sistem komputer.

Dalam konteks Indonesia, kejahatan siber berkaitan erat dengan Undang-Undang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024. Pengaturan tersebut menjadi dasar penting dalam menilai perbuatan seperti akses ilegal, intersepsi ilegal, manipulasi informasi elektronik, gangguan terhadap sistem elektronik, penyebaran konten melanggar hukum, serta penyalahgunaan informasi dan transaksi elektronik (Republik Indonesia, 2024b).

Selain UU ITE, kejahatan siber juga berkaitan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Hal ini karena banyak kejahatan siber dilakukan melalui pencurian, pengumpulan, pengungkapan, penggunaan, atau penyalahgunaan data pribadi secara tidak sah. Data pribadi yang bocor dapat digunakan untuk penipuan, pinjaman online ilegal, pengambilalihan akun, pemalsuan identitas, pemerasan, dan kejahatan lanjutan lainnya. Oleh sebab itu, pelindungan data pribadi menjadi bagian penting dalam pencegahan dan penanganan kejahatan siber (Republik Indonesia, 2022b).

Dalam kajian hukum teknologi informasi, kejahatan siber sering dibedakan menjadi dua kelompok besar, yaitu *cyber-dependent crime* dan *cyber-enabled crime*. *Cyber-dependent crime* adalah kejahatan yang hanya dapat dilakukan dengan teknologi informasi, seperti peretasan, penyebaran malware, serangan ransomware, pencurian database, dan serangan *distributed denial of service* atau DDoS. Sementara itu, *cyber-enabled crime* adalah kejahatan konvensional yang diperluas, dipercepat, atau dipermudah oleh teknologi digital, seperti penipuan online, pemerasan, perjudian online, perdagangan ilegal, ujaran kebencian, dan penyebaran konten melanggar hukum (UNODC, 2013).

Dengan demikian, kejahatan siber adalah bentuk kejahatan yang lahir dari penyalahgunaan teknologi informasi. Kejahatan ini dapat menyerang sistem elektronik secara langsung, tetapi juga dapat menggunakan sistem elektronik sebagai media untuk melakukan kejahatan terhadap manusia, organisasi, atau masyarakat. Pemahaman ini penting karena penanganan kejahatan siber tidak cukup hanya menggunakan pendekatan hukum pidana konvensional, tetapi juga memerlukan pemahaman tentang sistem elektronik, bukti digital, keamanan informasi, perlindungan data, dan kerja sama lintas lembaga.

8.1.2 Karakteristik Kejahatan Siber

Kejahatan siber memiliki karakteristik yang berbeda dari kejahatan konvensional. Perbedaan ini menyebabkan proses pencegahan, penyelidikan, pembuktian, dan penegakan hukumnya membutuhkan pendekatan khusus. Dalam kejahatan konvensional, pelaku dan korban sering berada pada ruang fisik yang sama atau setidaknya dapat dilacak melalui bukti fisik. Sebaliknya, dalam kejahatan siber, pelaku dapat berada

di lokasi yang jauh, menggunakan identitas palsu, memanfaatkan server luar negeri, dan meninggalkan jejak dalam bentuk data elektronik.

Karakteristik pertama adalah bersifat lintas batas wilayah. Kejahatan siber dapat dilakukan dari satu negara, menggunakan infrastruktur digital di negara lain, dan menargetkan korban di negara berbeda. Kondisi ini menimbulkan persoalan yurisdiksi karena aparat penegak hukum harus menentukan hukum negara mana yang berlaku, lembaga mana yang berwenang, serta bagaimana mekanisme kerja sama internasional dilakukan. Oleh karena itu, penanganan kejahatan siber sering membutuhkan koordinasi antara aparat penegak hukum, penyedia layanan internet, platform digital, lembaga keuangan, dan otoritas lintas negara (Council of Europe, 2001).

Karakteristik kedua adalah tidak selalu terlihat secara fisik. Dalam kejahatan konvensional, kerugian sering tampak secara langsung, seperti barang hilang, bangunan rusak, atau korban mengalami luka. Dalam kejahatan siber, kerugian dapat terjadi tanpa kontak fisik antara pelaku dan korban. Contohnya adalah pencurian data, pengambilalihan akun, pembobolan saldo digital, pemalsuan identitas, atau penyebaran informasi palsu. Meskipun tidak tampak secara fisik, dampaknya dapat sangat besar karena dapat menyebar cepat dan menjangkau banyak korban.

Karakteristik ketiga adalah penggunaan identitas digital yang mudah disamarkan. Pelaku kejahatan siber dapat menggunakan akun palsu, email sementara, VPN, proxy, bot, identitas orang lain, atau perangkat yang telah dikompromikan. Penyamaran ini membuat proses identifikasi pelaku menjadi lebih sulit. Dalam beberapa kasus, pelaku tidak hanya menyembunyikan identitasnya, tetapi juga menggunakan identitas korban untuk melakukan kejahatan lanjutan. Contohnya adalah pengambilalihan akun media sosial untuk menipu kontak korban atau penggunaan data pribadi korban untuk mengajukan pinjaman online ilegal.

Karakteristik keempat adalah kecepatan dan jangkauan yang sangat luas. Satu tautan phishing dapat dikirim kepada ribuan orang dalam waktu singkat. Malware dapat menyebar melalui jaringan komputer dan menginfeksi banyak perangkat. Informasi palsu dapat viral dalam hitungan menit. Penipuan online juga dapat menargetkan banyak korban secara bersamaan melalui pesan otomatis. Kecepatan ini menyebabkan pencegahan

dan penanganan kejahatan siber harus dilakukan secara cepat, terkoordinasi, dan berbasis bukti digital.

Karakteristik kelima adalah bergantung pada data dan bukti elektronik. Kejahatan siber meninggalkan jejak dalam bentuk log akses, alamat IP, metadata, email, percakapan digital, riwayat transaksi, file, kode program, tangkapan layar, atau aktivitas sistem. Bukti tersebut berbeda dari bukti fisik biasa karena mudah diubah, dihapus, dipindahkan, atau dimanipulasi. Oleh sebab itu, pembuktian dalam perkara kejahatan siber membutuhkan prinsip forensik digital, seperti menjaga keaslian bukti, integritas data, rantai penguasaan barang bukti, dan prosedur akuisisi data yang benar (Casey, 2011).

Karakteristik keenam adalah memiliki kompleksitas teknis. Tidak semua kejahatan siber dilakukan dengan kemampuan teknis tinggi karena banyak penipuan online berbasis rekayasa sosial atau *social engineering*. Namun, beberapa jenis kejahatan seperti peretasan, ransomware, eksploitasi celah keamanan, pencurian database, dan serangan DDoS membutuhkan pemahaman teknis tertentu. Kompleksitas ini menuntut aparat penegak hukum, penyidik, jaksa, hakim, ahli digital, dan pengelola sistem elektronik untuk memahami aspek hukum sekaligus aspek teknis teknologi informasi.

Karakteristik ketujuh adalah dapat menimbulkan korban massal. Satu kebocoran data pada platform digital dapat berdampak kepada jutaan pengguna. Satu serangan terhadap sistem layanan publik dapat mengganggu banyak masyarakat. Satu penipuan investasi online dapat merugikan korban dari berbagai daerah. Oleh karena itu, kejahatan siber tidak hanya berdampak pada individu, tetapi juga dapat berdampak pada kepentingan publik dan kepercayaan masyarakat terhadap sistem digital.

Karakteristik kedelapan adalah modusnya cepat berubah. Pelaku kejahatan siber terus menyesuaikan cara kerja dengan perkembangan teknologi, kebiasaan pengguna, dan celah keamanan baru. Ketika masyarakat mulai mengenali satu bentuk penipuan, pelaku dapat mengganti pola komunikasi, tampilan situs, nama aplikasi, atau identitas digital yang digunakan. Karena itu, hukum dan penegakan hukum tidak boleh hanya berorientasi pada bentuk kejahatan yang sudah lama dikenal, tetapi juga harus mampu mengikuti perkembangan modus baru.

Karakteristik kesembilan adalah sering memanfaatkan kelemahan manusia. Banyak kejahatan siber tidak dimulai dari peretasan teknis, tetapi dari manipulasi psikologis. Pelaku dapat menakut-nakuti korban, menawarkan hadiah palsu, berpura-pura sebagai petugas bank, meminta kode OTP, mengirim tautan palsu, atau membuat korban percaya bahwa ia sedang berkomunikasi dengan pihak resmi. Teknik ini dikenal sebagai *social engineering*. Artinya, keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran, literasi digital, dan kehati-hatian pengguna.

Karakteristik kesepuluh adalah melibatkan banyak pihak dalam ekosistem digital. Dalam satu kasus kejahatan siber, dapat terlibat korban, pelaku, platform digital, penyedia layanan internet, penyedia cloud, bank, penyedia dompet digital, marketplace, operator telekomunikasi, dan aparat penegak hukum. Banyaknya pihak ini membuat penanganan kejahatan siber membutuhkan koordinasi. Platform digital dan penyelenggara sistem elektronik juga memiliki tanggung jawab untuk menyediakan sistem yang aman, menjaga data pengguna, serta membantu proses penanganan insiden sesuai ketentuan hukum yang berlaku.

Untuk memudahkan pemahaman, karakteristik kejahatan siber dapat diringkas dalam tabel berikut.

Tabel 8.1: Karakteristik Kejahatan Siber dan Implikasi Hukumnya

Karakteristik	**Penjelasan**	**Contoh**	**Implikasi Hukum**
Lintas batas wilayah	Pelaku, korban, server, dan bukti digital dapat berada di wilayah hukum berbeda	Penipuan online dari luar negeri	Membutuhkan kerja sama lintas negara dan kejelasan yurisdiksi
Tidak selalu terlihat fisik	Kerugian terjadi melalui sistem digital tanpa pertemuan langsung	Akun diambil alih, data dicuri, saldo digital hilang	Pembuktian tidak cukup mengandalkan bukti fisik
Identitas digital mudah disamarkan	Pelaku dapat menggunakan akun palsu, VPN, proxy, atau identitas orang lain	Penipuan memakai profil palsu	Penyidik perlu menelusuri jejak digital dan identitas elektronik

Karakteristik	Penjelasan	Contoh	Implikasi Hukum
Cepat dan luas	Serangan dapat menyebar ke banyak korban dalam waktu singkat	Phishing massal, penyebaran malware	Penanganan harus cepat agar kerugian tidak meluas
Berbasis bukti elektronik	Bukti berupa log, metadata, email, file, transaksi, atau percakapan digital	Riwayat login dan alamat IP	Membutuhkan forensik digital dan rantai penguasaan barang bukti
Kompleks secara teknis	Sebagian kejahatan membutuhkan keahlian teknis tertentu	Ransomware, DDoS, eksploitasi celah keamanan	Aparat perlu dukungan ahli teknologi informasi
Korban dapat massal	Satu serangan dapat berdampak pada banyak pengguna	Kebocoran database platform digital	Penanganan perlu memperhatikan perlindungan korban secara luas
Modus cepat berubah	Cara pelaku mengikuti perkembangan teknologi dan kebiasaan pengguna	Penipuan melalui aplikasi baru atau tautan palsu	Regulasi dan literasi digital harus terus diperbarui
Memanfaatkan kelemahan manusia	Pelaku memanipulasi emosi, ketakutan, atau kepercayaan korban	OTP scam, social engineering	Pencegahan memerlukan edukasi dan literasi keamanan digital
Melibatkan banyak pihak	Kasus dapat melibatkan platform, bank, ISP, cloud, dan aparat hukum	Pelacakan transaksi hasil penipuan online	Membutuhkan koordinasi antar lembaga dan penyedia layanan

Tabel 8.1 menunjukkan bahwa kejahatan siber memiliki sifat yang kompleks. Kompleksitas tersebut bukan hanya disebabkan oleh penggunaan teknologi, tetapi juga oleh keterlibatan banyak pihak, luasnya dampak, dan sulitnya pembuktian. Oleh karena itu, penanganan kejahatan siber perlu menggabungkan pendekatan hukum pidana, hukum teknologi informasi, pelindungan data pribadi, keamanan informasi, dan forensik digital.

Dalam praktiknya, kejahatan siber juga berhubungan dengan tata kelola keamanan siber. Keamanan siber tidak hanya bertujuan melindungi perangkat atau jaringan, tetapi juga melindungi data, layanan digital, transaksi elektronik, dan kepercayaan masyarakat. Kerangka NIST

Cybersecurity Framework menekankan pentingnya fungsi tata kelola, identifikasi, perlindungan, deteksi, respons, dan pemulihan dalam pengelolaan risiko keamanan siber (NIST, 2024). Kerangka ini relevan karena kejahatan siber sering terjadi ketika organisasi gagal mengenali risiko, melindungi sistem, mendeteksi serangan, merespons insiden, atau memulihkan layanan setelah terjadi gangguan.

Bagi mahasiswa, pemahaman mengenai pengertian dan karakteristik kejahatan siber penting karena hampir seluruh aktivitas akademik dan sosial telah terhubung dengan teknologi. Mahasiswa menggunakan email, sistem informasi akademik, media sosial, e-learning, dompet digital, mobile banking, marketplace, penyimpanan cloud, dan berbagai aplikasi komunikasi. Setiap penggunaan teknologi tersebut memiliki risiko apabila tidak disertai literasi hukum dan keamanan digital. Tindakan seperti mengambil akun tanpa izin, menyebarkan data pribadi orang lain, menyebarkan informasi palsu, menggunakan perangkat lunak bajakan, atau mencoba membobol sistem kampus bukan sekadar pelanggaran etika, tetapi dapat menjadi persoalan hukum.

8.2 Jenis-Jenis Kejahatan Siber

Kejahatan siber memiliki bentuk yang beragam karena teknologi informasi dapat digunakan untuk menyerang sistem, mencuri data, memanipulasi transaksi, menyebarkan konten melanggar hukum, maupun menipu pengguna. Jenis-jenis kejahatan siber tidak selalu berdiri sendiri. Dalam satu peristiwa, beberapa jenis kejahatan dapat terjadi secara bersamaan. Misalnya, pelaku dapat mengirim tautan phishing, mencuri kredensial akun, masuk ke akun korban, mengambil data pribadi, lalu menggunakan data tersebut untuk penipuan atau pengambilalihan dana.

Secara umum, kejahatan siber dapat dibedakan menjadi dua kelompok besar, yaitu **kejahatan yang bergantung pada teknologi digital** dan **kejahatan yang difasilitasi oleh teknologi digital**. Kejahatan yang bergantung pada teknologi digital hanya dapat dilakukan melalui komputer, jaringan, atau sistem elektronik, seperti peretasan, malware, ransomware, dan serangan terhadap server. Sementara itu, kejahatan yang difasilitasi oleh teknologi digital merupakan kejahatan konvensional yang diperluas melalui internet, seperti penipuan, pemerasan, pencemaran nama baik, perjudian online, perdagangan ilegal, dan eksploitasi konten terlarang (UNODC, 2026).

Gambar 8.2: Jenis-Jenis Kejahatan Siber

Pembagian jenis kejahatan siber penting untuk membantu memahami objek serangan, cara kerja pelaku, bentuk kerugian, dan dasar hukum yang dapat digunakan. Convention on Cybercrime atau Budapest Convention mengelompokkan beberapa tindak pidana siber seperti akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, penyalahgunaan perangkat, pemalsuan berbasis komputer, dan penipuan berbasis komputer (Council of Europe, 2001). Dalam konteks Indonesia, jenis-jenis kejahatan siber juga berkaitan dengan Undang-Undang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah melalui Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi apabila tindakannya berkaitan dengan penyalahgunaan data pribadi (Republik Indonesia, 2024; Republik Indonesia, 2022).

8.2.1 Akses Ilegal terhadap Sistem Elektronik

Akses ilegal adalah tindakan memasuki, mengakses, atau menggunakan komputer, jaringan, akun, server, atau sistem elektronik tanpa hak atau tanpa izin dari pemilik sistem. Bentuk ini sering dikenal sebagai *unauthorized access* atau peretasan. Akses ilegal dapat dilakukan untuk sekadar melihat

isi sistem, mencuri data, mengubah informasi, memasang malware, mengambil alih akun, atau membuka jalan bagi kejahatan lanjutan.

Contoh akses ilegal adalah seseorang masuk ke akun media sosial orang lain tanpa izin, membobol sistem informasi akademik, mengakses database pelanggan secara tidak sah, atau mengambil alih panel administrator sebuah website. Dalam hukum siber, akses ilegal dianggap serius karena melanggar prinsip kerahasiaan dan keamanan sistem elektronik. Budapest Convention juga menempatkan akses ilegal sebagai salah satu bentuk utama tindak pidana terhadap sistem komputer (Council of Europe, 2001).

Dalam praktiknya, akses ilegal sering menjadi tahap awal dari kejahatan lain. Setelah berhasil masuk ke sistem, pelaku dapat mencuri data, menghapus file, mengubah tampilan website, menyebarkan malware, atau memeras korban. Oleh karena itu, akses ilegal tidak boleh dianggap sebagai tindakan ringan, meskipun pelaku belum sempat mengambil keuntungan ekonomi. Tindakan masuk tanpa hak ke sistem elektronik tetap dapat menimbulkan risiko hukum karena merusak keamanan, kepercayaan, dan integritas sistem digital.

8.2.2 Intersepsi Ilegal dan Penyadapan Digital

Intersepsi ilegal adalah tindakan menyadap, merekam, menangkap, atau memantau komunikasi elektronik tanpa hak. Bentuk komunikasi yang dapat menjadi sasaran antara lain pesan email, percakapan aplikasi, panggilan suara berbasis internet, data yang dikirim melalui jaringan, atau aktivitas pengguna dalam sistem tertentu. Intersepsi ilegal berbahaya karena melanggar kerahasiaan komunikasi dan privasi pengguna.

Contoh intersepsi ilegal adalah penyadapan komunikasi pribadi, pemasangan perangkat lunak mata-mata, pemantauan lalu lintas data tanpa izin, atau pencurian kode OTP yang dikirim melalui pesan. Dalam kehidupan sehari-hari, intersepsi juga dapat terjadi ketika pelaku memanfaatkan jaringan Wi-Fi tidak aman untuk mencuri data login pengguna. Tindakan semacam ini dapat menjadi pintu masuk untuk pencurian identitas, pengambilalihan akun, dan penipuan digital.

Intersepsi ilegal memiliki hubungan erat dengan perlindungan privasi digital. Komunikasi elektronik pada dasarnya merupakan bagian dari ruang pribadi seseorang. Jika komunikasi tersebut disadap atau direkam tanpa dasar

hukum yang sah, maka korban dapat mengalami kerugian berupa bocornya informasi pribadi, kerugian ekonomi, tekanan psikologis, atau pencemaran reputasi. Karena itu, penanganan intersepsi ilegal perlu memperhatikan aspek hukum pidana, pelindungan data pribadi, dan keamanan komunikasi elektronik.

8.2.3 Gangguan Data dan Gangguan Sistem

Gangguan data adalah tindakan mengubah, merusak, menghapus, menambahkan, memindahkan, atau membuat data elektronik tidak dapat digunakan sebagaimana mestinya. Sementara itu, gangguan sistem adalah tindakan yang menyebabkan sistem elektronik tidak dapat bekerja secara normal. Kedua jenis kejahatan ini menyerang integritas dan ketersediaan data serta sistem komputer.

Contoh gangguan data adalah menghapus database, mengubah nilai akademik, memanipulasi catatan transaksi, atau mengganti isi dokumen elektronik. Contoh gangguan sistem adalah serangan terhadap server, perusakan website, pengiriman trafik palsu secara massal, atau tindakan lain yang membuat layanan digital tidak dapat diakses. UNODC menjelaskan bahwa gangguan terhadap data dan sistem dapat mencakup tindakan menekan, mengubah, menambah, mengirim, menghapus, atau merusak data, sistem, dan layanan (UNODC, 2013).

Gangguan sistem sering terlihat dalam bentuk serangan *distributed denial of service* atau DDoS. Dalam serangan ini, pelaku mengirimkan permintaan dalam jumlah sangat besar ke server sehingga layanan menjadi lambat atau tidak dapat diakses. Dampaknya dapat merugikan banyak pihak, terutama jika yang diserang adalah layanan publik, sistem keuangan, layanan kesehatan, pendidikan, atau perdagangan elektronik. Kerugian yang muncul tidak hanya berupa kerusakan teknis, tetapi juga hilangnya kepercayaan pengguna terhadap penyelenggara sistem elektronik.

8.2.4 Malware, Ransomware, dan Perangkat Berbahaya

Malware adalah perangkat lunak berbahaya yang dibuat untuk merusak sistem, mencuri data, memata-matai aktivitas pengguna, mengambil alih perangkat, atau membuka akses tidak sah ke sistem (Fairuzabadi et al., 2023). Bentuk malware dapat berupa virus, worm, trojan, spyware,

keylogger, adware berbahaya, dan ransomware. Malware biasanya menyebar melalui lampiran email, tautan palsu, aplikasi tidak resmi, perangkat penyimpanan eksternal, situs berbahaya, atau celah keamanan sistem.

Ransomware merupakan salah satu bentuk malware yang sangat merugikan. Dalam serangan ransomware, pelaku mengunci atau mengenkripsi data korban, kemudian meminta tebusan agar data dapat dibuka kembali. Serangan ini sering menargetkan perusahaan, rumah sakit, sekolah, lembaga pemerintah, dan pengguna pribadi. Dampaknya dapat berupa berhentinya layanan, kehilangan data penting, biaya pemulihan yang besar, dan risiko kebocoran data.

Jenis kejahatan ini menunjukkan bahwa perangkat lunak dapat menjadi instrumen utama dalam kejahatan siber. Dalam beberapa kasus, pelaku tidak harus menyerang korban secara langsung. Pelaku cukup menyebarkan malware melalui tautan atau file, kemudian malware bekerja otomatis mengambil data, merekam aktivitas, atau membuka akses jarak jauh. Oleh karena itu, pencegahan terhadap malware membutuhkan keamanan teknis, pembaruan sistem, penggunaan perangkat lunak resmi, antivirus, pencadangan data, dan kehati-hatian pengguna.

8.2.5 Penipuan Online dan Phishing

Penipuan online adalah bentuk kejahatan siber yang bertujuan memperoleh keuntungan dengan cara memperdaya korban melalui media digital. Bentuknya dapat berupa toko online palsu, investasi palsu, lowongan kerja palsu, undian palsu, pinjaman online ilegal, penipuan transfer dana, penipuan identitas petugas bank, dan penipuan melalui media sosial. Kejahatan ini termasuk *cyber-enabled crime* karena penipuan pada dasarnya merupakan kejahatan konvensional, tetapi jangkauannya menjadi lebih luas karena difasilitasi oleh internet (UNODC, 2013).

Salah satu bentuk penipuan online yang paling sering terjadi adalah phishing. Phishing adalah teknik menipu korban agar memberikan informasi penting, seperti username, password, PIN, OTP, nomor kartu, atau data pribadi lainnya. Pelaku biasanya membuat pesan, email, situs, atau tampilan aplikasi palsu yang menyerupai lembaga resmi. Korban kemudian diarahkan untuk

memasukkan data rahasia, yang selanjutnya digunakan pelaku untuk mengambil alih akun atau melakukan transaksi tidak sah.

Penipuan online banyak memanfaatkan kelemahan psikologis korban. Pelaku dapat menggunakan tekanan waktu, rasa takut, janji hadiah, rasa kasihan, atau kepercayaan terhadap lembaga tertentu. Misalnya, korban diberi pesan bahwa rekeningnya akan diblokir jika tidak segera mengisi formulir tertentu. Dalam kondisi panik, korban dapat memberikan OTP atau password kepada pelaku. Karena itu, penipuan online tidak hanya perlu ditangani dengan pendekatan hukum, tetapi juga dengan literasi digital dan edukasi keamanan pengguna.

8.2.6 Pencurian Identitas dan Penyalahgunaan Data Pribadi

Pencurian identitas adalah tindakan mengambil, menggunakan, atau memanfaatkan identitas orang lain tanpa izin untuk memperoleh keuntungan atau melakukan perbuatan melawan hukum. Identitas yang disalahgunakan dapat berupa nama, NIK, alamat, nomor telepon, foto, akun media sosial, tanda tangan, data biometrik, nomor rekening, atau data keuangan. Dalam ruang digital, pencurian identitas sering terjadi setelah data pribadi korban bocor, dicuri melalui phishing, atau dikumpulkan dari berbagai sumber terbuka.

Penyalahgunaan data pribadi menjadi isu penting karena data dapat digunakan untuk kejahatan lanjutan. Data pribadi yang bocor dapat digunakan untuk membuat akun palsu, mengajukan pinjaman online ilegal, mengambil alih akun, melakukan penipuan, atau menyebarkan informasi pribadi korban. Undang-Undang Nomor 27 Tahun 2022 mengatur bahwa pelindungan data pribadi merupakan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data guna menjamin hak konstitusional subjek data pribadi (Republik Indonesia, 2022).

Jenis kejahatan ini menunjukkan bahwa data pribadi memiliki nilai ekonomi dan nilai strategis dalam ekosistem digital. Semakin lengkap data yang diperoleh pelaku, semakin besar peluang data tersebut digunakan untuk merugikan korban. Oleh sebab itu, masyarakat perlu memahami bahwa menyebarkan foto kartu identitas, membagikan OTP, mengisi formulir tidak jelas, atau mengunggah informasi pribadi secara berlebihan dapat meningkatkan risiko pencurian identitas.

8.2.7 Konten Ilegal dan Penyalahgunaan Media Digital

Kejahatan siber juga dapat berbentuk penyebaran konten ilegal melalui media digital. Konten ilegal dapat berupa konten yang melanggar kesusilaan, perjudian online, pemerasan atau pengancaman, pencemaran nama baik, ujaran kebencian, informasi bohong yang merugikan masyarakat, eksploitasi seksual, dan konten lain yang dilarang oleh hukum. Jenis kejahatan ini berbeda dari serangan teknis terhadap sistem, karena objek utamanya adalah isi informasi yang disebarkan.

Penyebaran konten ilegal menjadi berbahaya karena internet memungkinkan informasi menjangkau banyak orang dengan sangat cepat. Satu unggahan, pesan, video, atau gambar dapat disalin, disebarkan ulang, dan disimpan oleh banyak pengguna. Akibatnya, kerugian korban dapat berlangsung lama meskipun konten awal sudah dihapus. Dalam konteks hukum Indonesia, pengaturan mengenai konten digital yang melanggar hukum berkaitan dengan UU ITE dan perubahan-perubahannya (Republik Indonesia, 2024).

Perlu dipahami bahwa tidak semua konten negatif otomatis menjadi tindak pidana. Penilaian hukum harus memperhatikan unsur perbuatan, kesengajaan, akibat, konteks, dan ketentuan hukum yang berlaku. Oleh karena itu, pembahasan lebih rinci mengenai dasar hukum dan pertanggungjawaban pidana akan dibahas pada subbab berikutnya. Dalam subbab ini, konten ilegal cukup dipahami sebagai salah satu jenis kejahatan siber yang memanfaatkan media digital untuk menyebarkan informasi yang dilarang hukum.

8.2.8 Kejahatan Keuangan Digital

Kejahatan keuangan digital adalah kejahatan siber yang menyasar transaksi, akun, sistem pembayaran, layanan perbankan digital, dompet digital, investasi online, pinjaman online, atau aset digital. Bentuknya dapat berupa pembobolan akun mobile banking, pencurian saldo dompet digital, transaksi tidak sah, skema investasi palsu, manipulasi pembayaran, pencurian kartu kredit, dan pinjaman online ilegal.

Kejahatan ini berkembang karena aktivitas keuangan masyarakat semakin banyak dilakukan melalui sistem elektronik. Pembayaran digital memberikan kemudahan, tetapi juga membuka peluang bagi pelaku untuk memanfaatkan kelalaian pengguna, kelemahan sistem, atau celah verifikasi.

Contohnya adalah pelaku mengaku sebagai petugas bank, meminta korban menyebutkan kode OTP, lalu menggunakan kode tersebut untuk mengambil alih akun. Dalam kasus lain, pelaku membuat aplikasi atau situs palsu untuk memperoleh data keuangan korban.

Kejahatan keuangan digital biasanya menimbulkan kerugian langsung berupa hilangnya uang atau aset. Namun, dampaknya tidak berhenti pada kerugian finansial. Korban juga dapat kehilangan akses akun, mengalami tekanan psikologis, masuk dalam tagihan pinjaman ilegal, atau mengalami penyalahgunaan identitas. Karena itu, perlindungan terhadap transaksi digital perlu melibatkan keamanan sistem, verifikasi identitas, edukasi pengguna, mekanisme pengaduan, dan kerja sama antara lembaga keuangan, platform digital, serta aparat penegak hukum.

8.2.9 Pelanggaran Hak Kekayaan Intelektual Digital

Pelanggaran hak kekayaan intelektual digital adalah tindakan menggunakan, menggandakan, menyebarkan, menjual, atau memodifikasi karya digital tanpa izin dari pemegang hak. Bentuknya dapat berupa pembajakan perangkat lunak, penyebaran film bajakan, penggunaan musik tanpa lisensi, plagiarisme konten digital, penggunaan desain tanpa izin, penjualan akun ilegal, atau penyebaran e-book tanpa hak.

Kejahatan ini sering dianggap ringan karena produk digital mudah disalin dan disebarkan. Padahal, karya digital tetap memiliki nilai ekonomi dan perlindungan hukum. Pembajakan perangkat lunak, misalnya, tidak hanya merugikan pemilik hak cipta, tetapi juga dapat membahayakan pengguna karena perangkat lunak bajakan sering mengandung malware. Dengan demikian, pelanggaran kekayaan intelektual digital tidak hanya berkaitan dengan hak ekonomi pencipta, tetapi juga berkaitan dengan keamanan pengguna dan etika digital.

Dalam lingkungan akademik, jenis kejahatan ini relevan bagi mahasiswa karena berkaitan dengan penggunaan software, e-book, jurnal, gambar, video, dan materi pembelajaran digital. Mahasiswa perlu memahami bahwa kemudahan mengakses dan menyalin konten digital tidak berarti semua konten bebas digunakan. Penggunaan karya digital tetap harus memperhatikan izin, lisensi, kutipan, dan batas penggunaan yang wajar.

8.2.10 Kekerasan, Pelecehan, dan Perundungan Siber

Kekerasan digital, pelecehan online, dan perundungan siber merupakan bentuk kejahatan atau pelanggaran yang menyerang martabat, rasa aman, dan reputasi seseorang melalui media digital. Bentuknya dapat berupa penghinaan, ancaman, penyebaran foto pribadi, doxing, penyebaran fitnah, komentar merendahkan, pesan intimidatif, pelecehan seksual berbasis elektronik, atau tindakan mempermalukan korban secara online.

Jenis kejahatan ini sering terjadi di media sosial, aplikasi pesan, forum online, gim daring, dan platform komunitas digital. Dampaknya dapat serius karena korban tidak hanya mengalami gangguan reputasi, tetapi juga tekanan psikologis, rasa takut, isolasi sosial, dan kerugian dalam kehidupan akademik maupun pekerjaan. Kejahatan ini juga dapat berlangsung lama karena jejak digital sulit dihapus sepenuhnya.

Kekerasan dan pelecehan digital menunjukkan bahwa kejahatan siber tidak selalu berbentuk serangan terhadap server atau pencurian data. Manusia juga dapat menjadi target langsung dari penyalahgunaan teknologi. Karena itu, hukum teknologi informasi perlu memperhatikan perlindungan terhadap individu sebagai pengguna ruang digital, bukan hanya perlindungan terhadap sistem elektronik.

Untuk memberikan gambaran yang lebih ringkas, jenis-jenis kejahatan siber dapat dilihat dalam tabel berikut.

Tabel 8.2: Jenis-Jenis Kejahatan Siber, Contoh, dan Dampaknya

Jenis Kejahatan Siber	Penjelasan Singkat	Contoh	Dampak bagi Korban
Akses ilegal	Masuk ke sistem, akun, atau jaringan tanpa izin	Membobol akun media sosial, masuk ke server tanpa hak	Akun diambil alih, data dicuri, sistem rusak
Intersepsi ilegal	Menyadap atau menangkap komunikasi elektronik tanpa hak	Penyadapan pesan, pencurian OTP	Privasi terganggu, akun dapat diambil alih

Jenis Kejahatan Siber	Penjelasan Singkat	Contoh	Dampak bagi Korban
Gangguan data	Mengubah, menghapus, atau merusak data elektronik	Menghapus database, mengubah nilai akademik	Data tidak valid, layanan terganggu
Gangguan sistem	Menghambat atau merusak kerja sistem elektronik	DDoS, deface website	Layanan tidak dapat diakses, kerugian operasional
Malware dan ransomware	Perangkat lunak berbahaya untuk merusak, mencuri, atau mengunci data	Virus, spyware, ransomware	Data hilang, sistem terkunci, korban diperas
Penipuan online dan phishing	Menipu korban melalui media digital untuk memperoleh data atau uang	Link palsu, toko online palsu, investasi palsu	Kerugian uang, pencurian data, transaksi tidak sah
Pencurian identitas	Menggunakan identitas orang lain tanpa izin	Membuat akun palsu memakai data korban	Pinjaman ilegal, penipuan atas nama korban
Penyalahgunaan data pribadi	Mengumpulkan atau menggunakan data pribadi secara tidak sah	Menjual database pelanggan	Pelanggaran privasi, penipuan lanjutan
Konten ilegal	Menyebarkan informasi atau konten yang dilarang hukum	Ujaran kebencian, perjudian online, ancaman	Reputasi rusak, keresahan masyarakat
Kejahatan keuangan digital	Menyerang akun, transaksi, atau layanan keuangan digital	Pembobolan e-wallet, mobile banking, kartu kredit	Saldo hilang, transaksi ilegal

Jenis Kejahatan Siber	Penjelasan Singkat	Contoh	Dampak bagi Korban
Pelanggaran HKI digital	Menggandakan atau menyebarkan karya digital tanpa izin	Software bajakan, film bajakan, e-book ilegal	Kerugian pencipta, risiko malware
Perundungan dan pelecehan siber	Menyerang martabat atau rasa aman seseorang secara digital	Cyberbullying, doxing, ancaman online	Tekanan psikologis, reputasi rusak

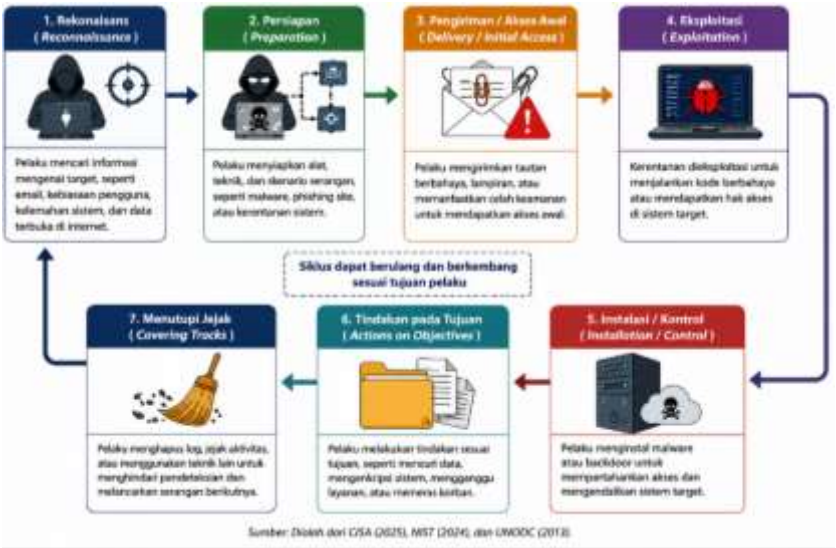
Tabel 8.2 menunjukkan bahwa jenis kejahatan siber sangat beragam. Sebagian jenis menyerang sistem elektronik secara teknis, seperti akses ilegal, gangguan sistem, dan malware. Sebagian lainnya menyerang pengguna sebagai manusia, seperti penipuan online, pencurian identitas, pelecehan digital, dan perundungan siber. Ada pula jenis kejahatan yang menyerang kepentingan ekonomi dan hak hukum, seperti kejahatan keuangan digital dan pelanggaran kekayaan intelektual digital.

8.3 Modus Operandi Kejahatan Siber

Modus operandi kejahatan siber adalah pola, cara, teknik, atau tahapan yang digunakan pelaku untuk melakukan tindakan melawan hukum melalui sistem elektronik. Pembahasan mengenai modus operandi penting karena jenis kejahatan siber tidak hanya dapat dikenali dari akibat yang ditimbulkan, tetapi juga dari cara pelaku memperoleh akses, memanipulasi korban, menyembunyikan identitas, mengeksploitasi sistem, mengambil data, atau memperoleh keuntungan. Dengan memahami modus operandi, masyarakat, organisasi, penyelenggara sistem elektronik, dan aparat penegak hukum dapat lebih mudah mengenali risiko, melakukan pencegahan, serta mengumpulkan bukti digital ketika terjadi insiden.

Modus kejahatan siber terus berkembang mengikuti perubahan teknologi dan perilaku pengguna. Pada awalnya, kejahatan siber banyak dipahami sebagai peretasan sistem komputer. Namun, dalam praktik modern, banyak kejahatan siber justru memanfaatkan kelemahan manusia, seperti rasa takut, rasa percaya, ketidaktahuan, kelalaian, atau keinginan memperoleh keuntungan cepat. Oleh karena itu, modus operandi kejahatan siber tidak hanya bersifat teknis, tetapi juga psikologis, sosial, ekonomi, dan hukum. UNODC menjelaskan bahwa kejahatan siber dapat mencakup tindakan

berbasis teknologi seperti malware, hacking, DDoS, serta tindakan yang memanfaatkan teknologi untuk memperluas kejahatan konvensional seperti penipuan dan pemerasan digital (UNODC, 2013).



Gambar 8.3: Alur Modus Operandi Kejahatan Siber

Dalam konteks hukum Indonesia, pemahaman terhadap modus operandi kejahatan siber berkaitan dengan UU ITE dan perubahan-perubahannya, terutama karena tindakan pelaku dapat berbentuk akses ilegal, gangguan terhadap sistem elektronik, manipulasi informasi elektronik, penyebaran konten melanggar hukum, atau penyalahgunaan transaksi elektronik. Undang-Undang Nomor 1 Tahun 2024 merupakan perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sehingga menjadi salah satu rujukan penting dalam memahami dasar hukum penanganan kejahatan siber di Indonesia (Republik Indonesia, 2024).

8.3.1 Rekayasa Sosial (*Social Engineering*)

Rekayasa sosial atau *social engineering* merupakan modus kejahatan siber yang memanfaatkan kelemahan psikologis manusia untuk memperoleh informasi, akses, atau tindakan tertentu dari korban. Dalam modus ini, pelaku tidak selalu menyerang sistem secara langsung, tetapi memanipulasi korban agar korban sendiri memberikan informasi sensitif atau melakukan

tindakan yang menguntungkan pelaku. Informasi yang diminta dapat berupa password, PIN, OTP, nomor kartu, data identitas, data rekening, atau akses ke akun digital.

Pelaku rekayasa sosial biasanya membangun situasi yang membuat korban panik, percaya, tergesa-gesa, atau merasa sedang berhadapan dengan pihak resmi. Misalnya, pelaku mengaku sebagai petugas bank, pegawai marketplace, petugas kurir, admin kampus, customer service dompet digital, atau pihak keamanan sistem. Setelah korban percaya, pelaku akan meminta korban membuka tautan tertentu, mengisi formulir palsu, mengirim kode OTP, mengunduh aplikasi, atau melakukan transfer dana. OJK menjelaskan bahwa *social engineering* dapat dilakukan melalui telepon, SMS, atau media lain untuk mengarahkan korban agar memberikan informasi penting atau membuka situs tertentu (OKJ, 2015).

Modus rekayasa sosial menunjukkan bahwa keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada perilaku pengguna. Sistem yang kuat dapat tetap ditembus apabila pengguna memberikan akses secara sukarela karena tertipu. Banyak kejahatan siber terhadap individu berhasil karena pelaku memanfaatkan faktor manusia, seperti kepercayaan, emosi, kebiasaan, dan keterbatasan pemahaman pengguna. Karena itu, edukasi, literasi digital, dan kebiasaan verifikasi menjadi bagian penting dalam mencegah rekayasa sosial (Nurse, 2018; OJK, 2015).

8.3.2 Phishing, Spoofing, dan Situs Palsu

Phishing adalah modus penipuan digital dengan cara membuat korban percaya bahwa pesan, email, situs, tautan, atau aplikasi yang diterima berasal dari pihak resmi. Tujuannya adalah memperoleh data rahasia, seperti username, password, PIN, OTP, nomor kartu, atau informasi pribadi lainnya. Modus ini sering dilakukan melalui email, SMS, pesan WhatsApp, media sosial, iklan palsu, atau situs web yang dibuat menyerupai layanan resmi.

Dalam praktiknya, phishing sering dikombinasikan dengan spoofing. Spoofing adalah tindakan memalsukan identitas digital, seperti alamat email, nomor telepon, nama pengirim, tampilan situs, logo lembaga, atau domain yang mirip dengan situs resmi. Misalnya, pelaku membuat situs yang tampilannya menyerupai bank atau marketplace, lalu meminta korban login. Setelah korban memasukkan data akun, data tersebut langsung masuk ke

pelaku. Phishing dapat dipahami sebagai bentuk kejahatan siber berbasis rekayasa sosial dan pemalsuan situs yang bertujuan mencuri data rahasia korban (Gharibi, 2012).

Di Indonesia, modus phishing juga sering dikaitkan dengan pencurian OTP dan pembajakan akun. Kominfo mengingatkan masyarakat agar tidak membagikan kode rahasia OTP karena kode tersebut penting untuk dilindungi dan dapat dimanfaatkan pelaku untuk mengambil alih akun digital korban (Kementerian Kominfo RI, 2020). OJK juga mengingatkan agar pengguna layanan keuangan digital tidak memberikan data rahasia seperti PIN, password, OTP, nomor kartu, dan informasi pribadi kepada pihak lain karena dapat disalahgunakan untuk kejahatan digital (OKJ, 2015). Dengan demikian, phishing bukan hanya persoalan teknis, tetapi juga bentuk manipulasi kepercayaan yang memanfaatkan tampilan digital seolah-olah resmi (Gharibi, 2012).

8.3.3 Malware dan Ransomware

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak sistem, mencuri data, memantau aktivitas pengguna, mengambil alih perangkat, atau membuka akses tidak sah ke sistem. Bentuk malware dapat berupa virus, worm, trojan, spyware, keylogger, adware berbahaya, dan ransomware. Malware dapat masuk melalui lampiran email, tautan palsu, aplikasi bajakan, file unduhan tidak resmi, perangkat penyimpanan eksternal, atau celah keamanan sistem.

Ransomware merupakan salah satu bentuk malware yang paling merugikan. Dalam modus ini, pelaku mengenkripsi atau mengunci data korban, kemudian meminta tebusan agar data tersebut dapat dibuka kembali. Dalam beberapa kasus, pelaku tidak hanya mengunci data, tetapi juga mengancam akan menyebarkan data korban apabila tebusan tidak dibayar. CISA menjelaskan bahwa pencegahan ransomware perlu memperhatikan beberapa vektor awal serangan, seperti kerentanan sistem yang terbuka ke internet, konfigurasi yang salah, kredensial yang bocor, phishing, malware awal, bentuk rekayasa sosial lanjutan, dan pihak ketiga atau penyedia layanan terkelola (CISA, 2025).

Modus malware dan ransomware menunjukkan bahwa pelaku dapat menyerang korban tanpa interaksi langsung. Korban cukup membuka file,

mengklik tautan, memasang aplikasi palsu, atau menggunakan perangkat lunak bajakan. Setelah malware aktif, pelaku dapat mencuri data, merekam aktivitas keyboard, mengambil tangkapan layar, atau mengendalikan perangkat dari jarak jauh. NIST Cybersecurity Framework 2.0 menekankan pentingnya fungsi govern, identify, protect, detect, respond, dan recover dalam mengelola risiko keamanan siber, termasuk risiko serangan malware dan ransomware (NIST, 2024). Dengan demikian, pencegahan ransomware perlu dilakukan melalui pembaruan sistem, pencadangan data, pembatasan akses, autentikasi kuat, deteksi dini, dan kesiapan pemulihan (CISA, 2025; NIST, 2024).

8.3.4 Eksploitasi Kerentanan Sistem

Eksploitasi kerentanan sistem adalah modus kejahatan siber dengan memanfaatkan kelemahan pada perangkat lunak, konfigurasi server, aplikasi web, sistem operasi, jaringan, atau perangkat keras. Kerentanan tersebut dapat muncul karena sistem tidak diperbarui, konfigurasi keamanan lemah, penggunaan password bawaan, celah pada kode program, kesalahan validasi input, atau layanan yang terbuka ke internet tanpa perlindungan memadai.

Pelaku biasanya melakukan pemindaian untuk mencari sistem yang rentan. Setelah menemukan celah, pelaku dapat masuk ke sistem, mengambil data, mengubah tampilan website, menanam malware, membuat akun administrator baru, atau menjadikan sistem korban sebagai bagian dari serangan lanjutan. Dalam Budapest Convention, tindakan seperti akses ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat termasuk kategori penting dalam kriminalisasi kejahatan terhadap sistem komputer (Council of Europe, 2001).

Eksploitasi kerentanan tidak selalu dilakukan oleh pelaku yang sangat ahli. Saat ini banyak alat otomatis yang dapat digunakan untuk mencari celah keamanan. Hal ini membuat organisasi yang tidak melakukan pembaruan sistem menjadi lebih rentan. CISA menempatkan kerentanan yang terbuka ke internet dan salah konfigurasi sebagai salah satu vektor awal yang umum dalam insiden ransomware dan pemerasan data (CISA, 2025). Oleh karena itu, organisasi perlu menerapkan manajemen kerentanan, pengujian keamanan, pembaruan rutin, audit konfigurasi, dan pembatasan layanan yang dapat diakses dari internet (Council of Europe, 2001; CISA, 2025).

8.3.5 Pencurian Kredensial dan Pengambilalihan Akun

Pencurian kredensial adalah modus kejahatan siber yang bertujuan memperoleh data akses pengguna, seperti username, password, PIN, token, kode OTP, pertanyaan keamanan, atau cookie sesi login. Setelah kredensial diperoleh, pelaku dapat mengambil alih akun korban. Akun yang diambil alih dapat berupa akun email, media sosial, marketplace, mobile banking, dompet digital, sistem akademik, layanan cloud, atau akun kerja organisasi.

Pencurian kredensial dapat dilakukan melalui phishing, keylogger, malware, kebocoran database, situs palsu, brute force, credential stuffing, atau rekayasa sosial. *Credential stuffing* terjadi ketika pelaku mencoba menggunakan kombinasi username dan password yang bocor dari satu layanan untuk masuk ke layanan lain. Modus ini berbahaya karena banyak pengguna memakai password yang sama untuk beberapa akun. CISA menegaskan bahwa MFA merupakan praktik penting untuk mengurangi ancaman pelaku yang menggunakan kredensial yang telah dikompromikan untuk memperoleh akses dan melakukan aktivitas berbahaya (CISA, 2022).

Dalam layanan keuangan digital, pencurian kredensial sering dikombinasikan dengan pencurian OTP. Pelaku dapat mengaku sebagai petugas bank, meminta korban menyebutkan kode OTP, lalu menggunakan kode tersebut untuk masuk atau melakukan transaksi. OJK mengingatkan bahwa data seperti PIN, nomor kartu, CVV, dan OTP tidak boleh diberikan kepada pihak lain karena dapat digunakan untuk transaksi ilegal (OJK, 2015). Dengan demikian, pencurian kredensial perlu dipahami sebagai pintu masuk menuju banyak kejahatan lanjutan, seperti pengurasan saldo, pencurian identitas, penipuan terhadap kontak korban, dan penyalahgunaan data pribadi (CISA, 2022; OJK, 2015).

8.3.6 Botnet dan Serangan DDoS

Botnet adalah jaringan perangkat yang telah terinfeksi malware dan dikendalikan oleh pelaku dari jarak jauh. Perangkat yang menjadi bagian dari botnet dapat berupa komputer, server, kamera CCTV, router, perangkat IoT, atau perangkat lain yang terhubung ke internet. Pemilik perangkat sering tidak menyadari bahwa perangkatnya telah dikendalikan oleh pihak lain. Botnet dapat digunakan untuk mengirim spam, menyebarkan malware, mencuri data, melakukan penipuan klik, atau melancarkan serangan DDoS.

Serangan DDoS atau *distributed denial of service* adalah modus yang bertujuan membuat layanan digital tidak dapat diakses oleh pengguna sah. Pelaku mengirimkan trafik dalam jumlah sangat besar ke server atau jaringan korban sehingga sistem menjadi lambat, tidak stabil, atau berhenti bekerja. Tandon (2020) menjelaskan bahwa DDoS dilakukan dengan membanjiri bandwidth atau sumber daya target menggunakan banyak sistem yang telah dikompromikan sehingga pengguna sah tidak dapat mengakses layanan.

Dari sudut hukum, DDoS dapat dipahami sebagai bentuk gangguan terhadap sistem elektronik karena menghambat fungsi normal sistem. Budapest Convention memasukkan *system interference* sebagai tindakan yang menghambat secara serius fungsi sistem komputer melalui input, transmisi, perusakan, penghapusan, perubahan, atau penekanan data komputer (Council of Europe, 2001). Dampak DDoS dapat sangat besar jika menyerang layanan publik, perbankan, pendidikan, kesehatan, atau e-commerce. Karena itu, pencegahan DDoS membutuhkan pemantauan trafik, mitigasi jaringan, layanan proteksi DDoS, segmentasi sistem, dan prosedur respons insiden (Tandon, 2020).

8.3.7 Manipulasi Transaksi dan Penipuan Keuangan Digital

Manipulasi transaksi dan penipuan keuangan digital merupakan modus yang menyasar sistem pembayaran, mobile banking, dompet digital, kartu kredit, marketplace, pinjaman online, investasi digital, atau layanan keuangan berbasis aplikasi. Pelaku dapat menggunakan berbagai cara, seperti mengirim tautan palsu, membuat aplikasi palsu, mengaku sebagai petugas bank, meminta OTP, memalsukan bukti transfer, membuat toko online palsu, atau menjanjikan investasi dengan keuntungan tinggi dalam waktu singkat.

Dalam modus ini, pelaku biasanya menciptakan keadaan mendesak agar korban tidak sempat memeriksa kebenaran informasi. Contohnya, korban diberi tahu bahwa rekeningnya bermasalah, paketnya tertahan, akun dompet digitalnya akan diblokir, atau ada transaksi mencurigakan yang harus segera diverifikasi. Setelah korban mengikuti arahan pelaku, dana korban dapat dipindahkan, akun diambil alih, atau data pribadi digunakan untuk kejahatan lain. OJK menjelaskan bahwa modus berbasis *social engineering* dalam layanan elektronik dapat dilakukan dengan mengelabui nasabah agar

memberikan data rahasia seperti PIN, nomor kartu, masa berlaku kartu, dan CVV (OJK, 2015).

Dalam sektor inovasi teknologi keuangan, OJK juga menyoroti risiko fraud seperti ransomware, *social network engineering*, penggunaan AI untuk membuat phishing lebih meyakinkan, peniruan suara, dan deepfake untuk meminta transfer dana atau memperoleh informasi sensitif (OJK, 2024). Oleh karena itu, manipulasi transaksi keuangan digital perlu dipahami sebagai modus gabungan antara rekayasa sosial, pencurian identitas, penyalahgunaan sistem, dan kelemahan literasi pengguna. Pencegahannya memerlukan autentikasi berlapis, verifikasi transaksi, edukasi nasabah, pengaduan cepat, pemblokiran rekening atau akun mencurigakan, dan koordinasi antara penyedia layanan keuangan, platform digital, OJK, Bank Indonesia, dan aparat penegak hukum (OJK, 2015; OJK, 2024).

8.3.8 Pemerasan Digital dan Penyalahgunaan Data Pribadi

Pemerasan digital adalah modus kejahatan siber dengan cara mengancam korban agar menyerahkan uang, data, akses, atau keuntungan tertentu. Ancaman dapat berupa penyebaran foto pribadi, penyebaran percakapan, pengungkapan data sensitif, perusakan reputasi, penguncian sistem, atau pembocoran informasi rahasia. Dalam beberapa kasus, pemerasan digital dilakukan setelah pelaku memperoleh data korban melalui phishing, peretasan, malware, doxing, atau kebocoran data.

Penyalahgunaan data pribadi menjadi bagian penting dari modus ini. Data seperti NIK, alamat, nomor telepon, foto, informasi keluarga, riwayat transaksi, dan akun media sosial dapat digunakan untuk menekan korban. Pelaku dapat mengancam akan menyebarkan data tersebut kepada publik, kantor, keluarga, atau teman korban. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan pentingnya pelindungan data pribadi dalam rangkaian pemrosesan data untuk menjamin hak subjek data pribadi (Republik Indonesia, 2022).

Pemerasan digital juga dapat muncul dalam bentuk ransomware, yaitu ketika pelaku mengunci data dan meminta tebusan. Dalam bentuk lain, pelaku dapat melakukan *sextortion*, doxing, atau ancaman penyebaran informasi pribadi. UNODC menempatkan pemerasan, malware, hacking, dan kejahatan berbasis data sebagai bagian dari aktivitas kriminal siber yang

dapat dilakukan oleh kelompok kejahatan terorganisasi (UNODC, 2013). Dengan demikian, pemerasan digital perlu ditangani bukan hanya sebagai persoalan kerugian ekonomi, tetapi juga sebagai pelanggaran terhadap privasi, martabat, dan keamanan korban (Republik Indonesia, 2022; UNODC, 2013).

8.3.9 Pemanfaatan AI, Deepfake, dan Otomatisasi Serangan

Perkembangan kecerdasan buatan turut memengaruhi modus operandi kejahatan siber. AI dapat digunakan untuk membuat pesan phishing yang lebih rapi, meniru gaya bahasa lembaga resmi, membuat gambar palsu, meniru suara, membuat video deepfake, melakukan pencarian target secara otomatis, atau menghasilkan skrip penipuan dalam berbagai bahasa. Dengan kemampuan tersebut, pelaku dapat membuat serangan yang lebih meyakinkan dan lebih sulit dikenali oleh korban.

Deepfake dapat digunakan untuk meniru wajah atau suara seseorang, misalnya atasan perusahaan, pejabat, tokoh publik, keluarga, atau rekan kerja. Dalam konteks penipuan bisnis, pelaku dapat menggunakan suara atau video palsu untuk memerintahkan transfer dana. Schmitt dan Flechais (2023) menjelaskan bahwa generative AI dapat memperkuat serangan rekayasa sosial melalui pembuatan konten realistis, personalisasi target, dan otomatisasi infrastruktur serangan.

OJK juga menyoroti bahwa serangan berbasis AI dapat digunakan untuk membuat email phishing lebih meyakinkan, meniru suara manusia dalam panggilan telepon, dan menganalisis data keuangan untuk mengidentifikasi target fraud (OJK, 2024). Hal ini menunjukkan bahwa modus kejahatan siber semakin adaptif. Jika sebelumnya korban dapat mengenali penipuan dari bahasa yang buruk atau tampilan yang mencurigakan, maka penggunaan AI dapat membuat pesan, suara, dan tampilan digital terlihat lebih alami. Oleh karena itu, pencegahan kejahatan siber pada era AI memerlukan verifikasi berlapis, prosedur konfirmasi manual, literasi deepfake, serta kebijakan keamanan yang lebih ketat dalam organisasi (Schmitt & Flechais, 2023).

Untuk memudahkan pemahaman, berbagai modus operandi kejahatan siber dapat diringkas dalam tabel berikut.

Tabel 8.3: Modus Operandi Kejahatan Siber dan Pola Serangannya

Modus Operandi	Pola Serangan	Contoh Praktik	Dampak bagi Korban
Rekayasa sosial	Memanipulasi korban agar memberikan data atau melakukan tindakan tertentu	Pelaku mengaku sebagai petugas bank dan meminta OTP	Akun diambil alih, saldo hilang, data bocor
Phishing dan spoofing	Membuat pesan, situs, atau identitas palsu yang menyerupai pihak resmi	Link palsu marketplace atau bank	Password, PIN, dan data pribadi dicuri
Malware	Menyisipkan perangkat lunak berbahaya ke perangkat korban	File lampiran berisi virus atau keylogger	Data dicuri, perangkat dikendalikan
Ransomware	Mengunci atau mengenkripsi data korban lalu meminta tebusan	Data perusahaan dikunci dan diminta pembayaran	Operasional terganggu, data hilang, pemerasan
Eksploitasi kerentanan	Memanfaatkan celah sistem atau konfigurasi yang lemah	Server tidak diperbarui lalu dibobol	Sistem rusak, data dicuri, layanan berhenti
Pencurian kredensial	Mengambil username, password, PIN, OTP, atau token login	Credential stuffing atau pencurian OTP	Pengambilalihan akun dan transaksi ilegal
Botnet dan DDoS	Menggunakan banyak perangkat terinfeksi untuk membanjiri server	Website layanan publik tidak bisa diakses	Gangguan layanan dan kerugian operasional
Manipulasi transaksi	Memalsukan instruksi pembayaran atau bukti transaksi	Bukti transfer palsu atau instruksi transfer palsu	Kerugian finansial
Pemerasan digital	Mengancam menyebarkan data atau konten pribadi	Ancaman doxing atau sextortion	Tekanan psikologis dan kerugian reputasi
AI dan deepfake	Menggunakan AI untuk membuat konten palsu yang meyakinkan	Suara atasan palsu meminta transfer dana	Penipuan lebih sulit dikenali

Tabel 8.3 menunjukkan bahwa modus operandi kejahatan siber dapat menyerang tiga titik utama, yaitu manusia, sistem, dan data. Serangan terhadap manusia dilakukan melalui rekayasa sosial, phishing, penipuan, dan pemerasan. Serangan terhadap sistem dilakukan melalui malware,

ransomware, eksploitasi celah, botnet, dan DDoS. Sementara itu, serangan terhadap data dilakukan melalui pencurian kredensial, penyalahgunaan data pribadi, pencurian identitas, dan kebocoran informasi.

8.4 Dasar Hukum Penanganan Kejahatan Siber

Dasar hukum penanganan kejahatan siber diperlukan karena tindak pidana di ruang digital memiliki karakter yang berbeda dari kejahatan konvensional. Kejahatan siber dapat dilakukan tanpa pertemuan fisik antara pelaku dan korban, menggunakan sistem elektronik, melibatkan data digital, serta sering melintasi batas wilayah negara. Oleh karena itu, penanganannya tidak cukup hanya mengandalkan hukum pidana umum, tetapi juga membutuhkan aturan khusus mengenai informasi elektronik, transaksi elektronik, pelindungan data pribadi, penyelenggaraan sistem elektronik, pembuktian digital, serta kerja sama internasional.

Gambar 8.4: Kerangka Dasar Hukum Penanganan Kejahatan Siber

Dalam konteks Indonesia, dasar hukum kejahatan siber terutama bertumpu pada Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, hukum acara pidana, serta peraturan pelaksana yang mengatur penyelenggaraan sistem elektronik. Selain itu, perkembangan hukum internasional seperti Budapest Convention, pedoman UNODC, dan praktik kerja sama kepolisian internasional juga penting dijadikan rujukan konseptual karena kejahatan siber sering bersifat lintas negara (Council of Europe, 2001; UNODC, 2013).

8.4.1 Kedudukan Dasar Hukum dalam Penanganan Kejahatan Siber

Dasar hukum memiliki peran penting dalam menentukan apakah suatu perbuatan di ruang digital dapat dikualifikasikan sebagai tindak pidana. Prinsip utama dalam hukum pidana adalah asas legalitas, yaitu seseorang tidak dapat dipidana kecuali berdasarkan aturan hukum yang telah ada sebelumnya. Dalam konteks kejahatan siber, asas legalitas menjadi penting karena tidak semua tindakan yang dianggap merugikan secara digital otomatis dapat dipidana. Perbuatan tersebut harus memenuhi unsur yang diatur dalam peraturan perundang-undangan, baik unsur perbuatan, kesalahan, akibat, maupun hubungan antara pelaku dan perbuatan (Republik Indonesia, 2023; Republik Indonesia, 2024). UU No. 1 Tahun 2023 tentang KUHP berlaku mulai 2 Januari 2026 dan menjadi dasar umum hukum pidana nasional, sedangkan UU No. 1 Tahun 2024 mengubah beberapa ketentuan UU ITE sebagai pengaturan khusus di bidang informasi dan transaksi elektronik.

Kedudukan dasar hukum juga berfungsi untuk menentukan lembaga yang berwenang melakukan penanganan, jenis alat bukti yang dapat digunakan, prosedur penyidikan, serta bentuk sanksi yang dapat dijatuhkan. Dalam perkara siber, bukti tidak hanya berupa benda fisik, tetapi juga dapat berupa informasi elektronik, dokumen elektronik, log sistem, metadata, riwayat transaksi, rekaman komunikasi, dan jejak aktivitas digital. Oleh karena itu, hukum acara pidana dan ketentuan khusus dalam UU ITE perlu dipahami secara bersamaan agar proses penegakan hukum tetap sah, akuntabel, dan tidak melanggar hak-hak pihak yang diperiksa (Republik Indonesia, 2025; Casey, 2011). UU No. 20 Tahun 2025 tentang KUHAP mulai berlaku pada 2 Januari 2026 dan mencabut UU No. 8 Tahun 1981, sehingga pembahasan hukum acara pidana perlu memperhatikan pembaruan ini.

Secara praktis, dasar hukum penanganan kejahatan siber dapat dibagi menjadi beberapa lapis. Lapis pertama adalah hukum pidana materiil yang menentukan perbuatan terlarang dan sanksinya. Lapis kedua adalah hukum acara pidana yang mengatur proses penyelidikan, penyidikan, penuntutan, persidangan, dan pembuktian. Lapis ketiga adalah regulasi sektor digital, seperti penyelenggaraan sistem elektronik, perdagangan elektronik, dan pelindungan data pribadi. Lapis keempat adalah rujukan internasional yang

membantu memahami standar global dalam kriminalisasi, pembuktian, dan kerja sama lintas negara (Council of Europe, 2001; INTERPOL, 2026). Council of Europe menjelaskan bahwa Budapest Convention memuat kriminalisasi perbuatan, perangkat hukum acara, serta kerja sama internasional dalam penanganan cybercrime dan bukti elektronik, sedangkan INTERPOL menekankan pentingnya dukungan kerja sama global dalam menghadapi ancaman siber.

8.4.2 Undang-Undang Informasi dan Transaksi Elektronik sebagai Dasar Utama

Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE merupakan dasar hukum utama dalam penanganan banyak bentuk kejahatan siber di Indonesia. UU ITE mengatur informasi elektronik, dokumen elektronik, transaksi elektronik, sistem elektronik, tanda tangan elektronik, penyelenggara sistem elektronik, serta sejumlah perbuatan yang dilarang dalam ruang digital. Karena itu, UU ITE sering digunakan untuk menangani kasus seperti akses ilegal, intersepsi ilegal, gangguan terhadap sistem elektronik, manipulasi informasi elektronik, penyebaran konten melanggar hukum, dan penipuan berbasis informasi elektronik (Republik Indonesia, 2008; Republik Indonesia, 2024). UU No. 1 Tahun 2024 merupakan perubahan kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Sebagai aturan khusus, UU ITE memiliki hubungan erat dengan asas *lex specialis derogat legi generali*, yaitu aturan khusus dapat mengesampingkan aturan umum sepanjang mengatur hal yang sama secara lebih khusus. Dalam perkara siber, KUHP dapat tetap digunakan apabila perbuatan pelaku memenuhi unsur tindak pidana umum, seperti penipuan, pemerasan, pengancaman, penghinaan, atau pemalsuan. Namun, apabila perbuatan tersebut berkaitan secara khusus dengan sistem elektronik, informasi elektronik, dokumen elektronik, atau transaksi elektronik, maka UU ITE menjadi rujukan penting dalam penilaian hukumnya (Republik Indonesia, 2023; Republik Indonesia, 2024). KUHP baru juga menyatakan Buku Kesatu menjadi pedoman bagi penerapan Buku Kedua dan undang-undang di luar KUHP, kecuali ditentukan lain oleh undang-undang.

Dalam UU ITE, beberapa perbuatan yang relevan dengan kejahatan siber antara lain akses tanpa hak ke sistem elektronik, intersepsi tanpa hak,

perubahan atau perusakan informasi elektronik, gangguan terhadap sistem elektronik, penyebaran konten tertentu yang dilarang, serta manipulasi informasi elektronik agar dianggap seolah-olah data yang sah. Ketentuan ini menunjukkan bahwa UU ITE tidak hanya mengatur perilaku pengguna internet, tetapi juga perlindungan terhadap kerahasiaan, integritas, dan ketersediaan sistem elektronik. Kerangka ini sejalan dengan Budapest Convention yang mengatur kejahatan terhadap kerahasiaan, integritas, dan ketersediaan data serta sistem komputer (Council of Europe, 2001; Republik Indonesia, 2024). Budapest Convention juga menempatkan illegal access, illegal interception, data interference, dan system interference sebagai bentuk utama cybercrime.

Meskipun demikian, penerapan UU ITE harus dilakukan secara hati-hati agar tidak menimbulkan tafsir yang terlalu luas. Penegakan hukum harus memperhatikan unsur kesengajaan, tanpa hak, akibat yang ditimbulkan, konteks perbuatan, serta batas antara ekspresi digital dan tindak pidana. Dalam perkembangannya, UU No. 1 Tahun 2024 lahir sebagai perubahan kedua untuk menyesuaikan beberapa ketentuan UU ITE yang sebelumnya menimbulkan perdebatan dan kebutuhan kepastian hukum (Sitompul, 2024). Sumber JDIH Komdigi juga mencatat bahwa UU No. 1 Tahun 2024 memberi perubahan terhadap pengaturan penyelenggaraan sistem dan transaksi elektronik serta pengaturan pidana.

8.4.3 KUHP dan Hukum Acara Pidana dalam Perkara Siber

Selain UU ITE, KUHP tetap memiliki peran dalam penanganan kejahatan siber. Banyak kejahatan siber pada dasarnya merupakan bentuk baru dari kejahatan konvensional yang dilakukan melalui sarana digital. Penipuan online, pemerasan digital, pengancaman melalui media sosial, pemalsuan identitas, perjudian online, dan penghinaan digital dapat memiliki hubungan dengan tindak pidana yang dikenal dalam hukum pidana umum. Oleh karena itu, aparat penegak hukum perlu menilai apakah perbuatan tersebut lebih tepat dikenakan ketentuan KUHP, UU ITE, atau kombinasi keduanya sesuai unsur perbuatan yang terbukti (Republik Indonesia, 2023; UNODC, 2013). UU No. 1 Tahun 2023 tentang KUHP berlaku pada 2 Januari 2026 dan berisi aturan umum serta tindak pidana dalam Buku Kesatu dan Buku Kedua.

KUHP berfungsi sebagai dasar hukum pidana materiil, sedangkan hukum acara pidana mengatur bagaimana proses penegakan hukum dilakukan. Dalam perkara siber, hukum acara pidana mengatur tahapan mulai dari penyelidikan, penyidikan, penetapan tersangka, penggeledahan, penyitaan, pemeriksaan saksi dan ahli, penuntutan, pemeriksaan di persidangan, hingga putusan pengadilan. Prosedur ini penting agar penanganan kejahatan siber tidak hanya mengejar pelaku, tetapi juga tetap menjaga hak tersangka, korban, saksi, dan pihak lain yang terlibat (Republik Indonesia, 2025; Casey, 2011). UU No. 20 Tahun 2025 tentang KUHAP berlaku mulai 2 Januari 2026 dan menggantikan UU No. 8 Tahun 1981.

Dalam perkara siber, hukum acara pidana memiliki tantangan khusus karena bukti elektronik bersifat mudah berubah, mudah disalin, mudah dihapus, dan dapat berada di server yang berbeda wilayah. Oleh karena itu, proses pengamanan barang bukti digital harus memperhatikan keaslian, integritas, serta rantai penguasaan barang bukti. Bukti digital yang diperoleh dengan prosedur yang lemah dapat dipersoalkan di persidangan karena keabsahannya diragukan. Casey (2011) menekankan pentingnya prosedur forensik digital untuk menjaga keandalan bukti elektronik dalam proses hukum, sedangkan INTERPOL menegaskan bahwa bukti digital bersifat mudah berubah dan membutuhkan dukungan kerja sama penegakan hukum secara global (Casey, 2011; INTERPOL, 2026). INTERPOL secara eksplisit menyebut digital evidence sebagai bukti yang mudah berubah dalam konteks respons global terhadap ancaman siber.

Dengan demikian, KUHP dan hukum acara pidana tidak dapat dipisahkan dari penanganan kejahatan siber. UU ITE dapat menjadi dasar khusus untuk menilai perbuatan di ruang elektronik, tetapi proses pembuktian dan penegakan hukumnya tetap memerlukan hukum acara pidana. Kombinasi antara hukum pidana materiil, UU ITE, dan hukum acara pidana menjadi penting agar penanganan kejahatan siber memiliki dasar yang jelas, tidak sewenang-wenang, dan dapat dipertanggungjawabkan di pengadilan (Republik Indonesia, 2023; Republik Indonesia, 2025). Kedua aturan pidana nasional tersebut saat ini telah memasuki rezim baru karena KUHP dan KUHAP baru sama-sama berlaku mulai 2 Januari 2026.

8.4.4 Undang-Undang Pelindungan Data Pribadi dalam Kejahatan Siber

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi atau UU PDP merupakan dasar hukum penting dalam penanganan kejahatan siber yang berkaitan dengan data pribadi. Banyak kejahatan siber dilakukan dengan cara mencuri, mengumpulkan, menjual, menyebarkan, atau menggunakan data pribadi tanpa hak. Data pribadi yang bocor dapat digunakan untuk penipuan, pencurian identitas, pinjaman online ilegal, pembajakan akun, pemerasan digital, dan penyalahgunaan layanan keuangan. Oleh karena itu, UU PDP menjadi pelengkap penting bagi UU ITE dalam memberikan perlindungan terhadap individu sebagai subjek data pribadi (Republik Indonesia, 2022; Solove, 2021). UU PDP mengatur asas, jenis data pribadi, hak subjek data, pemrosesan data pribadi, kewajiban pengendali dan prosesor data, sanksi administratif, penyelesaian sengketa, larangan penggunaan data pribadi, dan ketentuan pidana.

UU PDP membedakan data pribadi menjadi data pribadi umum dan data pribadi spesifik. Pembedaan ini penting dalam kejahatan siber karena tidak semua data memiliki tingkat risiko yang sama. Data seperti nama, alamat, nomor telepon, email, data keuangan, data biometrik, data kesehatan, dan data anak dapat menimbulkan dampak yang berbeda apabila disalahgunakan. Semakin sensitif data yang dicuri atau disebarkan, semakin besar potensi kerugian bagi korban. Prinsip serupa juga dikenal dalam GDPR yang menempatkan perlindungan individu dalam pemrosesan data pribadi sebagai bagian penting dari tata kelola data modern (Republik Indonesia, 2022; European Parliament and Council of the European Union, 2016). GDPR merupakan Regulation (EU) 2016/679 yang mengatur perlindungan orang perseorangan dalam pemrosesan data pribadi.

Dalam penanganan kejahatan siber, UU PDP dapat digunakan untuk menilai apakah suatu pemrosesan data pribadi dilakukan secara sah atau melanggar hukum. Misalnya, pengambilan data pelanggan tanpa izin, penjualan database pengguna, penggunaan data untuk membuka akun palsu, atau penyebaran data pribadi korban dapat dikaji melalui prinsip pelindungan data pribadi. UU PDP juga penting karena memperkuat posisi korban sebagai subjek data yang memiliki hak atas keamanan, kerahasiaan,

pembatasan penggunaan, dan pemulihan apabila terjadi pelanggaran data (Republik Indonesia, 2022; OECD, 2013).

UU PDP juga memiliki hubungan dengan kewajiban pengendali dan prosesor data. Dalam konteks platform digital, organisasi yang mengumpulkan dan mengelola data pengguna wajib menerapkan pengamanan yang memadai. Apabila terjadi kebocoran atau penyalahgunaan data, perlu dinilai apakah ada kelalaian dalam pengelolaan data, lemahnya sistem keamanan, atau pelanggaran prinsip pemrosesan data. NIST Cybersecurity Framework 2.0 menekankan pentingnya fungsi tata kelola, identifikasi, perlindungan, deteksi, respons, dan pemulihan dalam mengelola risiko keamanan siber, sehingga relevan dengan kewajiban organisasi dalam melindungi data pribadi (NIST, 2024; Republik Indonesia, 2022). NIST CSF 2.0 menyebut fungsi govern, identify, protect, detect, respond, dan recover sebagai bagian dari pengelolaan insiden keamanan siber.

8.4.5 Peraturan Penyelenggaraan Sistem Elektronik dan Transaksi Digital

Penanganan kejahatan siber juga berkaitan dengan regulasi penyelenggaraan sistem elektronik. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur aspek penting dalam penggunaan sistem elektronik, seperti penyelenggaraan sistem, transaksi elektronik, dokumen elektronik, tanda tangan elektronik, sertifikasi elektronik, serta kewajiban penyelenggara sistem elektronik. Aturan ini penting karena kejahatan siber sering terjadi pada layanan yang disediakan oleh penyelenggara sistem elektronik, seperti platform digital, layanan cloud, marketplace, aplikasi keuangan, dan sistem informasi organisasi (Republik Indonesia, 2019b). PP No. 71 Tahun 2019 berlaku sejak 10 Oktober 2019 dan mencabut PP No. 82 Tahun 2012.

Regulasi penyelenggaraan sistem elektronik memberikan dasar bahwa pihak yang mengelola sistem digital harus memperhatikan keamanan, keandalan, dan tanggung jawab dalam penyelenggaraan layanan. Jika suatu sistem lemah, tidak aman, atau tidak memiliki mekanisme pengendalian risiko yang memadai, maka pengguna dapat mengalami kerugian akibat kebocoran data, transaksi tidak sah, pencurian akun, atau gangguan layanan. Oleh sebab itu, penanganan kejahatan siber tidak hanya berfokus pada pelaku langsung,

tetapi juga dapat menilai tanggung jawab penyelenggara sistem elektronik dalam menyediakan sistem yang aman (Republik Indonesia, 2019a; NIST, 2024). NIST CSF 2.0 menempatkan fungsi govern, identify, protect, detect, respond, dan recover sebagai kerangka pengelolaan risiko keamanan siber organisasi.

Selain PP 71 Tahun 2019, Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik juga relevan dalam penanganan kejahatan siber yang terjadi dalam transaksi digital. Banyak kasus penipuan online, barang tidak dikirim, identitas penjual palsu, manipulasi bukti transaksi, dan penyalahgunaan marketplace berkaitan dengan aktivitas perdagangan elektronik. Dalam konteks ini, PP PMSE dapat menjadi dasar untuk memahami hubungan hukum antara pelaku usaha, konsumen, dan platform digital (Republik Indonesia, 2019b). PP No. 80 Tahun 2019 berlaku sejak 25 November 2019 dan mengatur perdagangan melalui sistem elektronik (Republik Indonesia, 2019a).

Peraturan penyelenggaraan sistem elektronik dan perdagangan elektronik juga penting dalam menentukan pencegahan dan pemulihan. Misalnya, platform perlu menyediakan mekanisme pelaporan, penanganan akun palsu, pemutusan akses terhadap konten atau aktivitas melanggar hukum, perlindungan data pengguna, serta kerja sama dengan aparat penegak hukum. Dengan demikian, dasar hukum kejahatan siber tidak hanya berada pada aturan pidana, tetapi juga pada aturan administratif dan sektoral yang mengatur tata kelola layanan digital (Republik Indonesia, 2019a; Republik Indonesia, 2019b). Kedua PP tersebut sama-sama berada dalam bidang telekomunikasi, informatika, siber, internet, dan transaksi elektronik.

8.4.6 Kerja Sama Internasional dan Standar Global Penanganan Kejahatan Siber

Kejahatan siber sering bersifat lintas negara karena pelaku, korban, server, rekening, domain, data, dan perangkat dapat berada di wilayah hukum yang berbeda. Kondisi ini menyebabkan penanganan kejahatan siber membutuhkan kerja sama internasional. Aparat penegak hukum suatu negara sering tidak dapat langsung mengambil data atau menindak pelaku yang berada di negara lain tanpa mekanisme hukum yang sah. Oleh karena

itu, kerja sama internasional menjadi bagian penting dalam penanganan cybercrime dan bukti elektronik (Council of Europe, 2001; UNODC, 2013).

Budapest Convention merupakan salah satu rujukan internasional penting dalam penanganan kejahatan siber. Konvensi ini mengatur kriminalisasi perbuatan siber, perangkat hukum acara untuk penyidikan dan pengamanan bukti elektronik, serta kerja sama internasional. Perbuatan yang diatur mencakup akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, penyalahgunaan perangkat, pemalsuan berbasis komputer, penipuan berbasis komputer, dan pelanggaran tertentu yang berkaitan dengan konten serta hak kekayaan intelektual (Council of Europe, 2001; Council of Europe, 2024). Council of Europe menjelaskan bahwa Budapest Convention menyediakan kriminalisasi perbuatan, alat hukum acara untuk investigasi dan pengamanan bukti elektronik, serta kerja sama internasional yang efektif.

Selain Budapest Convention, lembaga internasional seperti UNODC dan INTERPOL juga memiliki peran penting dalam memberikan pedoman, fasilitasi kerja sama, pertukaran informasi, dan peningkatan kapasitas aparat penegak hukum. UNODC menekankan bahwa kejahatan siber merupakan tantangan global yang membutuhkan kerangka hukum, kapasitas investigasi, dan kerja sama lintas negara. INTERPOL juga menyediakan platform berbagi informasi yang aman, dukungan operasional, dan koordinasi bagi penegak hukum global dalam menghadapi ancaman siber (UNODC, 2013; INTERPOL, 2026). INTERPOL menyatakan bahwa pihaknya mendukung penegak hukum global untuk merespons ancaman siber utama melalui kolaborasi dan platform berbagi informasi yang aman.

Standar global juga penting dalam aspek tata kelola keamanan siber. NIST Cybersecurity Framework 2.0, misalnya, tidak secara langsung menjadi hukum pidana, tetapi dapat menjadi rujukan tata kelola risiko keamanan siber bagi organisasi. Kerangka ini membantu organisasi mengidentifikasi aset, melindungi sistem, mendeteksi insiden, merespons serangan, dan memulihkan layanan setelah insiden. Dalam konteks hukum, standar seperti ini dapat membantu menilai apakah organisasi telah menerapkan praktik keamanan yang wajar dan bertanggung jawab (NIST, 2024; ISO/IEC, 2022). NIST CSF 2.0 menjelaskan bahwa fungsi govern, identify, dan protect membantu pencegahan serta persiapan insiden, sedangkan govern, detect, respond, dan recover membantu menemukan dan mengelola insiden.

Untuk memudahkan pemahaman, dasar hukum dan rujukan penanganan kejahatan siber dapat diringkas dalam tabel berikut.

Tabel 8.4: Dasar Hukum dan Rujukan Penanganan Kejahatan Siber

Dasar Hukum/Rujukan	Ruang Lingkup	Relevansi dalam Penanganan Kejahatan Siber
UU No. 1 Tahun 2024 tentang Perubahan Kedua UU ITE	Informasi elektronik, transaksi elektronik, sistem elektronik, larangan perbuatan digital tertentu	Menjadi dasar utama penanganan akses ilegal, intersepsi ilegal, gangguan sistem, manipulasi informasi elektronik, dan konten digital melanggar hukum
UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi	Data pribadi, hak subjek data, kewajiban pengendali/prosesor data, larangan penggunaan data pribadi	Digunakan dalam perkara pencurian data, penyalahgunaan data pribadi, kebocoran data, dan pencurian identitas
UU No. 1 Tahun 2023 tentang KUHP	Aturan umum dan tindak pidana nasional	Menjadi dasar pidana umum untuk penipuan, pemerasan, pengancaman, pemalsuan, dan tindak pidana lain yang dapat dilakukan melalui media digital
UU No. 20 Tahun 2025 tentang KUHAP	Proses penyelidikan, penyidikan, penuntutan, persidangan, dan pembuktian	Menjadi dasar hukum acara dalam proses penanganan perkara siber sejak penyidikan sampai persidangan
PP No. 71 Tahun 2019 tentang PSTE	Penyelenggaraan sistem elektronik dan transaksi elektronik	Mengatur tanggung jawab penyelenggara sistem elektronik dalam menyediakan sistem yang aman dan andal
PP No. 80 Tahun 2019 tentang PMSE	Perdagangan melalui sistem elektronik	Relevan untuk kasus penipuan online, transaksi

Dasar Hukum/Rujukan	Ruang Lingkup	Relevansi dalam Penanganan Kejahatan Siber
		e-commerce bermasalah, dan tanggung jawab platform dalam perdagangan digital
Budapest Convention	Kriminalisasi cybercrime, prosedur hukum acara, dan kerja sama internasional	Menjadi rujukan global untuk pengaturan cybercrime dan bukti elektronik
UNODC dan INTERPOL	Pedoman, kerja sama, pertukaran informasi, dan peningkatan kapasitas penegak hukum	Membantu penanganan kejahatan siber lintas negara dan kejahatan terorganisasi digital
NIST Cybersecurity Framework 2.0	Tata kelola risiko keamanan siber	Menjadi rujukan organisasi dalam pencegahan, deteksi, respons, dan pemulihan insiden siber

Tabel 8.4 menunjukkan bahwa penanganan kejahatan siber tidak hanya menggunakan satu dasar hukum. UU ITE memang menjadi dasar utama untuk banyak kasus siber, tetapi UU PDP, KUHP, KUHAP, PP PSTE, PP PMSE, dan rujukan internasional tetap diperlukan untuk memberikan penanganan yang lebih utuh. Perkara siber sering melibatkan perbuatan pidana, bukti elektronik, data pribadi, transaksi digital, tanggung jawab platform, serta kerja sama lintas negara. Oleh karena itu, penegak hukum perlu memahami hubungan antarketentuan tersebut agar penerapan hukum tidak keliru.

8.5 Pertanggungjawaban Pidana dalam Kejahatan Siber

Pertanggungjawaban pidana dalam kejahatan siber berkaitan dengan pertanyaan apakah seseorang, kelompok, korporasi, atau pihak tertentu dapat dimintai tanggung jawab atas perbuatan melawan hukum yang dilakukan melalui sistem elektronik. Dalam hukum pidana, tidak semua kerugian digital otomatis menimbulkan pertanggungjawaban pidana. Suatu perbuatan

baru dapat dipertanggungjawabkan secara pidana apabila terdapat dasar hukum yang jelas, perbuatan yang memenuhi unsur tindak pidana, kesalahan pelaku, kemampuan bertanggung jawab, serta hubungan antara perbuatan pelaku dan akibat yang ditimbulkan.

Dalam konteks kejahatan siber, pembuktian pertanggungjawaban pidana sering lebih kompleks dibandingkan perkara konvensional. Pelaku dapat menyamarkan identitas, menggunakan perangkat orang lain, memakai jaringan publik, memanfaatkan akun palsu, menggunakan server luar negeri, atau menghapus jejak digital. Oleh karena itu, pertanggungjawaban pidana dalam kejahatan siber tidak cukup hanya dilihat dari adanya akun, perangkat, atau alamat IP tertentu. Aparat penegak hukum perlu membuktikan siapa pelaku sebenarnya, bagaimana perbuatannya dilakukan, apa niat atau kesalahannya, bukti elektronik apa yang mendukung, serta ketentuan hukum mana yang dilanggar (Casey, 2011; UNODC, 2013).

Secara umum, pertanggungjawaban pidana dalam kejahatan siber dapat berkaitan dengan pelaku perseorangan, pelaku yang bekerja sama dengan pihak lain, korporasi, penyelenggara sistem elektronik, atau pihak yang membantu terjadinya tindak pidana. Dalam perkara tertentu, satu peristiwa siber dapat melibatkan beberapa bentuk pertanggungjawaban sekaligus. Misalnya, dalam kasus pencurian data, terdapat pihak yang meretas sistem, pihak yang membeli data, pihak yang menjual data, pihak yang menggunakan data untuk penipuan, dan pihak organisasi yang lalai menjaga keamanan sistem. Oleh karena itu, pertanggungjawaban pidana dalam kejahatan siber harus dianalisis secara hati-hati agar tidak keliru menetapkan pihak yang bertanggung jawab.

8.5.1 Konsep Pertanggungjawaban Pidana

Pertanggungjawaban pidana merupakan hubungan antara perbuatan pidana dengan kesalahan pelaku. Dalam hukum pidana, seseorang tidak cukup hanya terbukti melakukan perbuatan yang dilarang, tetapi juga harus dapat dipersalahkan atas perbuatan tersebut. Prinsip ini dikenal melalui asas bahwa tidak ada pidana tanpa kesalahan. Artinya, pemidanaan harus didasarkan pada adanya perbuatan yang dilarang oleh hukum dan adanya kesalahan pada diri pelaku (Moeljatno, 2008; Remmelink, 2003).

Dalam kejahatan siber, konsep ini tetap berlaku. Pelaku tidak dapat dipidana hanya karena perangkatnya digunakan untuk menyerang sistem atau akunnya muncul dalam suatu aktivitas digital. Harus dibuktikan bahwa pelaku memiliki hubungan nyata dengan perbuatan tersebut, mengetahui atau menghendaki perbuatan itu, atau setidaknya lalai dalam kondisi yang menurut hukum dapat menimbulkan pertanggungjawaban pidana. Dengan demikian, pembuktian pertanggungjawaban pidana harus membedakan antara pemilik perangkat, pengguna perangkat, pihak yang akunnya dibajak, dan pelaku yang benar-benar melakukan tindak pidana (Casey, 2011; UNODC, 2013).

Dalam sistem hukum Indonesia, pertanggungjawaban pidana juga berkaitan dengan asas legalitas. Asas ini menegaskan bahwa seseorang hanya dapat dipidana berdasarkan aturan hukum yang telah ada sebelum perbuatan dilakukan. Dalam konteks kejahatan siber, asas legalitas penting karena perkembangan teknologi sering melahirkan modus baru yang belum tentu secara langsung disebutkan dalam undang-undang. Oleh karena itu, aparat penegak hukum perlu menghubungkan perbuatan digital dengan unsur tindak pidana yang sudah diatur, baik dalam UU ITE, UU PDP, KUHP, maupun peraturan terkait lainnya (Republik Indonesia, 2023a, 2024b). UU Nomor 1 Tahun 2024 merupakan perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sedangkan UU Nomor 1 Tahun 2023 tentang KUHP menjadi dasar umum hukum pidana nasional.

Pertanggungjawaban pidana juga harus memperhatikan kemampuan bertanggung jawab. Seseorang hanya dapat dimintai pertanggungjawaban pidana apabila ia mampu memahami akibat perbuatannya dan mampu menentukan kehendaknya. Dalam konteks digital, hal ini dapat menjadi penting apabila pelaku adalah anak, orang dengan gangguan kejiwaan, atau orang yang berada dalam kondisi tertentu yang memengaruhi kemampuan bertanggung jawab. Dengan demikian, pertanggungjawaban pidana tidak hanya menilai perbuatan secara teknis, tetapi juga keadaan pelaku sebagai subjek hukum (Moeljatno, 2008; Republik Indonesia, 2023).

8.5.2 Unsur Perbuatan Melawan Hukum dalam Ruang Siber

Perbuatan melawan hukum dalam ruang siber dapat berbentuk tindakan aktif maupun pasif. Tindakan aktif misalnya mengakses sistem tanpa hak,

menyebarkan malware, mencuri data, mengubah informasi elektronik, melakukan penipuan online, atau menyebarkan konten melanggar hukum. Tindakan pasif dapat berupa kelalaian tertentu yang menyebabkan sistem tidak aman, data pribadi bocor, atau kewajiban hukum tidak dipenuhi. Namun, untuk dapat dipidana, perbuatan tersebut harus memenuhi unsur yang diatur dalam undang-undang (Republik Indonesia, 2022; Republik Indonesia, 2024).

Gambar 8.5: Alur Pertanggungjawaban Pidana dalam Kejahatan Siber

Dalam UU ITE, beberapa perbuatan digital yang dapat dikaitkan dengan pertanggungjawaban pidana antara lain akses tanpa hak, intersepsi tanpa hak, manipulasi informasi elektronik, gangguan terhadap sistem elektronik, dan penyebaran informasi elektronik tertentu yang dilarang. Unsur “tanpa hak”

menjadi penting karena tidak semua akses terhadap sistem elektronik merupakan kejahatan. Seorang administrator sistem, auditor keamanan, atau pengguna yang memiliki izin dapat mengakses sistem secara sah. Sebaliknya, akses menjadi bermasalah apabila dilakukan tanpa izin, melampaui kewenangan, atau bertujuan melakukan perbuatan melawan hukum (Republik Indonesia, 2024; Council of Europe, 2001). Budapest Convention juga menempatkan *illegal access*, *illegal interception*, *data interference*, dan *system interference* sebagai bentuk penting tindak pidana terhadap sistem komputer.

Perbuatan melawan hukum dalam ruang siber juga dapat terjadi melalui penyalahgunaan data pribadi. UU PDP mengatur bahwa data pribadi harus diproses berdasarkan prinsip, dasar pemrosesan, dan tujuan yang sah. Pengumpulan, penggunaan, pengungkapan, penjualan, atau penyebaran data pribadi tanpa hak dapat menimbulkan konsekuensi hukum. Dalam banyak kasus, pencurian data pribadi menjadi awal dari tindak pidana lain, seperti penipuan, pemerasan, pencurian identitas, atau pinjaman online ilegal (Republik Indonesia, 2022; Solove, 2021). UU Nomor 27 Tahun 2022 mengatur jenis data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, larangan penggunaan data pribadi, serta ketentuan pidana terkait pelindungan data pribadi.

Analisis perbuatan melawan hukum dalam ruang siber harus memperhatikan konteks teknis. Misalnya, tindakan memindai sistem belum tentu sama dengan peretasan apabila dilakukan dalam kegiatan pengujian keamanan yang sah. Namun, pemindaian yang dilanjutkan dengan eksploitasi celah, pencurian data, atau perusakan sistem dapat masuk dalam kategori perbuatan melawan hukum. Oleh karena itu, unsur tindakan, izin, kewenangan, tujuan, akibat, dan bukti digital perlu dinilai secara menyeluruh (Casey, 2011; Council of Europe, 2001).

8.5.3 Kesalahan, Kesengajaan, dan Kelalaian dalam Kejahatan Siber

Kesalahan merupakan unsur penting dalam pertanggungjawaban pidana. Dalam kejahatan siber, kesalahan dapat berbentuk kesengajaan maupun kelalaian. Kesengajaan terjadi ketika pelaku mengetahui dan menghendaki perbuatan serta akibatnya, misalnya dengan sengaja mencuri data, menyebarkan malware, mengirim tautan phishing, atau masuk ke sistem

tanpa izin. Kelalaian terjadi ketika seseorang tidak berhati-hati dalam kondisi yang seharusnya dapat diperkirakan menimbulkan risiko hukum atau kerugian (Moeljatno, 2008; Remmelink, 2003).

Kesengajaan dalam kejahatan siber dapat dilihat dari beberapa indikator, seperti penggunaan alat peretas, penyamaran identitas, pengiriman pesan palsu secara massal, pembuatan situs tiruan, pencatatan kredensial korban, atau upaya menghapus jejak digital. Misalnya, pelaku yang membuat situs palsu menyerupai bank dan menggunakannya untuk mencuri password korban menunjukkan adanya rencana dan kehendak untuk melakukan penipuan. Dalam kasus seperti ini, kesengajaan dapat dibuktikan melalui rangkaian tindakan, alat yang digunakan, komunikasi pelaku, dan jejak digital yang ditemukan (Casey, 2011; UNODC, 2013).

Kelalaian dalam kejahatan siber sering muncul dalam konteks pengelolaan sistem elektronik dan data pribadi. Organisasi atau pihak pengendali data dapat dipersoalkan apabila tidak menerapkan langkah pengamanan yang wajar, tidak menutup celah keamanan yang diketahui, tidak membatasi akses data, atau tidak merespons insiden secara memadai. Dalam konteks UU PDP, pengendali dan prosesor data memiliki kewajiban dalam pemrosesan data pribadi. Jika kewajiban tersebut diabaikan dan menimbulkan kerugian, maka dapat muncul konsekuensi administratif, perdata, atau pidana sesuai ketentuan hukum yang berlaku (Republik Indonesia, 2022; NIST, 2024).

Namun, tidak semua insiden keamanan otomatis berarti ada kesalahan pidana. Suatu sistem dapat tetap diserang meskipun sudah menerapkan keamanan yang wajar. Oleh karena itu, penilaian kesalahan harus membedakan antara serangan yang tidak dapat dicegah secara wajar dan kelalaian nyata dalam pengamanan sistem. Standar keamanan seperti NIST Cybersecurity Framework dapat digunakan sebagai rujukan tata kelola risiko, meskipun bukan satu-satunya dasar untuk menentukan pertanggungjawaban pidana. NIST CSF 2.0 menekankan fungsi *govern*, *identify*, *protect*, *detect*, *respond*, dan *recover* dalam pengelolaan risiko keamanan siber (NIST, 2024; Republik Indonesia, 2022).

8.5.4 Pertanggungjawaban Pelaku Perseorangan

Pelaku perseorangan adalah subjek yang paling umum dalam pertanggungjawaban pidana kejahatan siber. Pelaku dapat berupa individu

yang melakukan akses ilegal, menyebarkan malware, mencuri data, melakukan penipuan online, melakukan pemerasan digital, atau menyebarkan konten yang melanggar hukum. Dalam menentukan pertanggungjawaban pelaku perseorangan, aparat penegak hukum perlu membuktikan identitas pelaku, hubungan pelaku dengan akun atau perangkat yang digunakan, unsur perbuatan, unsur kesalahan, serta akibat yang ditimbulkan (Casey, 2011; UNODC, 2013).

Pembuktian terhadap pelaku perseorangan dalam kejahatan siber sering menghadapi tantangan karena identitas digital dapat dipalsukan. Seseorang dapat menggunakan akun palsu, jaringan publik, VPN, perangkat orang lain, atau akun yang telah dibajak. Karena itu, alamat IP atau akun digital tidak boleh dipahami sebagai satu-satunya bukti pelaku. Bukti tersebut perlu dikaitkan dengan bukti lain, seperti perangkat yang digunakan, riwayat login, metadata, transaksi, komunikasi, saksi, penguasaan akun, dan motif pelaku. Prinsip ini penting agar tidak terjadi kesalahan identifikasi terhadap orang yang sebenarnya menjadi korban pembajakan akun (Casey, 2011; INTERPOL, 2026).

Pelaku perseorangan juga dapat bertanggung jawab atas kejahatan siber yang dilakukan bersama-sama. Dalam praktiknya, penipuan online atau pencurian data sering melibatkan beberapa orang dengan peran berbeda. Ada yang membuat situs palsu, mengirim pesan phishing, menarik dana, menyediakan rekening penampung, menjual data, atau menyembunyikan hasil kejahatan. Setiap pihak dapat dimintai pertanggungjawaban sesuai peran, kesengajaan, dan kontribusinya dalam tindak pidana (Republik Indonesia, 2023; UNODC, 2013).

Pertanggungjawaban pelaku perseorangan juga perlu memperhatikan kedudukan korban. Dalam kasus tertentu, korban mungkin secara tidak sadar membantu pelaku, misalnya dengan memberikan OTP karena tertipu. Namun, hal tersebut tidak serta-merta menghapus pertanggungjawaban pidana pelaku. Rekayasa sosial justru menunjukkan adanya manipulasi terhadap korban. Oleh karena itu, penilaian pidana harus membedakan antara kelalaian korban dalam menjaga data dan tindakan aktif pelaku yang memperdaya korban (Nurse, 2018).

8.5.5 Pertanggungjawaban Korporasi dan Penyelenggara Sistem Elektronik

Dalam ekosistem digital, pertanggungjawaban pidana tidak hanya dapat melekat pada individu, tetapi juga pada korporasi. Korporasi dapat dimintai pertanggungjawaban apabila tindak pidana dilakukan untuk kepentingan korporasi, dilakukan oleh pengurus atau pihak yang memiliki hubungan kerja, atau terjadi karena kebijakan, pembiaran, atau kelalaian dalam pengendalian organisasi. Konsep ini penting karena banyak layanan digital dikelola oleh badan usaha yang mengumpulkan data, memproses transaksi, dan menyediakan sistem elektronik bagi pengguna (Republik Indonesia, 2023; Republik Indonesia, 2022).

Penyelenggara sistem elektronik memiliki kewajiban untuk menyelenggarakan sistem secara andal, aman, dan bertanggung jawab. Jika platform, aplikasi, atau organisasi mengelola data pengguna, maka organisasi tersebut harus menerapkan pengamanan yang memadai. Kegagalan menjaga keamanan sistem dapat menimbulkan kebocoran data, pengambilalihan akun, transaksi tidak sah, dan kerugian pengguna. Dalam konteks ini, penilaian tanggung jawab tidak hanya diarahkan kepada pelaku langsung yang menyerang sistem, tetapi juga dapat menilai apakah penyelenggara sistem elektronik telah memenuhi kewajiban hukumnya (Republik Indonesia, 2019; NIST, 2024).

UU PDP juga memberikan dasar penting untuk menilai tanggung jawab pengendali data pribadi dan prosesor data pribadi. Pengendali data menentukan tujuan dan kendali pemrosesan data, sedangkan prosesor data memproses data atas nama pengendali. Apabila terjadi penyalahgunaan data, kebocoran data, atau pemrosesan tanpa dasar yang sah, perlu dianalisis apakah terdapat pelanggaran kewajiban oleh pengendali atau prosesor data. Dalam hal tertentu, pelanggaran dapat menimbulkan sanksi administratif, gugatan perdata, atau ketentuan pidana sesuai undang-undang (European Parliament and Council of the European Union, 2016a; Republik Indonesia, 2022b).

Namun, pertanggungjawaban korporasi atau penyelenggara sistem elektronik tidak boleh disimpulkan secara otomatis hanya karena terjadi insiden. Harus dilihat apakah terdapat pelanggaran kewajiban, kelalaian yang nyata, keuntungan yang diperoleh, pembiaran, atau kegagalan

menerapkan pengamanan yang wajar. Penilaian ini membutuhkan analisis hukum dan teknis, termasuk audit keamanan, kebijakan internal, pembagian kewenangan, prosedur respons insiden, dokumentasi pengamanan, serta bukti komunikasi organisasi (NIST, 2024; Casey, 2011).

8.5.6 Penyertaan, Pembantuan, dan Peran Pihak Lain

Kejahatan siber sering dilakukan secara bersama-sama. Dalam satu kasus penipuan online, misalnya, terdapat pelaku yang mencari target, membuat pesan palsu, mengelola akun media sosial, membuat situs phishing, menyediakan rekening penampung, menarik dana, dan menjual data korban. Meskipun tidak semua pihak melakukan tindakan utama, masing-masing dapat memiliki peran dalam terlaksananya tindak pidana. Oleh karena itu, konsep penyertaan dan pembantuan menjadi penting dalam pertanggungjawaban pidana kejahatan siber (Republik Indonesia, 2023; UNODC, 2013).

Penyertaan dapat terjadi ketika beberapa orang bekerja sama melakukan kejahatan siber. Pembantuan dapat terjadi ketika seseorang memberi sarana, informasi, akun, rekening, perangkat, atau akses yang memudahkan pelaku melakukan kejahatan. Misalnya, seseorang yang menyediakan rekening untuk menampung hasil penipuan online dapat diperiksa apakah ia mengetahui tujuan penggunaan rekening tersebut. Jika ia mengetahui bahwa rekening digunakan untuk menampung hasil kejahatan, maka dapat timbul pertanggungjawaban sesuai perannya (Moeljatno, 2008; Republik Indonesia, 2023a).

Dalam ekosistem digital, peran pihak lain juga dapat muncul melalui penyedia layanan, pengelola grup, admin platform, pemilik server, penyedia domain, atau pihak yang memperjualbelikan data. Tidak semua pihak tersebut otomatis bertanggung jawab pidana. Pertanggungjawaban harus dilihat berdasarkan pengetahuan, niat, kendali, manfaat, dan kontribusi nyata terhadap tindak pidana. Pihak yang hanya menyediakan layanan umum tanpa mengetahui adanya kejahatan tentu berbeda dengan pihak yang secara sadar membantu menyembunyikan, memfasilitasi, atau memperoleh keuntungan dari kejahatan siber (UNODC, 2013; Council of Europe, 2001).

Dalam beberapa kasus, pembuktian penyertaan dan pembantuan lebih sulit daripada membuktikan pelaku utama. Pelaku dapat menggunakan

komunikasi terenkripsi, akun sementara, pembayaran digital, atau identitas palsu. Oleh sebab itu, bukti digital seperti riwayat percakapan, transaksi, metadata, alamat IP, catatan transfer, log akses, dan keterkaitan akun menjadi penting untuk menunjukkan hubungan antar pelaku. Namun, bukti tersebut tetap harus diperoleh dan dianalisis dengan prosedur yang sah agar dapat digunakan dalam proses hukum (Casey, 2011; INTERPOL, 2026).

8.5.7 Pembuktian Pertanggungjawaban Pidana dalam Kejahatan Siber

Pembuktian merupakan bagian penting dalam menentukan pertanggungjawaban pidana. Dalam kejahatan siber, pembuktian tidak hanya bertujuan menunjukkan bahwa suatu peristiwa terjadi, tetapi juga membuktikan siapa pelakunya, apa perannya, bagaimana perbuatan dilakukan, unsur hukum apa yang terpenuhi, serta apakah terdapat kesalahan pada diri pelaku. Oleh karena itu, bukti elektronik memiliki posisi yang sangat penting dalam perkara siber (Casey, 2011; Republik Indonesia, 2024).

Bukti elektronik dapat berupa informasi elektronik, dokumen elektronik, log akses, metadata, rekaman percakapan, email, tangkapan layar, file, riwayat transaksi, alamat IP, data perangkat, rekaman CCTV digital, dan catatan aktivitas sistem. Namun, bukti elektronik memiliki karakter yang mudah diubah, dihapus, disalin, atau dimanipulasi. Karena itu, pengumpulan dan analisis bukti elektronik harus memperhatikan prinsip forensik digital, seperti integritas data, keaslian bukti, dokumentasi proses, serta rantai penguasaan barang bukti (Casey, 2011; INTERPOL, 2026).

Dalam hukum Indonesia, UU ITE memberikan pengakuan terhadap informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah sepanjang memenuhi ketentuan peraturan perundang-undangan. Hal ini menjadi dasar penting karena banyak perkara siber tidak memiliki bukti fisik seperti perkara konvensional. Namun, pengakuan terhadap bukti elektronik tetap harus diikuti dengan pembuktian bahwa bukti tersebut asli, relevan, dan diperoleh secara sah (Republik Indonesia, 2024b, 2025a). UU Nomor 20 Tahun 2025 tentang KUHAP mengatur pembaruan hukum acara pidana dan mulai berlaku pada 2 Januari 2026, sehingga pembahasan pembuktian pidana perlu memperhatikan rezim hukum acara terbaru.

Pembuktian pertanggungjawaban pidana juga membutuhkan ahli. Ahli digital forensik dapat membantu menjelaskan cara kerja sistem, asal jejak digital, integritas file, hubungan perangkat dengan aktivitas tertentu, atau kemungkinan manipulasi bukti. Ahli hukum pidana dapat membantu menjelaskan unsur tindak pidana dan pertanggungjawaban pidana. Kombinasi antara bukti digital, keterangan saksi, keterangan ahli, keterangan korban, dan alat bukti lain diperlukan agar putusan tidak hanya berdasarkan dugaan teknis yang belum teruji (Casey, 2011; UNODC, 2013).

Untuk memudahkan pemahaman, unsur pertanggungjawaban pidana dalam kejahatan siber dapat diringkas dalam tabel berikut.

Tabel 8.5: Unsur Pertanggungjawaban Pidana dalam Kejahatan Siber

Unsur Pertanggungjawaban	Penjelasan	Contoh dalam Kejahatan Siber	Bukti yang Dapat Digunakan
Dasar hukum	Perbuatan harus diatur sebagai tindak pidana	Akses ilegal, pencurian data, penyebaran malware	UU ITE, UU PDP, KUHP, aturan terkait
Perbuatan pidana	Ada tindakan atau kelalaian yang memenuhi unsur delik	Mengirim phishing, membobol akun, menyebarkan data pribadi	Log akses, pesan, tautan, file, rekaman transaksi
Melawan hukum	Perbuatan dilakukan tanpa hak atau bertentangan dengan hukum	Masuk ke sistem tanpa izin	Hak akses, otorisasi, kebijakan sistem
Kesalahan	Ada kesengajaan atau kelalaian yang dapat dipersalahkan	Sengaja membuat situs palsu untuk mencuri password	Riwayat komunikasi, alat yang digunakan, pola tindakan
Kemampuan bertanggung jawab	Pelaku mampu memahami dan mengendalikan perbuatannya	Pelaku dewasa dan sadar melakukan penipuan online	Identitas pelaku, pemeriksaan kondisi pelaku
Hubungan sebab-akibat	Ada hubungan antara perbuatan dan kerugian	Data dicuri lalu dipakai untuk pinjaman ilegal	Jejak transaksi, korelasi waktu, bukti penggunaan data

Unsur Pertanggungjawaban	Penjelasan	Contoh dalam Kejahatan Siber	Bukti yang Dapat Digunakan
Identitas pelaku	Pelaku harus dapat dihubungkan dengan akun, perangkat, atau tindakan	Akun pelaku digunakan untuk mengirim link palsu	Metadata, IP, perangkat, saksi, transaksi
Peran pelaku	Menentukan apakah pelaku utama, pembantu, atau peserta	Penyedia rekening penampung hasil penipuan	Bukti transfer, komunikasi, pembagian hasil

Tabel 8.5 menunjukkan bahwa pertanggungjawaban pidana dalam kejahatan siber tidak cukup hanya dibuktikan melalui adanya kerugian. Penegak hukum harus membuktikan dasar hukum, perbuatan pidana, sifat melawan hukum, kesalahan, kemampuan bertanggung jawab, hubungan sebab-akibat, identitas pelaku, dan peran pelaku. Dengan kata lain, pertanggungjawaban pidana harus dibangun melalui rangkaian bukti yang sah, bukan hanya dugaan berdasarkan akun, nomor telepon, atau alamat IP tertentu.

8.6 Pencegahan dan Penanggulangan Kejahatan Siber

Pencegahan dan penanggulangan kejahatan siber merupakan bagian penting dalam hukum teknologi informasi karena kejahatan siber tidak cukup ditangani setelah terjadi kerugian. Karakter kejahatan siber yang cepat, lintas batas, mudah menyebar, dan berbasis bukti elektronik menuntut pendekatan yang lebih menyeluruh. Pendekatan tersebut harus mencakup tata kelola keamanan, perlindungan sistem, literasi pengguna, pelindungan data pribadi, deteksi dini, respons insiden, penegakan hukum, serta pemulihan korban.

Pencegahan kejahatan siber bertujuan mengurangi peluang terjadinya serangan, sedangkan penanggulangan bertujuan mengendalikan dampak ketika insiden telah terjadi. Keduanya tidak dapat dipisahkan. Sistem yang aman dapat mengurangi risiko serangan, tetapi tidak ada sistem yang sepenuhnya bebas dari ancaman. Oleh karena itu, organisasi, pemerintah, platform digital, lembaga pendidikan, pelaku usaha, dan masyarakat perlu memiliki kemampuan untuk mencegah, mendeteksi, merespons, dan memulihkan diri dari insiden siber.

Gambar 8.6: Siklus Pencegahan dan Penanggulangan Kejahatan Siber

Dalam konteks Indonesia, pencegahan dan penanggulangan kejahatan siber berkaitan dengan beberapa dasar hukum dan kebijakan, seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Perpres Nomor 47 Tahun 2023 menempatkan strategi keamanan siber dan manajemen krisis siber sebagai acuan bagi instansi penyelenggara negara dan pemangku kepentingan untuk membangun stabilitas keamanan siber nasional (Republik Indonesia, 2023).

8.6.1 Pencegahan Berbasis Tata Kelola Keamanan Siber

Pencegahan kejahatan siber perlu dimulai dari tata kelola keamanan siber. Tata kelola keamanan siber adalah cara organisasi mengatur kebijakan,

struktur tanggung jawab, prosedur, sumber daya, dan pengawasan untuk melindungi sistem elektronik dan data yang dikelolanya. Tanpa tata kelola yang jelas, keamanan siber sering hanya dipahami sebagai urusan teknis, seperti memasang antivirus atau firewall. Padahal, keamanan siber juga berkaitan dengan keputusan manajemen, budaya organisasi, tanggung jawab hukum, dan kepatuhan terhadap regulasi.

Kerangka NIST Cybersecurity Framework 2.0 menempatkan fungsi **Govern, Identify, Protect, Detect, Respond,** dan **Recover** sebagai fungsi utama dalam pengelolaan risiko keamanan siber. Fungsi tersebut menunjukkan bahwa keamanan siber harus dimulai dari tata kelola, pengenalan aset dan risiko, perlindungan sistem, deteksi insiden, respons terhadap serangan, serta pemulihan setelah insiden (NIST, 2024). Dalam konteks nasional, Peraturan Presiden Nomor 47 Tahun 2023 juga menegaskan pentingnya strategi keamanan siber dan manajemen krisis siber sebagai acuan bersama bagi pemangku kepentingan (Republik Indonesia, 2023).

Tata kelola keamanan siber dapat diwujudkan melalui beberapa langkah. Pertama, organisasi perlu menetapkan kebijakan keamanan informasi yang jelas. Kedua, organisasi perlu membagi peran dan tanggung jawab pengelola sistem, pengguna, pimpinan, dan tim keamanan. Ketiga, organisasi perlu melakukan identifikasi aset digital penting, seperti server, database, aplikasi, akun administrator, data pelanggan, dan sistem transaksi. Keempat, organisasi perlu melakukan penilaian risiko secara berkala. Kelima, organisasi perlu menyiapkan prosedur pelaporan dan respons insiden.

Bagi penyelenggara sistem elektronik, tata kelola keamanan siber juga berkaitan dengan kewajiban menyediakan sistem elektronik yang andal, aman, dan bertanggung jawab. Peraturan Pemerintah Nomor 71 Tahun 2019 mengatur penyelenggaraan sistem dan transaksi elektronik sebagai dasar penting bagi tata kelola layanan digital di Indonesia (Republik Indonesia, 2019). Dengan demikian, pencegahan kejahatan siber tidak hanya bergantung pada kesadaran pengguna, tetapi juga pada tanggung jawab organisasi dan penyelenggara sistem elektronik dalam membangun sistem yang aman.

8.6.2 Penguatan Sistem, Infrastruktur, dan Kontrol Teknis

Pencegahan kejahatan siber juga membutuhkan penguatan teknis terhadap sistem dan infrastruktur digital. Penguatan teknis bertujuan menutup celah yang dapat dimanfaatkan pelaku, seperti password lemah, sistem tidak diperbarui, konfigurasi server yang salah, akses administrator yang terlalu luas, jaringan tidak tersegmentasi, atau tidak adanya pencadangan data. Banyak insiden siber terjadi bukan hanya karena pelaku sangat canggih, tetapi karena sistem dasar organisasi tidak dikelola secara aman.

Beberapa kontrol teknis yang penting diterapkan adalah penggunaan autentikasi multifaktor, pembaruan sistem secara berkala, manajemen kerentanan, pencadangan data, pembatasan hak akses, enkripsi data penting, pemantauan log, penggunaan perangkat lunak resmi, segmentasi jaringan, dan perlindungan terhadap email berbahaya. CISA menempatkan praktik seperti rencana respons insiden, pengamanan akun, perlindungan terhadap malware, dan pengujian pemulihan sebagai bagian dari target kinerja keamanan siber yang dapat membantu organisasi mengurangi risiko serangan (CISA, 2022). NIST juga menekankan fungsi **Protect** dan **Detect** sebagai bagian penting untuk mengurangi peluang serangan dan menemukan aktivitas mencurigakan lebih awal (NIST, 2024).

Dalam konteks ransomware, pencegahan teknis menjadi sangat penting. Serangan ransomware dapat mengunci data, menghentikan layanan, dan memaksa korban membayar tebusan. CISA melalui *StopRansomware Guide* menekankan pentingnya pencegahan dan respons ransomware, termasuk pencadangan data, pembaruan sistem, pengamanan akses, pelatihan pengguna, dan kesiapan respons insiden (CISA, 2022). Oleh karena itu, organisasi tidak cukup hanya memiliki backup, tetapi juga harus memastikan backup tersebut terpisah, terlindungi, dan dapat dipulihkan ketika sistem utama diserang.

Penguatan teknis juga perlu memperhatikan prinsip hak akses minimum. Artinya, setiap pengguna hanya diberikan akses sesuai kebutuhan tugasnya. Akun administrator tidak boleh digunakan untuk aktivitas sehari-hari, password tidak boleh dipakai bersama, dan akses ke database penting harus dibatasi. Jika satu akun berhasil diambil alih, pembatasan akses dapat mencegah kerusakan yang lebih luas. Dengan demikian, penguatan sistem

bukan hanya memasang perangkat keamanan, tetapi juga mengatur cara orang mengakses dan menggunakan sistem.

8.6.3 Pelindungan data pribadi sebagai Upaya Pencegahan

Data pribadi sering menjadi sasaran utama kejahatan siber. Pelaku dapat mencuri data pribadi untuk melakukan penipuan, pencurian identitas, pengambilalihan akun, pinjaman online ilegal, pemerasan, atau penjualan data di forum gelap. Oleh karena itu, pelindungan data pribadi harus menjadi bagian dari pencegahan kejahatan siber. Pelindungan data pribadi tidak hanya berarti menyimpan data secara aman, tetapi juga membatasi data yang dikumpulkan, menentukan tujuan pemrosesan, membatasi akses, serta menghapus data yang tidak lagi diperlukan.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur asas, jenis data pribadi, hak subjek data, pemrosesan data pribadi, kewajiban pengendali dan prosesor data, sanksi administratif, penyelesaian sengketa, larangan penggunaan data pribadi, dan ketentuan pidana (Republik Indonesia, 2022). Dalam konteks pencegahan kejahatan siber, ketentuan ini penting karena data pribadi yang tidak dikelola secara benar dapat menjadi pintu masuk bagi kejahatan lanjutan.

Pencegahan berbasis pelindungan data pribadi dapat dilakukan dengan prinsip minimalisasi data, pembatasan tujuan, keamanan pemrosesan, transparansi, dan akuntabilitas. Organisasi tidak seharusnya mengumpulkan data yang tidak diperlukan. Data yang dikumpulkan harus digunakan sesuai tujuan yang sah. Akses terhadap data harus dibatasi. Pengguna juga harus memperoleh informasi yang jelas mengenai bagaimana datanya dikumpulkan, digunakan, disimpan, dan dibagikan. Prinsip ini sejalan dengan kewajiban pengendali dan prosesor data dalam UU PDP serta tata kelola risiko keamanan siber dalam NIST CSF 2.0 (Republik Indonesia, 2022; NIST, 2024).

Pelindungan data pribadi juga berkaitan dengan manajemen insiden. Apabila terjadi kebocoran data, organisasi perlu segera mengidentifikasi jenis data yang terdampak, jumlah subjek data yang terdampak, penyebab insiden, tindakan pemulihan, serta kewajiban pemberitahuan sesuai ketentuan hukum. Jika organisasi lambat merespons, kerugian korban dapat semakin besar karena data yang bocor dapat digunakan untuk penipuan lanjutan.

Dengan demikian, pelindungan data pribadi harus ditempatkan sebagai langkah pencegahan sekaligus bagian dari penanggulangan setelah insiden terjadi.

8.6.4 Peningkatan Literasi Keamanan Siber Masyarakat

Banyak kejahatan siber berhasil bukan karena sistem teknologi sangat lemah, tetapi karena pengguna tertipu. Modus seperti phishing, penipuan OTP, tautan palsu, toko online palsu, investasi palsu, dan rekayasa sosial memanfaatkan ketidaktahuan atau kepanikan korban. Oleh karena itu, literasi keamanan siber masyarakat menjadi salah satu bentuk pencegahan yang sangat penting.

Literasi keamanan siber mencakup kemampuan mengenali risiko digital, membedakan situs resmi dan palsu, tidak membagikan OTP atau PIN, menggunakan password kuat, mengaktifkan autentikasi multifaktor, memeriksa reputasi penjual, menghindari tautan mencurigakan, menggunakan aplikasi resmi, menyimpan bukti transaksi, dan melapor melalui saluran resmi apabila terjadi penipuan. OJK dalam materi literasi keuangan digital menjelaskan bahwa transformasi digital di sektor keuangan menghadirkan ancaman berbeda, seperti pencurian data pribadi secara online, serangan siber, dan kebocoran transaksi digital (OJK, 2024). CISA juga menempatkan praktik keamanan dasar dan respons insiden sebagai bagian dari target peningkatan ketahanan keamanan siber organisasi dan pengguna (CISA, 2026).

Peningkatan literasi perlu dilakukan secara berkelanjutan. Sekali sosialisasi tidak cukup karena modus kejahatan siber terus berubah. Edukasi keamanan siber dapat dilakukan melalui kampanye publik, pelatihan kampus, panduan penggunaan aplikasi, simulasi phishing, poster keamanan digital, video edukasi, dan materi pembelajaran. Di lingkungan pendidikan, mahasiswa perlu dilatih mengenali risiko akun akademik, email kampus, plagiarisme digital, penggunaan software ilegal, penyebaran data pribadi, dan etika penggunaan media sosial.

Literasi keamanan siber juga perlu menekankan sikap skeptis. Pengguna harus membiasakan diri memeriksa ulang informasi sebelum mengklik tautan, mengirim data, mengunduh file, atau melakukan transfer dana. Pesan yang terlihat resmi tetap perlu diverifikasi melalui kanal resmi. Tawaran

hadiah, investasi cepat kaya, ancaman pemblokiran akun, dan permintaan data rahasia harus diperlakukan sebagai tanda bahaya. Dengan demikian, literasi keamanan siber bukan hanya pengetahuan teknis, tetapi juga kebiasaan berpikir kritis dalam ruang digital.

8.6.5 Deteksi Dini dan Pelaporan Insiden Siber

Pencegahan kejahatan siber tidak selalu berhasil menghentikan semua serangan. Oleh karena itu, deteksi dini menjadi bagian penting dalam penanggulangan. Deteksi dini bertujuan menemukan aktivitas mencurigakan sebelum menimbulkan kerusakan lebih besar. Aktivitas mencurigakan dapat berupa login dari lokasi tidak biasa, percobaan password berulang, peningkatan trafik yang tidak wajar, perubahan file sistem, pengiriman email massal, transaksi tidak biasa, atau munculnya akun administrator baru.

Deteksi dini dapat dilakukan melalui pemantauan log, sistem deteksi intrusi, sistem informasi keamanan, analisis anomali, pemantauan endpoint, dan pelaporan pengguna. NIST CSF 2.0 menempatkan fungsi **Detect** sebagai bagian penting dalam menemukan kemungkinan insiden keamanan siber, sedangkan fungsi **Respond** dan **Recover** digunakan untuk mengelola dampak setelah insiden ditemukan (NIST, 2024b). Dalam konteks Indonesia, BSSN melalui pengaturan pengelolaan insiden siber memuat panduan mengenai penanggulangan dan pemulihan insiden siber (BSSN, 2024).

Pelaporan insiden juga penting. Banyak korban terlambat melapor karena malu, takut, atau merasa kerugiannya kecil. Padahal, laporan awal dapat membantu pemblokiran akun, pembekuan rekening, pengamanan sistem, pengumpulan bukti, dan pencegahan korban berikutnya. Organisasi perlu memiliki jalur pelaporan internal yang jelas, misalnya melalui helpdesk keamanan, tim CSIRT, email resmi, atau sistem tiket. Masyarakat juga perlu diarahkan untuk menggunakan jalur pengaduan resmi, baik kepada platform, bank, penyedia layanan, maupun aparat penegak hukum.

Deteksi dini dan pelaporan insiden harus didukung budaya keamanan. Pengguna tidak boleh takut melaporkan kesalahan, misalnya terlanjur mengklik tautan phishing atau membuka lampiran mencurigakan. Jika organisasi terlalu menyalahkan pengguna, insiden justru dapat

disembunyikan. Sebaliknya, budaya pelaporan yang terbuka dapat mempercepat respons dan mengurangi dampak serangan. Dengan demikian, deteksi dini tidak hanya bergantung pada perangkat teknis, tetapi juga pada partisipasi manusia.

8.6.6 Respons Insiden dan Forensik Digital

Respons insiden adalah tindakan yang dilakukan ketika serangan atau pelanggaran keamanan telah terjadi. Respons insiden bertujuan membatasi kerusakan, menjaga bukti, memulihkan layanan, dan mencegah serangan berulang. Dalam insiden siber, respons yang terlambat dapat memperbesar kerugian karena data dapat terus dicuri, sistem dapat semakin rusak, dan pelaku dapat menghapus jejak digital.

Respons insiden umumnya mencakup tahap persiapan, identifikasi, penahanan, eradikasi, pemulihan, dan evaluasi. Pada tahap persiapan, organisasi menyiapkan tim, prosedur, kontak darurat, backup, dan alat respons. Pada tahap identifikasi, organisasi menentukan jenis insiden dan ruang lingkup serangan. Pada tahap penahanan, organisasi membatasi penyebaran serangan. Pada tahap eradikasi, organisasi menghapus malware, menutup celah, atau menghapus akses pelaku. Pada tahap pemulihan, layanan dikembalikan secara aman. Pada tahap evaluasi, organisasi menilai penyebab insiden dan memperbaiki kelemahan yang ditemukan. Panduan BSSN mengenai pengelolaan insiden siber dan panduan CISA tentang ransomware sama-sama menekankan pentingnya perencanaan, penanggulangan, pemulihan, dan kesiapan respons terhadap insiden (BSSN, 2024; CISA, 2025).

Forensik digital juga menjadi bagian penting dalam penanggulangan kejahatan siber. Bukti elektronik dapat berupa log, metadata, file, email, pesan, riwayat login, transaksi, alamat IP, dan salinan sistem. Bukti tersebut harus diamankan agar tidak berubah atau hilang. INTERPOL menegaskan bahwa bukti digital bersifat mudah berubah dan penegakan hukum global memerlukan dukungan kerja sama serta platform pertukaran informasi yang aman (INTERPOL, 2026). Oleh karena itu, organisasi tidak boleh sembarangan menghapus file, memformat perangkat, atau mengubah konfigurasi sebelum bukti penting diamankan.

Respons insiden yang baik harus menyeimbangkan dua kepentingan. Pertama, organisasi perlu segera memulihkan layanan agar aktivitas pengguna tidak terganggu terlalu lama. Kedua, organisasi perlu menjaga bukti agar proses hukum tetap dapat dilakukan. Jika pemulihan dilakukan tanpa memperhatikan bukti, pelaku mungkin sulit dilacak. Sebaliknya, jika organisasi terlalu lama menahan sistem tanpa pemulihan, kerugian operasional dapat membesar. Karena itu, respons insiden membutuhkan koordinasi antara tim teknis, manajemen, bagian hukum, komunikasi publik, dan aparat penegak hukum.

8.6.7 Koordinasi Kelembagaan dan Penegakan Hukum

Penanggulangan kejahatan siber membutuhkan koordinasi banyak pihak. Dalam satu kasus penipuan digital, misalnya, dapat terlibat korban, platform, bank, penyedia dompet digital, operator telekomunikasi, penyedia internet, penyedia cloud, dan aparat penegak hukum. Jika koordinasi lemah, pelaku dapat memindahkan dana, menghapus akun, mengganti nomor, atau menyembunyikan data sebelum tindakan hukum dilakukan.

Koordinasi kelembagaan penting karena kejahatan siber sering bersifat lintas sektor dan lintas wilayah. Peraturan Presiden Nomor 47 Tahun 2023 menempatkan Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber sebagai acuan bagi instansi penyelenggara negara dan pemangku kepentingan untuk mewujudkan kekuatan dan kapabilitas siber nasional (Republik Indonesia, 2023a). Di sisi lain, UU ITE menjadi dasar penting dalam menangani perbuatan melawan hukum yang berkaitan dengan informasi elektronik, transaksi elektronik, dan sistem elektronik (Republik Indonesia, 2024b).

Penegakan hukum terhadap kejahatan siber harus memperhatikan kecepatan dan ketepatan. Kecepatan diperlukan karena jejak digital dan aliran dana dapat berpindah dengan cepat. Ketepatan diperlukan agar tidak terjadi kesalahan identifikasi pelaku. Alamat IP, nomor telepon, rekening, atau akun digital perlu dikaitkan dengan bukti lain agar tidak salah menuduh pihak yang sebenarnya menjadi korban pembajakan akun. Oleh karena itu, penegakan hukum kejahatan siber membutuhkan penyidik yang memahami hukum, teknologi, bukti elektronik, serta prosedur forensik digital.

Koordinasi internasional juga dapat diperlukan apabila pelaku, server, domain, atau data berada di luar negeri. INTERPOL menyatakan bahwa pihaknya mendukung penegakan hukum global dalam merespons ancaman siber melalui kerja sama dan platform pertukaran informasi yang aman (INTERPOL, 2026). Dengan demikian, penanggulangan kejahatan siber tidak dapat hanya mengandalkan korban dan aparat lokal, tetapi membutuhkan kerja sama antara negara, lembaga penegak hukum, regulator, penyedia layanan digital, dan masyarakat.

8.6.8 Pemulihan Korban dan Evaluasi Pasca-Insiden

Penanggulangan kejahatan siber tidak selesai ketika serangan berhenti atau pelaku ditemukan. Korban masih membutuhkan pemulihan. Pemulihan dapat berupa pengembalian akses akun, penggantian password, pemblokiran kartu atau rekening, pemulihan data, penghapusan konten ilegal, pemberitahuan kepada pihak terdampak, pemulihan reputasi, pendampingan hukum, dan dukungan psikologis apabila korban mengalami tekanan akibat ancaman atau pelecehan digital.

Dalam kerangka keamanan siber, fungsi **Recover** bertujuan memulihkan layanan dan kemampuan organisasi setelah insiden terjadi. NIST CSF 2.0 menempatkan pemulihan sebagai salah satu fungsi utama dalam pengelolaan risiko keamanan siber (NIST, 2024). Panduan CISA mengenai ransomware juga menekankan pentingnya pemulihan layanan, pencadangan, dan pengujian rencana respons untuk mengurangi dampak serangan (CISA, 2022).

Pemulihan korban juga harus dikaitkan dengan pelindungan data pribadi. Jika insiden menyebabkan kebocoran data, organisasi perlu menilai data apa yang bocor, siapa saja yang terdampak, risiko apa yang mungkin terjadi, dan langkah apa yang harus dilakukan untuk mengurangi kerugian. UU PDP memberikan dasar bahwa pelindungan data pribadi merupakan bagian dari upaya menjamin hak subjek data pribadi dalam rangkaian pemrosesan data pribadi (Republik Indonesia, 2022b). Dengan demikian, korban tidak hanya dipandang sebagai pihak yang mengalami kerugian teknis, tetapi juga sebagai subjek hukum yang haknya harus dipulihkan.

Evaluasi pasca-insiden diperlukan agar kejadian serupa tidak terulang. Evaluasi dapat mencakup analisis penyebab insiden, kelemahan sistem,

kelalaian prosedur, respons yang terlambat, kurangnya literasi pengguna, atau tidak adanya backup yang memadai. Hasil evaluasi harus diterjemahkan menjadi perbaikan nyata, seperti pembaruan kebijakan, pelatihan ulang, peningkatan kontrol akses, audit keamanan, penguatan monitoring, dan uji coba respons insiden. Dengan demikian, setiap insiden siber seharusnya menjadi sumber pembelajaran untuk memperkuat ketahanan digital.

Untuk memudahkan pemahaman, strategi pencegahan dan penanggulangan kejahatan siber dapat diringkas dalam tabel berikut.

Tabel 8.6: Strategi Pencegahan dan Penanggulangan Kejahatan Siber

Aspek	Tujuan	Contoh Tindakan	Pihak yang Berperan
Tata kelola keamanan siber	Mengatur kebijakan, tanggung jawab, dan pengawasan keamanan	Kebijakan keamanan, penilaian risiko, pembagian peran	Pimpinan organisasi, pengelola sistem, regulator
Penguatan teknis	Mengurangi celah serangan pada sistem	MFA, patching, backup, enkripsi, segmentasi jaringan	Tim TI, penyelenggara sistem elektronik
Pelindungan data pribadi	Mencegah penyalahgunaan data korban	Minimalisasi data, pembatasan akses, keamanan database	Pengendali data, prosesor data, platform
Literasi keamanan siber	Mengurangi risiko korban tertipu modus digital	Edukasi phishing, larangan membagikan OTP, penggunaan aplikasi resmi	Pemerintah, kampus, platform, masyarakat
Deteksi dini	Menemukan serangan sebelum meluas	Pemantauan log, deteksi anomali, pelaporan pengguna	Tim keamanan, CSIRT, pengguna
Respons insiden	Mengendalikan dampak serangan	Identifikasi, isolasi sistem, pengamanan bukti, pemulihan layanan	Tim respons insiden, manajemen, aparat hukum
Forensik digital	Menjaga dan menganalisis bukti elektronik	Akuisisi data, analisis log, dokumentasi rantai bukti	Ahli forensik digital, penyidik
Penegakan hukum	Menindak pelaku dan memberi kepastian hukum	Pelaporan, penyidikan, kerja sama platform dan bank	Kepolisian, kejaksaan,

Aspek	Tujuan	Contoh Tindakan	Pihak yang Berperan
			pengadilan, regulator
Pemulihan korban	Mengurangi dampak kerugian korban	Pemulihan akun, pemblokiran rekening, penghapusan konten, pendampingan	Platform, bank, aparat hukum, lembaga bantuan
Evaluasi pasca-insiden	Mencegah kejadian berulang	Audit keamanan, pelatihan ulang, perbaikan SOP	Organisasi, regulator, tim keamanan

Tabel 8.6 menunjukkan bahwa pencegahan dan penanggulangan kejahatan siber tidak dapat dilakukan oleh satu pihak saja. Pengguna perlu berhati-hati, organisasi perlu membangun sistem yang aman, platform perlu bertanggung jawab, regulator perlu mengawasi, dan aparat penegak hukum perlu menindak pelaku secara tepat. Jika salah satu pihak lemah, risiko kejahatan siber tetap tinggi.

Pencegahan dan penanggulangan kejahatan siber harus dilakukan secara menyeluruh. Pencegahan dilakukan melalui tata kelola keamanan siber, penguatan sistem, pelindungan data pribadi, dan literasi digital. Penanggulangan dilakukan melalui deteksi dini, pelaporan, respons insiden, forensik digital, koordinasi kelembagaan, penegakan hukum, pemulihan korban, dan evaluasi pasca-insiden. Pendekatan ini penting karena kejahatan siber tidak hanya menyerang teknologi, tetapi juga menyerang kepercayaan masyarakat terhadap ruang digital.

Bab 9
Pembuktian dan Forensik Digital

9.1 Konsep Pembuktian dalam Perkara Digital

Pembuktian merupakan bagian penting dalam proses hukum karena melalui pembuktian hakim, penyidik, penuntut umum, advokat, maupun para pihak dapat menilai apakah suatu peristiwa hukum benar-benar terjadi, siapa pihak yang bertanggung jawab, dan bagaimana hubungan antara perbuatan, akibat, serta alat bukti yang diajukan. Dalam perkara konvensional, pembuktian umumnya bertumpu pada alat bukti yang bersifat fisik atau langsung, seperti keterangan saksi, surat, benda, maupun keterangan ahli. Namun, dalam perkara digital, pembuktian memiliki karakter yang lebih kompleks karena jejak peristiwa sering kali tersimpan dalam bentuk data elektronik, log sistem, metadata, rekaman komunikasi, dokumen elektronik, file digital, transaksi elektronik, alamat IP, rekaman CCTV digital, data perangkat, maupun aktivitas pada platform daring.

Perkara digital dapat dipahami sebagai perkara hukum yang sebagian atau seluruh peristiwanya terjadi melalui sistem elektronik, jaringan komputer, internet, perangkat digital, atau platform berbasis teknologi informasi. Perkara ini tidak hanya terbatas pada kejahatan siber seperti peretasan, pencurian data, phishing, atau penyebaran malware, tetapi juga mencakup sengketa transaksi elektronik, pencemaran nama baik melalui media sosial, penyalahgunaan data pribadi, pelanggaran hak cipta digital, manipulasi dokumen elektronik, serta sengketa yang melibatkan komunikasi atau perjanjian elektronik. Oleh karena itu, pembuktian dalam perkara digital tidak dapat dilepaskan dari kemampuan untuk memahami hubungan antara perbuatan hukum, sistem elektronik yang digunakan, serta jejak digital yang ditinggalkan oleh para pihak.

Dalam hukum Indonesia, kedudukan bukti elektronik semakin penting setelah adanya pengakuan terhadap informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah. Undang-Undang Informasi dan Transaksi Elektronik menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah dan menjadi perluasan dari alat bukti yang berlaku dalam hukum

acara di Indonesia (Republik Indonesia, 2024b). Pengakuan ini menunjukkan bahwa bukti dalam perkara digital tidak harus selalu berbentuk fisik, tetapi dapat berupa data elektronik sepanjang memenuhi persyaratan keabsahan, relevansi, keaslian, dan dapat dipertanggungjawabkan secara hukum.

Meskipun demikian, pengakuan terhadap bukti elektronik tidak berarti bahwa setiap data digital secara otomatis dapat diterima sebagai bukti yang kuat. Bukti digital memiliki sifat yang mudah disalin, diubah, dipindahkan, dihapus, dimanipulasi, atau disembunyikan. Data elektronik juga dapat tersebar di berbagai lokasi, seperti perangkat pengguna, server penyedia layanan, sistem penyimpanan awan, aplikasi pesan, media sosial, dan jaringan organisasi. Oleh karena itu, pembuktian dalam perkara digital membutuhkan pendekatan yang hati-hati agar bukti yang diajukan tidak hanya tersedia secara teknis, tetapi juga dapat dipercaya secara hukum.

Konsep pembuktian dalam perkara digital setidaknya mencakup tiga aspek utama, yaitu aspek hukum, aspek teknis, dan aspek prosedural. Aspek hukum berkaitan dengan dasar pengakuan bukti elektronik, relevansi bukti terhadap perkara, serta kesesuaiannya dengan ketentuan hukum acara. Aspek teknis berkaitan dengan cara memperoleh, menyimpan, memeriksa, dan menganalisis data elektronik agar tidak merusak integritas bukti. Sementara itu, aspek prosedural berkaitan dengan tata cara penanganan bukti sejak ditemukan, diamankan, diperiksa, disimpan, hingga diajukan dalam proses hukum. Ketiga aspek ini harus berjalan secara terpadu agar bukti digital memiliki nilai pembuktian yang kuat.

Dalam perspektif forensik digital, pembuktian tidak hanya bertujuan menemukan data, tetapi juga memastikan bahwa data tersebut dapat menjelaskan suatu peristiwa secara objektif. Forensik digital berperan membantu proses pembuktian dengan cara mengidentifikasi, mengamankan, memperoleh, menganalisis, dan melaporkan bukti digital secara sistematis. Pedoman internasional seperti ISO/IEC 27037 menekankan pentingnya proses identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital agar bukti yang diperoleh tetap memiliki nilai pembuktian (ISO/IEC, 2012). Sementara itu, NIST menjelaskan bahwa teknik forensik dapat digunakan untuk mendukung investigasi insiden teknologi informasi, termasuk dalam memahami aktivitas pada komputer, jaringan, dan sistem elektronik (Kent et al., 2006).

Gambar 9.1: Alur Konseptual Pembuktian Dalam Perkara Digital

Dalam praktiknya, bukti digital dapat berasal dari berbagai sumber. Pada perangkat komputer, bukti dapat berupa file, folder, riwayat akses, log sistem, cache, registry, atau data yang telah dihapus tetapi masih dapat dipulihkan. Pada perangkat seluler, bukti dapat berupa pesan, panggilan, lokasi, foto, video, aplikasi, serta riwayat aktivitas pengguna. Pada jaringan, bukti dapat berupa alamat IP, log akses, catatan koneksi, paket data, dan aktivitas server. Pada platform daring, bukti dapat berupa unggahan, komentar, percakapan, transaksi, metadata akun, serta catatan aktivitas pengguna. Keragaman sumber ini menunjukkan bahwa pembuktian digital memerlukan pemahaman lintas bidang antara hukum, teknologi informasi, keamanan siber, dan forensik digital.

Hal penting lainnya dalam pembuktian perkara digital adalah relevansi antara bukti dengan unsur perkara. Bukti digital tidak cukup hanya menunjukkan bahwa suatu data ada, tetapi harus mampu menjelaskan keterkaitannya dengan peristiwa hukum yang sedang diperiksa. Misalnya, dalam kasus phishing, bukti yang relevan tidak hanya berupa tautan palsu, tetapi juga catatan pengiriman pesan, alamat domain, rekening penerima dana, log akses, data korban, serta hubungan antara pelaku dengan sarana yang digunakan. Dalam perkara pencemaran nama baik melalui media sosial, bukti yang relevan dapat mencakup tangkapan layar, URL, waktu unggahan, identitas akun, metadata, serta keterangan ahli untuk menjelaskan keaslian dan keterhubungan bukti tersebut.

Selain relevansi, pembuktian digital juga harus memperhatikan keaslian dan integritas bukti. Keaslian berkaitan dengan pertanyaan apakah bukti tersebut benar berasal dari sumber yang dinyatakan. Integritas berkaitan dengan apakah bukti tersebut masih utuh dan tidak mengalami perubahan sejak

diperoleh hingga diajukan dalam proses hukum. Untuk menjaga integritas, pemeriksaan forensik digital biasanya menggunakan metode seperti pencatatan waktu, dokumentasi prosedur, penggunaan *hash value*, pembuatan salinan forensik, serta pengamanan media penyimpanan. Prosedur tersebut penting karena perubahan kecil pada data digital dapat memengaruhi nilai pembuktiannya.

> Pembuktian dalam perkara digital merupakan proses yang menggabungkan prinsip hukum pembuktian dan prinsip teknis forensik digital. Bukti elektronik memiliki kedudukan penting dalam proses hukum, tetapi kekuatannya bergantung pada cara bukti tersebut diperoleh, dijaga, dianalisis, dan dihubungkan dengan unsur perkara. Oleh karena itu, pembuktian digital tidak boleh hanya dipahami sebagai kegiatan mengumpulkan tangkapan layar atau file elektronik, melainkan sebagai proses ilmiah dan hukum yang bertujuan membangun hubungan yang rasional, sah, dan dapat dipertanggungjawabkan antara jejak digital dengan peristiwa hukum yang dibuktikan.

9.2 Kedudukan Bukti Elektronik dalam Proses Hukum

Kedudukan bukti elektronik dalam proses hukum menjadi semakin penting seiring dengan meningkatnya penggunaan teknologi informasi dalam berbagai aktivitas masyarakat. Banyak peristiwa hukum pada era digital tidak lagi meninggalkan bukti dalam bentuk fisik semata, tetapi juga meninggalkan jejak elektronik yang tersimpan dalam perangkat, sistem elektronik, jaringan internet, platform digital, maupun layanan berbasis komputasi awan. Bukti tersebut dapat berupa informasi elektronik, dokumen elektronik, percakapan digital, rekaman transaksi, log sistem, metadata, alamat IP, rekaman CCTV digital, surel, unggahan media sosial, data lokasi, file, serta hasil cetak dari informasi elektronik.

Dalam konteks hukum Indonesia, bukti elektronik memperoleh kedudukan penting karena telah diakui sebagai alat bukti hukum yang sah. Undang-Undang Informasi dan Transaksi Elektronik menyatakan bahwa informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah. Ketentuan ini menunjukkan bahwa bukti elektronik bukan sekadar pelengkap dalam proses hukum, tetapi dapat digunakan sebagai dasar pembuktian sepanjang memenuhi ketentuan peraturan perundang-undangan (Republik Indonesia, 2008, 2016, 2024).

Pengakuan tersebut memperluas konsep alat bukti dalam hukum acara, karena pembuktian tidak lagi terbatas pada bukti tertulis dalam bentuk kertas atau benda fisik.

Kedudukan bukti elektronik semakin kuat dalam hukum acara pidana terbaru. Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana memasukkan bukti elektronik sebagai salah satu alat bukti dalam perkara pidana. Hal ini menunjukkan adanya penyesuaian hukum acara terhadap perkembangan teknologi informasi dan kebutuhan pembuktian modern (Republik Indonesia, 2025a). Dengan adanya pengakuan tersebut, aparat penegak hukum, jaksa, advokat, hakim, ahli, dan para pihak dalam perkara memiliki dasar hukum yang lebih jelas dalam menggunakan bukti elektronik untuk membuktikan suatu peristiwa hukum.

Meskipun demikian, kedudukan bukti elektronik tetap harus dipahami secara hati-hati. Tidak semua data digital secara otomatis memiliki kekuatan pembuktian yang sama. Bukti elektronik harus dinilai berdasarkan beberapa aspek, yaitu relevansi dengan perkara, keaslian sumber, integritas data, cara perolehan yang sah, serta keterkaitan bukti dengan perbuatan hukum yang sedang diperiksa. Bukti elektronik yang diperoleh tanpa prosedur yang benar, tidak dapat diverifikasi keasliannya, atau mengalami perubahan tanpa dokumentasi yang jelas dapat dipersoalkan dalam proses hukum.

Dalam perkara pidana, bukti elektronik dapat digunakan untuk membuktikan unsur tindak pidana, hubungan antara pelaku dan perbuatan, waktu terjadinya peristiwa, sarana yang digunakan, serta akibat yang ditimbulkan. Misalnya, dalam kasus penipuan daring, bukti elektronik dapat berupa pesan percakapan, tautan palsu, rekening penerima dana, riwayat transaksi, alamat IP, data akun, dan log akses. Dalam kasus akses ilegal terhadap sistem elektronik, bukti dapat berupa catatan login, aktivitas server, jejak perubahan data, perangkat yang digunakan, dan hasil analisis forensik digital. Dengan demikian, bukti elektronik dapat membantu menjelaskan rangkaian peristiwa yang sulit dibuktikan hanya dengan keterangan saksi atau dokumen fisik.

Dalam perkara perdata, bukti elektronik juga memiliki kedudukan penting, terutama dalam sengketa transaksi elektronik, perjanjian elektronik, pembayaran digital, layanan marketplace, pelanggaran kontrak daring, dan

sengketa konsumen digital. Dokumen elektronik seperti surat elektronik, bukti transfer, invoice digital, rekam transaksi aplikasi, bukti pemesanan, serta percakapan antara penjual dan pembeli dapat digunakan untuk menunjukkan adanya hubungan hukum antara para pihak. Dalam konteks ini, bukti elektronik berfungsi untuk menunjukkan adanya kesepakatan, pelaksanaan kewajiban, wanprestasi, kerugian, atau tanggung jawab hukum pihak tertentu.

Kedudukan bukti elektronik juga penting dalam perkara administrasi dan tata usaha negara, terutama ketika pelayanan publik, perizinan, dokumen pemerintahan, dan komunikasi resmi telah menggunakan sistem elektronik. Dokumen elektronik dalam sistem pemerintahan dapat menjadi bukti adanya keputusan, tindakan administrasi, pengajuan permohonan, persetujuan, penolakan, atau rekam aktivitas layanan publik. Oleh karena itu, pengelolaan sistem elektronik yang andal, aman, dan terdokumentasi menjadi penting agar bukti elektronik yang dihasilkan dapat dipercaya apabila digunakan dalam proses hukum.

Agar lebih mudah dipahami, kedudukan bukti elektronik dalam beberapa jenis perkara dapat dijelaskan sebagai berikut.

Tabel 9.1: Kedudukan bukti elektronik dalam berbagai jenis perkara hukum

Jenis Perkara	Contoh Bukti Elektronik	Fungsi dalam Pembuktian
Pidana siber	Log akses, alamat IP, pesan phishing, file malware, riwayat transaksi	Membuktikan perbuatan, pelaku, sarana, waktu, dan akibat tindak pidana
Perdata digital	Kontrak elektronik, bukti transfer, invoice digital, percakapan aplikasi	Membuktikan hubungan hukum, kesepakatan, prestasi, wanprestasi, dan kerugian
Perlindungan konsumen	Bukti pemesanan, iklan digital, ulasan produk, riwayat komplain	Membuktikan informasi yang diberikan pelaku usaha dan kerugian konsumen
Pelindungan data pribadi	Bukti kebocoran data, log akses, riwayat pemrosesan data, notifikasi insiden	Membuktikan penyalahgunaan data, kelalaian, atau pelanggaran kewajiban pengendali data
Administrasi pemerintahan	Dokumen elektronik, tanda terima elektronik, rekam layanan sistem	Membuktikan keputusan, tindakan, atau proses administrasi berbasis elektronik

Tabel 9.1 menunjukkan bahwa bukti elektronik memiliki fungsi yang berbeda bergantung pada jenis perkara yang sedang diperiksa. Dalam perkara pidana, bukti elektronik cenderung digunakan untuk membuktikan adanya perbuatan pidana dan keterlibatan pelaku. Dalam perkara perdata, bukti elektronik lebih banyak digunakan untuk menunjukkan adanya hubungan hukum dan kerugian. Sementara itu, dalam perkara perlindungan data pribadi dan administrasi pemerintahan, bukti elektronik dapat digunakan untuk menilai kepatuhan, kelalaian, atau tanggung jawab pihak yang mengelola sistem dan data.

Kekuatan pembuktian bukti elektronik sangat bergantung pada kemampuannya untuk memenuhi prinsip keaslian dan integritas. Keaslian berkaitan dengan apakah bukti benar berasal dari sumber yang dinyatakan, sedangkan integritas berkaitan dengan apakah isi bukti tetap utuh dan tidak berubah sejak diperoleh hingga diajukan dalam proses hukum. Dalam praktik forensik digital, prinsip ini dapat dijaga melalui dokumentasi prosedur, penggunaan nilai hash, pembuatan salinan forensik, pencatatan waktu, serta pengamanan media penyimpanan (Casey, 2011; ISO/IEC, 2012). Tanpa jaminan keaslian dan integritas, bukti elektronik dapat diperdebatkan karena data digital mudah disalin, diubah, dihapus, atau dimanipulasi.

Selain itu, bukti elektronik harus diperoleh secara sah. Cara memperoleh bukti menjadi faktor penting karena bukti yang diperoleh melalui akses tanpa hak, pelanggaran privasi, penyadapan ilegal, atau manipulasi sistem dapat menimbulkan persoalan hukum. Dalam proses hukum, keabsahan bukti tidak hanya dinilai dari isi data, tetapi juga dari cara data tersebut diperoleh, disimpan, dan diajukan. Oleh karena itu, aparat penegak hukum dan pihak yang mengajukan bukti perlu memperhatikan prosedur hukum dan prinsip forensik digital agar bukti elektronik dapat diterima dan dipertimbangkan secara layak.

Peran ahli juga sangat penting dalam menjelaskan kedudukan bukti elektronik di persidangan. Hakim dan para pihak tidak selalu memiliki pemahaman teknis yang memadai mengenai cara kerja sistem elektronik, metadata, log akses, enkripsi, pemulihan data, atau analisis perangkat digital. Oleh karena itu, ahli forensik digital dapat membantu menjelaskan asal-usul bukti, proses akuisisi, metode analisis, kemungkinan perubahan data, serta hubungan antara bukti elektronik dengan peristiwa hukum yang diperiksa.

Keterangan ahli menjadi jembatan antara aspek teknis bukti digital dan penilaian hukum dalam proses persidangan (Casey, 2011; Kent et al., 2006).

> Bukti elektronik memiliki kedudukan yang penting dan sah dalam proses hukum di Indonesia. Pengakuan terhadap bukti elektronik menunjukkan bahwa sistem hukum telah beradaptasi dengan perkembangan teknologi informasi. Namun, kekuatan pembuktiannya tetap bergantung pada keaslian, integritas, relevansi, legalitas perolehan, dan kemampuan bukti tersebut menjelaskan hubungan antara peristiwa digital dengan persoalan hukum yang diperiksa. Oleh karena itu, bukti elektronik harus dikelola secara hati-hati melalui prosedur hukum dan forensik digital yang dapat dipertanggungjawabkan.

9.3 Prinsip Dasar Forensik Digital

Forensik digital merupakan proses ilmiah yang digunakan untuk mengidentifikasi, memperoleh, mengamankan, menganalisis, dan menyajikan bukti digital agar dapat digunakan dalam proses hukum. Dalam perkara digital, bukti sering kali berbentuk data elektronik yang tersimpan pada komputer, perangkat seluler, server, jaringan, sistem elektronik, media penyimpanan, aplikasi, maupun layanan berbasis komputasi awan. Karena data digital memiliki sifat yang mudah diubah, disalin, dipindahkan, dihapus, atau dimanipulasi, maka pemeriksaan terhadap bukti digital harus dilakukan berdasarkan prinsip-prinsip yang ketat dan dapat dipertanggungjawabkan secara ilmiah maupun hukum.

Prinsip dasar forensik digital diperlukan agar bukti elektronik yang diperoleh tidak kehilangan nilai pembuktiannya. Bukti digital yang ditemukan dalam suatu perangkat atau sistem tidak cukup hanya dikumpulkan, tetapi harus dijaga keaslian, integritas, relevansi, dan keterhubungannya dengan perkara. Oleh karena itu, proses forensik digital harus dilakukan secara hati-hati, terdokumentasi, objektif, dan sesuai prosedur. Pedoman forensik digital seperti ISO/IEC 27037 menekankan bahwa proses identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital harus dilakukan dengan cara yang menjaga keutuhan data serta memungkinkan proses tersebut dapat diverifikasi kembali (ISO/IEC, 2012). Sejalan dengan itu, NIST menjelaskan bahwa forensik digital berfungsi untuk mendukung investigasi melalui

pengumpulan dan analisis data dari komputer, jaringan, serta media penyimpanan secara sistematis (Kent et al., 2006).

Prinsip pertama dalam forensik digital adalah **legalitas**. Setiap tindakan pemeriksaan, pengambilan, dan analisis bukti digital harus dilakukan berdasarkan kewenangan yang sah dan sesuai dengan ketentuan hukum yang berlaku. Legalitas menjadi penting karena bukti digital sering kali berkaitan dengan hak privasi, data pribadi, rahasia komunikasi, dokumen organisasi, dan akses terhadap sistem elektronik. Apabila bukti diperoleh melalui cara yang melanggar hukum, seperti akses tanpa hak, penyadapan ilegal, atau pengambilan data tanpa dasar kewenangan, maka bukti tersebut dapat dipersoalkan dalam proses hukum. Oleh karena itu, pemeriksa forensik digital harus memastikan bahwa proses pengumpulan bukti memiliki dasar hukum, izin, surat tugas, perintah penyidikan, atau persetujuan yang sah sesuai konteks perkara.

Prinsip kedua adalah **integritas bukti**. Integritas berarti bahwa bukti digital harus dijaga agar tidak berubah sejak pertama kali ditemukan hingga diajukan dalam proses hukum. Data digital sangat rentan mengalami perubahan, baik karena aktivitas pengguna, proses sistem otomatis, kesalahan pemeriksa, maupun tindakan manipulasi. Untuk menjaga integritas, pemeriksa forensik digital biasanya menggunakan teknik seperti pembuatan salinan forensik, penggunaan write blocker, pencatatan nilai hash, serta dokumentasi setiap tindakan yang dilakukan terhadap bukti. Nilai hash berfungsi sebagai sidik jari digital yang dapat digunakan untuk membandingkan apakah suatu file atau media penyimpanan masih sama dengan kondisi awalnya (Casey, 2011; ISO/IEC, 2012).

Prinsip ketiga adalah **keaslian bukti**. Keaslian berkaitan dengan pertanyaan apakah bukti benar berasal dari sumber yang dinyatakan dan apakah bukti tersebut dapat dikaitkan dengan peristiwa hukum tertentu. Dalam perkara digital, keaslian tidak selalu mudah dibuktikan karena akun dapat dipalsukan, dokumen dapat dimodifikasi, tangkapan layar dapat direkayasa, dan identitas digital dapat disamarkan. Oleh karena itu, pemeriksaan forensik digital tidak boleh hanya bergantung pada tampilan luar suatu data, tetapi perlu menelusuri sumber, metadata, waktu pembuatan, riwayat perubahan, log sistem, alamat IP, perangkat yang digunakan, serta hubungan antara data dengan pengguna atau peristiwa yang diperiksa.

Prinsip keempat adalah **rantai penguasaan bukti** atau *chain of custody*. Rantai penguasaan bukti merupakan dokumentasi yang menjelaskan siapa yang menemukan bukti, kapan bukti ditemukan, bagaimana bukti diamankan, siapa yang memindahkan atau memeriksa bukti, di mana bukti disimpan, serta tindakan apa saja yang dilakukan terhadap bukti tersebut. Prinsip ini penting karena bukti digital dapat berpindah dari satu pihak ke pihak lain, mulai dari penyidik, pemeriksa forensik, laboratorium digital, jaksa, hingga pengadilan. Tanpa dokumentasi rantai penguasaan yang jelas, keaslian dan integritas bukti dapat dipertanyakan (Casey, 2011).

Prinsip kelima adalah **objektivitas dan netralitas pemeriksa**. Pemeriksa forensik digital harus bekerja berdasarkan data dan metode ilmiah, bukan berdasarkan asumsi, tekanan pihak tertentu, atau keinginan untuk membenarkan satu kesimpulan sejak awal. Analisis forensik digital harus dilakukan secara objektif dengan memperhatikan kemungkinan yang mendukung maupun yang melemahkan dugaan. Dalam konteks ini, pemeriksa tidak hanya mencari bukti yang memberatkan, tetapi juga harus terbuka terhadap bukti yang dapat menjelaskan konteks lain dari suatu peristiwa. Objektivitas sangat penting karena hasil pemeriksaan forensik digital dapat memengaruhi putusan hukum, reputasi seseorang, dan pertanggungjawaban pidana atau perdata.

Prinsip keenam adalah **keterulangan dan keterujian proses**. Pemeriksaan forensik digital harus dilakukan dengan metode yang dapat dijelaskan, diuji, dan apabila diperlukan dapat diulang oleh pemeriksa lain. Prinsip ini penting untuk memastikan bahwa hasil analisis tidak hanya bergantung pada pendapat subjektif pemeriksa, tetapi dapat diverifikasi melalui prosedur yang jelas. Oleh karena itu, setiap tahapan pemeriksaan perlu didokumentasikan, termasuk alat yang digunakan, versi perangkat lunak, parameter analisis, waktu pemeriksaan, metode ekstraksi data, dan hasil yang diperoleh. Dokumentasi yang baik memungkinkan pihak lain menilai apakah proses pemeriksaan dilakukan secara benar dan dapat dipercaya (Kent et al., 2006).

Prinsip ketujuh adalah **kehati-hatian dalam menangani bukti asli**. Dalam praktik forensik digital, pemeriksaan sebaiknya tidak dilakukan langsung terhadap media asli apabila hal tersebut berisiko mengubah data. Pemeriksa biasanya membuat salinan forensik terlebih dahulu, kemudian analisis dilakukan terhadap salinan tersebut. Media asli disimpan dalam kondisi aman untuk menjaga kemungkinan pemeriksaan ulang. Prinsip ini sejalan

dengan pedoman forensik digital yang menekankan bahwa tindakan terhadap bukti digital tidak boleh mengubah data asli, kecuali dalam kondisi tertentu yang tidak dapat dihindari dan harus dijelaskan secara memadai (ACPO, 2012; ISO/IEC, 2012).

Prinsip kedelapan adalah **kerahasiaan dan perlindungan data**. Bukti digital sering kali berisi informasi pribadi, data sensitif, rahasia bisnis, dokumen internal organisasi, komunikasi pribadi, atau informasi pihak ketiga yang tidak selalu berhubungan langsung dengan perkara. Oleh karena itu, pemeriksa forensik digital wajib menjaga kerahasiaan data yang ditemukan selama proses pemeriksaan. Data yang tidak relevan dengan perkara sebaiknya tidak disebarluaskan atau digunakan di luar kepentingan hukum yang sah. Prinsip ini penting agar proses pembuktian tidak menimbulkan pelanggaran baru terhadap hak privasi dan pelindungan data pribadi.

Agar lebih mudah dipahami, prinsip dasar forensik digital dapat diringkas sebagai berikut.

Tabel 9.2: Prinsip dasar Forensik Digital Dalam Pembuktian Perkara Digital

Prinsip	**Makna Utama**	**Tujuan dalam Pembuktian**
Legalitas	Pemeriksaan dilakukan berdasarkan dasar hukum dan kewenangan yang sah	Mencegah bukti dipersoalkan karena diperoleh secara tidak sah
Integritas	Bukti dijaga agar tidak berubah sejak ditemukan hingga diajukan	Menjamin bukti tetap utuh dan dapat dipercaya
Keaslian	Bukti dapat diverifikasi sumber dan keterkaitannya dengan perkara	Menunjukkan bahwa bukti benar berasal dari sumber yang dinyatakan
Chain of custody	Riwayat penguasaan dan perpindahan bukti terdokumentasi	Menjamin bukti tidak disalahgunakan, diganti, atau dimanipulasi
Objektivitas	Pemeriksa bekerja berdasarkan data dan metode ilmiah	Menghindari kesimpulan yang bias atau tidak berdasar
Keterulangan	Proses pemeriksaan dapat diuji atau diulang	Memperkuat validitas hasil analisis forensik
Kehati-hatian	Analisis tidak merusak atau mengubah bukti asli	Menjaga nilai pembuktian bukti digital

Prinsip	Makna Utama	Tujuan dalam Pembuktian
Kerahasiaan	Data yang ditemukan dilindungi dari penyalahgunaan	Melindungi privasi dan data sensitif para pihak

Berdasarkan Tabel 9.2, dapat dipahami bahwa forensik digital tidak hanya berkaitan dengan kemampuan teknis menemukan dan membaca data elektronik. Lebih dari itu, forensik digital harus dilaksanakan dengan prinsip hukum dan etika yang ketat. Kesalahan kecil dalam proses pengambilan, penyimpanan, atau analisis bukti digital dapat menyebabkan bukti kehilangan nilai pembuktian. Misalnya, apabila perangkat diperiksa tanpa dokumentasi, file dibuka langsung sehingga metadata berubah, atau bukti dipindahkan tanpa pencatatan, maka pihak lain dapat meragukan keutuhan dan keabsahan bukti tersebut.

Dalam proses hukum, prinsip dasar forensik digital memiliki fungsi untuk membangun kepercayaan terhadap bukti elektronik. Hakim, jaksa, penyidik, advokat, dan para pihak perlu diyakinkan bahwa bukti yang diajukan benar-benar berasal dari sumber yang sah, tidak berubah, diperoleh melalui prosedur yang benar, dan dianalisis dengan metode yang dapat dipertanggungjawabkan. Oleh karena itu, laporan forensik digital harus disusun secara jelas, sistematis, dan dapat dipahami oleh pihak hukum yang mungkin tidak memiliki latar belakang teknis. Laporan tersebut perlu menjelaskan objek pemeriksaan, metode yang digunakan, temuan penting, batasan analisis, serta kesimpulan yang didukung oleh data.

> Prinsip dasar forensik digital menjadi fondasi penting dalam pembuktian perkara digital. Prinsip legalitas, integritas, keaslian, rantai penguasaan bukti, objektivitas, keterulangan, kehati-hatian, dan kerahasiaan harus diterapkan secara konsisten agar bukti elektronik dapat digunakan secara sah dan meyakinkan dalam proses hukum. Tanpa penerapan prinsip-prinsip tersebut, bukti digital berisiko dipersoalkan, baik dari sisi teknis maupun dari sisi hukum. Oleh karena itu, forensik digital perlu dipahami sebagai proses ilmiah, teknis, dan yuridis yang saling berkaitan dalam mendukung penegakan hukum di era digital.

9.4 Tahapan Identifikasi, Akuisisi, Analisis, dan Pelaporan Bukti Digital

Tahapan forensik digital merupakan rangkaian kegiatan sistematis yang dilakukan untuk menemukan, memperoleh, memeriksa, menganalisis, dan menyajikan bukti digital agar dapat digunakan dalam proses hukum. Tahapan ini penting karena bukti digital memiliki karakter yang berbeda dengan bukti fisik. Data digital dapat berubah secara otomatis ketika perangkat dinyalakan, aplikasi dibuka, jaringan tersambung, atau sistem melakukan proses tertentu. Oleh karena itu, pemeriksaan bukti digital harus dilakukan dengan metode yang hati-hati, terdokumentasi, dan dapat dipertanggungjawabkan.

Dalam praktik forensik digital, tahapan pemeriksaan umumnya mencakup identifikasi, akuisisi, analisis, dan pelaporan. Tahapan tersebut sejalan dengan pedoman internasional yang menekankan pentingnya proses identifikasi, pengumpulan, akuisisi, preservasi, pemeriksaan, analisis, dan pelaporan bukti digital (ISO/IEC, 2012; Kent et al., 2006). Meskipun istilah yang digunakan dalam berbagai pedoman dapat berbeda, tujuan utamanya tetap sama, yaitu menjaga agar bukti digital diperoleh secara sah, tetap utuh, dapat diverifikasi, dan memiliki hubungan yang jelas dengan perkara yang diperiksa.

Gambar 9.2: Alur Tahapan Forensik Digital Dalam Pembuktian Perkara Digital

Tahap pertama adalah **identifikasi bukti digital**. Identifikasi merupakan proses awal untuk menentukan sumber, jenis, lokasi, dan potensi relevansi bukti digital yang berkaitan dengan suatu perkara. Pada tahap ini, pemeriksa

perlu memahami peristiwa hukum yang sedang diperiksa, sistem elektronik yang digunakan, pihak yang terlibat, perangkat yang mungkin menyimpan data, serta jenis informasi yang dibutuhkan. Identifikasi tidak hanya dilakukan terhadap perangkat fisik seperti komputer, laptop, telepon seluler, hard disk, flash disk, dan kamera digital, tetapi juga terhadap sumber nonfisik seperti akun media sosial, surel, layanan penyimpanan awan, server, log aplikasi, basis data, dan sistem jaringan.

Dalam tahap identifikasi, pemeriksa perlu menentukan apakah suatu sumber data memiliki potensi nilai pembuktian. Misalnya, dalam perkara penipuan daring, sumber bukti dapat berupa percakapan aplikasi pesan, tautan situs palsu, rekening tujuan transfer, riwayat transaksi, alamat IP, domain, serta data akun yang digunakan pelaku. Dalam perkara akses ilegal, sumber bukti dapat berupa log server, rekaman aktivitas login, perubahan konfigurasi sistem, file yang dimodifikasi, atau perangkat yang digunakan untuk melakukan akses. Dengan demikian, identifikasi berfungsi sebagai dasar untuk menentukan bukti mana yang perlu diamankan dan bagaimana cara terbaik untuk memperolehnya.

Tahap identifikasi juga harus dilakukan dengan memperhatikan risiko perubahan data. Beberapa data digital bersifat volatil, yaitu mudah hilang apabila perangkat dimatikan, jaringan terputus, atau sistem mengalami perubahan. Contoh data volatil adalah isi memori sementara, koneksi jaringan aktif, proses yang sedang berjalan, dan sesi login yang masih terbuka. Oleh karena itu, pemeriksa harus menentukan prioritas penanganan bukti berdasarkan tingkat kerentanannya. Data yang mudah hilang perlu segera diamankan, sedangkan data yang lebih stabil dapat ditangani setelah prosedur awal dilakukan.

Tahap kedua adalah **akuisisi bukti digital**. Akuisisi merupakan proses memperoleh atau menyalin data digital dari sumber bukti dengan cara yang menjaga keaslian dan integritas data. Dalam forensik digital, akuisisi tidak boleh dilakukan secara sembarangan karena kesalahan dalam proses penyalinan dapat mengubah metadata, merusak file, atau menimbulkan keraguan terhadap keutuhan bukti. Oleh karena itu, akuisisi sebaiknya dilakukan menggunakan metode forensik yang dapat menghasilkan salinan data secara utuh dan dapat diverifikasi.

Akuisisi dapat dilakukan dalam beberapa bentuk, bergantung pada jenis bukti dan kondisi perangkat. Pada perangkat penyimpanan seperti hard disk

atau flash disk, akuisisi dapat dilakukan melalui pembuatan citra forensik atau forensic image. Citra forensik merupakan salinan bit demi bit dari media penyimpanan sehingga tidak hanya menyalin file yang terlihat, tetapi juga ruang kosong, file tersembunyi, file yang telah dihapus, dan struktur sistem file. Pada perangkat seluler, akuisisi dapat dilakukan melalui ekstraksi logis, ekstraksi sistem file, atau ekstraksi fisik, sesuai dengan kemampuan alat forensik dan kondisi perangkat. Pada sistem jaringan atau layanan awan, akuisisi dapat dilakukan melalui pengambilan log, ekspor data, permintaan data kepada penyedia layanan, atau pengamanan rekaman aktivitas sistem.

Dalam proses akuisisi, penggunaan nilai hash menjadi sangat penting. Nilai hash adalah nilai unik yang dihasilkan dari suatu data atau file melalui algoritma tertentu. Apabila data berubah sedikit saja, nilai hash akan berubah. Oleh karena itu, nilai hash digunakan untuk membandingkan apakah bukti asli dan salinan forensik memiliki isi yang sama. Selain itu, pemeriksa perlu mendokumentasikan waktu akuisisi, perangkat yang digunakan, kondisi barang bukti, identitas pemeriksa, metode akuisisi, serta hasil verifikasi. Dokumentasi ini menjadi bagian penting dari rantai penguasaan bukti atau chain of custody (Casey, 2011; ISO/IEC, 2012).

Tahap ketiga adalah **analisis bukti digital**. Analisis merupakan proses memeriksa data yang telah diperoleh untuk menemukan informasi yang relevan dengan perkara. Pada tahap ini, pemeriksa tidak lagi sekadar mengumpulkan bukti, tetapi berusaha memahami makna, pola, hubungan, dan konteks dari data digital. Analisis dapat mencakup pemeriksaan file, metadata, riwayat aktivitas, log sistem, komunikasi digital, riwayat akses internet, data lokasi, transaksi elektronik, struktur folder, aplikasi yang digunakan, serta jejak penghapusan atau manipulasi data.

Analisis forensik digital harus dilakukan secara objektif dan berdasarkan metode yang dapat dijelaskan. Pemeriksa perlu membedakan antara data yang relevan, data yang tidak relevan, dan data yang memerlukan verifikasi tambahan. Misalnya, adanya file tertentu pada sebuah perangkat belum tentu membuktikan bahwa pemilik perangkat membuat atau menggunakan file tersebut. Pemeriksa perlu menilai waktu pembuatan file, akun pengguna yang aktif, riwayat akses, metadata, sumber unduhan, serta keterkaitan dengan bukti lain. Dengan demikian, analisis forensik tidak boleh berhenti pada temuan teknis, tetapi harus menjelaskan hubungan antara temuan tersebut dengan peristiwa hukum yang sedang diperiksa.

Dalam perkara digital, analisis sering kali memerlukan korelasi berbagai sumber bukti. Sebagai contoh, dalam kasus pengambilalihan akun, pemeriksa dapat membandingkan log akses akun, alamat IP, lokasi akses, perangkat yang digunakan, waktu perubahan kata sandi, surel pemulihan, dan aktivitas transaksi setelah akun dikuasai. Dalam kasus penyebaran dokumen elektronik tanpa izin, pemeriksa dapat menelusuri metadata dokumen, waktu pembuatan, riwayat pengiriman, platform distribusi, dan akun yang mengunggah dokumen. Korelasi tersebut membantu membangun rangkaian peristiwa yang lebih utuh dan dapat dipahami dalam proses hukum.

Tahap analisis juga perlu memperhatikan batasan teknis. Tidak semua data dapat dipulihkan, tidak semua akun dapat diidentifikasi secara pasti, dan tidak semua aktivitas digital meninggalkan jejak yang lengkap. Beberapa kendala yang dapat muncul antara lain enkripsi, penghapusan data, kerusakan perangkat, penggunaan jaringan anonim, akun palsu, data yang berada di luar yurisdiksi, atau keterbatasan akses terhadap server penyedia layanan. Oleh karena itu, laporan analisis harus menyampaikan temuan secara proporsional, termasuk batasan pemeriksaan dan tingkat keyakinan terhadap kesimpulan yang dibuat.

Tahap keempat adalah **pelaporan bukti digital**. Pelaporan merupakan proses menyusun hasil pemeriksaan forensik digital ke dalam bentuk laporan yang sistematis, jelas, dan dapat dipahami oleh pihak hukum. Laporan forensik digital tidak hanya ditujukan kepada ahli teknologi informasi, tetapi juga kepada penyidik, jaksa, advokat, hakim, dan pihak lain yang mungkin tidak memiliki latar belakang teknis. Oleh karena itu, laporan harus menjelaskan objek pemeriksaan, metode yang digunakan, alat yang dipakai, langkah pemeriksaan, temuan penting, analisis, kesimpulan, serta keterkaitan temuan dengan perkara.

Laporan forensik digital yang baik harus memenuhi beberapa karakteristik. Pertama, laporan harus objektif, yaitu menyajikan temuan berdasarkan data dan bukan asumsi. Kedua, laporan harus transparan, yaitu menjelaskan metode dan tahapan pemeriksaan sehingga dapat ditinjau kembali. Ketiga, laporan harus terstruktur, yaitu disusun secara runtut mulai dari latar belakang pemeriksaan hingga kesimpulan. Keempat, laporan harus dapat diverifikasi, yaitu menyertakan informasi teknis yang memungkinkan

pemeriksaan ulang apabila diperlukan. Kelima, laporan harus menggunakan bahasa yang jelas agar temuan teknis dapat dipahami dalam konteks hukum.

Agar tahapan forensik digital lebih mudah dipahami, ringkasan proses dapat disajikan dalam tabel berikut.

Tabel 9.3 Tahapan utama forensik digital dan output pemeriksaan:

Tahapan	Kegiatan Utama	Output yang Diharapkan
Identifikasi	Menentukan sumber, jenis, lokasi, dan relevansi bukti digital	Daftar potensi bukti digital dan prioritas penanganan
Akuisisi	Mengamankan dan menyalin data dengan metode forensik	Salinan forensik, nilai hash, dan dokumentasi akuisisi
Analisis	Memeriksa, menghubungkan, dan menafsirkan data digital	Temuan forensik yang relevan dengan perkara
Pelaporan	Menyusun hasil pemeriksaan secara sistematis	Laporan forensik digital yang dapat digunakan dalam proses hukum

Tabel 9.3 menunjukkan bahwa setiap tahapan forensik digital memiliki fungsi dan keluaran yang berbeda. Identifikasi menghasilkan daftar sumber bukti yang perlu diperiksa. Akuisisi menghasilkan salinan forensik dan dokumentasi yang menjaga integritas bukti. Analisis menghasilkan temuan yang menjelaskan hubungan antara data digital dan perkara. Pelaporan menghasilkan dokumen resmi yang dapat digunakan untuk mendukung pembuktian dalam proses hukum. Keterpaduan seluruh tahapan tersebut menentukan apakah bukti digital dapat dipertanggungjawabkan secara teknis dan yuridis.

Dalam konteks proses hukum di Indonesia, tahapan forensik digital perlu ditempatkan sebagai bagian dari upaya menjaga nilai pembuktian bukti elektronik. Informasi elektronik dan dokumen elektronik telah diakui sebagai alat bukti hukum yang sah dalam Undang-Undang Informasi dan Transaksi Elektronik (Republik Indonesia, 2008, 2016b, 2024b). Namun, pengakuan hukum tersebut harus didukung oleh prosedur penanganan bukti yang benar. Bukti elektronik yang tidak jelas asal-usulnya, tidak terdokumentasi proses perolehannya, atau tidak dapat dijamin integritasnya dapat dipersoalkan dalam proses pembuktian.

Dengan demikian, tahapan identifikasi, akuisisi, analisis, dan pelaporan merupakan inti dari proses forensik digital. Identifikasi memastikan bahwa sumber bukti yang relevan dapat ditemukan. Akuisisi memastikan bahwa

bukti diperoleh tanpa merusak integritas data. Analisis memastikan bahwa data digital dapat dimaknai secara objektif dan dikaitkan dengan perkara. Pelaporan memastikan bahwa hasil pemeriksaan dapat dipahami dan digunakan dalam proses hukum. Apabila seluruh tahapan tersebut dilakukan secara benar, bukti digital akan memiliki nilai pembuktian yang lebih kuat dan dapat mendukung penegakan hukum secara lebih akurat di era digital.

9.5 Keaslian, Integritas, dan Rantai Penguasaan Bukti Digital

Keaslian, integritas, dan rantai penguasaan bukti digital merupakan tiga unsur penting yang menentukan apakah bukti elektronik dapat dipercaya dan dipertimbangkan dalam proses hukum. Bukti digital berbeda dengan bukti fisik karena mudah disalin, diubah, dipindahkan, dihapus, atau dimanipulasi tanpa meninggalkan perubahan yang mudah dilihat secara kasatmata. Oleh karena itu, keberadaan bukti digital saja belum cukup untuk membuktikan suatu peristiwa hukum. Bukti tersebut harus dapat dijelaskan sumbernya, dijaga keutuhannya, dan didokumentasikan proses penguasaannya sejak pertama kali ditemukan sampai diajukan dalam proses hukum.

Dalam perkara digital, keaslian bukti berkaitan dengan pertanyaan apakah bukti benar berasal dari sumber yang dinyatakan. Misalnya, apakah suatu pesan benar berasal dari akun tertentu, apakah dokumen elektronik benar dibuat oleh pihak tertentu, atau apakah log sistem benar mencatat aktivitas pengguna pada waktu tertentu. Keaslian penting karena identitas digital dapat dipalsukan, akun dapat diretas, tangkapan layar dapat dimanipulasi, dan dokumen elektronik dapat diubah. Oleh karena itu, pemeriksaan keaslian bukti digital tidak cukup hanya melihat tampilan luar, tetapi perlu memperhatikan metadata, sumber data, waktu pembuatan, riwayat perubahan, log akses, perangkat yang digunakan, serta keterkaitan bukti dengan bukti lain.

Keaslian bukti digital juga berkaitan dengan kemampuan menghubungkan bukti dengan subjek hukum tertentu. Dalam proses pembuktian, bukti digital harus mampu menunjukkan hubungan antara data, perangkat, akun, pengguna, dan peristiwa hukum. Sebagai contoh, dalam perkara pencemaran nama baik melalui media sosial, tangkapan layar unggahan dapat menjadi petunjuk awal, tetapi pemeriksaan lebih lanjut tetap diperlukan untuk

memastikan URL, waktu unggahan, identitas akun, alamat IP, perangkat yang digunakan, dan kemungkinan adanya akses oleh pihak lain. Dengan demikian, keaslian bukti digital tidak hanya menyangkut apakah data tersebut ada, tetapi juga apakah data tersebut dapat dipertanggungjawabkan asal-usul dan keterhubungannya.

Selain keaslian, integritas bukti digital menjadi unsur yang sangat penting. Integritas berarti bahwa bukti digital tetap utuh dan tidak mengalami perubahan sejak diperoleh hingga digunakan dalam proses hukum. Perubahan kecil pada file, metadata, atau struktur data dapat memengaruhi nilai pembuktian. Oleh karena itu, pemeriksa forensik digital harus menjaga agar bukti asli tidak berubah selama proses penanganan. Prinsip ini sejalan dengan pedoman forensik digital yang menekankan pentingnya identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital agar data yang berpotensi menjadi bukti tetap terjaga keutuhannya (ISO/IEC, 2012).

Salah satu cara untuk menjaga integritas bukti digital adalah menggunakan nilai hash. Nilai hash merupakan hasil perhitungan algoritmik terhadap suatu data atau file yang berfungsi seperti sidik jari digital. Apabila isi data berubah sedikit saja, nilai hash akan berubah. Oleh karena itu, nilai hash dapat digunakan untuk membandingkan bukti asli dan salinan forensik. Jika nilai hash keduanya sama, maka salinan tersebut dapat dianggap identik dengan data asli. Dalam praktik forensik digital, penggunaan nilai hash membantu pemeriksa menjelaskan bahwa data yang dianalisis tidak berubah sejak proses akuisisi dilakukan (Casey, 2011; Kent et al., 2006).

Selain penggunaan nilai hash, integritas bukti digital juga perlu dijaga melalui pembuatan salinan forensik, penggunaan perangkat pelindung seperti *write blocker*, penyimpanan media bukti dalam tempat yang aman, serta dokumentasi seluruh tindakan yang dilakukan terhadap bukti. Analisis sebaiknya dilakukan terhadap salinan forensik, bukan langsung terhadap media asli, agar bukti asli tetap dapat dipertahankan dalam kondisi semula. Apabila pemeriksaan harus dilakukan terhadap sistem yang sedang aktif, tindakan tersebut perlu dijelaskan secara rinci karena sistem aktif dapat mengalami perubahan data secara otomatis.

Unsur penting berikutnya adalah rantai penguasaan bukti digital atau chain of custody. Rantai penguasaan bukti adalah catatan yang menunjukkan riwayat penguasaan, perpindahan, penyimpanan, dan pemeriksaan bukti

sejak pertama kali ditemukan sampai diajukan dalam proses hukum. Dalam konteks bukti digital, chain of custody menjadi sangat penting karena data dapat berpindah dari perangkat ke salinan forensik, dari penyidik ke ahli forensik, dari laboratorium ke jaksa, dan dari jaksa ke pengadilan. Setiap perpindahan tersebut harus dapat ditelusuri agar tidak muncul keraguan terhadap keaslian dan integritas bukti.

Dokumentasi rantai penguasaan bukti setidaknya memuat identitas bukti, waktu dan lokasi perolehan, pihak yang menemukan atau menerima bukti, kondisi awal bukti, tindakan yang dilakukan, alat yang digunakan, nilai hash, media penyimpanan, tempat penyimpanan, serta pihak yang menerima bukti pada setiap perpindahan. Dokumentasi ini berfungsi untuk menunjukkan bahwa bukti tidak diganti, tidak dimanipulasi, dan tidak digunakan di luar prosedur yang sah. Tanpa chain of custody yang jelas, pihak lawan dapat mempertanyakan apakah bukti yang diajukan di pengadilan masih sama dengan bukti yang ditemukan pada awal pemeriksaan.

Gambar 9.3: Alur Rantai Penguasaan Bukti Digital

Agar hubungan antara keaslian, integritas, dan rantai penguasaan bukti digital lebih mudah dipahami, ketiganya dapat diringkas sebagai berikut.

Tabel 9.4: Unsur keaslian, integritas, dan rantai penguasaan bukti digital

Unsur	Pertanyaan Utama	Cara Menjaga atau Membuktikan
Keaslian	Apakah bukti benar berasal dari sumber yang dinyatakan?	Pemeriksaan metadata, log akses, sumber data, akun, perangkat, URL, dan keterkaitan dengan bukti lain

Unsur	Pertanyaan Utama	Cara Menjaga atau Membuktikan
Integritas	Apakah bukti tetap utuh dan tidak berubah?	Penggunaan hash value, salinan forensik, write blocker, preservasi media, dan dokumentasi tindakan
Chain of custody	Siapa yang menguasai bukti sejak ditemukan sampai diajukan?	Formulir penguasaan bukti, pencatatan waktu, identitas petugas, lokasi penyimpanan, dan riwayat perpindahan bukti

Tabel 9.4 menunjukkan bahwa keaslian, integritas, dan chain of custody memiliki fokus yang berbeda, tetapi saling berkaitan. Keaslian memastikan bahwa bukti berasal dari sumber yang benar. Integritas memastikan bahwa bukti tidak mengalami perubahan. Sementara itu, chain of custody memastikan bahwa seluruh proses penguasaan bukti dapat ditelusuri dan dipertanggungjawabkan. Apabila salah satu unsur tersebut lemah, maka kekuatan pembuktian bukti digital dapat berkurang.

Dalam proses hukum, ketiga unsur tersebut sangat penting karena bukti elektronik telah diakui sebagai alat bukti hukum yang sah dalam sistem hukum Indonesia (Republik Indonesia, 2008, 2016b, 2024b). Namun, pengakuan hukum tersebut tetap harus didukung oleh prosedur penanganan bukti yang benar. Bukti elektronik yang tidak jelas sumbernya, tidak dapat dijamin keutuhannya, atau tidak memiliki dokumentasi penguasaan yang baik dapat menimbulkan keraguan. Oleh karena itu, bukti digital harus dikelola dengan prinsip kehati-hatian sejak tahap awal pemeriksaan.

Dengan demikian, keaslian, integritas, dan rantai penguasaan bukti digital merupakan fondasi penting dalam pembuktian perkara digital. Keaslian memastikan bukti dapat dikaitkan dengan sumber yang tepat, integritas memastikan bukti tetap utuh, dan *chain of custody* memastikan seluruh proses penanganan bukti dapat ditelusuri. Penerapan ketiga unsur ini akan memperkuat nilai pembuktian bukti elektronik dan membantu proses hukum berjalan secara lebih objektif, akurat, dan dapat dipertanggungjawabkan.

9.6 Tantangan Pembuktian Digital di Pengadilan

Pembuktian digital di pengadilan menghadirkan tantangan yang lebih kompleks dibandingkan pembuktian dalam perkara konvensional. Hal ini disebabkan karena bukti digital memiliki karakter yang tidak selalu terlihat

secara fisik, mudah berubah, dapat disalin tanpa mengurangi bentuk aslinya, dan sering tersimpan pada sistem elektronik yang tersebar di berbagai lokasi. Bukti digital dapat berada pada perangkat pribadi, server perusahaan, sistem penyimpanan awan, platform media sosial, aplikasi pesan, jaringan komputer, atau penyedia layanan yang berada di luar wilayah hukum Indonesia. Kondisi tersebut menuntut proses pembuktian yang tidak hanya memahami aspek hukum, tetapi juga aspek teknis teknologi informasi dan forensik digital.

Tantangan pertama adalah sifat bukti digital yang mudah berubah dan mudah dimanipulasi. Data elektronik dapat mengalami perubahan ketika perangkat dinyalakan, aplikasi dibuka, file dipindahkan, sistem melakukan pembaruan otomatis, atau jaringan kembali terhubung. Selain itu, bukti seperti tangkapan layar, dokumen elektronik, rekaman percakapan, dan metadata dapat direkayasa apabila tidak diperoleh dari sumber yang sah dan tidak diverifikasi melalui metode forensik digital. Oleh karena itu, pengadilan perlu menilai apakah bukti digital yang diajukan benar-benar dapat dipertanggungjawabkan keaslian dan integritasnya. Tanpa verifikasi yang memadai, bukti digital berisiko hanya menjadi tampilan visual yang belum tentu menggambarkan fakta sebenarnya.

Tantangan kedua adalah kesulitan membuktikan hubungan antara bukti digital dengan pelaku. Dalam ruang digital, seseorang dapat menggunakan akun palsu, identitas anonim, jaringan privat virtual, perangkat orang lain, atau sistem yang telah diretas. Akibatnya, keberadaan suatu unggahan, pesan, transaksi, atau aktivitas login belum tentu secara langsung membuktikan bahwa pemilik akun atau pemilik perangkat adalah pelaku. Pembuktian perlu menghubungkan berbagai unsur, seperti identitas akun, alamat IP, perangkat yang digunakan, lokasi akses, pola aktivitas, riwayat komunikasi, dan bukti pendukung lain. Dengan demikian, pembuktian digital tidak cukup hanya menunjukkan bahwa suatu data ada, tetapi juga harus menjelaskan siapa yang mengendalikan atau menggunakan data tersebut pada saat peristiwa terjadi.

Tantangan ketiga berkaitan dengan validitas dan keandalan proses forensik digital. Bukti elektronik telah diakui sebagai alat bukti hukum yang sah dalam hukum Indonesia, tetapi kekuatan pembuktiannya tetap bergantung pada cara bukti tersebut diperoleh, diamankan, dianalisis, dan dilaporkan (Republik Indonesia, 2008, 2016b, 2024b). Apabila proses akuisisi bukti

tidak menggunakan prosedur yang benar, nilai hash tidak dicatat, salinan forensik tidak dibuat, atau rantai penguasaan bukti tidak terdokumentasi, maka bukti tersebut dapat dipersoalkan di pengadilan. Pedoman forensik digital seperti ISO/IEC 27037 menekankan pentingnya identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital untuk menjaga nilai pembuktian (ISO/IEC, 2012). Sementara itu, NIST menekankan bahwa proses forensik perlu dilakukan melalui tahapan yang sistematis agar hasil pemeriksaan dapat dipertanggungjawabkan (Kent et al., 2006).

Tantangan keempat adalah keterbatasan pemahaman teknis dalam proses persidangan. Tidak semua pihak dalam proses hukum memiliki latar belakang teknologi informasi. Hakim, jaksa, advokat, atau para pihak mungkin memahami aspek hukum, tetapi belum tentu memahami konsep metadata, log sistem, alamat IP, enkripsi, hash value, file recovery, malware, atau sistem komputasi awan. Kondisi ini dapat menyebabkan kesulitan dalam menilai bobot bukti digital. Oleh karena itu, keterangan ahli menjadi sangat penting untuk menjelaskan bagaimana bukti diperoleh, bagaimana data dianalisis, apa makna temuan teknis, serta sejauh mana bukti tersebut dapat dikaitkan dengan perkara yang diperiksa.

Tantangan kelima adalah keberadaan data pada pihak ketiga atau platform digital. Dalam banyak perkara, data yang diperlukan untuk pembuktian tidak berada pada korban atau pelaku, tetapi tersimpan pada penyedia layanan, seperti marketplace, bank digital, operator telekomunikasi, platform media sosial, penyedia surel, atau penyedia layanan komputasi awan. Misalnya, dalam perkara penipuan daring, korban mungkin hanya memiliki bukti percakapan dan bukti transfer, sedangkan data teknis seperti alamat IP, riwayat login, perangkat yang digunakan, dan data akun berada pada platform. Apabila platform tidak kooperatif, tidak memiliki mekanisme penyimpanan log yang baik, atau berada di luar yurisdiksi nasional, proses pembuktian menjadi lebih sulit.

Tantangan keenam adalah persoalan yurisdiksi. Aktivitas digital sering melampaui batas wilayah negara. Pelaku dapat berada di satu negara, korban berada di negara lain, server berada di negara berbeda, dan transaksi dilakukan melalui sistem pembayaran lintas negara. Dalam kondisi tersebut, aparat penegak hukum dapat menghadapi kendala dalam memperoleh data, meminta keterangan platform, melakukan penyitaan elektronik, atau menindak pelaku. Persoalan yurisdiksi menunjukkan bahwa pembuktian

digital tidak hanya bergantung pada hukum nasional, tetapi juga membutuhkan kerja sama internasional, mekanisme bantuan hukum timbal balik, dan koordinasi dengan penyedia layanan global.

Tantangan ketujuh adalah penggunaan teknologi enkripsi, anonimitas, dan penghapusan data. Enkripsi memang penting untuk melindungi keamanan informasi dan privasi pengguna, tetapi dalam konteks penegakan hukum dapat menjadi kendala ketika data yang relevan tidak dapat dibuka atau dianalisis. Selain itu, pelaku dapat menggunakan aplikasi yang menyediakan fitur pesan hilang otomatis, penyimpanan terenkripsi, akun sementara, atau layanan anonim untuk menyembunyikan jejak digital. Penghapusan data juga tidak selalu mudah ditangani, terutama jika perangkat telah diformat, akun telah ditutup, atau data berada pada server yang tidak dapat diakses. Meskipun sebagian data masih dapat dipulihkan melalui teknik forensik digital, hasilnya sangat bergantung pada kondisi perangkat, sistem, dan waktu penanganan.

Tantangan kedelapan berkaitan dengan keseimbangan antara kebutuhan pembuktian dan perlindungan hak individu. Proses pembuktian digital sering melibatkan data pribadi, komunikasi privat, informasi keuangan, lokasi, foto, video, dokumen pribadi, dan informasi pihak ketiga. Oleh karena itu, pengumpulan dan pemeriksaan bukti digital harus memperhatikan prinsip legalitas, proporsionalitas, dan perlindungan data pribadi. Upaya penegakan hukum tidak boleh dilakukan dengan cara yang melanggar hak privasi secara berlebihan. Dalam konteks ini, pengadilan perlu menilai apakah bukti diperoleh melalui prosedur yang sah dan apakah penggunaan data tersebut relevan dengan perkara yang diperiksa.

Tantangan kesembilan adalah perbedaan kualitas bukti digital yang diajukan oleh para pihak. Dalam praktik, bukti digital yang diajukan sering kali hanya berupa tangkapan layar, cetakan percakapan, foto tampilan aplikasi, atau dokumen elektronik tanpa metadata pendukung. Bukti seperti ini dapat membantu memberikan gambaran awal, tetapi masih perlu diverifikasi. Tangkapan layar, misalnya, dapat diedit atau tidak menampilkan konteks percakapan secara lengkap. Oleh karena itu, apabila memungkinkan, bukti sebaiknya dilengkapi dengan URL, waktu akses, sumber asli, metadata, log sistem, nilai hash, atau keterangan ahli. Semakin lengkap konteks teknis bukti, semakin kuat pula kedudukannya dalam proses pembuktian.

Tantangan kesepuluh adalah kebutuhan untuk menyajikan bukti digital dalam bahasa yang dapat dipahami di pengadilan. Hasil pemeriksaan forensik digital sering kali berisi istilah teknis yang sulit dipahami oleh pihak nonteknis. Apabila laporan forensik terlalu teknis, maka substansi pembuktiannya dapat sulit dinilai. Sebaliknya, apabila laporan terlalu sederhana, maka aspek teknis yang penting dapat terabaikan. Oleh karena itu, laporan forensik digital perlu disusun secara seimbang, yaitu tetap akurat secara teknis tetapi dapat dipahami secara hukum. Ahli forensik digital perlu menjelaskan temuan dengan bahasa yang jelas, menunjukkan hubungan antara bukti dan perkara, serta menyampaikan batasan pemeriksaan secara objektif.

Agar lebih mudah dipahami, tantangan pembuktian digital di pengadilan dapat diringkas sebagai berikut.

Tantangan	**Bentuk Permasalahan**	**Dampak terhadap Pembuktian**
Perubahan dan manipulasi data	Data dapat diubah, dihapus, disalin, atau direkayasa	Keaslian dan integritas bukti dapat dipersoalkan
Identifikasi pelaku	Akun palsu, VPN, perangkat bersama, atau identitas anonim	Hubungan antara bukti dan pelaku sulit dibuktikan
Validitas forensik	Akuisisi tidak sesuai prosedur, hash tidak dicatat, chain of custody lemah	Bukti dapat kehilangan nilai pembuktian
Keterbatasan pemahaman teknis	Istilah dan proses teknis sulit dipahami pihak hukum	Penilaian terhadap bobot bukti menjadi tidak optimal
Data berada pada platform	Log dan metadata dikuasai penyedia layanan	Pihak berperkara kesulitan memperoleh bukti lengkap
Yurisdiksi lintas negara	Server, pelaku, dan korban berada di wilayah berbeda	Proses permintaan data dan penegakan hukum menjadi lambat
Enkripsi dan anonimitas	Data terkunci, pesan hilang otomatis, akun anonim	Jejak digital sulit ditemukan atau dianalisis
Perlindungan privasi	Bukti mengandung data pribadi atau komunikasi privat	Perlu keseimbangan antara pembuktian dan hak individu
Bukti tidak lengkap	Hanya berupa tangkapan layar atau cetakan percakapan	Bukti memerlukan verifikasi tambahan
Penyajian teknis di pengadilan	Laporan terlalu teknis atau tidak menjelaskan konteks hukum	Hakim dan para pihak sulit memahami makna bukti

Tabel 9.5 menunjukkan bahwa tantangan pembuktian digital tidak hanya berkaitan dengan keberadaan bukti, tetapi juga dengan cara memperoleh, memverifikasi, menghubungkan, dan menjelaskan bukti tersebut dalam proses hukum. Bukti digital dapat memiliki nilai pembuktian yang kuat apabila diperoleh secara sah, dianalisis secara ilmiah, dan disajikan secara jelas. Sebaliknya, bukti digital dapat menjadi lemah apabila tidak dapat diverifikasi, tidak jelas sumbernya, atau tidak memiliki dokumentasi penanganan yang memadai.

Menghadapi berbagai tantangan tersebut, penguatan pembuktian digital perlu dilakukan melalui beberapa langkah. Aparat penegak hukum perlu meningkatkan kemampuan forensik digital, pengadilan perlu memahami karakter bukti elektronik, ahli perlu menyusun laporan yang objektif dan mudah dipahami, serta platform digital perlu menyediakan mekanisme penyimpanan dan pemberian data yang akuntabel sesuai ketentuan hukum. Selain itu, masyarakat juga perlu memiliki kesadaran untuk menyimpan bukti digital secara benar ketika mengalami peristiwa hukum, misalnya dengan menyimpan tautan, waktu kejadian, bukti transaksi, percakapan lengkap, dan informasi pendukung lainnya.

> Tantangan pembuktian digital di pengadilan merupakan konsekuensi dari berkembangnya aktivitas hukum di ruang digital. Pengakuan terhadap bukti elektronik sebagai alat bukti yang sah perlu diikuti oleh kemampuan teknis, prosedur forensik yang benar, dokumentasi yang kuat, dan pemahaman hukum yang memadai. Pembuktian digital tidak cukup hanya menghadirkan data elektronik, tetapi harus mampu menunjukkan bahwa data tersebut asli, utuh, relevan, diperoleh secara sah, dan dapat menjelaskan peristiwa hukum yang diperiksa. Apabila tantangan tersebut dapat diatasi, bukti digital dapat menjadi instrumen penting dalam mewujudkan penegakan hukum yang lebih akurat, adil, dan responsif terhadap perkembangan teknologi.

Bab 10
Hukum Kekayaan Intelektual Digital

10.1 Konsep Kekayaan Intelektual dalam Dunia Digital

Perkembangan teknologi informasi dan komunikasi telah mengubah cara manusia menciptakan, menggunakan, menyebarluaskan, dan memanfaatkan karya intelektual. Jika pada era konvensional hasil kreativitas manusia umumnya diwujudkan dalam bentuk fisik seperti buku, lukisan, rekaman musik, atau produk industri, maka pada era digital karya intelektual banyak hadir dalam bentuk data, file elektronik, perangkat lunak, konten multimedia, maupun informasi yang dapat disimpan, diproses, dan didistribusikan melalui jaringan internet. Perubahan tersebut melahirkan konsep kekayaan intelektual digital yang memiliki karakteristik berbeda dibandingkan dengan kekayaan intelektual dalam lingkungan konvensional.

Gambar 10.1: Ekosistem Kekayaan Intelektual Digital

Secara umum, kekayaan intelektual merupakan hak yang diberikan oleh hukum kepada seseorang atau badan hukum atas hasil olah pikir, kreativitas, kemampuan intelektual, dan inovasi yang memiliki nilai ekonomi maupun nilai moral (Koto et al., 2023). Perlindungan tersebut diberikan untuk

mendorong terciptanya inovasi, memberikan penghargaan kepada pencipta atau inventor, serta menciptakan iklim yang kondusif bagi perkembangan ilmu pengetahuan, teknologi, seni, dan budaya.

Dalam dunia digital, objek kekayaan intelektual tidak lagi terbatas pada bentuk fisik, tetapi berkembang menjadi berbagai bentuk karya digital seperti perangkat lunak komputer, aplikasi seluler, basis data, desain antarmuka pengguna (*user interface*), karya fotografi digital, video digital, konten media sosial, karya audiovisual, permainan digital, karya berbasis kecerdasan buatan, hingga aset digital yang berbasis teknologi *blockchain*. Meskipun berbentuk digital, karya-karya tersebut tetap merupakan hasil kreativitas manusia yang memiliki nilai ekonomi dan oleh karena itu memerlukan perlindungan hukum yang memadai (Koto et al., 2023).

Karakteristik utama kekayaan intelektual dalam dunia digital adalah kemudahan reproduksi dan distribusi. Berbeda dengan karya fisik yang memerlukan biaya produksi dan distribusi yang relatif besar, karya digital dapat diperbanyak dan disebarluaskan dalam jumlah tidak terbatas dengan biaya yang sangat rendah dan dalam waktu yang sangat singkat. Sebuah karya musik, film, perangkat lunak, atau buku elektronik dapat disalin dan didistribusikan ke berbagai negara hanya dalam hitungan detik melalui internet. Kondisi ini memberikan peluang besar bagi penyebaran ilmu pengetahuan dan kreativitas, namun sekaligus meningkatkan risiko pelanggaran hak kekayaan intelektual seperti pembajakan, penggandaan tanpa izin, dan distribusi ilegal.

Selain mudah direproduksi, karya digital juga memiliki sifat lintas batas negara (*borderless*). Sebuah karya yang dibuat di suatu negara dapat diakses, digunakan, atau bahkan disalahgunakan oleh pihak lain di negara yang berbeda tanpa hambatan geografis. Karakteristik ini menimbulkan tantangan hukum terkait yurisdiksi, penegakan hukum, dan harmonisasi regulasi antarnegara dalam perlindungan kekayaan intelektual (Febriharini, 2016).

Konsep kekayaan intelektual dalam dunia digital juga berkaitan erat dengan keseimbangan antara perlindungan hak eksklusif pemegang hak dan kepentingan publik dalam memperoleh akses terhadap informasi dan pengetahuan. Perlindungan yang terlalu ketat berpotensi menghambat inovasi dan penyebaran ilmu pengetahuan, sedangkan perlindungan yang terlalu lemah dapat mengurangi insentif bagi pencipta untuk menghasilkan karya baru. Oleh karena itu, sistem hukum kekayaan intelektual berupaya

menciptakan keseimbangan antara hak ekonomi pencipta, hak moral pencipta, dan kepentingan masyarakat luas.

Dalam konteks digital, perlindungan kekayaan intelektual tidak hanya mencakup hak cipta, tetapi juga meliputi berbagai rezim hukum lainnya seperti paten atas invensi berbasis teknologi, merek dalam perdagangan elektronik, desain industri untuk produk digital, rahasia dagang dalam pengembangan perangkat lunak, serta perlindungan terhadap tata letak sirkuit terpadu dan basis data elektronik. Dengan demikian, hukum kekayaan intelektual digital merupakan bidang yang bersifat multidisipliner dan mencakup berbagai aspek teknologi, ekonomi, bisnis, serta hukum (Republik Indonesia, 2014a, 2016c, 2016a).

Perkembangan teknologi baru seperti kecerdasan buatan (*artificial intelligence*), teknologi *blockchain*, komputasi awan (*cloud computing*), dan teknologi generatif semakin memperluas ruang lingkup kekayaan intelektual digital. Muncul berbagai pertanyaan hukum baru mengenai kepemilikan karya yang dihasilkan oleh sistem kecerdasan buatan, perlindungan terhadap aset digital berbasis *token*, serta mekanisme lisensi dan distribusi karya melalui platform digital. Persoalan-persoalan tersebut menunjukkan bahwa konsep kekayaan intelektual terus berkembang mengikuti perubahan teknologi dan model bisnis digital (Fadillah & Pasundan, 2024). Konsep kekayaan intelektual dalam dunia digital tidak hanya berkaitan dengan perlindungan terhadap hasil kreativitas dan inovasi, tetapi juga menyangkut upaya menciptakan ekosistem digital yang adil, kompetitif, dan berkelanjutan. Perlindungan hukum yang efektif terhadap kekayaan intelektual diharapkan mampu mendorong lahirnya inovasi baru, meningkatkan daya saing ekonomi digital, serta memberikan penghargaan yang layak kepada para pencipta, inventor, dan pelaku industri kreatif di era transformasi digital.

10.2 Hak Cipta atas Konten Digital

Hak cipta merupakan hak eksklusif yang diberikan kepada pencipta atau pemegang hak atas suatu karya untuk mengatur penggunaan, penggandaan, distribusi, pertunjukan, pengumuman, maupun pemanfaatan ekonomi dari karya tersebut. Dalam konteks digital, hak cipta memberikan perlindungan

terhadap berbagai bentuk karya yang diwujudkan dalam format elektronik atau dapat diakses melalui jaringan komputer dan internet.

Konten digital memiliki karakteristik yang berbeda dibandingkan karya konvensional. Salah satu karakteristik utama adalah kemudahan dalam melakukan reproduksi dengan kualitas yang identik dengan karya asli. Sebuah file musik, video, atau dokumen digital dapat disalin berkali-kali tanpa mengalami penurunan kualitas. Selain itu, internet memungkinkan distribusi karya secara instan kepada jutaan pengguna di berbagai negara dalam waktu yang sangat singkat. Kondisi ini menciptakan peluang ekonomi yang besar bagi pencipta, namun sekaligus meningkatkan risiko pelanggaran hak cipta.

Pelanggaran hak cipta atas konten digital dapat terjadi dalam berbagai bentuk, seperti penggandaan tanpa izin, distribusi ilegal melalui situs berbagi file, penggunaan gambar atau video tanpa mencantumkan sumber dan izin, pengunggahan ulang karya orang lain di media sosial, hingga penggunaan perangkat lunak bajakan. Dalam banyak kasus, pelanggaran terjadi karena adanya anggapan bahwa informasi yang tersedia di internet dapat digunakan secara bebas tanpa memperhatikan hak pemiliknya. Padahal, keberadaan suatu karya di ruang digital tidak menghilangkan hak hukum yang melekat pada penciptanya.

Objek perlindungan hak cipta dalam lingkungan digital sangat beragam. Karya tulis seperti artikel, blog, buku elektronik, dan jurnal ilmiah memperoleh perlindungan hukum sejak karya tersebut diwujudkan dalam bentuk nyata. Demikian pula dengan karya fotografi digital, ilustrasi, video kreatif, rekaman audio, animasi, permainan komputer, hingga perangkat lunak dan aplikasi komputer. Perlindungan tersebut berlaku tanpa memerlukan proses pendaftaran terlebih dahulu, meskipun pencatatan hak cipta dapat memberikan manfaat tambahan sebagai alat bukti apabila terjadi sengketa.

Dalam ekonomi digital modern, konten digital memiliki nilai ekonomi yang sangat tinggi. Kreator konten, pengembang perangkat lunak, desainer grafis, penulis, musisi, dan pembuat video memperoleh pendapatan dari lisensi penggunaan karya, iklan, langganan, penjualan digital, maupun kerja sama komersial lainnya. Oleh karena itu, perlindungan hak cipta menjadi instrumen penting untuk memastikan bahwa pencipta memperoleh penghargaan dan manfaat ekonomi yang layak atas hasil kreativitasnya.

Konsep hak moral dan hak ekonomi menjadi dua aspek utama dalam hak cipta atas konten digital. Hak moral berkaitan dengan hubungan pribadi antara pencipta dan karyanya, seperti hak untuk dicantumkan namanya sebagai pencipta dan hak untuk menolak perubahan terhadap karya yang dapat merusak reputasi atau integritas pencipta. Sementara itu, hak ekonomi memberikan kewenangan kepada pemegang hak cipta untuk memperoleh keuntungan finansial dari penggunaan karyanya oleh pihak lain.

Di era platform digital dan media sosial, muncul tantangan baru terkait penggunaan ulang konten oleh pengguna lain. Praktik seperti mengunggah ulang video, menggunakan musik sebagai latar belakang konten, mengutip artikel secara berlebihan, atau memanfaatkan karya visual tanpa izin sering kali menimbulkan perdebatan mengenai batas antara penggunaan yang sah dan pelanggaran hak cipta. Perkembangan teknologi juga menghadirkan mekanisme perlindungan digital seperti *Digital Rights Management* (DRM), *watermark* digital, sistem identifikasi konten otomatis, dan teknologi pelacakan distribusi karya. Teknologi tersebut membantu pemegang hak cipta dalam mengendalikan distribusi karya dan mendeteksi penggunaan yang tidak sah. Meskipun demikian, efektivitas perlindungan teknologi tetap memerlukan dukungan regulasi hukum serta kesadaran masyarakat dalam menghormati hak kekayaan intelektual.

Selain tantangan teknis, hak cipta atas konten digital juga menghadapi persoalan lintas yurisdiksi. Sebuah karya yang dibuat di satu negara dapat diakses, disalin, dan didistribusikan di negara lain hanya dalam hitungan detik. Kondisi ini menuntut adanya kerja sama internasional dan harmonisasi peraturan untuk menjamin perlindungan hak cipta secara global. Berbagai perjanjian internasional di bidang hak kekayaan intelektual berperan penting dalam menciptakan standar perlindungan yang dapat diterapkan oleh berbagai negara.

Kesadaran hukum masyarakat menjadi faktor penting dalam menjaga keberlangsungan ekosistem digital yang sehat. Pengguna internet perlu memahami bahwa setiap karya digital merupakan hasil kreativitas, waktu, tenaga, dan investasi dari penciptanya. Menghormati hak cipta tidak hanya merupakan kewajiban hukum, tetapi juga bentuk penghargaan terhadap inovasi dan kreativitas yang menjadi fondasi utama perkembangan teknologi informasi. Hak cipta atas konten digital memiliki peran strategis dalam mendorong pertumbuhan ekonomi kreatif, melindungi kepentingan

pencipta, serta menciptakan keseimbangan antara akses informasi dan perlindungan terhadap karya intelektual. Dalam era transformasi digital yang terus berkembang, pemahaman terhadap hak cipta menjadi kompetensi penting bagi setiap individu maupun organisasi yang terlibat dalam penciptaan dan pemanfaatan konten digital.

10.3 Perlindungan Merek, Domain, dan Identitas Digital

Perkembangan teknologi informasi telah mengubah cara individu, perusahaan, dan organisasi membangun keberadaan dan reputasinya di ruang digital. Jika pada masa lalu identitas suatu entitas lebih banyak diwujudkan melalui produk fisik, lokasi usaha, atau dokumen resmi, maka pada era digital identitas tersebut juga direpresentasikan melalui merek, nama domain, situs web, aplikasi, akun media sosial, dan berbagai bentuk identitas elektronik lainnya. Kondisi ini menyebabkan perlindungan hukum terhadap merek, domain, dan identitas digital menjadi bagian penting dalam hukum teknologi informasi dan hukum kekayaan intelektual (Republik Indonesia, 2016a, 2024c).

Merek memiliki fungsi utama sebagai tanda pembeda yang memungkinkan masyarakat mengenali asal barang atau jasa tertentu. Dalam lingkungan digital, fungsi tersebut menjadi semakin penting karena interaksi antara pelaku usaha dan konsumen sebagian besar berlangsung melalui platform elektronik. Konsumen sering kali mengambil keputusan berdasarkan nama merek, logo, atau identitas visual yang muncul pada situs web, aplikasi, maupun media sosial. Oleh karena itu, merek tidak hanya memiliki nilai ekonomi, tetapi juga menjadi representasi reputasi dan kepercayaan publik terhadap suatu produk atau layanan (Republik Indonesia, 2016c).

Dari perspektif hukum, pemilik merek yang telah memperoleh perlindungan hukum memiliki hak eksklusif untuk menggunakan merek tersebut dalam kegiatan perdagangan serta berhak melarang pihak lain menggunakan tanda yang memiliki persamaan pada pokoknya atau keseluruhannya untuk barang atau jasa sejenis. Perlindungan tersebut menjadi instrumen penting dalam menghadapi berbagai bentuk pelanggaran yang muncul di ruang digital, seperti pemalsuan merek, penggunaan logo tanpa izin, peniruan identitas bisnis, maupun penyalahgunaan reputasi perusahaan untuk tujuan komersial tertentu (Republik Indonesia, 2016c).

Selain merek, nama domain juga memiliki posisi strategis dalam kegiatan ekonomi digital. Nama domain merupakan alamat unik yang digunakan untuk mengidentifikasi suatu situs web di internet dan berfungsi sebagai sarana utama bagi pengguna untuk mengakses layanan digital suatu organisasi atau perusahaan. Dalam praktiknya, nama domain sering kali memiliki nilai ekonomi yang sangat tinggi karena berkaitan langsung dengan identitas bisnis dan kemudahan akses konsumen terhadap suatu layanan (Kementerian Komunikasi dan Informatika Republik Indonesia, 2013).

Hubungan antara merek dan nama domain sering kali menimbulkan persoalan hukum ketika terdapat pihak yang mendaftarkan nama domain yang identik atau menyerupai merek milik pihak lain. Praktik tersebut dikenal sebagai *cybersquatting*, yaitu tindakan memperoleh atau menggunakan nama domain dengan tujuan mengambil keuntungan dari reputasi atau popularitas merek yang telah dikenal masyarakat. Dalam beberapa kasus, pelaku mendaftarkan nama domain tertentu untuk dijual kembali kepada pemilik merek dengan harga yang tinggi atau digunakan untuk mengalihkan pengunjung ke situs lain demi memperoleh keuntungan ekonomi (ICANN, 2020; Kementerian Komunikasi dan Informatika Republik Indonesia, 2013).

Tindakan tersebut dapat menimbulkan kerugian yang tidak hanya bersifat finansial, tetapi juga merusak reputasi pemilik merek serta menyesatkan konsumen. Oleh karena itu, sistem hukum memberikan mekanisme penyelesaian sengketa nama domain baik melalui prosedur administratif maupun melalui proses peradilan apabila terdapat pelanggaran terhadap hak atas merek atau perbuatan melawan hukum. Dalam praktik bisnis modern, pendaftaran nama domain yang sesuai dengan merek perusahaan menjadi langkah preventif yang penting untuk mengurangi risiko sengketa di kemudian hari (ICANN, 2020; Republik Indonesia, 2016c).

Di samping merek dan nama domain, identitas digital juga menjadi aspek yang semakin penting dalam kehidupan masyarakat modern. Identitas digital merupakan representasi elektronik dari individu atau organisasi yang digunakan dalam berbagai aktivitas di ruang siber. Bentuk identitas tersebut dapat berupa alamat surat elektronik, nama pengguna, akun media sosial, tanda tangan elektronik, sertifikat digital, maupun berbagai atribut elektronik lainnya yang memungkinkan seseorang atau organisasi dikenali dalam sistem digital (Republik Indonesia, 2019b, 2024b).

Dalam perspektif hukum teknologi informasi, identitas digital memiliki nilai pembuktian dan pertanggungjawaban hukum yang sangat penting, terutama dalam transaksi elektronik dan komunikasi digital. Identitas digital menjadi dasar bagi proses autentikasi dan verifikasi yang menentukan apakah suatu tindakan benar-benar dilakukan oleh pihak yang berwenang. Penyalahgunaan identitas digital dapat menimbulkan konsekuensi hukum yang serius (Republik Indonesia, 2019; Republik Indonesia, 2024).

Perkembangan teknologi informasi telah memunculkan berbagai bentuk pelanggaran yang berkaitan dengan identitas digital, seperti pencurian identitas, pemalsuan akun, peniruan profil perusahaan, hingga penggunaan identitas pihak lain untuk melakukan penipuan daring. Fenomena akun palsu yang menggunakan nama dan logo perusahaan atau tokoh publik merupakan salah satu contoh yang sering ditemukan dalam praktik. Tindakan tersebut berpotensi menyesatkan masyarakat, merugikan pemilik identitas yang sah, serta menimbulkan kerugian ekonomi maupun reputasi (Republik Indonesia, 2024).

Perlindungan terhadap identitas digital tidak hanya bergantung pada instrumen hukum, tetapi juga memerlukan dukungan teknologi keamanan yang memadai. Penggunaan autentikasi multifaktor, sertifikat digital, tanda tangan elektronik, dan mekanisme verifikasi identitas menjadi bagian penting dalam menjaga keaslian identitas dalam lingkungan digital. Kombinasi antara perlindungan hukum dan penerapan teknologi keamanan menjadi pendekatan yang diperlukan untuk menghadapi kompleksitas ancaman di ruang siber (Republik Indonesia, 2019; Republik Indonesia, 2024).

Karakter internet yang bersifat global juga menimbulkan tantangan tersendiri dalam penegakan hukum. Pelanggaran terhadap merek, nama domain, dan identitas digital sering kali melibatkan pihak-pihak yang berada di negara yang berbeda sehingga menimbulkan persoalan yurisdiksi dan perbedaan sistem hukum. Sebuah nama domain dapat didaftarkan di satu negara, digunakan di negara lain, dan menimbulkan kerugian bagi perusahaan yang beroperasi secara internasional. Kondisi tersebut menunjukkan pentingnya kerja sama internasional dan harmonisasi regulasi dalam memberikan perlindungan hukum yang efektif terhadap aset digital (ICANN, 2020; Republik Indonesia, 2016).

Perkembangan teknologi seperti kecerdasan buatan, otomatisasi sistem, dan teknologi manipulasi identitas digital juga menghadirkan tantangan hukum baru yang memerlukan respons regulasi yang adaptif. Sistem hukum dituntut untuk mampu mengikuti perkembangan teknologi agar tetap relevan dalam memberikan perlindungan terhadap hak dan kepentingan para pihak yang beraktivitas di ruang digital (Republik Indonesia, 2019; Republik Indonesia, 2024).

Merek, nama domain, dan identitas digital merupakan aset yang memiliki nilai ekonomi, hukum, dan reputasi yang sangat penting dalam era transformasi digital. Perlindungan hukum terhadap ketiga elemen tersebut tidak hanya bertujuan menjaga hak pemiliknya, tetapi juga menciptakan kepastian hukum, melindungi konsumen, serta mendukung terciptanya ekosistem digital yang aman, terpercaya, dan berkelanjutan (Republik Indonesia, 2016; Republik Indonesia, 2019; Republik Indonesia, 2024).

10.4 Lisensi Digital dan Penggunaan Perangkat Lunak

Hampir seluruh sistem digital modern bergantung pada penggunaan perangkat lunak untuk menjalankan fungsi operasional maupun layanan kepada pengguna. Seiring dengan meningkatnya ketergantungan terhadap perangkat lunak, aspek hukum yang mengatur penggunaan, distribusi, dan pemanfaatannya menjadi semakin penting dalam kerangka hukum teknologi informasi (Republik Indonesia, 2014a; WIPO, 2025).

Berbeda dengan barang fisik pada umumnya, penggunaan perangkat lunak tidak selalu disertai dengan perpindahan hak kepemilikan kepada pengguna. Dalam sebagian besar transaksi perangkat lunak, pengguna sebenarnya hanya memperoleh hak untuk menggunakan perangkat lunak tersebut berdasarkan syarat dan ketentuan tertentu yang ditetapkan oleh pemegang hak cipta atau pengembang perangkat lunak. Hak penggunaan tersebut diberikan melalui suatu mekanisme hukum yang dikenal sebagai lisensi (Republik Indonesia, 2014).

Lisensi digital merupakan izin yang diberikan oleh pemegang hak kepada pihak lain untuk menggunakan suatu produk digital, termasuk perangkat lunak, dalam batasan dan kondisi tertentu. Melalui lisensi, pemegang hak cipta tetap mempertahankan kepemilikan atas karya intelektualnya, sementara pengguna memperoleh hak untuk memanfaatkan perangkat lunak

sesuai dengan ruang lingkup penggunaan yang telah disepakati. Lisensi berfungsi sebagai instrumen hukum yang mengatur hubungan antara pemilik hak dan pengguna perangkat lunak (Republik Indonesia, 2014).

Dalam praktiknya, lisensi perangkat lunak dapat mengatur berbagai aspek penggunaan, seperti jumlah perangkat yang diperbolehkan untuk menginstal perangkat lunak, jangka waktu penggunaan, hak untuk melakukan modifikasi, hak distribusi ulang, serta batasan penggunaan untuk tujuan komersial maupun nonkomersial. Pelanggaran terhadap ketentuan lisensi dapat menimbulkan konsekuensi hukum karena dianggap sebagai pelanggaran terhadap hak kekayaan intelektual pemegang hak cipta (Republik Indonesia, 2014).

Secara umum, terdapat berbagai model lisensi yang berkembang dalam industri perangkat lunak. Salah satu model yang paling umum adalah lisensi proprietari atau lisensi tertutup, yaitu lisensi yang memberikan hak penggunaan kepada pengguna tanpa memberikan akses terhadap kode sumber perangkat lunak. Dalam model ini, pengguna hanya diperbolehkan menggunakan perangkat lunak sesuai dengan ketentuan yang telah ditetapkan oleh pengembang dan tidak diperkenankan melakukan modifikasi atau distribusi ulang tanpa izin (Republik Indonesia, 2014).

Di sisi lain, perkembangan komunitas teknologi informasi melahirkan konsep perangkat lunak sumber terbuka atau *open source software*. Model ini memberikan akses kepada pengguna untuk mempelajari, memodifikasi, dan mendistribusikan kembali perangkat lunak sesuai dengan ketentuan lisensi yang berlaku. Meskipun memberikan kebebasan yang lebih luas dibandingkan lisensi proprietari, perangkat lunak sumber terbuka tetap berada dalam kerangka perlindungan hukum hak cipta. Kebebasan penggunaan yang diberikan bukan berarti perangkat lunak tersebut tidak memiliki pemilik atau berada dalam domain publik, melainkan merupakan bentuk pemberian hak penggunaan yang diatur secara hukum melalui lisensi tertentu (Open Source Initiative, 2026; Republik Indonesia, 2014a).

Kesalahpahaman mengenai konsep lisensi sering kali menjadi penyebab terjadinya pelanggaran hukum di bidang teknologi informasi. Banyak pengguna beranggapan bahwa perangkat lunak yang dapat diunduh melalui internet dapat digunakan secara bebas tanpa memperhatikan ketentuan lisensinya. Padahal, setiap perangkat lunak memiliki aturan penggunaan yang mengikat secara hukum dan harus dipatuhi oleh pengguna.

Penggunaan perangkat lunak di luar ruang lingkup lisensi dapat dikategorikan sebagai pelanggaran hak cipta dan menimbulkan tanggung jawab hukum bagi pelakunya (Republik Indonesia, 2014).

Salah satu bentuk pelanggaran yang paling sering terjadi adalah penggunaan perangkat lunak bajakan atau perangkat lunak tanpa lisensi yang sah. Praktik ini meliputi penggandaan, distribusi, instalasi, maupun penggunaan perangkat lunak tanpa izin dari pemegang hak cipta. Selain menimbulkan kerugian ekonomi bagi pengembang perangkat lunak, penggunaan perangkat lunak ilegal juga meningkatkan risiko keamanan siber karena perangkat lunak yang dimodifikasi secara tidak sah sering kali mengandung program berbahaya, celah keamanan, atau mekanisme pencurian data pengguna (Republik Indonesia, 2014; Republik Indonesia, 2024).

Dalam lingkungan organisasi dan perusahaan, penggunaan perangkat lunak tanpa lisensi juga dapat menimbulkan risiko hukum dan reputasi yang signifikan. Audit kepatuhan lisensi perangkat lunak menjadi salah satu mekanisme yang sering dilakukan untuk memastikan bahwa seluruh perangkat lunak yang digunakan telah sesuai dengan hak penggunaan yang dimiliki organisasi. Ketidakpatuhan terhadap ketentuan lisensi dapat berujung pada tuntutan ganti rugi, sanksi administratif, maupun kewajiban pembayaran kompensasi kepada pemegang hak (Xu et al., 2022).

Perkembangan teknologi komputasi awan dan layanan berbasis langganan turut mengubah model lisensi perangkat lunak tradisional. Jika sebelumnya perangkat lunak umumnya diperoleh melalui pembelian satu kali untuk penggunaan permanen, saat ini banyak perangkat lunak yang menggunakan model berlangganan dengan pembayaran berkala. Dalam model tersebut, pengguna memperoleh hak akses selama periode tertentu sesuai dengan perjanjian layanan yang berlaku. Perubahan ini menunjukkan bahwa lisensi digital terus berkembang mengikuti perubahan model bisnis dalam industri teknologi informasi (Republik Indonesia, 2019).

Selain mengatur hak dan kewajiban pengguna, lisensi digital juga memiliki fungsi penting dalam memberikan kepastian hukum bagi pengembang perangkat lunak. Melalui lisensi, pengembang dapat menentukan batas tanggung jawab, perlindungan terhadap kekayaan intelektual, serta mekanisme penyelesaian sengketa apabila terjadi pelanggaran atau

penggunaan yang tidak sesuai dengan ketentuan yang telah ditetapkan (Republik Indonesia, 2014).

Karakter teknologi informasi yang bersifat global juga menimbulkan tantangan tersendiri dalam penegakan hukum terkait lisensi perangkat lunak. Sebuah perangkat lunak dapat dikembangkan di satu negara, didistribusikan melalui internet, dan digunakan oleh pengguna di berbagai yurisdiksi yang memiliki sistem hukum berbeda. Perlindungan hukum terhadap perangkat lunak memerlukan kerja sama internasional dan harmonisasi regulasi agar hak pemegang lisensi maupun pengguna dapat terlindungi secara efektif (WIPO, 2025).

Pemahaman terhadap hak dan kewajiban yang timbul dari suatu lisensi tidak hanya penting bagi pengembang perangkat lunak, tetapi juga bagi individu, organisasi, dan institusi yang memanfaatkan teknologi informasi dalam aktivitas sehari-hari. Kepatuhan terhadap ketentuan lisensi menjadi bagian penting dalam menciptakan ekosistem digital yang sehat, aman, dan menghormati hak kekayaan intelektual (Republik Indonesia, 2014; Open Source Initiative, n.d.).

10.5 Pelanggaran Kekayaan Intelektual di Internet

Perkembangan internet telah memberikan kemudahan yang luar biasa dalam menciptakan, menyimpan, menyebarluaskan, dan mengakses informasi. Berbagai bentuk karya intelektual seperti tulisan, musik, film, perangkat lunak, fotografi, desain grafis, karya ilmiah, hingga konten media sosial dapat didistribusikan secara cepat kepada pengguna di seluruh dunia tanpa batasan geografis. Meskipun memberikan manfaat besar bagi perkembangan ekonomi digital dan industri kreatif, kemudahan tersebut juga meningkatkan risiko terjadinya pelanggaran terhadap hak kekayaan intelektual (Republik Indonesia, 2014; WIPO, 2025).

Karakteristik utama internet yang memungkinkan reproduksi dan distribusi informasi dengan biaya rendah serta kecepatan tinggi menjadikan pelanggaran kekayaan intelektual lebih mudah dilakukan dibandingkan pada era media konvensional. Sebuah karya digital dapat disalin, dimodifikasi, dan disebarluaskan kepada jutaan pengguna hanya dalam hitungan detik tanpa mengurangi kualitas karya asli. Kondisi ini menciptakan tantangan

baru bagi sistem hukum dalam melindungi hak para pencipta dan pemegang hak kekayaan intelektual (Republik Indonesia, 2014; WIPO, 2025).

Gambar 10.2: Bentuk Pelanggaran Kekayaan Intelektual di Internet

Salah satu bentuk pelanggaran yang paling sering terjadi adalah pelanggaran hak cipta melalui penggandaan dan distribusi karya tanpa izin dari pemegang hak. Praktik ini dapat berupa penyebaran film, musik, buku elektronik, perangkat lunak, maupun karya visual melalui situs berbagi file, media sosial, atau platform digital lainnya. Pengunggahan ulang karya milik orang lain tanpa izin, penggunaan foto dan video tanpa persetujuan pemiliknya, serta penyalinan artikel secara keseluruhan tanpa mencantumkan sumber juga merupakan bentuk pelanggaran hak cipta yang banyak ditemukan dalam lingkungan digital (Republik Indonesia, 2014).

Selain hak cipta, pelanggaran terhadap merek juga semakin sering terjadi di internet. Pelaku dapat menggunakan nama, logo, atau identitas visual yang menyerupai merek terkenal untuk menarik perhatian konsumen atau memperoleh keuntungan ekonomi secara tidak sah. Praktik tersebut sering ditemukan pada situs perdagangan elektronik, media sosial, maupun layanan digital yang memanfaatkan reputasi suatu merek untuk meningkatkan kepercayaan pengguna. Tindakan tersebut tidak hanya merugikan pemilik

merek, tetapi juga berpotensi menyesatkan konsumen mengenai asal usul barang atau jasa yang ditawarkan (Republik Indonesia, 2016c).

Internet juga memunculkan berbagai bentuk pelanggaran terkait nama domain dan identitas digital. Pendaftaran nama domain yang menyerupai merek terkenal, penggunaan akun palsu yang mengatasnamakan perusahaan atau tokoh publik, serta penyalahgunaan identitas digital untuk kepentingan komersial merupakan contoh pelanggaran yang semakin meningkat seiring dengan berkembangnya aktivitas ekonomi digital. Dalam banyak kasus, tindakan tersebut dilakukan untuk memperoleh keuntungan finansial, melakukan penipuan, atau memanfaatkan reputasi pihak lain (Republik Indonesia, 2016c, 2024b).

Pelanggaran kekayaan intelektual di internet juga dapat terjadi dalam bentuk penggunaan perangkat lunak tanpa lisensi atau distribusi perangkat lunak bajakan. Perangkat lunak yang disebarluaskan tanpa izin dari pemegang hak cipta tidak hanya merugikan pengembang secara ekonomi, tetapi juga dapat meningkatkan risiko keamanan siber bagi pengguna. Perangkat lunak ilegal sering kali dimodifikasi dengan menyisipkan program berbahaya yang dapat digunakan untuk mencuri data atau merusak sistem komputer pengguna (Republik Indonesia, 2014; Republik Indonesia, 2024).

Kemajuan teknologi digital juga menghadirkan bentuk pelanggaran baru yang sebelumnya tidak dikenal dalam lingkungan konvensional. Teknologi manipulasi gambar, video, dan suara memungkinkan seseorang menciptakan konten yang menyerupai karya atau identitas pihak lain tanpa persetujuan pemiliknya. Selain itu, perkembangan teknologi kecerdasan buatan memungkinkan pembuatan dan reproduksi konten dalam jumlah besar yang menimbulkan pertanyaan baru mengenai batas penggunaan karya yang dilindungi oleh hak kekayaan intelektual (Republik Indonesia, 2014; Republik Indonesia, 2024; WIPO, 2025).

Dari perspektif hukum, pelanggaran kekayaan intelektual di internet tetap merupakan pelanggaran hukum meskipun dilakukan dalam ruang digital. Prinsip dasar perlindungan hak kekayaan intelektual tetap berlaku terhadap karya yang dipublikasikan secara daring sebagaimana perlindungan yang diberikan terhadap karya dalam bentuk fisik. Fakta bahwa suatu karya tersedia di internet tidak berarti karya tersebut dapat digunakan, disalin, dimodifikasi, atau didistribusikan secara bebas tanpa izin dari pemegang hak (Republik Indonesia, 2014).

Penegakan hukum terhadap pelanggaran kekayaan intelektual di internet menghadapi berbagai tantangan. Salah satu tantangan utama adalah sifat internet yang bersifat lintas negara sehingga pelaku, korban, dan infrastruktur digital yang digunakan dapat berada pada yurisdiksi yang berbeda. Selain itu, anonimitas pengguna internet serta kemudahan dalam membuat akun atau situs baru menyebabkan proses identifikasi pelaku pelanggaran menjadi lebih kompleks dibandingkan pelanggaran konvensional (Republik Indonesia, 2019; WIPO, 2025).

Untuk mengatasi permasalahan tersebut, berbagai mekanisme perlindungan telah dikembangkan, baik melalui instrumen hukum maupun teknologi. Pemegang hak dapat menggunakan sistem pelaporan pelanggaran pada platform digital, teknologi pengenalan konten otomatis, tanda air digital (*digital watermark*), maupun sistem manajemen hak digital (*Digital Rights Management* atau DRM) untuk mengendalikan penggunaan dan distribusi karya mereka. Di sisi lain, penyedia layanan digital juga memiliki tanggung jawab tertentu dalam menangani konten yang melanggar hak kekayaan intelektual sesuai dengan ketentuan hukum yang berlaku (Republik Indonesia, 2014; Republik Indonesia, 2019; WIPO, 2025).

10.6 Strategi Perlindungan Karya Digital

Perlindungan karya digital memerlukan strategi yang tidak hanya bertumpu pada instrumen hukum, tetapi juga melibatkan pendekatan teknologi, manajerial, kontraktual, dan edukatif. Hal ini penting karena karya digital memiliki karakteristik mudah disalin, dimodifikasi, disebarluaskan, dan digunakan kembali dalam berbagai platform digital. Oleh karena itu, pencipta, pemegang hak, organisasi, maupun pengguna teknologi perlu memahami langkah-langkah perlindungan yang dapat dilakukan agar hak kekayaan intelektual tetap terjaga dalam ekosistem digital (Republik Indonesia, 2014; WIPO, 2025).

Strategi pertama adalah memastikan bahwa karya digital memiliki dokumentasi kepemilikan yang jelas. Meskipun hak cipta timbul secara otomatis sejak suatu ciptaan diwujudkan dalam bentuk nyata, pencatatan hak cipta tetap penting sebagai alat bukti apabila terjadi sengketa di kemudian hari. Pencipta dapat menyimpan dokumen pendukung seperti file asli, tanggal pembuatan, riwayat revisi, bukti publikasi, kontrak kerja sama, serta

bukti komunikasi yang menunjukkan proses penciptaan karya. Dalam konteks Indonesia, pencatatan hak cipta melalui Direktorat Jenderal Kekayaan Intelektual dapat menjadi langkah administratif yang memperkuat posisi hukum pencipta atau pemegang hak (DJKI, 2026; Republik Indonesia, 2014a).

Gambar 10.3: Strategi Perlindungan Karya Digital

Strategi kedua adalah menggunakan lisensi yang jelas dalam setiap distribusi karya digital. Lisensi berfungsi untuk menjelaskan batas penggunaan karya, termasuk apakah karya dapat digandakan, dimodifikasi, digunakan untuk kepentingan komersial, atau didistribusikan kembali oleh pihak lain. Untuk karya seperti tulisan, gambar, video, atau materi pembelajaran, pencipta dapat menggunakan model lisensi tertentu seperti *Creative Commons* sesuai dengan kebutuhan. Sementara itu, untuk perangkat lunak, pengembang perlu menentukan apakah karya akan didistribusikan dengan lisensi tertutup, lisensi sumber terbuka, atau model lisensi lain yang sesuai dengan tujuan penggunaan dan perlindungan hukum (Creative Commons, 2024; Republik Indonesia, 2014a).

Strategi ketiga adalah menerapkan perlindungan teknologi terhadap karya digital. Beberapa mekanisme yang dapat digunakan antara lain tanda air digital (*digital watermark*), metadata kepemilikan, sistem manajemen hak digital (*Digital Rights Management* atau DRM), enkripsi, pembatasan akses, serta sistem pelacakan penggunaan konten. Teknologi tersebut dapat

membantu pencipta atau pemegang hak dalam mengidentifikasi karya, mengontrol distribusi, dan mendeteksi penggunaan yang tidak sah. Namun, perlindungan teknologi tidak dapat berdiri sendiri karena tetap memerlukan dukungan hukum, kebijakan internal, serta kesadaran pengguna untuk menghormati hak kekayaan intelektual (Republik Indonesia, 2014; WIPO, 2025).

Strategi keempat adalah melakukan pengawasan dan penanganan pelanggaran secara aktif. Pemegang hak dapat melakukan pemantauan berkala terhadap penggunaan karya di internet, media sosial, situs berbagi file, dan platform perdagangan elektronik. Apabila ditemukan penggunaan tanpa izin, langkah awal yang dapat dilakukan adalah mengumpulkan bukti digital, seperti tangkapan layar, alamat tautan, waktu akses, identitas akun, dan salinan konten yang dilanggar. Setelah itu, pemegang hak dapat mengajukan laporan kepada penyedia platform, mengirimkan peringatan resmi, atau menempuh mekanisme hukum apabila pelanggaran menimbulkan kerugian yang signifikan (Republik Indonesia, 2014; Republik Indonesia, 2024).

Strategi kelima adalah memperkuat perjanjian dan kebijakan internal dalam organisasi. Organisasi yang menghasilkan karya digital, seperti perusahaan teknologi, lembaga pendidikan, media, atau komunitas kreatif, perlu memiliki aturan yang jelas mengenai kepemilikan karya, penggunaan aset digital, hak dan kewajiban pegawai, penggunaan perangkat lunak berlisensi, serta prosedur publikasi konten. Perjanjian kerja, perjanjian lisensi, perjanjian kerja sama, dan ketentuan penggunaan platform perlu disusun secara jelas agar tidak menimbulkan sengketa mengenai siapa pemilik hak atas suatu karya digital (Republik Indonesia, 2014; Republik Indonesia, 2019).

Strategi keenam adalah menjaga keamanan sistem digital yang digunakan untuk menyimpan dan mendistribusikan karya. Karya digital yang disimpan dalam sistem elektronik perlu dilindungi dari pencurian data, akses tanpa izin, pengubahan file, dan distribusi ilegal. Upaya perlindungan dapat dilakukan melalui penggunaan autentikasi multifaktor, pengaturan hak akses, pencadangan data, audit keamanan, serta penggunaan sistem elektronik yang andal dan aman. Dalam konteks penyelenggaraan sistem elektronik, aspek keamanan, keandalan, dan tanggung jawab penyelenggara

sistem menjadi bagian penting dari perlindungan karya digital (Republik Indonesia, 2019; Republik Indonesia, 2024).

Strategi ketujuh adalah meningkatkan literasi hukum dan etika digital. Banyak pelanggaran kekayaan intelektual terjadi bukan hanya karena niat mengambil keuntungan, tetapi juga karena rendahnya pemahaman bahwa karya yang tersedia di internet tetap dilindungi oleh hukum. Pengguna internet perlu memahami bahwa mengunduh, menyalin, mengunggah ulang, memodifikasi, atau menggunakan karya orang lain untuk kepentingan komersial tanpa izin dapat menimbulkan konsekuensi hukum. Edukasi mengenai hak cipta, lisensi digital, atribusi, penggunaan wajar, dan etika berbagi konten menjadi bagian penting dalam membangun budaya digital yang menghormati karya intelektual (Republik Indonesia, 2014; WIPO, 2025).

Strategi perlindungan karya digital pada akhirnya harus dilakukan secara terpadu. Pencatatan hak cipta memberikan kekuatan pembuktian, lisensi memberikan kejelasan penggunaan, teknologi membantu pengendalian distribusi, keamanan sistem mencegah penyalahgunaan, dan edukasi membangun kesadaran pengguna. Dengan penerapan strategi tersebut, perlindungan karya digital tidak hanya menjadi tanggung jawab pencipta atau pemegang hak, tetapi juga menjadi bagian dari upaya bersama untuk menciptakan ekosistem digital yang adil, aman, produktif, dan berkelanjutan.

Bab 11
Hukum E-Commerce dan Transaksi Elektronik

11.1 Konsep E-Commerce dalam Perspektif Hukum

Electronic Commerce (*e-commerce*) atau Perdagangan melalui Sistem Elektronik, selanjutnya disebut PMSE, dalam hukum didefinisikan melalui Pasal 1 angka 24 Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan sebagaimana telah diubah dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang. Ketentuan tersebut menyebutkan bahwa "Perdagangan melalui Sistem Elektronik adalah Perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik" (Republik Indonesia, 2014b). Fokus Undang-Undang ini meliputi aspek perdagangan yang menjelaskan hubungan bisnis antara pelaku usaha, konsumen, dan pemerintah, serta definisi dan kewenangan pemerintah dalam mengatur penyelenggaraan PMSE.

Landasan hukum agar transaksi *e-commerce* yang dilakukan secara elektronik memiliki dasar hukum yang sama dengan transaksi konvensional diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya disebut UU ITE. Definisi Transaksi Elektronik diatur dalam Pasal 1 angka 2 UU ITE, yaitu "Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya" (Republik Indonesia, 2008).

Secara sederhana, pemetaan pengaturan dapat dilihat sebagai berikut.

Tabel 11.1: Pemetaan Pengaturan E-Commerce dalam UU Perdagangan dan UU ITE

Aspek	**UU Perdagangan**	**UU ITE**
Ruang lingkup	Pada intinya mengatur kegiatan perdagangan barang dan/atau jasa, termasuk PMSE.	Pada pokoknya mengatur bahwa pemesanan, persetujuan/kontrak, dan pembayaran yang dilakukan secara elektronik juga sah berdasarkan hukum. Ruang lingkup UU ITE tidak terbatas pada *e-commerce*, melainkan mencakup seluruh penyelenggaraan transaksi elektronik, termasuk informasi elektronik, dokumen elektronik, sistem elektronik, tanda tangan elektronik, serta pemanfaatan teknologi informasi secara umum.
Mengatur	Hak dan kewajiban pelaku usaha dan konsumen, termasuk informasi produk dalam *marketplace*.	Keabsahan kontrak elektronik.
Tujuan	Menjamin perdagangan elektronik berlangsung secara transparan, adil, dan melindungi konsumen.	Menjamin transaksi elektronik memiliki kekuatan hukum dan dapat menjadi alat bukti.

Hubungan konseptual dapat digambarkan sebagai berikut.

Gambar 11.1: Hubungan Konseptual E-Commerce sebagai Bagian dari Transaksi Elektronik

Contoh kegiatan:

Tabel 11.2; Contoh Perbedaan E-Commerce dan Transaksi Elektronik

Kegiatan	***E-Commerce***	**Transaksi Elektronik**	**Keterangan**
Membeli barang di *marketplace*/jual beli sepatu di *marketplace*, atau memesan makanan melalui aplikasi.	Ya	Ya	Ada transaksi jual beli.
Transfer uang melalui *mobile banking* sebagai transaksi elektronik, tanda tangan elektronik sebagai kontrak elektronik, mengirimkan *invoice* melalui *e-mail* sebagai dokumen elektronik, dan membayar pajak secara *online* sebagai pelayanan publik *e-government*.	Tidak	Ya	Tidak ada kegiatan jual beli barang/jasa.

Kegiatan tersebut merupakan transaksi elektronik. Artinya, definisi yang termuat dalam regulasi memberikan dasar hukum bagi pelaksanaan transaksi perdagangan secara digital di Indonesia.

Selain diatur dalam Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan sebagaimana telah diubah dengan Undang-Undang Nomor 6 Tahun 2023 dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024, penyelenggaraan *e-commerce* juga didukung oleh peraturan pelaksana. Peraturan pelaksana berfungsi untuk memberikan pengaturan yang lebih teknis dan operasional sehingga ketentuan yang diatur dalam Undang-Undang dapat diterapkan secara efektif.

Salah satu peraturan pelaksana yang utama adalah Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE). Peraturan ini merupakan pelaksanaan Pasal 66 Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan yang secara khusus mengatur penyelenggaraan perdagangan melalui sistem elektronik. Pasal 2 PP Nomor 80 Tahun 2019 mengatur berbagai aspek PMSE, antara lain pihak yang melakukan PMSE; syarat dalam PMSE; penyelenggara PMSE; kewajiban pelaku usaha; bukti transaksi PMSE; iklan elektronik; penawaran, penerimaan, dan konfirmasi elektronik; kontrak elektronik; perlindungan data pribadi; pembayaran dalam PMSE; pengiriman barang dan jasa dalam

PMSE; penukaran barang atau jasa dan pembatalan pembelian dalam PMSE; penyelesaian sengketa dalam PMSE; serta pembinaan dan pengawasan oleh pemerintah. Dengan demikian, PP Nomor 80 Tahun 2019 menjadi landasan operasional dalam penyelenggaraan *e-commerce* di Indonesia (Republik Indonesia, 2019a).

Sementara itu, UU ITE beserta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, selanjutnya disebut PP PSTE, mengatur aspek hukum dan teknis penyelenggaraan transaksi elektronik secara lebih luas. Pengaturannya meliputi keabsahan informasi dan dokumen elektronik, kontrak dan tanda tangan elektronik, penyelenggaraan sistem elektronik, keamanan sistem, penggunaan sertifikat elektronik, hak dan kewajiban para pihak, serta tanggung jawab Penyelenggara Sistem Elektronik, selanjutnya disebut PSE (Republik Indonesia, 2019b). Keempat regulasi tersebut saling melengkapi dalam membangun sistem hukum *e-commerce*, termasuk transaksi elektronik di Indonesia.

11.2 Para Pihak dalam Transaksi E-Commerce

Pada perdagangan konvensional yang diatur dalam KUHPerdata, hubungan hukum perjanjian jual beli hanya melibatkan pihak penjual dan pembeli. Artinya, dalam perspektif hukum perdata, penjual dan pembeli merupakan subjek hukum yang bertindak sebagai para pihak dalam perjanjian jual beli. Dalam transaksi *e-commerce*, kedudukan hukum penjual dan pembeli pada dasarnya sama dengan transaksi konvensional di dunia nyata. Transaksi tersebut dilakukan oleh para pihak terkait yang tidak bertemu secara langsung, sedangkan media pembentukan perjanjiannya dilakukan melalui sistem elektronik. Dengan demikian, perbedaannya terletak pada transaksi *e-commerce* yang melibatkan pihak-pihak yang lebih kompleks.

Dalam transaksi *e-commerce*, pihak-pihak yang terkait antara lain (Y. S. Wulandari, 2018):

1. Penjual atau *merchant* sebagai pelaku usaha;
2. Pembeli atau konsumen;
3. Bank sebagai pihak penyalur dana dari pembeli atau konsumen kepada penjual atau pelaku usaha/*merchant*;
4. *Provider* sebagai penyedia jasa layanan akses internet.

Selain itu, pihak utama lainnya adalah Penyelenggara Perdagangan Melalui Sistem Elektronik (*marketplace*) sebagai pihak yang menyediakan sarana komunikasi elektronik yang mempertemukan penjual dengan pembeli dalam melakukan transaksi, seperti *marketplace* Tokopedia, Shopee, Lazada, atau Bukalapak. Pada praktiknya, penyelenggara PMSE sekaligus merupakan Penyelenggara Sistem Elektronik (PSE) karena mengoperasikan aplikasi atau situs web yang digunakan dalam transaksi. PSE bertanggung jawab menjaga keamanan sistem, kerahasiaan data, ketersediaan layanan, serta keutuhan informasi elektronik sesuai dengan ketentuan peraturan perundang-undangan. Pihak pendukung lainnya adalah penyedia jasa logistik atau pengiriman yang berperan sebagai sarana agar barang sampai kepada pembeli setelah pembayaran berhasil dilakukan.

Sebagaimana dijelaskan dalam Pasal 4 PP Nomor 80 Tahun 2019 tentang PMSE, pihak yang melakukan PMSE dapat terdiri atas pelaku usaha, konsumen, pribadi, dan instansi penyelenggara negara sesuai dengan ketentuan peraturan perundang-undangan yang selanjutnya disebut para pihak (Republik Indonesia, 2019a). Selanjutnya, dijelaskan bahwa PMSE merupakan hubungan hukum privat yang dapat dilakukan antara pelaku usaha dengan pelaku usaha, pelaku usaha dengan konsumen, pribadi dengan pribadi, serta instansi penyelenggara negara dengan pelaku usaha sesuai dengan ketentuan peraturan perundang-undangan. Sementara itu, PP PSTE membagi PSE ke dalam lingkup publik dan privat. Secara umum, *e-commerce* merupakan PSE lingkup privat. Pasal 1 angka 6 PP PSTE menyebutkan bahwa PSE lingkup privat adalah penyelenggaraan sistem elektronik oleh orang, badan usaha, dan masyarakat (Republik Indonesia, 2019b).

Oleh karena itu, hubungan hukum *e-commerce* juga melibatkan hubungan hukum dengan penyelenggara *platform* atau *marketplace*, penyedia jasa pembayaran, penyedia jasa logistik, penyelenggara sistem elektronik, serta pihak pendukung lainnya. Masing-masing pihak memiliki hak, kewajiban, dan tanggung jawab yang berbeda sesuai dengan fungsi dan perjanjian yang mengikatnya. Dengan demikian, dalam satu transaksi *e-commerce* dapat terbentuk beberapa hubungan hukum secara bersamaan.

11.3 Keabsahan Perjanjian Elektronik

Perihal keabsahan perjanjian diatur dalam ketentuan umum utama hukum perdata mengenai syarat sah perjanjian. Pasal 1320 KUHPerdata menegaskan bahwa perjanjian baru sah dan mengikat bagi para pihak apabila memenuhi empat syarat sah perjanjian, yaitu (Subekti, 2008):

1. Sepakat mereka yang mengikatkan dirinya.

   Kata sepakat berarti para pihak yang mengikatkan diri, yakni para pihak yang mengadakan perjanjian, harus saling setuju dan seia sekata dalam hal-hal pokok dari perjanjian yang akan diadakan tersebut (Arief, 2016). Selanjutnya, Pasal 1321 KUHPerdata menegaskan bahwa tiada sepakat yang sah apabila sepakat itu mengandung kekhilafan, diperoleh dengan paksaan, atau diperoleh melalui penipuan.

2. Kecakapan untuk membuat suatu perikatan.

   Pasal 1329 KUHPerdata menerangkan bahwa setiap orang adalah cakap untuk membuat perikatan-perikatan, kecuali ia oleh undang-undang dinyatakan tidak cakap. Orang yang dinyatakan tidak cakap diatur dalam Pasal 1330 KUHPerdata, di antaranya: a. orang-orang yang belum dewasa. Pasal 330 KUHPerdata menerangkan bahwa belum dewasa adalah mereka yang belum genap berusia 21 tahun dan/atau belum menikah. Artinya, seseorang yang sudah menikah meskipun usianya di bawah 21 tahun dianggap telah dewasa. Undang-Undang Perkawinan Nomor 16 Tahun 2019 mengatur batas usia perkawinan bagi pria dan wanita, yaitu 19 tahun. Sementara itu, Undang-Undang Nomor 30 Tahun 2004 tentang Jabatan Notaris menggunakan ukuran dewasa 18 tahun atau telah menikah. Dari beberapa peraturan tersebut, dalam hukum dikenal asas *lex specialis derogat legi generali*, yaitu aturan yang khusus mengesampingkan aturan yang umum. Oleh karena itu, dalam hal perbuatan hukum berupa pembuatan perjanjian yang dilakukan di hadapan pejabat notaris, ukuran yang lebih khusus merujuk pada Undang-Undang Jabatan Notaris; b. mereka yang ditaruh di bawah pengampuan. Pasal 433 KUHPerdata menjelaskan bahwa setiap orang dewasa yang selalu berada dalam keadaan dungu, sakit otak, atau mata gelap harus ditaruh di bawah pengampuan, meskipun ia kadang-kadang cakap mempergunakan pikirannya. Selain itu, seorang dewasa juga dapat ditaruh di bawah pengampuan karena keborosannya; c. disebutkan juga orang-orang perempuan, namun hal ini menjadi tidak berlaku sejak

berlakunya Undang-Undang Perkawinan Nomor 1 Tahun 1974 Pasal 31 jo. Undang-Undang Nomor 16 Tahun 2019 tentang Perubahan atas Undang-Undang Perkawinan, yang menerangkan bahwa kedudukan suami dan istri seimbang dalam melakukan perbuatan hukum; d. dalam hal lain yang ditentukan oleh undang-undang, seseorang dapat dinyatakan tidak diperbolehkan membuat perjanjian tertentu.

Meskipun KUHPerdata tidak secara langsung mengatur mengenai siapa yang cakap, penjelasan mengenai orang yang dinyatakan tidak cakap tersebut dapat digunakan untuk mengetahui orang yang dianggap cakap, yaitu telah berusia paling sedikit 18 tahun atau telah menikah, sehat jasmani dan rohani serta tidak berada di bawah pengampuan, dan tidak dilarang oleh undang-undang untuk membuat perjanjian.

3. Suatu hal tertentu.

   Syarat ini diatur dalam Pasal 1332 KUHPerdata yang menjelaskan bahwa hanya barang-barang yang dapat diperdagangkan saja yang dapat menjadi pokok suatu perjanjian. Suatu hal tertentu juga berarti hanya barang yang terbuka dalam lalu lintas perdagangan, termasuk harta warisan yang sudah sah dibagi dan menjadi milik ahli warisnya, yang dapat dijadikan objek perjanjian. Syarat suatu hal tertentu merujuk pada objek perjanjian. Objek perjanjian harus merupakan sesuatu yang dapat ditentukan secara jelas, termasuk spesifikasi barangnya secara rinci, dapat diperdagangkan, mungkin dilakukan, dan dapat dinilai dengan uang (Budiono, 2014).

4. Suatu sebab yang halal.

   Pasal 1337 KUHPerdata menjelaskan bahwa suatu sebab adalah terlarang apabila bertentangan dengan undang-undang, kesusilaan, dan ketertiban umum. Sebab dari perjanjian merupakan isi perjanjian itu sendiri atau tujuan para pihak ketika mengadakan perjanjian, yaitu mempunyai dasar yang sah, patut, atau pantas (Ilyas, 2012). Dengan demikian, dapat diketahui bahwa isi dan tujuan perjanjian yang dibuat oleh para pihak tidak boleh melanggar undang-undang, kesusilaan, dan ketertiban umum.

Keempat syarat perjanjian tersebut berlaku secara kumulatif, artinya harus terpenuhi seluruhnya. Syarat pertama dan kedua disebut syarat subjektif karena berkaitan dengan subjek perjanjian. Akibat tidak terpenuhinya syarat

pertama dan kedua sebagai syarat subjektif adalah suatu perjanjian dapat dibatalkan. Sementara itu, syarat ketiga dan keempat disebut syarat objektif karena berkaitan dengan objek perjanjian. Akibat tidak terpenuhinya syarat ketiga dan keempat sebagai syarat objektif adalah suatu perjanjian batal demi hukum.

Kontrak elektronik (*e-contract*) merupakan salah satu bentuk perjanjian tidak bernama (*innominaat*), yaitu perjanjian yang tidak diatur secara khusus dalam Kitab Undang-Undang Hukum Perdata (KUHPerdata), tetapi berkembang dalam praktik masyarakat sebagai konsekuensi dari kemajuan teknologi, perkembangan zaman, dan kebutuhan dunia usaha. Meskipun tidak memiliki pengaturan khusus dalam KUHPerdata, keabsahan kontrak elektronik secara normatif tetap harus memenuhi syarat sah perjanjian sebagaimana diatur dalam Pasal 1320 KUHPerdata.

Pasal 1338 KUHPerdata menegaskan bahwa setiap perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi para pihak yang membuatnya. Ketentuan tersebut menunjukkan bahwa perjanjian yang telah memenuhi syarat sah sebagaimana diatur dalam Pasal 1320 KUHPerdata mempunyai kekuatan mengikat sehingga para pihak wajib melaksanakan seluruh hak dan kewajiban yang telah disepakati serta tidak diperkenankan mengingkari isi perjanjian. Dengan demikian, kontrak elektronik sebagaimana kontrak konvensional juga memiliki kekuatan hukum layaknya undang-undang bagi para pihak yang membuatnya (Suwardi, 2015).

Syarat sah perjanjian elektronik juga telah diatur dalam Pasal 46 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Ketentuan ini selaras dengan Pasal 1320 KUHPerdata tentang syarat sah perjanjian. Kontrak elektronik dianggap sah apabila (Republik Indonesia, 2019b):

a. Terdapat kesepakatan para pihak;
b. Dilakukan oleh subjek hukum yang cakap atau yang berwenang mewakili sesuai dengan ketentuan peraturan perundang-undangan;
c. Terdapat hal tertentu; dan
d. Objek transaksi tidak boleh bertentangan dengan peraturan perundang-undangan, kesusilaan, dan ketertiban umum.

Kemudian, kontrak elektronik juga harus memuat hal-hal yang telah diatur dalam Pasal 47 ayat (3) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang

Penyelenggaraan Sistem dan Transaksi Elektronik, dengan paling sedikit memuat (Republik Indonesia, 2019b):

a. Data identitas para pihak;
b. Objek dan spesifikasi;
c. Persyaratan Transaksi Elektronik;
d. Harga dan biaya;
e. Prosedur dalam hal terdapat pembatalan oleh para pihak;
f. Ketentuan yang memberikan hak kepada pihak yang dirugikan untuk dapat mengembalikan barang dan/atau meminta penggantian produk jika terdapat cacat tersembunyi; dan
g. Pilihan hukum penyelesaian Transaksi Elektronik.

11.4 Sistem Pembayaran dan Keamanan Transaksi Digital

Mekanisme pembayaran dalam perkembangan digital merupakan bagian yang tidak dapat dipisahkan dari transaksi elektronik yang menjadi sarana penyelesaian kewajiban pembayaran. Keberadaan sistem pembayaran yang cepat, aman, dan efisien mendorong meningkatnya kepercayaan masyarakat dalam melakukan transaksi digital.

Pasal 60–61 PP PMSE pada pokoknya mengatur bahwa dalam Perdagangan Melalui Sistem Elektronik (PMSE), pembayaran dapat dilakukan melalui sistem elektronik dengan menggunakan mata uang sesuai dengan ketentuan peraturan perundang-undangan. Mekanisme pembayaran dapat memanfaatkan sistem perbankan atau sistem pembayaran elektronik lainnya yang telah memperoleh izin dari instansi berwenang. Selain itu, Penyelenggara Perdagangan Melalui Sistem Elektronik (PPMSE), baik dalam negeri maupun luar negeri, dapat bekerja sama dengan penyelenggara jasa sistem pembayaran, dengan kewajiban melaporkan kerja sama tersebut kepada Menteri. Untuk menjamin keamanan transaksi, penyelenggara jasa sistem pembayaran wajib memenuhi standar keamanan sistem elektronik yang ditetapkan oleh otoritas yang berwenang, yaitu Badan Siber dan Sandi Negara (BSSN), Bank Indonesia, dan/atau Otoritas Jasa Keuangan (OJK) (Republik Indonesia, 2019a).

Berdasarkan cara pelaksanaannya, sistem pembayaran dapat dibedakan menjadi pembayaran tunai (*cash payment*) dan pembayaran nontunai (*non-cash payment*). Pembayaran tunai dilakukan menggunakan uang kartal,

sedangkan pembayaran nontunai dilakukan melalui instrumen perbankan atau sistem pembayaran elektronik tanpa menggunakan uang tunai secara fisik. Dalam transaksi *e-commerce*, kedua metode pembayaran tersebut dapat digunakan. Pembayaran tunai umumnya diterapkan melalui metode *Cash on Delivery* (COD), yaitu mekanisme pembayaran yang dilakukan oleh pembeli pada saat barang diterima dari kurir atau penyedia jasa logistik. Meskipun proses pemesanan dilakukan secara elektronik, pembayaran harga barang dapat dilakukan secara tunai saat penyerahan barang. Namun, dalam praktiknya, tidak semua *marketplace* membuka kesempatan pembayaran dengan metode COD.

Sementara itu, pembayaran nontunai merupakan metode yang paling umum digunakan dalam *e-commerce*. Pembayaran ini dilakukan secara elektronik melalui berbagai instrumen, seperti transfer bank, *virtual account*, kartu debit, kartu kredit, uang elektronik (*e-money*), dompet elektronik (*e-wallet*), *Quick Response Code Indonesian Standard* (QRIS), maupun layanan *payment gateway*. Pada metode ini, dana dikirim secara elektronik dari pembeli kepada penjual atau melalui penyedia jasa pembayaran sesuai dengan mekanisme yang berlaku pada *platform e-commerce*.

Sebagaimana amanat PP PSTE yang mengatur keamanan sistem elektronik, Pasal 25 dan Pasal 26 pada pokoknya menerangkan bahwa Penyelenggara Sistem Elektronik wajib menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan format dan masa retensi yang ditetapkan berdasarkan ketentuan peraturan perundang-undangan. Selain itu, Penyelenggara Sistem Elektronik wajib menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu Informasi Elektronik dan/atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan (Republik Indonesia, 2019b).

11.5 Tanggung Jawab Marketplace dan Penjual Online

Marketplace merupakan *platform* yang bertindak sebagai perantara yang mempertemukan banyak penjual (*merchant*) dengan banyak pembeli. Penyelenggara *marketplace* pada umumnya tidak menjual produknya sendiri, melainkan menyediakan pasar virtual beserta infrastruktur pendukungnya, seperti sistem pencairan dana, sistem pembayaran, dan sistem pengiriman. Oleh karena perannya sebagai fasilitator utama, hukum

memberikan tanggung jawab khusus kepada penyelenggara *marketplace* (R. Lina Sinaulan et al., 2025).

Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) menegaskan dan mendefinisikan secara khusus Penyelenggara Perdagangan Melalui Sistem Elektronik (PPMSE), termasuk penyelenggara *marketplace*. Peraturan ini menetapkan sejumlah kewajiban bagi PPMSE. Pertama, PPMSE wajib menyediakan fasilitas yang memungkinkan penjual memberikan informasi produk secara lengkap dan benar. Kedua, PPMSE wajib memiliki mekanisme untuk menerima laporan atau pengaduan dari masyarakat. Ketiga, PPMSE wajib menjaga keamanan sistem elektronik dari gangguan dan akses ilegal. Selain itu, PPMSE juga wajib menyimpan data dan informasi PMSE yang terkait dengan transaksi keuangan dalam jangka waktu paling singkat 10 tahun sejak data dan informasi diperoleh, serta menyimpan data dan informasi PMSE yang tidak terkait dengan transaksi keuangan dalam jangka waktu paling singkat 5 tahun sejak data dan informasi diperoleh. Jika terjadi kerugian pada konsumen dan PPMSE terbukti tidak melaksanakan kewajibannya untuk menyediakan *platform* yang aman, maka PPMSE dapat turut bertanggung jawab atas kerugian tersebut. Regulasi ini bertujuan untuk memastikan bahwa *marketplace* tidak hanya menjadi *platform* yang nyaman, tetapi juga aman dan terpercaya (R. Lina Sinaulan et al., 2025; Republik Indonesia, 2019b).

Penjual *online* merupakan pihak yang secara langsung melakukan transaksi dengan konsumen sehingga bertanggung jawab atas barang atau jasa yang diperdagangkan. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, selanjutnya disebut UU PK, menjadi dasar utama yang mengatur tanggung jawab penjual sebagai pelaku usaha terhadap konsumen. Pasal 7 UU PK menerangkan kewajiban pelaku usaha, antara lain: a. beritikad baik dalam melakukan kegiatan usahanya; b. memberikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan, dan pemeliharaan; c. memperlakukan atau melayani konsumen secara benar, jujur, dan tidak diskriminatif; d. menjamin mutu barang dan/atau jasa yang diproduksi dan/atau diperdagangkan berdasarkan ketentuan standar mutu barang dan/atau jasa yang berlaku; e. memberi kesempatan kepada konsumen untuk menguji dan/atau mencoba barang dan/atau jasa tertentu serta memberi jaminan dan/atau garansi atas barang yang dibuat dan/atau

diperdagangkan; f. memberi kompensasi, ganti rugi, dan/atau penggantian atas kerugian akibat penggunaan, pemakaian, dan pemanfaatan barang dan/atau jasa yang diperdagangkan; dan g. memberi kompensasi, ganti rugi, dan/atau penggantian apabila barang dan/atau jasa yang diterima atau dimanfaatkan tidak sesuai dengan perjanjian (Republik Indonesia, 1999b).

Kemudian, Pasal 8 UU PK mengatur perbuatan yang dilarang bagi pelaku usaha. Pelaku usaha dilarang memproduksi dan/atau memperdagangkan barang dan/atau jasa yang: a. tidak memenuhi atau tidak sesuai dengan standar yang dipersyaratkan oleh peraturan; b. tidak sesuai dengan berat bersih, isi bersih, atau jumlah hitungan sebagaimana dinyatakan dalam label barang; c. tidak sesuai dengan ukuran, takaran, timbangan, dan jumlah dalam hitungan sebenarnya; d. tidak sesuai dengan kondisi, jaminan, atau keistimewaan sebagaimana dinyatakan dalam label barang; e. tidak sesuai dengan mutu, tingkatan, komposisi, proses pengolahan, gaya, mode, atau penggunaan tertentu sebagaimana dinyatakan dalam label barang dan/atau jasa; f. tidak sesuai dengan janji yang dinyatakan dalam label; g. tidak mencantumkan tanggal kedaluwarsa atau jangka waktu penggunaan/pemanfaatan yang paling baik atas barang tertentu; h. tidak mengikuti ketentuan berproduksi secara halal sebagaimana pernyataan "halal" yang dicantumkan dalam label; i. tidak memasang label atau membuat penjelasan barang yang memuat nama barang, ukuran, berat/isi bersih atau netto, komposisi, aturan pakai, tanggal pembuatan, akibat sampingan, nama dan alamat pelaku usaha, serta keterangan lain untuk penggunaan yang menurut ketentuan harus dipasang; dan j. tidak mencantumkan informasi dan/atau petunjuk penggunaan barang dalam bahasa Indonesia sesuai dengan ketentuan peraturan perundang-undangan.

Selanjutnya, pelaku usaha dilarang memperdagangkan barang yang rusak, cacat atau bekas, dan tercemar tanpa memberikan informasi secara lengkap dan benar atas barang yang dimaksud. Pelaku usaha juga dilarang memperdagangkan sediaan farmasi dan pangan yang rusak, cacat atau bekas, dan tercemar, baik dengan maupun tanpa memberikan informasi secara lengkap dan benar. Pelaku usaha yang melakukan pelanggaran terhadap ketentuan tersebut wajib menarik barang dari peredaran. Pasal 19 UU PK menegaskan tanggung jawab pelaku usaha untuk memberikan ganti rugi atas kerusakan, pencemaran, dan/atau kerugian konsumen akibat mengonsumsi

barang dan/atau jasa yang dihasilkan atau diperdagangkan (Republik Indonesia, 1999b).

PP PMSE juga mengatur kewajiban pelaku usaha yang melakukan perdagangan melalui sistem elektronik. Pasal 3 PP PMSE mengatur prinsip PMSE, yaitu para pihak harus memperhatikan itikad baik, kehati-hatian, transparansi, keterpercayaan, akuntabilitas, keseimbangan, serta prinsip adil dan sehat. Selanjutnya, Pasal 13 PP PMSE mengatur bahwa dalam setiap PMSE, pelaku usaha wajib memberikan informasi yang benar, jelas, dan jujur tentang identitas subjek hukum yang didukung dengan data atau dokumen yang sah. Pelaku usaha juga wajib menyampaikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan terhadap barang dan/atau jasa yang diperdagangkan, termasuk sistem elektronik yang digunakan sesuai dengan karakteristik, fungsi, dan perannya dalam transaksi tersebut. Informasi yang benar, jelas, dan jujur tersebut paling sedikit meliputi kebenaran dan keakuratan informasi, kesesuaian antara informasi iklan dan fisik barang, kelayakan konsumsi barang dan/atau jasa, legalitas barang dan/atau jasa, serta kualitas, harga, dan aksesibilitas barang dan/atau jasa (Republik Indonesia, 2019a).

Kemudian, Pasal 56 PP PMSE menerangkan bahwa pelaku usaha wajib menyediakan Kontrak Elektronik yang dapat diunduh dan/atau disimpan oleh konsumen. Pasal 59 PP PMSE mengatur perlindungan terhadap data pribadi yang diperoleh dalam PMSE. Pelaku usaha bertanggung jawab menyimpan data pribadi sesuai dengan standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang. Prinsip tersebut meliputi bahwa data pribadi harus diperoleh secara jujur dan sah, hanya digunakan untuk satu tujuan atau lebih yang dideskripsikan secara spesifik dan sah, diperoleh secara layak, relevan, dan tidak terlalu luas dalam kaitannya dengan tujuan pengolahannya, serta harus akurat dan selalu mutakhir dengan memberikan kesempatan kepada pemilik data untuk memperbarui data pribadinya. Selain itu, data pribadi harus diproses sesuai tujuan perolehannya, sesuai dengan hak subjek pemilik data, dan pihak yang menyimpan data pribadi harus mempunyai sistem pengamanan yang patut untuk mencegah kebocoran. Data pribadi juga tidak boleh dikirim ke negara atau wilayah lain di luar Indonesia, kecuali jika negara atau wilayah tersebut oleh Menteri dinyatakan memiliki standar dan tingkat perlindungan yang sama dengan Indonesia (Republik Indonesia, 2019a).

Sementara itu, PP PSTE mengatur penyelenggaraan sistem elektronik secara umum, termasuk kewajiban menjaga keamanan sistem elektronik dan keandalan layanan yang digunakan dalam transaksi elektronik. Dalam konteks *marketplace*, PP PSTE memperkuat kewajiban PSE untuk menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab, sehingga transaksi elektronik dapat berjalan dengan menjamin perlindungan terhadap informasi elektronik, dokumen elektronik, dan data pengguna sesuai dengan ketentuan peraturan perundang-undangan (Republik Indonesia, 2019b).

11.6 Sengketa dalam Transaksi E-Commerce

Sengketa dalam transaksi *e-commerce* adalah perselisihan yang timbul antara para pihak yang melakukan transaksi elektronik, baik antara penjual dan pembeli, pembeli dengan penyelenggara *marketplace*, maupun antara pelaku usaha atau pembeli dengan penyedia layanan pembayaran atau logistik. Sengketa tersebut umumnya muncul karena adanya pelanggaran terhadap hak dan kewajiban para pihak sebagaimana telah disepakati dalam kontrak elektronik atau sebagaimana diatur dalam peraturan perundang-undangan. Oleh karena transaksi dilakukan secara elektronik, sengketa yang muncul memiliki karakteristik yang berbeda dengan transaksi konvensional, terutama terkait pembuktian elektronik, identitas para pihak, yurisdiksi, dan pelaksanaan putusan.

Sengketa dalam perdagangan elektronik dapat terjadi karena berbagai faktor, antara lain barang yang diterima tidak sesuai dengan perjanjian, adanya cacat produk, informasi yang menyesatkan, keterlambatan pengiriman, serta pelanggaran terhadap keamanan dan privasi konsumen dalam transaksi digital. Dalam perkembangan praktik hukum bisnis, sengketa juga dapat timbul karena pelanggaran terhadap standar keamanan produk dan wanprestasi pelaku usaha (Hutahaean et al., 2026). Mengenai jenis-jenis wanprestasi dalam hukum perdata, Ahmadi Miru menyatakan bahwa wanprestasi dapat berupa perbuatan tidak memenuhi prestasi sama sekali, prestasi yang dilakukan tidak sempurna, terlambat memenuhi prestasi, dan melakukan sesuatu yang dilarang dalam perjanjian (Khasanah et al., 2023).

Berdasarkan Pasal 4 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, konsumen memiliki hak untuk memperoleh kenyamanan, keamanan, dan keselamatan dalam mengonsumsi barang

dan/atau jasa; hak untuk memperoleh informasi yang benar, jelas, dan jujur; serta hak untuk mendapatkan kompensasi, ganti rugi, dan/atau penggantian apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya (Republik Indonesia, 1999). Menurut Shidarta sebagaimana dikutip dalam Hutahaean et al. (2026), lemahnya transparansi informasi dan rendahnya kepatuhan pelaku usaha terhadap etika bisnis menjadi salah satu penyebab utama timbulnya sengketa konsumen di Indonesia. Hal ini juga dapat diperburuk oleh kurangnya pengawasan terhadap *marketplace* yang beroperasi.

Bab 12
Hukum Fintech dan Ekonomi Digital

12.1 Pengertian Fintech dan Ekonomi Digital

Perkembangan teknologi informasi telah mengubah cara masyarakat melakukan aktivitas ekonomi dan keuangan. Jika sebelumnya kegiatan ekonomi banyak dilakukan secara langsung melalui toko fisik, kantor bank, atau lembaga keuangan konvensional, maka saat ini banyak aktivitas tersebut berpindah ke ruang digital. Masyarakat dapat membeli barang melalui marketplace, membayar tagihan menggunakan dompet digital, mentransfer uang melalui mobile banking, mengajukan pinjaman online, berinvestasi melalui aplikasi, hingga menggunakan QRIS untuk pembayaran sehari-hari. Perubahan ini menunjukkan bahwa teknologi telah menjadi bagian penting dalam sistem ekonomi modern.

Gambar 12.1: Hubungan Fintech dan Ekonomi Digital

Dalam konteks hukum teknologi informasi, dua istilah yang penting untuk dipahami adalah **fintech** dan **ekonomi digital**. Keduanya saling berkaitan, tetapi tidak sama. Ekonomi digital memiliki cakupan yang lebih luas karena mencakup seluruh aktivitas ekonomi yang menggunakan teknologi digital. Sementara itu, fintech lebih khusus merujuk pada pemanfaatan teknologi

dalam sektor keuangan. Dengan demikian, fintech merupakan salah satu bagian penting dari ekonomi digital.

Secara sederhana, **fintech** atau *financial technology* dapat dipahami sebagai pemanfaatan teknologi untuk menyediakan, mempercepat, mempermudah, atau mengubah layanan keuangan. Raharjo (2021) menjelaskan bahwa fintech merupakan gabungan antara jasa keuangan dan teknologi yang mengubah model bisnis keuangan dari cara konvensional menuju cara yang lebih digital. Perubahan tersebut tampak dalam layanan pembayaran elektronik, dompet digital, peer-to-peer lending, crowdfunding, investasi online, roboadvisor, cryptocurrency, blockchain, dan layanan perbankan digital.

Fintech hadir karena kebutuhan masyarakat terhadap layanan keuangan yang lebih cepat, mudah, murah, dan dapat diakses dari mana saja. Dalam sistem keuangan konvensional, seseorang biasanya harus datang ke kantor bank untuk membuka rekening, mengajukan pinjaman, melakukan transaksi, atau memperoleh layanan keuangan lainnya. Dengan fintech, banyak layanan tersebut dapat dilakukan melalui aplikasi mobile atau platform digital. Hal ini membuat fintech berperan penting dalam meningkatkan akses masyarakat terhadap layanan keuangan.

Wibowo (2024) menjelaskan bahwa fintech mengacu pada penggunaan teknologi untuk menyediakan layanan atau produk keuangan. Dalam pengertian ini, fintech tidak hanya terbatas pada aplikasi pembayaran, tetapi juga mencakup layanan keuangan berbasis teknologi seperti pembayaran online, integrasi data keuangan konsumen, pinjaman digital, aset kripto, blockchain, dan berbagai bentuk inovasi keuangan lainnya. Dengan demikian, fintech dapat dipahami sebagai inovasi di sektor keuangan yang memanfaatkan teknologi digital untuk menciptakan layanan baru atau memperbaiki layanan yang sudah ada.

Fintech dapat berbentuk berbagai layanan. Pertama, fintech dapat berbentuk layanan pembayaran digital, seperti dompet digital, QRIS, mobile payment, dan payment gateway. Kedua, fintech dapat berbentuk layanan pembiayaan, seperti peer-to-peer lending dan crowdfunding. Ketiga, fintech dapat berbentuk layanan investasi digital, seperti aplikasi investasi saham, reksa dana, aset kripto, dan roboadvisor. Keempat, fintech dapat berbentuk layanan pendukung sektor keuangan, seperti e-KYC, big data analytics, artificial intelligence, blockchain, dan regulatory technology.

Ekonomi digital memiliki pengertian yang lebih luas daripada fintech. **Ekonomi digital** adalah aktivitas ekonomi yang menggunakan teknologi digital dalam proses produksi, distribusi, konsumsi, transaksi, komunikasi, dan pengelolaan data. Affandi dan Iskandar (2025) menjelaskan bahwa ekonomi keuangan digital merupakan ranah ekonomi dan keuangan yang berbasis pada penggunaan teknologi digital, mencakup perdagangan elektronik, sistem pembayaran, layanan keuangan digital, serta pemanfaatan teknologi seperti Internet of Things, kecerdasan buatan, machine learning, dan blockchain.

Ekonomi digital tidak hanya berkaitan dengan sektor keuangan, tetapi juga mencakup perdagangan online, transportasi online, pendidikan digital, layanan kesehatan digital, pekerjaan berbasis platform, pemasaran digital, media sosial commerce, dan berbagai bentuk bisnis berbasis aplikasi. Dalam ekonomi digital, data menjadi aset penting karena aktivitas pengguna dapat dianalisis untuk memahami perilaku konsumen, menentukan strategi bisnis, meningkatkan layanan, dan mengembangkan produk baru.

Perbedaan utama antara fintech dan ekonomi digital terletak pada ruang lingkupnya. Fintech berfokus pada inovasi teknologi dalam layanan keuangan, sedangkan ekonomi digital mencakup seluruh kegiatan ekonomi yang memanfaatkan teknologi digital. Misalnya, marketplace seperti Tokopedia, Shopee, atau Lazada merupakan bagian dari ekonomi digital karena menjadi ruang transaksi barang dan jasa. Namun, ketika marketplace tersebut menyediakan sistem pembayaran digital, paylater, atau kerja sama dengan layanan pembiayaan, maka unsur fintech ikut hadir di dalam ekosistem tersebut.

Fintech dan ekonomi digital saling mendukung. Ekonomi digital membutuhkan sistem pembayaran dan layanan keuangan yang cepat agar transaksi berjalan lancar. Sebaliknya, fintech berkembang pesat karena semakin banyak masyarakat melakukan transaksi digital. Contohnya, pertumbuhan e-commerce mendorong kebutuhan terhadap dompet digital, virtual account, QRIS, paylater, dan layanan pembayaran cepat. Perkembangan transportasi online juga mendorong penggunaan pembayaran non-tunai dan dompet digital.

Dalam praktiknya, fintech menjadi infrastruktur penting bagi ekonomi digital. Tanpa sistem pembayaran digital, transaksi online akan sulit

berkembang. Tanpa layanan pembiayaan digital, sebagian konsumen dan pelaku usaha akan kesulitan memperoleh akses dana. Tanpa teknologi verifikasi identitas digital, layanan keuangan online akan lebih rentan terhadap penyalahgunaan identitas. Oleh karena itu, fintech tidak hanya menjadi inovasi bisnis, tetapi juga menjadi bagian dari fondasi ekonomi digital.

Perkembangan fintech juga mendorong inklusi keuangan. Inklusi keuangan berarti semakin banyak masyarakat yang dapat mengakses layanan keuangan formal. Masyarakat yang sebelumnya sulit memperoleh layanan bank karena jarak, dokumen, biaya, atau keterbatasan akses fisik dapat menggunakan layanan keuangan melalui aplikasi. Dalam hal ini, fintech dapat membantu pelaku UMKM, pekerja informal, masyarakat di daerah, dan generasi muda untuk lebih mudah melakukan pembayaran, menyimpan uang, memperoleh pinjaman, atau berinvestasi.

Namun, fintech juga membawa risiko hukum dan sosial. Risiko tersebut dapat berupa penyalahgunaan data pribadi, pinjaman online ilegal, penagihan intimidatif, bunga dan biaya yang tidak transparan, penipuan digital, pencurian identitas, transaksi tidak sah, kegagalan sistem, serta rendahnya literasi keuangan digital. Pratiwi & Erniwati (2022) menjelaskan bahwa perkembangan fintech, khususnya peer-to-peer lending, menimbulkan persoalan seperti fintech ilegal, penagihan intimidatif, dan penyebaran data pribadi nasabah. Hal ini menunjukkan bahwa fintech membutuhkan regulasi dan pengawasan yang kuat.

Regulasi fintech diperlukan untuk melindungi konsumen, menjaga stabilitas sistem keuangan, mencegah penyalahgunaan teknologi, dan memastikan pelaku usaha fintech bertindak secara bertanggung jawab. Purborini et al. (2025) menjelaskan bahwa regulasi fintech di Indonesia penting untuk mengatur perkembangan ekonomi digital, melindungi konsumen, menjaga stabilitas sistem keuangan, dan menciptakan lingkungan bisnis yang sehat. Dengan demikian, fintech harus dikembangkan secara seimbang antara inovasi dan perlindungan hukum.

Dari sisi hukum, fintech berkaitan dengan berbagai aspek regulasi. Pertama, fintech berkaitan dengan hukum transaksi elektronik karena layanan fintech dilakukan melalui sistem elektronik. Kedua, fintech berkaitan dengan pelindungan data pribadi karena layanan keuangan digital mengumpulkan dan memproses data pengguna. Ketiga, fintech berkaitan dengan hukum

perlindungan konsumen karena pengguna fintech berhak memperoleh informasi yang jelas, layanan yang aman, dan penyelesaian apabila dirugikan. Keempat, fintech berkaitan dengan hukum perbankan dan keuangan karena menyangkut pembayaran, pinjaman, investasi, dan pengelolaan dana.

Ekonomi digital juga memiliki implikasi hukum yang luas. Dalam ekonomi digital, transaksi dilakukan melalui platform, data konsumen diproses secara masif, iklan digital memengaruhi keputusan konsumen, kontrak elektronik menjadi dasar hubungan hukum, dan bukti elektronik digunakan dalam penyelesaian sengketa. Oleh karena itu, ekonomi digital memerlukan pengaturan mengenai e-commerce, perlindungan konsumen, pelindungan data pribadi, keamanan siber, kekayaan intelektual digital, pajak digital, dan tanggung jawab platform.

Fintech dan ekonomi digital juga mendorong munculnya konsep baru dalam tata kelola hukum. Salah satunya adalah perlunya regulasi yang adaptif. Regulasi adaptif berarti aturan hukum harus mampu mengikuti perkembangan teknologi tanpa menghambat inovasi. Wibowo (2024) menjelaskan bahwa perkembangan fintech menimbulkan persoalan karena teknologi sering bergerak lebih cepat daripada regulasi. Oleh sebab itu, pendekatan seperti regulatory sandbox menjadi penting untuk menguji inovasi fintech dalam lingkungan yang terkontrol sebelum diterapkan secara luas.

Selain regulasi adaptif, fintech juga membutuhkan penguatan literasi masyarakat. Literasi keuangan digital diperlukan agar masyarakat memahami manfaat dan risiko layanan keuangan digital. Pengguna fintech perlu memahami cara menjaga OTP, PIN, password, data pribadi, dan dokumen identitas. Pengguna juga perlu memahami bunga, biaya layanan, risiko pinjaman, syarat penggunaan aplikasi, serta cara mengajukan pengaduan apabila mengalami kerugian. Tanpa literasi yang memadai, masyarakat mudah menjadi korban penipuan, pinjaman online ilegal, atau penyalahgunaan data.

Secara umum, fintech dan ekonomi digital memiliki beberapa karakteristik utama.

1. **Berbasis teknologi digital**

   Fintech dan ekonomi digital menggunakan internet, aplikasi mobile, sistem elektronik, big data, kecerdasan buatan, blockchain, dan teknologi informasi lainnya untuk menjalankan aktivitas ekonomi dan keuangan.

2. **Cepat dan mudah diakses**

   Layanan dapat digunakan kapan saja dan dari mana saja selama pengguna memiliki perangkat digital dan akses internet.

3. **Berorientasi pada efisiensi**

   Teknologi digunakan untuk mempercepat proses transaksi, menurunkan biaya, mengurangi prosedur manual, dan meningkatkan kenyamanan pengguna.

4. **Mengandalkan data**

   Data pengguna, data transaksi, dan data perilaku digital menjadi bagian penting dalam pengambilan keputusan bisnis, analisis risiko, pemasaran, dan pengembangan layanan.

5. **Melibatkan banyak pihak**

   Ekosistem fintech dan ekonomi digital melibatkan konsumen, pelaku usaha, platform, bank, penyedia pembayaran, regulator, penyedia teknologi, dan pihak ketiga lainnya.

6. **Memiliki risiko hukum dan keamanan**

   Risiko dapat berupa kebocoran data, penipuan online, transaksi tidak sah, akses ilegal, pelanggaran privasi, dan sengketa konsumen.

7. **Membutuhkan regulasi dan pengawasan**

   Inovasi digital perlu diarahkan agar tetap melindungi konsumen, menjaga kepercayaan publik, dan mendukung stabilitas sistem keuangan.

Tabel berikut merangkum perbedaan antara fintech dan ekonomi digital.

Tabel 12.1: Perbedaan Fintech dan Ekonomi Digital

Aspek	Fintech	Ekonomi Digital
Pengertian	Pemanfaatan teknologi dalam layanan keuangan	Aktivitas ekonomi yang berbasis teknologi digital

Aspek	Fintech	Ekonomi Digital
Ruang lingkup	Lebih khusus pada sektor keuangan	Lebih luas, mencakup perdagangan, jasa, data, platform, dan keuangan
Contoh layanan	Dompet digital, QRIS, P2P lending, crowdfunding, mobile banking, investasi online	E-commerce, transportasi online, marketplace, digital marketing, fintech, layanan aplikasi
Fokus utama	Efisiensi, akses, dan inovasi layanan keuangan	Transformasi aktivitas ekonomi melalui teknologi digital
Risiko utama	Penyalahgunaan data, pinjol ilegal, transaksi tidak sah, keamanan sistem	Sengketa platform, perlindungan konsumen, privasi, monopoli data, keamanan siber
Regulasi terkait	OJK, Bank Indonesia, UU ITE, UU PDP, regulasi sektor keuangan	UU ITE, UU PDP, perlindungan konsumen, e-commerce, pajak digital, persaingan usaha
Hubungan keduanya	Bagian dari ekonomi digital	Mencakup fintech sebagai salah satu komponen

Dari tabel tersebut dapat dipahami bahwa fintech merupakan bagian dari ekonomi digital, tetapi memiliki fokus khusus pada sektor keuangan. Ekonomi digital membutuhkan fintech agar transaksi berjalan lebih cepat dan efisien. Sebaliknya, fintech berkembang karena masyarakat semakin aktif menggunakan layanan digital dalam kegiatan ekonomi sehari-hari.

Dalam konteks Indonesia, perkembangan fintech dan ekonomi digital sangat penting karena dapat mendukung pertumbuhan ekonomi nasional. Layanan pembayaran digital seperti QRIS dan BI-FAST mempercepat transaksi masyarakat. E-commerce membuka peluang bagi UMKM untuk menjual produk secara lebih luas. Layanan fintech dapat memperluas akses keuangan bagi masyarakat yang sebelumnya sulit dijangkau oleh lembaga keuangan konvensional. Namun, perkembangan tersebut harus tetap diimbangi dengan perlindungan konsumen, keamanan data, dan pengawasan yang efektif.

Dengan demikian, fintech dan ekonomi digital merupakan dua konsep penting dalam hukum teknologi informasi. Fintech adalah pemanfaatan teknologi dalam layanan keuangan, sedangkan ekonomi digital adalah aktivitas ekonomi yang berbasis teknologi digital. Keduanya membawa manfaat berupa kemudahan, efisiensi, inklusi keuangan, inovasi bisnis, dan pertumbuhan ekonomi. Namun, keduanya juga membawa risiko hukum

seperti penyalahgunaan data pribadi, penipuan online, transaksi tidak sah, pinjaman ilegal, dan sengketa konsumen. Oleh karena itu, pemahaman mengenai fintech dan ekonomi digital harus mencakup aspek teknologi, ekonomi, hukum, perlindungan konsumen, dan tata kelola digital.

12.2 Jenis-Jenis Layanan Fintech

Fintech atau teknologi finansial berkembang dalam berbagai bentuk layanan. Pada awalnya, teknologi keuangan lebih banyak digunakan untuk mendukung sistem internal perbankan, seperti pencatatan transaksi, pemrosesan data nasabah, dan sistem pembayaran. Namun, perkembangan internet, perangkat mobile, big data, kecerdasan buatan, dan blockchain membuat fintech berkembang menjadi layanan yang langsung digunakan oleh masyarakat. Saat ini, fintech tidak hanya berkaitan dengan bank, tetapi juga melibatkan perusahaan teknologi, startup, marketplace, penyedia dompet digital, platform pinjaman, perusahaan investasi, dan penyedia layanan keuangan berbasis aplikasi.

Gambar 12.2: Jenis-Jenis Layanan Fintech

Jenis-jenis fintech perlu dipahami karena setiap layanan memiliki karakteristik, manfaat, risiko, dan pengaturan hukum yang berbeda. Layanan pembayaran digital tentu memiliki risiko yang berbeda dengan pinjaman online. Demikian pula, investasi digital memiliki tantangan hukum yang

berbeda dengan crowdfunding atau aset kripto. Oleh karena itu, pengelompokan jenis fintech membantu mahasiswa memahami bagaimana teknologi digunakan dalam sektor keuangan serta bagaimana hukum merespons perkembangan tersebut.

Raharjo (2021) menjelaskan bahwa fintech mencakup berbagai layanan seperti pembayaran peer-to-peer, aplikasi seluler, transfer cryptocurrency, model peminjaman digital, crowdinvesting, roboadvisor, kecerdasan buatan, analitik tingkat lanjut, blockchain, asuransi, real estate, dan pinjaman. Hal ini menunjukkan bahwa fintech memiliki cakupan yang luas dan terus berkembang sesuai kebutuhan masyarakat dan inovasi teknologi.

Wibowo (2024) juga menjelaskan bahwa fintech mencakup penggunaan teknologi untuk menyediakan layanan atau produk keuangan, termasuk pembayaran online, integrasi data keuangan konsumen, pinjaman digital, blockchain, aset kripto, dan berbagai inovasi keuangan lainnya. Dalam konteks ekonomi digital, fintech menjadi bagian penting karena menyediakan infrastruktur keuangan bagi transaksi digital, seperti pembayaran, pembiayaan, investasi, dan pengelolaan risiko.

Secara umum, jenis-jenis fintech dapat dibagi ke dalam beberapa kelompok berikut.

12.2.1 Pembayaran Digital

Pembayaran digital merupakan salah satu jenis fintech yang paling banyak digunakan masyarakat. Layanan ini memungkinkan pengguna melakukan pembayaran tanpa uang tunai melalui aplikasi, kartu, kode QR, transfer digital, virtual account, atau dompet elektronik. Contohnya adalah QRIS, mobile banking, internet banking, payment gateway, dompet digital, dan pembayaran melalui aplikasi marketplace.

Pembayaran digital memberikan kemudahan karena transaksi dapat dilakukan secara cepat, praktis, dan tercatat secara elektronik. Masyarakat tidak perlu membawa uang tunai dalam jumlah besar. Pelaku usaha juga dapat menerima pembayaran dengan lebih mudah. Dalam konteks Indonesia, perkembangan QRIS dan BI-FAST menunjukkan bahwa sistem pembayaran digital menjadi bagian penting dari ekonomi keuangan digital. Affandi & Iskandar (2025) menjelaskan bahwa digitalisasi sistem

pembayaran mendorong integrasi, interkoneksi, dan interoperabilitas dalam ekosistem pembayaran nasional.

Namun, pembayaran digital juga memiliki risiko. Risiko tersebut antara lain pencurian akun, transaksi tidak sah, kesalahan transfer, phishing, penyalahgunaan OTP, kegagalan sistem, dan kebocoran data transaksi. Oleh sebab itu, penyedia layanan pembayaran digital harus memastikan keamanan sistem, pelindungan data pribadi, autentikasi pengguna, serta mekanisme pengaduan yang cepat.

12.2.2 Dompet Digital

Dompet digital atau e-wallet adalah layanan fintech yang memungkinkan pengguna menyimpan nilai uang secara elektronik dan menggunakannya untuk membayar transaksi. Dompet digital banyak digunakan untuk belanja online, transportasi online, pesan makanan, pembayaran tagihan, transfer dana, dan pembelian produk digital. Contohnya adalah OVO, GoPay, DANA, LinkAja, dan layanan serupa lainnya.

Dompet digital menjadi populer karena mudah digunakan dan terintegrasi dengan berbagai platform digital. Konsumen dapat melakukan pembayaran hanya melalui ponsel. Pelaku usaha kecil juga dapat menerima pembayaran digital tanpa harus memiliki sistem perbankan yang rumit. Dalam konteks ekonomi digital, dompet digital mempercepat peralihan masyarakat dari pembayaran tunai ke pembayaran non-tunai.

Risiko hukum dalam dompet digital berkaitan dengan saldo hilang, akun diretas, transaksi tidak dikenal, kegagalan top up, pengembalian dana yang tidak jelas, dan penyalahgunaan data pengguna. Dalam kasus seperti ini, konsumen membutuhkan perlindungan hukum, transparansi prosedur, dan mekanisme penyelesaian sengketa. Anami et al. (2025) menjelaskan bahwa sengketa saldo DANA menunjukkan pentingnya perlindungan hukum dalam kontrak digital dan layanan pembayaran elektronik.

12.2.3 Peer-to-Peer Lending

Peer-to-peer lending atau P2P lending adalah layanan pinjam meminjam uang berbasis teknologi informasi yang mempertemukan pemberi dana dan penerima dana melalui platform digital. Dalam model ini, platform fintech

bertindak sebagai penghubung antara pihak yang membutuhkan pinjaman dan pihak yang bersedia memberikan pendanaan.

P2P lending memberikan manfaat karena dapat memperluas akses pembiayaan bagi masyarakat dan pelaku usaha yang sulit memperoleh pinjaman dari lembaga keuangan konvensional. UMKM, pekerja informal, dan masyarakat yang belum memiliki akses bank dapat memperoleh pembiayaan secara lebih cepat melalui platform digital. Wibowo (2024) menjelaskan bahwa P2P lending merupakan salah satu bentuk fintech yang berkembang karena teknologi memungkinkan penyediaan layanan keuangan secara lebih mudah dan cepat.

Namun, P2P lending juga memiliki risiko besar. Risiko tersebut antara lain bunga tinggi, biaya tidak transparan, penagihan intimidatif, penyalahgunaan data pribadi, pinjaman ilegal, dan rendahnya literasi pengguna. Pratiwi dan Erniwati (2022) menjelaskan bahwa perkembangan fintech P2P lending di Indonesia menimbulkan masalah seperti fintech ilegal, penagihan yang mengintimidasi, dan penyebaran data pribadi nasabah. Oleh karena itu, layanan ini membutuhkan pengawasan ketat dari regulator.

12.2.4 Crowdfunding dan Crowdinvesting

Crowdfunding adalah layanan penggalangan dana secara digital dari banyak orang untuk mendukung suatu proyek, usaha, kegiatan sosial, atau kebutuhan tertentu. Crowdfunding dapat digunakan untuk kegiatan sosial, pendanaan usaha, proyek kreatif, pendidikan, kesehatan, maupun kegiatan kemanusiaan. Dalam praktiknya, crowdfunding dapat berbentuk donasi, hadiah, pinjaman, atau investasi.

Crowdinvesting merupakan bentuk crowdfunding yang memberikan peluang kepada masyarakat untuk berinvestasi pada suatu usaha atau proyek tertentu. Dalam model ini, masyarakat tidak hanya memberikan donasi, tetapi juga dapat memperoleh imbal hasil atau bagian keuntungan sesuai ketentuan yang berlaku.

Fintech jenis ini memberikan manfaat karena memperluas akses pendanaan. Pelaku usaha kecil dapat memperoleh modal dari masyarakat tanpa harus selalu bergantung pada bank. Masyarakat juga memiliki peluang untuk ikut mendukung proyek atau usaha tertentu. Namun, risikonya meliputi penipuan proyek, kegagalan usaha, informasi yang tidak transparan, dan

ketidakjelasan pertanggungjawaban pengelola dana. Oleh sebab itu, crowdfunding dan crowdinvesting memerlukan regulasi yang jelas, terutama terkait transparansi informasi dan perlindungan investor.

12.2.5 Investasi Digital

Investasi digital adalah layanan fintech yang memungkinkan masyarakat melakukan investasi melalui aplikasi atau platform online. Bentuknya dapat berupa investasi saham, reksa dana, obligasi, emas digital, aset kripto, atau instrumen investasi lainnya. Layanan ini membuat investasi lebih mudah diakses oleh masyarakat, terutama generasi muda.

Melalui investasi digital, pengguna dapat membuka akun, melakukan verifikasi identitas, membeli produk investasi, memantau portofolio, dan melakukan transaksi secara online. Teknologi membuat proses investasi menjadi lebih cepat, murah, dan mudah dipahami. Beberapa platform juga menggunakan fitur edukasi, simulasi risiko, dan rekomendasi investasi.

Namun, investasi digital juga memiliki risiko. Konsumen dapat mengalami kerugian karena kurang memahami risiko produk, tergoda imbal hasil tinggi, mengikuti rekomendasi tanpa analisis, atau menggunakan platform ilegal. Oleh karena itu, literasi keuangan digital sangat penting. Platform investasi digital harus memberikan informasi yang benar mengenai risiko, biaya, legalitas produk, dan mekanisme pengaduan.

12.2.6 Robo Advisor

Robo advisor adalah layanan fintech yang menggunakan algoritma dan kecerdasan buatan untuk memberikan rekomendasi investasi atau pengelolaan portofolio secara otomatis. Layanan ini biasanya meminta pengguna mengisi profil risiko, tujuan investasi, jangka waktu, dan kondisi keuangan. Setelah itu, sistem akan memberikan rekomendasi instrumen investasi yang sesuai dengan profil pengguna.

Robo advisor memberikan manfaat karena layanan konsultasi investasi dapat diakses dengan biaya lebih rendah dibandingkan penasihat keuangan tradisional. Masyarakat yang belum memiliki pengetahuan investasi mendalam dapat memperoleh rekomendasi awal melalui sistem. Namun, penggunaan robo advisor juga memiliki tantangan, terutama terkait akurasi

algoritma, transparansi metode rekomendasi, perlindungan data pengguna, dan tanggung jawab apabila rekomendasi merugikan konsumen.

Dari sisi hukum, robo advisor menimbulkan pertanyaan mengenai akuntabilitas. Jika rekomendasi investasi diberikan oleh algoritma, perlu dianalisis siapa yang bertanggung jawab apabila terjadi kerugian: pengguna, platform, penyedia algoritma, atau pihak yang mengelola produk investasi. Hal ini menunjukkan bahwa perkembangan fintech tidak hanya menyangkut kemudahan layanan, tetapi juga membutuhkan pengaturan tanggung jawab yang jelas.

12.2.7 Insurtech

Insurtech adalah pemanfaatan teknologi digital dalam layanan asuransi. Layanan ini mencakup pembelian polis secara online, klaim digital, penilaian risiko berbasis data, asuransi mikro, asuransi perjalanan digital, asuransi kesehatan berbasis aplikasi, dan penggunaan kecerdasan buatan dalam proses underwriting.

Insurtech membuat layanan asuransi lebih mudah diakses. Konsumen dapat membeli produk asuransi, membaca polis, membayar premi, dan mengajukan klaim melalui aplikasi. Proses administrasi juga menjadi lebih cepat dan efisien. Namun, tantangan hukum dalam insurtech berkaitan dengan transparansi informasi polis, pengecualian pertanggungan, penggunaan data kesehatan, kejelasan klaim, dan perlindungan konsumen.

Pelaku usaha insurtech harus memastikan bahwa konsumen memahami manfaat, risiko, premi, masa pertanggungan, dan pengecualian polis. Informasi yang tidak jelas dapat menimbulkan sengketa ketika konsumen mengajukan klaim. Oleh karena itu, prinsip informasi yang benar dan transparan sangat penting dalam layanan insurtech.

12.2.8 Blockchain dan Aset Kripto

Blockchain merupakan teknologi pencatatan data yang bersifat terdistribusi dan dapat digunakan untuk mencatat transaksi secara aman dan transparan. Dalam fintech, blockchain banyak dikaitkan dengan cryptocurrency, token digital, smart contract, dan aset keuangan digital. Wibowo (2024) menjelaskan bahwa teknologi blockchain menjadi salah satu aspek penting

dalam perkembangan fintech karena mengubah cara transaksi dan pencatatan dalam pasar keuangan modern.

Aset kripto merupakan bentuk aset digital yang menggunakan teknologi kriptografi dan blockchain. Aset ini dapat diperdagangkan melalui platform tertentu. Dalam ekonomi digital, aset kripto menarik perhatian karena menawarkan model baru dalam transaksi dan investasi. Namun, aset kripto juga memiliki risiko tinggi, seperti volatilitas harga, penipuan, pencucian uang, kehilangan akses dompet digital, dan ketidakpastian regulasi.

Dari sisi hukum, blockchain dan aset kripto membutuhkan pengaturan yang hati-hati. Regulasi perlu menjaga keseimbangan antara inovasi teknologi dan perlindungan masyarakat. Pengguna harus memahami bahwa aset kripto memiliki risiko yang berbeda dari instrumen keuangan konvensional. Platform penyedia layanan aset digital juga harus memperhatikan keamanan, transparansi, dan kepatuhan terhadap aturan anti pencucian uang.

12.2.9 Regtech dan Suptech

Regtech atau regulatory technology adalah penggunaan teknologi untuk membantu pelaku usaha memenuhi kewajiban regulasi. Contohnya adalah sistem pelaporan otomatis, pemantauan transaksi mencurigakan, verifikasi identitas digital, anti pencucian uang, dan kepatuhan terhadap pelindungan data pribadi.

Suptech atau supervisory technology adalah penggunaan teknologi oleh regulator untuk melakukan pengawasan secara lebih efektif. Dengan suptech, regulator dapat memantau data dalam jumlah besar, mendeteksi risiko, mengawasi kepatuhan, dan mengidentifikasi transaksi mencurigakan. Affandi & Iskandar (2025) menjelaskan bahwa supervisory technology penting dalam pengawasan sistem keuangan digital karena regulator perlu memantau aktivitas lembaga keuangan yang semakin kompleks.

Regtech dan suptech penting karena perkembangan fintech membuat transaksi keuangan semakin cepat, kompleks, dan berbasis data. Tanpa teknologi pengawasan yang memadai, regulator dapat kesulitan mengawasi risiko yang muncul. Oleh karena itu, teknologi tidak hanya digunakan oleh pelaku usaha, tetapi juga oleh regulator untuk menjaga stabilitas dan perlindungan konsumen.

12.2.10 Digital Banking

Digital banking adalah layanan perbankan yang dilakukan melalui sistem digital. Layanan ini mencakup pembukaan rekening online, transfer dana, pembayaran tagihan, pembelian produk keuangan, pengajuan pinjaman, pengelolaan kartu, dan layanan perbankan lainnya melalui aplikasi atau website. Digital banking berbeda dari mobile banking biasa apabila seluruh proses layanan dapat dilakukan secara digital dengan sedikit atau tanpa kehadiran fisik di kantor bank.

Raharjo (2021) menjelaskan bahwa perkembangan fintech dan perbankan digital membuat bank tidak lagi dapat hanya mengandalkan pola pelayanan tradisional. Nasabah semakin membutuhkan layanan yang cepat, mobile, efisien, dan dapat diakses dari mana saja. Hal ini mendorong bank untuk berkolaborasi dengan fintech atau mengembangkan layanan digitalnya sendiri.

Digital banking memberikan kemudahan, tetapi juga menimbulkan risiko seperti pencurian akun, social engineering, phishing, transaksi tidak sah, dan gangguan sistem. Oleh karena itu, bank digital wajib memperhatikan keamanan siber, pelindungan data pribadi, pengaduan nasabah, dan kepatuhan terhadap regulasi sektor jasa keuangan.

Tabel berikut merangkum jenis-jenis fintech dan contoh layanannya.

Tabel 12.2: Jenis-Jenis Layanan Fintech

Jenis Fintech	Pengertian Singkat	Contoh Layanan	Risiko Utama
Pembayaran digital	Layanan pembayaran berbasis elektronik	QRIS, payment gateway, mobile payment	Transaksi tidak sah, phishing, kegagalan sistem
Dompet digital	Penyimpanan dan penggunaan uang elektronik melalui aplikasi	OVO, GoPay, DANA, LinkAja	Saldo hilang, akun diretas, data bocor
P2P lending	Pinjam meminjam berbasis platform digital	Pinjaman online, pendanaan UMKM	Bunga tinggi, penagihan intimidatif, pinjol ilegal

Jenis Fintech	Pengertian Singkat	Contoh Layanan	Risiko Utama
Crowdfunding	Penggalangan dana dari banyak orang melalui platform	Donasi digital, pendanaan proyek	Penipuan proyek, informasi tidak transparan
Investasi digital	Investasi melalui aplikasi online	Saham, reksa dana, emas digital, aset kripto	Kerugian investasi, platform ilegal
Robo advisor	Rekomendasi investasi berbasis algoritma	Rekomendasi portofolio otomatis	Kesalahan algoritma, tanggung jawab tidak jelas
Insurtech	Layanan asuransi berbasis teknologi	Polis online, klaim digital	Informasi polis tidak jelas, sengketa klaim
Blockchain dan aset kripto	Teknologi pencatatan terdistribusi dan aset digital	Cryptocurrency, token digital	Volatilitas, penipuan, kehilangan akses
Regtech dan suptech	Teknologi untuk kepatuhan dan pengawasan	AML system, pelaporan otomatis, monitoring regulator	Ketergantungan sistem, keamanan data
Digital banking	Layanan bank berbasis digital	Bank digital, mobile banking, pembukaan rekening online	Phishing, pencurian akun, transaksi tidak sah

Dari tabel tersebut dapat dipahami bahwa fintech memiliki bentuk layanan yang sangat beragam. Setiap jenis fintech memiliki manfaat dan risiko yang berbeda. Oleh karena itu, pendekatan hukum terhadap fintech tidak dapat disamakan secara sederhana. Layanan pembayaran membutuhkan pengaturan mengenai keamanan transaksi. P2P lending membutuhkan pengaturan mengenai bunga, penagihan, dan perlindungan data. Investasi digital membutuhkan pengaturan mengenai transparansi risiko. Aset kripto membutuhkan pengaturan mengenai perdagangan, keamanan, dan pencegahan kejahatan keuangan.

Model layanan fintech juga dapat dibedakan berdasarkan hubungan para pihak. Pertama, terdapat model *business to consumer*, yaitu layanan yang diberikan langsung kepada konsumen, seperti dompet digital, mobile banking, dan aplikasi investasi. Kedua, terdapat model business to business, yaitu layanan fintech yang mendukung perusahaan lain, seperti payment gateway, regtech, dan sistem verifikasi identitas. Ketiga, terdapat model peer

to peer, yaitu platform yang mempertemukan pengguna secara langsung, seperti P2P lending dan crowdfunding.

Selain itu, terdapat model platform-based finance, yaitu layanan keuangan yang beroperasi melalui platform digital. Dalam model ini, platform memiliki peran penting sebagai penghubung, pengelola data, penyedia sistem transaksi, dan pengatur mekanisme layanan. Model ini menimbulkan tantangan hukum karena perlu menentukan siapa yang bertanggung jawab apabila terjadi sengketa, kerugian, atau penyalahgunaan data.

Perkembangan jenis-jenis fintech menunjukkan bahwa inovasi keuangan digital tidak dapat dipisahkan dari perlindungan hukum. Fintech memberikan manfaat berupa kemudahan, efisiensi, inklusi keuangan, dan inovasi layanan. Namun, fintech juga membawa risiko seperti kejahatan siber, penyalahgunaan data pribadi, transaksi tidak sah, pinjaman ilegal, penipuan investasi, dan sengketa konsumen. Oleh karena itu, fintech harus dikembangkan dengan prinsip kehati-hatian, keamanan, transparansi, akuntabilitas, dan perlindungan konsumen.

Dengan demikian, jenis-jenis fintech mencakup pembayaran digital, dompet digital, P2P lending, crowdfunding, investasi digital, robo advisor, insurtech, blockchain, aset kripto, regtech, suptech, dan digital banking. Setiap jenis layanan memiliki karakteristik, manfaat, dan risiko masing-masing. Pemahaman terhadap jenis-jenis fintech penting agar mahasiswa dapat menganalisis hubungan antara teknologi, layanan keuangan, regulasi, perlindungan konsumen, dan risiko hukum dalam ekonomi digital.

12.3 Regulasi Fintech di Indonesia

Regulasi fintech merupakan pengaturan hukum yang digunakan untuk mengawasi, mengarahkan, dan mengendalikan perkembangan layanan keuangan berbasis teknologi. Regulasi ini penting karena fintech tidak hanya menghadirkan kemudahan dan inovasi, tetapi juga membawa risiko hukum, ekonomi, teknologi, dan perlindungan konsumen. Dalam praktiknya, layanan fintech dapat berkaitan dengan pembayaran digital, dompet digital, peer-to-peer lending, crowdfunding, investasi online, aset kripto, digital banking, regtech, suptech, dan berbagai model layanan keuangan digital lainnya.

Gambar 12.3: Regulasi Fintech di Indonesia

Di Indonesia, perkembangan fintech berlangsung sangat cepat seiring meningkatnya penggunaan internet, smartphone, e-commerce, pembayaran non-tunai, dan layanan keuangan digital. Masyarakat dapat melakukan transaksi tanpa harus datang ke kantor bank atau lembaga keuangan. Pelaku usaha juga dapat menggunakan layanan fintech untuk menerima pembayaran, memperoleh modal, mengelola transaksi, dan menjangkau konsumen secara lebih luas. Namun, perkembangan tersebut perlu diatur agar tidak menimbulkan kerugian bagi konsumen dan tidak mengganggu stabilitas sistem keuangan.

Regulasi fintech diperlukan karena layanan keuangan digital menyangkut kepercayaan masyarakat. Konsumen memberikan data pribadi, menyimpan dana, melakukan pembayaran, mengajukan pinjaman, dan berinvestasi melalui sistem elektronik. Jika sistem tersebut tidak aman atau tidak diawasi, konsumen dapat mengalami kerugian. Bentuk kerugian dapat berupa saldo hilang, data pribadi bocor, pinjaman ilegal, bunga tidak transparan, penagihan intimidatif, transaksi tidak sah, dan penipuan investasi.

Purborini et al. (2025) menjelaskan bahwa regulasi fintech di Indonesia penting untuk mengatur perkembangan ekonomi digital, melindungi konsumen, menjaga stabilitas sistem keuangan, serta menciptakan lingkungan bisnis yang sehat. Regulasi yang baik tidak hanya bertujuan membatasi inovasi, tetapi juga memastikan bahwa inovasi fintech berjalan secara bertanggung jawab.

Secara umum, regulasi fintech di Indonesia melibatkan beberapa lembaga penting. Dua lembaga utama yang memiliki peran besar adalah **Bank Indonesia** dan **Otoritas Jasa Keuangan**. Bank Indonesia berwenang dalam bidang sistem pembayaran, stabilitas moneter, dan infrastruktur pembayaran. Sementara itu, Otoritas Jasa Keuangan berwenang dalam pengaturan dan pengawasan sektor jasa keuangan, termasuk layanan keuangan digital tertentu seperti peer-to-peer lending, inovasi teknologi sektor keuangan, dan perlindungan konsumen jasa keuangan.

12.3.1 Peran Bank Indonesia dalam Regulasi Fintech

Bank Indonesia memiliki peran penting dalam mengatur sistem pembayaran digital. Perkembangan pembayaran digital seperti QRIS, BI-FAST, uang elektronik, payment gateway, dan mobile payment membutuhkan pengawasan agar sistem pembayaran berjalan cepat, mudah, murah, aman, dan andal. Dalam ekonomi digital, sistem pembayaran menjadi infrastruktur utama karena hampir semua transaksi digital membutuhkan mekanisme pembayaran elektronik.

Affandi & Iskandar (2025) menjelaskan bahwa Bank Indonesia mengembangkan sistem pembayaran digital melalui berbagai inisiatif, seperti QRIS, BI-FAST, dan SNAP. QRIS menjadi standar pembayaran berbasis kode QR yang memudahkan masyarakat dan pelaku usaha melakukan transaksi. BI-FAST mendukung sistem pembayaran ritel yang instan, aman, dan efisien. Sementara itu, SNAP atau Standar Nasional Open API Pembayaran mendorong keterhubungan antara perbankan dan fintech.

Peran Bank Indonesia dalam regulasi fintech tidak hanya berkaitan dengan inovasi, tetapi juga dengan keamanan dan stabilitas. Sistem pembayaran digital harus dapat dipercaya masyarakat. Jika terjadi gangguan sistem, kebocoran data transaksi, atau transaksi tidak sah, kepercayaan masyarakat terhadap pembayaran digital dapat menurun. Oleh karena itu, regulasi sistem pembayaran perlu memastikan keamanan teknologi, perlindungan konsumen, dan kepatuhan penyelenggara jasa pembayaran.

Dalam konteks hukum teknologi informasi, pengaturan sistem pembayaran digital berkaitan dengan beberapa prinsip. Pertama, transaksi elektronik harus dapat dibuktikan. Kedua, sistem elektronik harus andal dan aman. Ketiga, konsumen harus memperoleh perlindungan apabila terjadi kesalahan

transaksi. Keempat, penyedia layanan harus memiliki tata kelola risiko yang baik. Kelima, data konsumen harus dilindungi sesuai prinsip pelindungan data pribadi.

12.3.2 Peran Otoritas Jasa Keuangan dalam Regulasi Fintech

Otoritas Jasa Keuangan memiliki peran penting dalam mengatur dan mengawasi layanan keuangan digital di sektor jasa keuangan. OJK mengawasi lembaga jasa keuangan dan inovasi teknologi sektor keuangan agar berjalan sesuai prinsip kehati-hatian, transparansi, akuntabilitas, dan perlindungan konsumen. Dalam layanan fintech, OJK berperan dalam pengawasan peer-to-peer lending, perlindungan konsumen jasa keuangan, serta pengaturan inovasi keuangan digital.

Pratiwi & Erniwati (2022) menjelaskan bahwa pemerintah melalui Bank Indonesia dan OJK telah mengeluarkan regulasi teknis terkait teknologi finansial. Salah satu contohnya adalah Peraturan Otoritas Jasa Keuangan tentang layanan pinjam meminjam uang berbasis teknologi informasi. Regulasi seperti ini diperlukan karena banyak fintech bermasalah, baik fintech legal maupun fintech ilegal, terutama dalam kasus pinjaman online, penagihan intimidatif, dan penyebaran data pribadi nasabah.

Dalam fintech P2P lending, OJK memiliki peran untuk memastikan bahwa penyelenggara layanan memiliki izin, mematuhi ketentuan operasional, menjaga data pengguna, mengelola risiko, dan memberikan informasi yang jelas kepada konsumen. P2P lending berbeda dari pinjaman konvensional karena prosesnya dilakukan melalui platform digital. Oleh karena itu, pengawasan tidak hanya menyangkut aspek keuangan, tetapi juga aspek teknologi, keamanan data, dan perilaku penagihan.

Peran OJK juga penting dalam membedakan fintech legal dan fintech ilegal. Fintech legal adalah penyelenggara yang terdaftar atau berizin sesuai ketentuan. Fintech ilegal adalah penyelenggara yang tidak memiliki izin dan sering beroperasi tanpa mengikuti aturan perlindungan konsumen. Fintech ilegal berisiko merugikan masyarakat karena dapat mengenakan bunga tinggi, melakukan penagihan kasar, mengakses data pribadi secara berlebihan, dan menyebarkan informasi pribadi debitur.

Dalam konteks perlindungan konsumen, OJK perlu memastikan bahwa pengguna layanan fintech memperoleh informasi yang benar, jelas, dan tidak

menyesatkan. Konsumen harus mengetahui biaya layanan, bunga, risiko, jangka waktu, denda, mekanisme pengaduan, dan konsekuensi hukum dari transaksi yang dilakukan. Jika informasi tidak transparan, konsumen dapat mengambil keputusan yang merugikan dirinya sendiri.

12.3.3 Regulatory Sandbox dalam Fintech

Regulatory sandbox merupakan salah satu pendekatan penting dalam regulasi fintech. Regulatory sandbox adalah ruang uji coba terbatas yang memungkinkan inovasi fintech diuji dalam lingkungan yang diawasi oleh regulator. Tujuannya adalah agar regulator dapat memahami model bisnis baru, risiko teknologi, dampak terhadap konsumen, dan kebutuhan pengaturan sebelum layanan diterapkan secara luas.

Wibowo (2024) menjelaskan bahwa perkembangan fintech menimbulkan masalah tempo karena teknologi bergerak lebih cepat daripada regulasi. Regulasi yang terlalu lambat dapat membuat hukum tertinggal dari inovasi. Sebaliknya, regulasi yang terlalu kaku dapat menghambat inovasi. Oleh karena itu, pendekatan adaptif seperti regulatory sandbox diperlukan agar inovasi tetap dapat berkembang, tetapi tetap berada dalam pengawasan.

Regulatory sandbox memiliki beberapa manfaat. Pertama, membantu regulator memahami inovasi fintech secara langsung. Kedua, memberikan ruang bagi pelaku usaha untuk menguji layanan baru tanpa langsung diterapkan secara luas. Ketiga, membantu mengidentifikasi risiko sebelum konsumen terdampak secara besar. Keempat, mendorong pembentukan regulasi yang lebih sesuai dengan karakter teknologi. Kelima, mempertemukan kepentingan inovasi dan perlindungan konsumen.

Namun, regulatory sandbox juga memiliki tantangan. Jika kriteria masuk terlalu rumit, pelaku usaha kecil akan sulit mengaksesnya. Jika pengawasan terlalu lemah, konsumen dapat tetap dirugikan. Jika mekanisme setelah sandbox tidak jelas, inovasi yang telah diuji dapat berhenti tanpa kepastian. Oleh karena itu, regulatory sandbox harus memiliki prosedur yang jelas, pengawasan yang memadai, perlindungan konsumen, dan mekanisme evaluasi.

12.3.4 Regulasi Fintech dan Perlindungan Konsumen

Salah satu tujuan utama regulasi fintech adalah melindungi konsumen. Konsumen fintech sering berada pada posisi yang lebih lemah dibandingkan penyedia layanan. Konsumen tidak selalu memahami teknologi, risiko produk keuangan, bunga, biaya, algoritma, kebijakan privasi, dan syarat layanan. Oleh sebab itu, regulasi perlu memastikan bahwa penyedia fintech bertanggung jawab atas layanan yang diberikan.

Perlindungan konsumen dalam fintech mencakup beberapa aspek berikut.

1. **Transparansi informasi**

   Penyelenggara fintech harus memberikan informasi yang jelas mengenai produk, biaya, bunga, risiko, jangka waktu, denda, dan mekanisme pengaduan.

2. **Keamanan transaksi**

   Sistem fintech harus dilengkapi pengamanan yang memadai untuk mencegah transaksi tidak sah, pencurian akun, phishing, dan penyalahgunaan data.

3. **Pelindungan data pribadi**

   Data pengguna harus dikumpulkan, digunakan, dan disimpan secara sah, terbatas, transparan, dan bertanggung jawab.

4. **Pengaduan dan penyelesaian sengketa**

   Konsumen harus memiliki akses terhadap mekanisme komplain, mediasi, refund, pemulihan akun, atau jalur hukum jika terjadi kerugian.

5. **Pencegahan praktik tidak etis**

   Penyelenggara fintech tidak boleh melakukan penagihan intimidatif, menggunakan informasi menyesatkan, menyembunyikan biaya, atau menyalahgunakan akses data.

6. **Pengawasan terhadap fintech ilegal**

   Pemerintah dan regulator perlu mencegah fintech ilegal agar tidak merugikan masyarakat.

Dalam kasus pinjaman online, perlindungan konsumen menjadi sangat penting karena banyak masyarakat menggunakan layanan ini dalam kondisi mendesak. Jika konsumen tidak memahami bunga, denda, risiko

keterlambatan, dan akses data aplikasi, maka konsumen dapat terjebak dalam masalah hukum dan ekonomi. Oleh sebab itu, regulasi fintech perlu dibarengi dengan literasi keuangan digital.

12.3.5 Tantangan Regulasi Fintech di Indonesia

Regulasi fintech di Indonesia menghadapi beberapa tantangan. Tantangan pertama adalah kecepatan perkembangan teknologi. Inovasi fintech berkembang lebih cepat daripada pembentukan regulasi. Model bisnis baru dapat muncul sebelum aturan hukumnya tersedia. Contohnya adalah perkembangan aset kripto, blockchain, paylater, artificial intelligence dalam penilaian kredit, dan layanan keuangan berbasis data.

Tantangan kedua adalah kompleksitas model bisnis fintech. Banyak layanan fintech melibatkan berbagai pihak, seperti platform, bank, penyedia pembayaran, penyedia teknologi, investor, debitur, konsumen, dan pihak ketiga pengelola data. Kompleksitas ini membuat tanggung jawab hukum tidak selalu mudah ditentukan.

Tantangan ketiga adalah fintech ilegal. Layanan fintech ilegal dapat muncul dan menyebar melalui aplikasi, website, media sosial, atau pesan pribadi. Fintech ilegal sering sulit diawasi karena dapat berganti nama, berpindah platform, atau beroperasi dari luar wilayah Indonesia. Hal ini menuntut kerja sama antara regulator, aparat penegak hukum, penyedia aplikasi, dan masyarakat.

Tantangan keempat adalah pelindungan data pribadi. Layanan fintech memproses data sensitif, seperti identitas, nomor telepon, alamat, rekening, riwayat transaksi, data pekerjaan, lokasi, bahkan kontak pengguna. Jika data tersebut disalahgunakan, konsumen dapat mengalami kerugian serius. Oleh karena itu, penerapan Undang-Undang Pelindungan Data Pribadi menjadi penting dalam sektor fintech.

Tantangan kelima adalah rendahnya literasi keuangan digital. Banyak pengguna fintech belum memahami cara membedakan layanan legal dan ilegal, risiko pinjaman online, keamanan OTP, biaya layanan, bunga, dan syarat kontrak digital. Rendahnya literasi membuat masyarakat mudah menjadi korban penipuan atau layanan tidak bertanggung jawab.

Tantangan keenam adalah pengawasan lintas sektor. Fintech berada di persimpangan antara sektor keuangan, teknologi informasi, perlindungan konsumen, data pribadi, keamanan siber, dan transaksi elektronik. Oleh karena itu, regulasi fintech membutuhkan koordinasi antara berbagai lembaga, seperti OJK, Bank Indonesia, Kominfo, Bappebti, PPATK, kepolisian, dan lembaga perlindungan konsumen.

12.3.6 Prinsip-Prinsip Regulasi Fintech

Agar regulasi fintech berjalan efektif, terdapat beberapa prinsip yang perlu diperhatikan.

1. **Prinsip kehati-hatian**

   Penyelenggara fintech harus mengelola risiko dengan baik, terutama risiko teknologi, keuangan, data pribadi, dan perlindungan konsumen.

2. **Prinsip transparansi**

   Informasi layanan harus disampaikan secara jelas dan mudah dipahami oleh pengguna.

3. **Prinsip akuntabilitas**

   Penyelenggara fintech harus dapat mempertanggungjawabkan sistem, keputusan, penggunaan data, dan penyelesaian masalah konsumen.

4. **Prinsip keamanan sistem**

   Sistem elektronik harus dirancang untuk mencegah akses ilegal, transaksi tidak sah, gangguan sistem, dan kebocoran data.

5. **Prinsip perlindungan konsumen**

   Konsumen harus dilindungi dari praktik tidak adil, informasi menyesatkan, penyalahgunaan data, dan layanan ilegal.

6. **Prinsip inovasi yang bertanggung jawab**

   Regulasi tidak boleh mematikan inovasi, tetapi inovasi juga tidak boleh mengabaikan hak konsumen dan stabilitas sistem keuangan.

7. **Prinsip adaptif**

   Regulasi perlu mampu menyesuaikan diri dengan perubahan teknologi dan model bisnis fintech.

Tabel berikut merangkum aspek penting regulasi fintech di Indonesia.

Tabel 12.3: Aspek Regulasi Fintech di Indonesia

Aspek Regulasi	Penjelasan	Contoh Penerapan
Sistem pembayaran	Pengaturan layanan pembayaran digital	QRIS, BI-FAST, payment gateway, uang elektronik
P2P lending	Pengawasan pinjam meminjam berbasis platform	Izin penyelenggara, batas bunga, penagihan, perlindungan data
Perlindungan konsumen	Perlindungan pengguna layanan fintech	Informasi transparan, pengaduan, penyelesaian sengketa
Pelindungan data pribadi	Pengaturan pemrosesan data pengguna	Persetujuan, pembatasan akses, keamanan data
Regulatory sandbox	Uji coba inovasi fintech dalam pengawasan	Pengujian model bisnis baru sebelum diterapkan luas
Keamanan sistem	Pengamanan sistem elektronik dan transaksi	Autentikasi, enkripsi, deteksi transaksi mencurigakan
Pengawasan fintech ilegal	Pencegahan layanan tidak berizin	Pemblokiran aplikasi, edukasi masyarakat, penindakan hukum
Koordinasi lembaga	Kerja sama regulator dan aparat	OJK, BI, Kominfo, PPATK, kepolisian

Regulasi fintech harus mampu menjaga keseimbangan antara inovasi dan perlindungan. Jika regulasi terlalu longgar, konsumen dapat dirugikan oleh layanan tidak bertanggung jawab. Jika regulasi terlalu ketat, inovasi dapat terhambat dan pelaku usaha sulit berkembang. Oleh sebab itu, pendekatan yang paling tepat adalah regulasi yang adaptif, berbasis risiko, dan berorientasi pada perlindungan masyarakat.

Dalam konteks hukum teknologi informasi, regulasi fintech memiliki peran strategis. Fintech mempertemukan hukum keuangan, hukum transaksi elektronik, hukum perlindungan konsumen, hukum pelindungan data pribadi, dan hukum keamanan siber. Oleh karena itu, analisis terhadap fintech tidak dapat dilakukan hanya dari sisi bisnis, tetapi juga harus memperhatikan norma hukum dan tanggung jawab penyelenggara sistem elektronik.

Dengan demikian, regulasi fintech di Indonesia merupakan bagian penting dari tata kelola ekonomi digital. Regulasi ini bertujuan melindungi konsumen, menjaga keamanan transaksi, mengawasi pelaku usaha, mencegah fintech ilegal, melindungi data pribadi, dan menjaga stabilitas sistem keuangan. Peran Bank Indonesia dan OJK sangat penting dalam

mengatur sistem pembayaran, layanan keuangan digital, dan perlindungan konsumen. Di sisi lain, masyarakat juga perlu meningkatkan literasi keuangan digital agar dapat menggunakan layanan fintech secara aman dan bertanggung jawab.

12.4 Perlindungan Pengguna Layanan Keuangan Digital

Pelindungan data pribadi dan keamanan transaksi merupakan aspek penting dalam layanan fintech. Fintech tidak hanya menyediakan layanan keuangan berbasis teknologi, tetapi juga mengelola data pengguna, memproses transaksi elektronik, menyimpan riwayat pembayaran, dan menghubungkan konsumen dengan berbagai layanan keuangan digital. Oleh karena itu, layanan fintech harus dibangun dengan sistem yang aman, transparan, dan bertanggung jawab.

Gambar 12.4: Perlindungan Pengguna Layanan Keuangan Digital

Dalam layanan fintech, data pribadi menjadi unsur utama. Pengguna biasanya diminta memberikan data seperti nama, nomor telepon, alamat email, nomor identitas, foto KTP, swafoto, alamat tempat tinggal, nomor rekening, lokasi, pekerjaan, penghasilan, riwayat transaksi, hingga data kontak tertentu. Data tersebut digunakan untuk proses registrasi, verifikasi identitas, penilaian risiko, pembayaran, pemberian pinjaman, pencegahan penipuan, dan pengelolaan layanan.

Affandi dan Iskandar (2025) menjelaskan bahwa data merupakan aset penting dalam ekonomi dan keuangan digital karena dapat digunakan untuk mendukung pengambilan keputusan, inovasi layanan, pengawasan, dan pengembangan sistem keuangan digital. Namun, penggunaan data dalam fintech harus tetap memperhatikan perlindungan konsumen dan prinsip kehati-hatian. Data yang tidak dikelola dengan benar dapat menimbulkan kerugian serius bagi pengguna.

Pelindungan data pribadi dalam fintech menjadi semakin penting karena layanan keuangan digital memproses data yang sensitif. Jika data tersebut bocor, dijual, disalahgunakan, atau diakses tanpa izin, konsumen dapat mengalami kerugian finansial, pencurian identitas, penagihan tidak wajar, penipuan, atau gangguan privasi. Oleh karena itu, penyelenggara fintech wajib memastikan bahwa data pribadi pengguna hanya dikumpulkan dan digunakan untuk tujuan yang sah.

Dalam konteks hukum Indonesia, pelindungan data pribadi berkaitan dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang ini memberikan dasar bahwa pemrosesan data pribadi harus dilakukan secara sah, terbatas, transparan, akurat, aman, dan bertanggung jawab. Dalam layanan fintech, prinsip tersebut berarti penyelenggara tidak boleh mengambil data secara berlebihan, menggunakan data di luar tujuan layanan, atau membagikan data kepada pihak lain tanpa dasar hukum yang jelas.

Pratiwi & Erniwati (2022) menunjukkan bahwa salah satu masalah serius dalam layanan fintech, terutama pinjaman online, adalah penyebaran data pribadi nasabah dan penagihan yang bersifat intimidatif. Hal ini menunjukkan bahwa pelindungan data pribadi tidak hanya berkaitan dengan keamanan teknologi, tetapi juga dengan etika bisnis, kepatuhan hukum, dan perlindungan martabat konsumen.

12.4.1 Jenis Data Pribadi dalam Layanan Fintech

Data pribadi dalam layanan fintech dapat dibedakan menjadi beberapa jenis. Pembagian ini penting agar mahasiswa memahami bahwa data dalam fintech tidak hanya berupa nama atau nomor identitas, tetapi juga mencakup data perilaku dan transaksi digital.

1. **Data identitas**

   Data ini mencakup nama, nomor induk kependudukan, foto KTP, swafoto, tanggal lahir, alamat, dan informasi pribadi lain yang digunakan untuk mengenali pengguna.

2. **Data kontak**

   Data ini mencakup nomor telepon, email, alamat rumah, kontak darurat, dan informasi komunikasi lainnya.

3. **Data keuangan**

   Data ini mencakup nomor rekening, saldo, riwayat pembayaran, transaksi masuk dan keluar, pinjaman, tagihan, dan informasi finansial pengguna.

4. **Data perangkat dan akses**

   Data ini mencakup alamat IP, jenis perangkat, lokasi akses, waktu login, sistem operasi, dan identitas perangkat.

5. **Data perilaku digital**

   Data ini mencakup pola transaksi, kebiasaan pembayaran, riwayat penggunaan aplikasi, preferensi layanan, dan data aktivitas pengguna.

6. **Data risiko dan kelayakan kredit**

   Dalam layanan pinjaman digital, data pengguna dapat dianalisis untuk menilai kemampuan membayar, risiko kredit, dan profil keuangan.

Wibowo (2024) menjelaskan bahwa fintech memanfaatkan teknologi untuk menyediakan layanan atau produk keuangan, termasuk pembayaran online, integrasi data keuangan konsumen, pinjaman digital, blockchain, dan inovasi keuangan lainnya. Karena itu, data menjadi elemen utama dalam penyelenggaraan fintech. Semakin banyak layanan yang berbasis data, semakin besar pula tanggung jawab penyelenggara untuk menjaga keamanan dan legalitas pemrosesan data.

12.4.2 Prinsip Pelindungan data pribadi dalam Fintech

Pelindungan data pribadi dalam fintech harus mengikuti beberapa prinsip dasar. Prinsip-prinsip ini penting agar pemrosesan data tidak merugikan konsumen.

1. **Prinsip legalitas**

   Data pribadi harus diproses berdasarkan dasar hukum yang sah. Penyelenggara fintech tidak boleh mengambil atau menggunakan data tanpa alasan yang jelas dan dibenarkan hukum.

2. **Prinsip persetujuan**

   Pengguna harus mengetahui data apa yang dikumpulkan, untuk tujuan apa data digunakan, dan kepada siapa data dapat dibagikan. Persetujuan tidak boleh diperoleh melalui informasi yang membingungkan.

3. **Prinsip pembatasan tujuan**

   Data hanya boleh digunakan untuk tujuan yang telah dijelaskan kepada pengguna. Misalnya, data untuk verifikasi identitas tidak boleh digunakan sembarangan untuk promosi atau disebarkan ke pihak lain.

4. **Prinsip minimalisasi data**

   Penyelenggara fintech hanya boleh mengumpulkan data yang benar-benar diperlukan. Pengumpulan data yang berlebihan dapat meningkatkan risiko penyalahgunaan.

5. **Prinsip keamanan**

   Data harus dilindungi dengan sistem keamanan yang memadai, seperti enkripsi, autentikasi, pembatasan akses, dan audit keamanan.

6. **Prinsip akuntabilitas**

   Penyelenggara fintech harus dapat mempertanggungjawabkan bagaimana data dikumpulkan, disimpan, digunakan, dibagikan, dan dihapus.

7. **Prinsip hak pengguna**

   Pengguna berhak mengetahui, memperbaiki, menarik persetujuan, dan meminta penghapusan data sesuai ketentuan hukum.

Affandi dan Iskandar (2025) menekankan bahwa dalam ekonomi keuangan digital, pemanfaatan data harus diimbangi dengan tata kelola yang baik, keamanan, pengawasan, dan perlindungan konsumen. Dengan demikian, pelindungan data pribadi dalam fintech tidak boleh dianggap sebagai urusan administratif semata, tetapi sebagai bagian dari kepercayaan publik terhadap sistem keuangan digital.

12.4.3 Keamanan Transaksi Digital dalam Fintech

Selain pelindungan data pribadi, keamanan transaksi digital juga menjadi aspek utama dalam fintech. Transaksi fintech dilakukan melalui sistem elektronik, sehingga risiko yang muncul berbeda dari transaksi konvensional. Dalam transaksi digital, pengguna dapat mengalami pencurian akun, penyalahgunaan OTP, phishing, transaksi tidak sah, saldo hilang, kesalahan transfer, atau kegagalan sistem.

Keamanan transaksi fintech mencakup perlindungan terhadap dana, akun, data, sistem pembayaran, dan bukti transaksi. Penyelenggara fintech harus memastikan bahwa setiap transaksi dapat diverifikasi, dicatat, dilacak, dan dipulihkan apabila terjadi masalah. Sistem yang tidak aman dapat menimbulkan kerugian finansial dan menurunkan kepercayaan masyarakat terhadap layanan fintech.

Raharjo (2021) menjelaskan bahwa perkembangan fintech dan perbankan digital mengubah cara masyarakat melakukan transaksi keuangan. Pembayaran non-tunai, aplikasi seluler, dompet digital, cryptocurrency, dan perbankan digital membuat transaksi semakin cepat dan praktis. Namun, perubahan ini juga menuntut perhatian terhadap keamanan sistem dan risiko kejahatan digital.

Keamanan transaksi fintech dapat dilakukan melalui beberapa mekanisme berikut.

1. **Autentikasi pengguna**

   Sistem harus memastikan bahwa orang yang melakukan transaksi adalah pengguna yang sah. Contohnya melalui PIN, password, OTP, biometrik, atau autentikasi dua faktor.

2. **Enkripsi data**

   Data transaksi perlu dilindungi agar tidak mudah dibaca atau diambil oleh pihak yang tidak berwenang.

3. **Pemantauan transaksi mencurigakan**

   Sistem perlu mendeteksi transaksi yang tidak biasa, seperti login dari lokasi asing, transaksi besar mendadak, atau percobaan akses berulang.

4. Notifikasi transaksi

   Pengguna perlu memperoleh pemberitahuan setiap kali terjadi transaksi agar dapat segera mengetahui aktivitas mencurigakan.

5. **Pembatasan akses internal**

   Tidak semua pegawai atau pihak ketiga boleh mengakses data konsumen. Akses harus dibatasi sesuai kebutuhan.

6. **Audit dan pengujian keamanan**

   Sistem fintech perlu diuji secara berkala untuk menemukan celah keamanan.

7. **Pemulihan layanan**

   Jika terjadi gangguan, penyelenggara harus memiliki prosedur pemulihan dan penyelesaian pengaduan.

12.4.4 Ancaman terhadap Data dan Transaksi Fintech

Ancaman terhadap data dan transaksi fintech dapat berasal dari berbagai pihak. Ancaman dapat dilakukan oleh peretas, pelaku penipuan, oknum internal, aplikasi ilegal, atau pihak ketiga yang menyalahgunakan akses. Ancaman juga dapat muncul karena kelalaian pengguna, seperti membagikan OTP, menggunakan password lemah, atau mengklik tautan palsu.

Beberapa ancaman utama dalam layanan fintech antara lain sebagai berikut.

1. **Phishing**

   Pelaku membuat tautan atau halaman palsu yang menyerupai layanan resmi untuk mencuri data login, OTP, atau informasi keuangan.

2. **Social engineering**

   Pelaku memanipulasi psikologis korban agar memberikan informasi rahasia, seperti PIN, password, atau kode verifikasi.

3. **Akses ilegal**

   Pihak tidak berwenang masuk ke akun pengguna atau sistem penyelenggara fintech.

4. **Malware**

   Perangkat pengguna dapat disusupi aplikasi berbahaya yang mencuri data atau mengendalikan aktivitas transaksi.

5. **Kebocoran data**

   Data pengguna dapat bocor karena kelemahan sistem, kelalaian pengelolaan, atau serangan siber.

6. **Penyalahgunaan data oleh pihak ketiga**

   Data yang diberikan kepada mitra atau pihak ketiga dapat digunakan di luar tujuan yang disepakati.

7. **Aplikasi fintech ilegal**

   Aplikasi tidak berizin dapat mengumpulkan data secara berlebihan dan menggunakannya untuk penagihan atau penipuan.

Purborini et al. (2025) menjelaskan bahwa regulasi fintech diperlukan untuk memastikan perlindungan konsumen, mitigasi risiko, dan kepatuhan perusahaan fintech terhadap tata kelola yang baik. Ancaman terhadap data dan transaksi menunjukkan bahwa fintech harus diawasi tidak hanya dari aspek keuangan, tetapi juga dari aspek teknologi dan perlindungan konsumen.

12.4.5 Tanggung Jawab Penyelenggara Fintech

Penyelenggara fintech memiliki tanggung jawab besar dalam melindungi data pribadi dan keamanan transaksi konsumen. Tanggung jawab ini tidak hanya muncul setelah terjadi kerugian, tetapi sejak tahap perancangan sistem, pendaftaran pengguna, pemrosesan transaksi, penyimpanan data, hingga penyelesaian sengketa.

Tanggung jawab penyelenggara fintech mencakup beberapa hal berikut.

1. **Menyediakan sistem yang aman**

   Sistem harus dirancang untuk mencegah akses ilegal, transaksi tidak sah, dan kebocoran data.

2. **Menyampaikan informasi secara transparan**

   Pengguna harus mengetahui syarat layanan, biaya, risiko, kebijakan privasi, dan mekanisme pengaduan.

3. **Memproses data sesuai hukum**

   Data pengguna harus diproses sesuai prinsip pelindungan data pribadi.

4. **Membatasi akses data**

   Data konsumen tidak boleh diakses oleh pihak yang tidak berkepentingan.

5. **Menangani pengaduan konsumen**

   Jika terjadi transaksi bermasalah, penyelenggara harus menyediakan jalur pengaduan yang mudah dan responsif.

6. **Memberikan pemulihan apabila terjadi kerugian**

   Jika kerugian terjadi karena kesalahan sistem atau kelalaian penyelenggara, konsumen berhak memperoleh penyelesaian yang adil.

7. **Melakukan edukasi kepada pengguna**

   Penyelenggara perlu memberi peringatan mengenai phishing, OTP, tautan palsu, dan keamanan akun.

Pratiwi & Erniwati (2022) menekankan bahwa perlindungan hukum terhadap nasabah fintech diperlukan karena layanan fintech dapat menimbulkan risiko seperti penyalahgunaan data dan praktik penagihan yang tidak sesuai. Oleh sebab itu, penyelenggara fintech harus bertanggung jawab tidak hanya terhadap kelancaran layanan, tetapi juga terhadap hak dan keamanan konsumennya.

12.4.6 Peran Konsumen dalam Menjaga Keamanan

Keamanan fintech tidak hanya bergantung pada penyelenggara layanan. Konsumen juga memiliki peran penting dalam menjaga keamanan akun, data pribadi, dan transaksi. Banyak kasus kerugian terjadi karena pengguna tidak berhati-hati, membagikan OTP, menggunakan password yang mudah ditebak, mengunduh aplikasi tidak resmi, atau mempercayai tautan palsu.

Konsumen perlu memahami bahwa data seperti OTP, PIN, password, kode verifikasi, dan akses akun tidak boleh diberikan kepada siapa pun. Pihak resmi penyelenggara fintech tidak akan meminta kode rahasia tersebut melalui telepon, pesan singkat, atau media sosial. Konsumen juga harus berhati-hati terhadap akun layanan pelanggan palsu yang mengatasnamakan platform resmi.

Raharjo (2021) menjelaskan bahwa perkembangan perbankan digital dan fintech membuat layanan keuangan semakin mobile dan mudah diakses. Kemudahan ini harus diimbangi dengan kesadaran pengguna dalam menjaga keamanan transaksi. Dalam ruang digital, kelalaian kecil seperti mengklik tautan palsu dapat menimbulkan kerugian besar.

Beberapa langkah yang perlu dilakukan konsumen antara lain:

1. menggunakan aplikasi resmi;
2. tidak membagikan OTP, PIN, dan password;
3. mengaktifkan autentikasi dua faktor;
4. menggunakan password yang kuat;
5. tidak mengklik tautan mencurigakan;
6. memeriksa legalitas penyelenggara fintech;
7. membaca kebijakan privasi dan syarat layanan;
8. menyimpan bukti transaksi;
9. segera melapor jika ada transaksi mencurigakan;
10. memperbarui aplikasi secara berkala.

Dengan perilaku yang hati-hati, konsumen dapat membantu mengurangi risiko penyalahgunaan data dan transaksi tidak sah.

12.4.7 Perlindungan Data dan Keamanan sebagai Dasar Kepercayaan

Kepercayaan adalah fondasi utama dalam layanan fintech. Konsumen bersedia menggunakan dompet digital, pembayaran online, pinjaman digital, atau investasi digital karena percaya bahwa sistem tersebut aman dan dapat diandalkan. Jika terjadi banyak kasus kebocoran data, saldo hilang, atau transaksi tidak sah, kepercayaan masyarakat terhadap fintech dapat menurun.

Perlindungan data dan keamanan transaksi menjadi dasar bagi keberlanjutan ekosistem fintech. Penyelenggara fintech yang memiliki sistem keamanan baik akan lebih dipercaya oleh konsumen. Sebaliknya, penyelenggara yang mengabaikan keamanan dapat kehilangan reputasi dan menghadapi tanggung jawab hukum.

Wibowo (2024) menjelaskan bahwa fintech membawa manfaat dan risiko, sehingga diperlukan regulasi adaptif untuk mengatasi kompleksitas pasar keuangan modern. Dalam konteks perlindungan data dan keamanan transaksi, regulasi yang adaptif harus mampu mengatur risiko baru tanpa menghambat inovasi. Hal ini penting agar fintech tetap berkembang, tetapi tidak mengorbankan hak konsumen.

Tabel berikut merangkum hubungan antara aspek perlindungan data, risiko, dan bentuk pengamanan dalam fintech.

Tabel 12.4: Perlindungan Data dan Keamanan Transaksi Fintech

Aspek	Risiko yang Muncul	Bentuk Perlindungan
Data identitas	Pencurian identitas, pinjaman palsu	Verifikasi identitas dan pembatasan akses
Data kontak	Penagihan intimidatif, penyebaran data	Persetujuan eksplisit dan pembatasan penggunaan
Data keuangan	Penipuan, transaksi tidak sah	Enkripsi dan autentikasi berlapis
Akun pengguna	Peretasan akun, pengambilalihan akses	Password kuat, OTP, biometrik
Transaksi digital	Saldo hilang, transaksi gagal	Notifikasi, audit transaksi, pusat bantuan
Sistem aplikasi	Serangan siber, gangguan layanan	Audit keamanan dan pemantauan sistem
Pihak ketiga	Penyalahgunaan data oleh mitra	Perjanjian pemrosesan data dan pengawasan
Pengaduan konsumen	Sengketa tidak selesai	Mekanisme komplain dan penyelesaian sengketa

Pelindungan data pribadi dan keamanan transaksi harus menjadi bagian dari desain awal layanan fintech. Prinsip ini dikenal sebagai pendekatan keamanan sejak perancangan atau security by design. Artinya, keamanan tidak boleh ditambahkan setelah masalah terjadi, tetapi harus menjadi bagian dari sistem sejak awal. Demikian pula, pelindungan data pribadi harus diterapkan sejak proses pengumpulan data, bukan hanya setelah data bocor.

Dengan demikian, pelindungan data pribadi dan keamanan transaksi fintech merupakan aspek fundamental dalam hukum fintech dan ekonomi digital. Layanan fintech membutuhkan data dan sistem elektronik untuk berjalan, tetapi penggunaan data dan teknologi harus dilakukan secara bertanggung

jawab. Penyelenggara fintech harus menjaga keamanan sistem, melindungi data pribadi, memberi informasi yang transparan, dan menyediakan mekanisme pengaduan. Konsumen juga perlu menjaga keamanan akunnya sendiri. Jika perlindungan data dan keamanan transaksi berjalan baik, maka kepercayaan masyarakat terhadap fintech akan semakin kuat.

12.5 Risiko Hukum dalam Pinjaman Online dan Pembayaran Digital

Perkembangan fintech memberikan banyak manfaat bagi masyarakat, pelaku usaha, dan sektor keuangan. Melalui fintech, masyarakat dapat melakukan pembayaran digital, mengajukan pinjaman, berinvestasi, membeli produk keuangan, menggunakan dompet digital, dan mengakses layanan perbankan tanpa harus datang langsung ke kantor fisik. Fintech juga mendorong efisiensi, memperluas inklusi keuangan, mempercepat transaksi, dan mendukung pertumbuhan ekonomi digital.

Gambar 12.5: Risiko Hukum dan Perlindungan Konsumen dalam Fintech

Namun, di balik manfaat tersebut, fintech juga membawa berbagai risiko hukum. Risiko ini muncul karena layanan fintech dijalankan melalui sistem elektronik, menggunakan data pribadi, melibatkan transaksi keuangan, dan sering kali diakses oleh masyarakat yang belum sepenuhnya memahami risiko layanan digital. Oleh karena itu, perlindungan konsumen menjadi bagian penting dalam pengaturan fintech.

Risiko hukum dalam fintech tidak hanya berkaitan dengan kerugian uang, tetapi juga dapat berkaitan dengan penyalahgunaan data pribadi, transaksi tidak sah, penipuan digital, kegagalan sistem, pelanggaran kontrak elektronik, pinjaman online ilegal, penagihan intimidatif, serta kurangnya transparansi informasi. Pratiwi & Erniwati (2022) menjelaskan bahwa perkembangan fintech, terutama peer-to-peer lending, menimbulkan persoalan seperti fintech ilegal, penagihan yang mengintimidasi, dan penyebaran data pribadi nasabah. Hal ini menunjukkan bahwa fintech membutuhkan pengawasan dan perlindungan hukum yang kuat.

Purborini et al. (2025) juga menjelaskan bahwa regulasi fintech di Indonesia penting untuk melindungi konsumen, memitigasi risiko layanan keuangan digital, menjaga stabilitas sistem keuangan, dan menciptakan lingkungan bisnis yang sehat. Dengan demikian, perlindungan konsumen fintech harus dipahami sebagai bagian dari tata kelola ekonomi digital yang bertanggung jawab.

12.5.1 Risiko Penyalahgunaan Data Pribadi

Salah satu risiko terbesar dalam layanan fintech adalah penyalahgunaan data pribadi. Untuk menggunakan layanan fintech, konsumen biasanya diminta memberikan data seperti nama, nomor telepon, alamat, email, nomor identitas, foto KTP, swafoto, rekening bank, lokasi, kontak darurat, riwayat transaksi, dan data pekerjaan. Data tersebut digunakan untuk verifikasi identitas, analisis risiko, pemrosesan transaksi, atau penilaian kelayakan pinjaman.

Masalah muncul ketika data tersebut dikumpulkan secara berlebihan, digunakan tanpa persetujuan yang jelas, disebarkan kepada pihak ketiga, atau bocor akibat lemahnya keamanan sistem. Dalam kasus pinjaman online ilegal, penyalahgunaan data sering terjadi melalui akses kontak, galeri, pesan, atau informasi pribadi pengguna. Data tersebut kemudian dapat digunakan untuk menekan, mempermalukan, atau mengintimidasi konsumen yang terlambat membayar.

Pelindungan data pribadi menjadi sangat penting karena data konsumen fintech bersifat sensitif. Apabila data keuangan dan identitas disalahgunakan, konsumen dapat mengalami kerugian ekonomi, pencemaran nama baik, penipuan identitas, dan gangguan psikologis. Oleh karena itu, penyelenggara

fintech wajib memproses data pribadi secara sah, terbatas, transparan, aman, dan bertanggung jawab.

12.5.2 Risiko Transaksi Tidak Sah dan Keamanan Sistem

Risiko lain dalam fintech adalah transaksi tidak sah. Transaksi tidak sah dapat terjadi karena akun pengguna diretas, OTP diberikan kepada pihak lain, pengguna terkena phishing, sistem aplikasi disusupi, atau terdapat kelemahan dalam sistem keamanan. Dalam layanan pembayaran digital dan dompet digital, risiko ini dapat menyebabkan saldo hilang, transaksi gagal, transfer tidak dikenal, atau dana berpindah tanpa izin pengguna.

Keamanan sistem menjadi tanggung jawab penting bagi penyelenggara fintech. Sistem fintech harus memiliki mekanisme autentikasi, enkripsi, deteksi transaksi mencurigakan, perlindungan akun, notifikasi transaksi, dan prosedur pemulihan apabila terjadi gangguan. Konsumen juga perlu menjaga keamanan akun dengan tidak membagikan OTP, PIN, password, kode verifikasi, atau data login kepada siapa pun.

Dalam konteks hukum, transaksi tidak sah dapat menimbulkan pertanyaan mengenai tanggung jawab. Perlu dianalisis apakah kerugian terjadi karena kelalaian pengguna, kelemahan sistem penyelenggara, serangan pihak ketiga, atau tindakan penipuan. Oleh karena itu, penyelesaian sengketa fintech harus memperhatikan bukti digital, riwayat transaksi, log sistem, dan kronologi kejadian.

12.5.3 Risiko Pinjaman Online Ilegal

Pinjaman online atau peer-to-peer lending merupakan salah satu layanan fintech yang paling banyak menimbulkan persoalan hukum. Pada dasarnya, layanan ini dapat membantu masyarakat memperoleh akses pembiayaan secara cepat. Namun, risiko muncul ketika layanan tersebut tidak berizin, tidak transparan, mengenakan bunga tinggi, menggunakan metode penagihan kasar, dan menyalahgunakan data pribadi.

Pinjaman online ilegal sering menawarkan proses pencairan yang cepat tanpa menjelaskan bunga, biaya, denda, dan risiko keterlambatan secara jelas. Konsumen yang sedang membutuhkan uang dapat tergoda menggunakan layanan tersebut tanpa memahami konsekuensinya. Setelah terjadi keterlambatan, konsumen dapat mengalami tekanan melalui pesan

intimidatif, penyebaran data pribadi, ancaman, atau kontak kepada keluarga dan rekan kerja.

Perlindungan konsumen terhadap pinjaman online ilegal perlu dilakukan melalui beberapa cara. Pertama, masyarakat harus memeriksa legalitas penyelenggara fintech melalui kanal resmi OJK. Kedua, konsumen perlu membaca syarat pinjaman, bunga, biaya, dan denda. Ketiga, pemerintah dan regulator perlu menindak aplikasi ilegal. Keempat, platform distribusi aplikasi perlu mencegah penyebaran aplikasi pinjaman ilegal. Kelima, literasi keuangan digital perlu diperkuat agar masyarakat tidak mudah terjebak.

12.5.4 Risiko Informasi yang Tidak Transparan

Dalam layanan fintech, informasi yang tidak transparan dapat merugikan konsumen. Informasi yang dimaksud meliputi biaya layanan, bunga, denda, risiko investasi, mekanisme pengaduan, kebijakan privasi, syarat kontrak, dan konsekuensi penggunaan layanan. Konsumen sering kali hanya menekan tombol "setuju" tanpa membaca seluruh syarat dan ketentuan.

Ketidakjelasan informasi dapat menimbulkan sengketa. Misalnya, konsumen merasa tidak mengetahui adanya biaya admin, bunga harian, denda keterlambatan, biaya penarikan dana, atau syarat pengembalian dana. Dalam investasi digital, konsumen dapat mengalami kerugian karena tidak memahami risiko produk yang dibeli. Dalam dompet digital, konsumen dapat kesulitan memperoleh refund karena syarat layanan tidak dipahami sejak awal.

Oleh sebab itu, penyelenggara fintech wajib memberikan informasi yang benar, jelas, jujur, dan mudah dipahami. Informasi tidak boleh disembunyikan dalam dokumen panjang yang sulit dibaca. Prinsip transparansi menjadi syarat penting dalam perlindungan konsumen fintech.

12.5.5 Risiko Penipuan dan Kejahatan Siber

Fintech juga rentan terhadap penipuan dan kejahatan siber. Bentuknya dapat berupa phishing, tautan palsu, akun layanan pelanggan palsu, aplikasi palsu, investasi bodong, penipuan top up, penipuan paylater, pencurian OTP, dan pengambilalihan akun. Pelaku kejahatan sering memanfaatkan

ketidaktahuan konsumen dan tampilan digital yang menyerupai layanan resmi.

Kejahatan siber dalam fintech dapat dilakukan secara cepat, lintas wilayah, dan menggunakan identitas palsu. Hal ini membuat penegakan hukum menjadi lebih sulit. Bukti yang digunakan pun umumnya berupa bukti elektronik, seperti tangkapan layar, riwayat transaksi, log akses, percakapan digital, email, dan data akun.

Untuk mencegah risiko tersebut, penyelenggara fintech perlu meningkatkan keamanan sistem dan edukasi pengguna. Konsumen juga harus berhati-hati terhadap tautan mencurigakan, akun palsu, tawaran investasi dengan keuntungan tidak masuk akal, dan permintaan OTP. Prinsip kehati-hatian menjadi penting dalam setiap transaksi fintech.

12.5.6 Risiko Kegagalan Sistem dan Gangguan Layanan

Karena fintech bergantung pada sistem elektronik, kegagalan sistem dapat menimbulkan kerugian bagi konsumen. Contohnya adalah aplikasi tidak dapat diakses, transaksi gagal tetapi saldo terpotong, keterlambatan pemrosesan dana, kesalahan pencatatan transaksi, atau gangguan pada layanan pembayaran. Dalam layanan keuangan digital, gangguan sistem dapat berdampak langsung pada kepercayaan konsumen.

Penyelenggara fintech harus memiliki sistem pemulihan, pusat bantuan, dokumentasi transaksi, dan prosedur penyelesaian masalah. Jika terjadi gangguan, konsumen harus memperoleh informasi yang jelas mengenai penyebab, status transaksi, estimasi penyelesaian, dan hak konsumen. Tanpa komunikasi yang baik, konsumen dapat merasa dirugikan dan kehilangan kepercayaan.

Kegagalan sistem juga berkaitan dengan tanggung jawab penyelenggara sistem elektronik. Penyelenggara fintech perlu memastikan bahwa sistem yang digunakan andal, aman, dan mampu melindungi transaksi konsumen. Dalam hal ini, aspek teknologi dan hukum tidak dapat dipisahkan.

12.5.7 Perlindungan Konsumen dalam Layanan Fintech

Perlindungan konsumen fintech bertujuan memberikan kepastian, keamanan, dan keadilan bagi pengguna layanan keuangan digital.

Konsumen harus dilindungi sejak sebelum menggunakan layanan, saat transaksi berlangsung, hingga setelah terjadi sengketa. Perlindungan tidak hanya dilakukan setelah kerugian terjadi, tetapi juga melalui pencegahan.

Perlindungan konsumen fintech mencakup beberapa prinsip berikut.

1. **Transparansi informasi**

   Penyelenggara fintech wajib memberikan informasi yang jelas tentang biaya, bunga, risiko, hak, kewajiban, dan mekanisme pengaduan.

2. **Keamanan sistem**

   Sistem fintech harus mampu melindungi akun, transaksi, data pribadi, dan dana konsumen.

3. **Pelindungan data pribadi**

   Data konsumen harus dikumpulkan dan digunakan secara sah, terbatas, dan bertanggung jawab.

4. **Persetujuan yang jelas**

   Konsumen harus mengetahui dan menyetujui penggunaan data serta syarat layanan secara sadar.

5. **Mekanisme pengaduan**

   Konsumen harus memiliki akses terhadap saluran komplain yang mudah, cepat, dan transparan.

6. **Penyelesaian sengketa**

   Jika terjadi kerugian, konsumen harus memperoleh jalur penyelesaian yang adil, baik melalui penyelenggara, regulator, mediasi, maupun jalur hukum.

7. **Pengawasan regulator**

   OJK, Bank Indonesia, dan lembaga terkait perlu mengawasi penyelenggara fintech agar mematuhi regulasi.

8. **Literasi keuangan digital**

   Konsumen perlu dibekali pemahaman mengenai manfaat, risiko, dan cara menggunakan layanan fintech secara aman.

12.5.8 Peran Konsumen dalam Melindungi Diri

Perlindungan konsumen tidak hanya menjadi tanggung jawab penyelenggara fintech dan regulator. Konsumen juga memiliki peran penting dalam melindungi dirinya sendiri. Banyak kasus kerugian fintech terjadi karena konsumen kurang berhati-hati, tidak membaca syarat layanan, mudah tergoda tawaran, atau membagikan data rahasia kepada pihak lain.

Beberapa langkah yang perlu dilakukan konsumen antara lain:

1. menggunakan layanan fintech yang berizin;
2. memeriksa legalitas platform melalui kanal resmi regulator;
3. membaca syarat dan ketentuan sebelum menyetujui layanan;
4. memahami biaya, bunga, denda, dan risiko;
5. tidak membagikan OTP, PIN, password, dan kode verifikasi;
6. tidak mengklik tautan mencurigakan;
7. menyimpan bukti transaksi;
8. segera melapor jika terjadi transaksi tidak dikenal;
9. tidak mudah percaya pada investasi dengan keuntungan tidak masuk akal;
10. menggunakan fitur keamanan tambahan seperti autentikasi dua faktor.

Dengan sikap hati-hati, konsumen dapat mengurangi risiko menjadi korban penipuan atau penyalahgunaan layanan fintech.

Tabel berikut merangkum risiko hukum dan bentuk perlindungan konsumen dalam layanan fintech.

Tabel 12.5: Risiko Hukum dan Perlindungan Konsumen dalam Fintech

Risiko Hukum	Contoh Kasus	Bentuk Perlindungan
Penyalahgunaan data pribadi	Data kontak disebarkan oleh pinjol ilegal	Persetujuan data, pembatasan akses, UU PDP
Transaksi tidak sah	Saldo e-wallet hilang atau akun diretas	Autentikasi, enkripsi, pemulihan akun
Pinjaman online ilegal	Bunga tinggi dan penagihan intimidatif	Pengawasan OJK, pemblokiran aplikasi ilegal
Informasi tidak transparan	Biaya dan bunga tidak dijelaskan jelas	Kewajiban transparansi informasi

Risiko Hukum	Contoh Kasus	Bentuk Perlindungan
Penipuan digital	Link palsu, akun CS palsu, investasi bodong	Edukasi konsumen dan penindakan hukum
Kegagalan sistem	Transaksi gagal tetapi saldo terpotong	Mekanisme pengaduan dan refund
Sengketa kontrak digital	Konsumen tidak memahami syarat layanan	Kontrak yang jelas dan mudah dipahami
Kebocoran data	Data identitas dan transaksi bocor	Keamanan sistem dan tanggung jawab pengendali data

Dari tabel tersebut dapat dipahami bahwa risiko fintech sangat beragam. Karena itu, perlindungan konsumen harus dilakukan secara menyeluruh. Perlindungan tidak cukup hanya dengan membuat aturan, tetapi juga harus diikuti pengawasan, keamanan sistem, edukasi masyarakat, dan mekanisme penyelesaian sengketa yang efektif.

Perlindungan konsumen fintech juga membutuhkan kerja sama banyak pihak. Penyelenggara fintech harus bertanggung jawab atas layanan dan sistemnya. Regulator harus melakukan pengawasan. Aparat penegak hukum harus menindak pelanggaran. Platform aplikasi harus membantu mencegah penyebaran layanan ilegal. Konsumen harus meningkatkan literasi dan kehati-hatian. Kolaborasi ini diperlukan agar ekosistem fintech berkembang secara sehat.

Dengan demikian, risiko hukum dan perlindungan konsumen merupakan aspek penting dalam fintech. Fintech tidak boleh hanya dilihat sebagai inovasi teknologi, tetapi juga sebagai layanan keuangan yang menyangkut hak dan kepentingan masyarakat. Oleh karena itu, setiap pengembangan fintech harus memperhatikan keamanan, transparansi, pelindungan data pribadi, kepatuhan hukum, dan tanggung jawab terhadap konsumen. Jika perlindungan konsumen berjalan baik, fintech dapat berkembang sebagai bagian dari ekonomi digital yang aman, inklusif, dan berkelanjutan.

12.6 Pengawasan dan Kepatuhan dalam Ekonomi Digital

Fintech memiliki peran penting dalam mendorong transformasi ekonomi digital di Indonesia. Melalui layanan keuangan berbasis teknologi, masyarakat dapat melakukan pembayaran, memperoleh pembiayaan, berinvestasi, mengelola dana, dan menggunakan layanan perbankan secara

lebih cepat dan mudah. Fintech juga membantu memperluas akses keuangan bagi masyarakat yang sebelumnya sulit dijangkau oleh lembaga keuangan konvensional.

Gambar 12.6: Tantangan dan Arah Pengembangan Fintech di Indonesia

Namun, perkembangan fintech tidak hanya membawa peluang. Fintech juga menghadirkan tantangan hukum, ekonomi, teknologi, sosial, dan kelembagaan. Tantangan tersebut perlu dipahami agar pengembangan fintech tidak hanya berorientasi pada inovasi, tetapi juga memperhatikan perlindungan konsumen, keamanan sistem, pelindungan data pribadi, stabilitas keuangan, dan kepastian hukum.

Affandi & Iskandar (2025) menjelaskan bahwa ekonomi keuangan digital berkembang melalui perdagangan elektronik, sistem pembayaran, layanan keuangan digital, serta penggunaan teknologi seperti kecerdasan buatan, machine learning, big data, dan blockchain. Perkembangan tersebut membuat layanan keuangan semakin kompleks dan membutuhkan tata kelola yang kuat. Oleh sebab itu, arah pengembangan fintech di Indonesia harus mampu menyeimbangkan antara inovasi teknologi dan perlindungan kepentingan masyarakat.

12.6.1 Tantangan Regulasi yang Tertinggal dari Perkembangan Teknologi

Salah satu tantangan utama fintech adalah kecepatan teknologi yang sering lebih cepat daripada pembentukan regulasi. Inovasi fintech dapat muncul

dalam bentuk layanan baru seperti dompet digital, paylater, peer-to-peer lending, aset kripto, robo advisor, open banking, dan layanan berbasis kecerdasan buatan. Sementara itu, proses pembentukan regulasi membutuhkan waktu karena harus melalui kajian, penyusunan aturan, konsultasi publik, dan koordinasi antarlembaga.

Kondisi ini dapat menimbulkan kekosongan hukum atau ketidakjelasan aturan. Ketika layanan baru muncul tetapi belum diatur secara jelas, konsumen dapat menghadapi risiko tanpa perlindungan yang memadai. Pelaku usaha juga dapat mengalami ketidakpastian karena belum mengetahui batasan hukum, persyaratan izin, dan tanggung jawab yang harus dipenuhi.

Wibowo (2024) menjelaskan bahwa fintech menimbulkan masalah tempo karena teknologi bergerak lebih cepat daripada regulasi. Regulasi yang terlalu lambat dapat membuat hukum tertinggal dari inovasi, sedangkan regulasi yang terlalu kaku dapat menghambat perkembangan layanan fintech. Oleh karena itu, regulasi fintech perlu bersifat adaptif, berbasis risiko, dan mampu menyesuaikan diri dengan perubahan teknologi.

Arah pengembangan yang diperlukan adalah memperkuat regulasi adaptif. Regulatory sandbox dapat digunakan untuk menguji inovasi fintech sebelum diterapkan secara luas. Dengan cara ini, regulator dapat memahami risiko layanan baru, sementara pelaku usaha tetap memiliki ruang untuk berinovasi. Regulasi juga perlu dirancang secara fleksibel agar dapat mengatur prinsip-prinsip utama tanpa harus terlalu cepat usang oleh perubahan teknologi.

12.6.2 Tantangan Perlindungan Konsumen Fintech

Perlindungan konsumen merupakan tantangan penting dalam pengembangan fintech. Konsumen fintech sering kali berada pada posisi yang lemah karena tidak selalu memahami cara kerja teknologi, risiko produk keuangan, syarat layanan, biaya, bunga, denda, dan penggunaan data pribadi. Dalam banyak kasus, konsumen hanya menekan tombol setuju tanpa membaca seluruh kontrak digital.

Risiko perlindungan konsumen dapat muncul dalam berbagai bentuk. Pada layanan pembayaran digital, konsumen dapat mengalami saldo hilang atau transaksi tidak sah. Pada pinjaman online, konsumen dapat menghadapi

bunga tinggi, biaya tidak transparan, dan penagihan intimidatif. Pada investasi digital, konsumen dapat tergoda oleh imbal hasil besar tanpa memahami risiko kerugian. Pada dompet digital, konsumen dapat mengalami kesulitan refund atau pemulihan akun.

Pratiwi & Erniwati (2022) menjelaskan bahwa perkembangan fintech, khususnya peer-to-peer lending, menimbulkan persoalan seperti fintech ilegal, penagihan intimidatif, dan penyebaran data pribadi nasabah. Hal ini menunjukkan bahwa perlindungan konsumen tidak cukup hanya dilakukan melalui penyediaan layanan pengaduan, tetapi juga harus mencakup pengawasan sejak awal terhadap legalitas, transparansi, dan perilaku pelaku usaha fintech.

Arah pengembangan yang diperlukan adalah memperkuat perlindungan konsumen berbasis pencegahan. Penyelenggara fintech harus menyampaikan informasi secara jelas, menyediakan mekanisme pengaduan yang mudah, memberi peringatan risiko, dan melindungi data pengguna. Regulator perlu memastikan bahwa fintech legal mematuhi standar perlindungan konsumen, sedangkan fintech ilegal harus ditindak secara tegas.

12.6.3 Tantangan Keamanan Siber dan Pelindungan data pribadi

Fintech sangat bergantung pada data dan sistem elektronik. Setiap transaksi fintech menghasilkan data pengguna, data pembayaran, data lokasi, data identitas, data rekening, data perangkat, dan data perilaku digital. Data tersebut berguna untuk verifikasi identitas, analisis risiko, pencegahan penipuan, dan peningkatan layanan. Namun, data juga dapat menjadi sumber risiko apabila tidak dikelola dengan baik.

Tantangan keamanan fintech meliputi pencurian akun, phishing, penyalahgunaan OTP, kebocoran data, akses ilegal, malware, social engineering, dan serangan terhadap sistem pembayaran. Apabila sistem fintech tidak aman, konsumen dapat mengalami kerugian finansial dan kehilangan kepercayaan terhadap layanan digital. Selain itu, kebocoran data pribadi dapat digunakan untuk penipuan identitas, pinjaman ilegal, atau kejahatan siber lainnya.

Affandi dan Iskandar (2025) menekankan bahwa data merupakan aset yang sangat berharga dalam ekonomi keuangan digital, sehingga pengumpulan dan analisis data harus dilakukan dengan baik untuk mendukung pengambilan keputusan yang strategis. Namun, pemanfaatan data juga harus diimbangi dengan perlindungan data dan etika penggunaannya. Dengan demikian, fintech harus menempatkan keamanan data sebagai bagian utama dari tata kelola layanan.

Arah pengembangan yang diperlukan adalah memperkuat standar keamanan siber, enkripsi, autentikasi berlapis, pemantauan transaksi mencurigakan, audit sistem, dan tata kelola data pribadi. Penyelenggara fintech juga harus menerapkan prinsip pembatasan data, persetujuan yang jelas, keamanan penyimpanan, dan pemberitahuan kepada konsumen apabila terjadi insiden data.

12.6.4 Tantangan Fintech Ilegal dan Penyalahgunaan Platform Digital

Fintech ilegal menjadi salah satu tantangan serius di Indonesia. Fintech ilegal dapat muncul melalui aplikasi, website, media sosial, pesan singkat, atau iklan digital. Layanan seperti ini sering tidak memiliki izin, tidak memiliki alamat jelas, tidak transparan mengenai biaya, dan tidak mengikuti standar perlindungan konsumen. Dalam pinjaman online ilegal, konsumen dapat dirugikan melalui bunga tinggi, denda berlebihan, intimidasi, serta penyebaran data pribadi.

Masalah fintech ilegal sulit diatasi karena pelaku dapat berganti nama, berpindah aplikasi, menggunakan server berbeda, atau menawarkan layanan melalui kanal tidak resmi. Masyarakat yang membutuhkan dana cepat sering menjadi sasaran karena mudah tergoda oleh proses pencairan yang cepat tanpa memahami risiko. Dalam situasi ini, literasi digital dan pengawasan platform menjadi sangat penting.

Purborini et al., (2025) menjelaskan bahwa regulasi fintech di Indonesia diperlukan untuk melindungi konsumen, memitigasi risiko, dan memastikan perusahaan fintech mematuhi prinsip tata kelola yang baik. Hal ini menunjukkan bahwa pengawasan terhadap fintech ilegal tidak hanya penting untuk melindungi individu, tetapi juga untuk menjaga kepercayaan terhadap ekosistem fintech secara keseluruhan.

Arah pengembangan yang diperlukan adalah memperkuat kerja sama antara OJK, Bank Indonesia, Kominfo, aparat penegak hukum, penyedia aplikasi, dan masyarakat. Pemerintah perlu mempercepat pemblokiran aplikasi ilegal, meningkatkan edukasi publik, dan menyediakan kanal pengecekan legalitas fintech. Konsumen juga harus dibiasakan memeriksa legalitas layanan sebelum menggunakan fintech.

12.6.5 Tantangan Literasi Keuangan Digital

Literasi keuangan digital menjadi syarat penting dalam penggunaan fintech. Banyak pengguna fintech belum memahami perbedaan antara fintech legal dan ilegal, risiko pinjaman online, biaya layanan, bunga, denda, keamanan OTP, kebijakan privasi, serta cara mengajukan pengaduan. Rendahnya literasi membuat masyarakat mudah menjadi korban penipuan digital atau layanan keuangan yang merugikan.

Literasi keuangan digital tidak hanya berarti mampu menggunakan aplikasi. Literasi juga berarti memahami hak dan kewajiban sebagai pengguna, membaca syarat layanan, menjaga keamanan data pribadi, menilai risiko produk keuangan, serta mengambil keputusan finansial secara bertanggung jawab. Konsumen yang hanya memahami kemudahan fintech tanpa memahami risikonya dapat mengambil keputusan yang merugikan.

Raharjo (2021) menjelaskan bahwa perkembangan fintech dan perbankan digital mengubah pola layanan keuangan dari cara tradisional menuju layanan yang lebih mobile, cepat, dan berbasis aplikasi. Perubahan ini membuat masyarakat perlu memahami cara kerja layanan keuangan digital, termasuk risiko keamanan, perubahan perilaku transaksi, dan konsekuensi penggunaan teknologi finansial.

Arah pengembangan yang diperlukan adalah memperkuat edukasi keuangan digital secara berkelanjutan. Edukasi dapat dilakukan melalui kampus, sekolah, komunitas UMKM, media sosial, aplikasi fintech, regulator, dan lembaga keuangan. Materi literasi perlu dibuat sederhana, praktis, dan sesuai kebutuhan masyarakat, misalnya cara mengenali pinjol ilegal, menjaga OTP, membaca bunga pinjaman, dan menghindari investasi bodong.

12.6.6 Tantangan Kolaborasi Antarlembaga

Fintech berada di persimpangan antara sektor keuangan, teknologi informasi, perlindungan konsumen, data pribadi, keamanan siber, dan penegakan hukum. Karena itu, pengembangan fintech tidak dapat hanya ditangani oleh satu lembaga. Diperlukan kolaborasi antara Bank Indonesia, OJK, Kominfo, Bappebti, PPATK, kepolisian, kementerian terkait, lembaga perlindungan konsumen, pelaku usaha, dan masyarakat.

Tantangan muncul ketika kewenangan lembaga saling beririsan. Misalnya, sistem pembayaran berada dalam ruang lingkup Bank Indonesia, P2P lending diawasi OJK, aset kripto berkaitan dengan otoritas perdagangan berjangka, data pribadi berkaitan dengan regulasi perlindungan data, dan kejahatan digital berkaitan dengan aparat penegak hukum. Jika koordinasi lemah, pengawasan fintech dapat menjadi tidak efektif.

Affandi dan Iskandar (2025) menjelaskan bahwa perkembangan digitalisasi sistem pembayaran dan sistem keuangan menimbulkan kompleksitas kegiatan usaha dan produk industri jasa keuangan. Kompleksitas tersebut mendorong pentingnya surveillance monitoring yang didukung teknologi, seperti suptech, agar regulator dapat mengawasi dan mengendalikan aktivitas lembaga keuangan secara lebih efektif.

Arah pengembangan yang diperlukan adalah memperkuat tata kelola kolaboratif. Setiap lembaga perlu memiliki pembagian kewenangan yang jelas, mekanisme pertukaran data, standar koordinasi, dan respons cepat terhadap kasus fintech bermasalah. Kolaborasi juga perlu melibatkan pelaku industri agar regulasi yang dibuat tetap realistis dan dapat diterapkan.

12.6.7 Tantangan Keseimbangan antara Inovasi dan Pengawasan

Fintech berkembang karena inovasi. Jika regulasi terlalu ketat, inovasi dapat terhambat. Pelaku usaha kecil atau startup dapat kesulitan berkembang karena beban kepatuhan yang terlalu berat. Namun, jika pengawasan terlalu longgar, konsumen dapat dirugikan dan stabilitas sistem keuangan dapat terganggu. Oleh karena itu, tantangan utama regulasi fintech adalah menjaga keseimbangan antara inovasi dan pengawasan.

Keseimbangan ini tidak mudah dicapai. Regulator harus memahami model bisnis baru, risiko teknologi, dampak ekonomi, serta hak konsumen. Pelaku usaha harus diberi ruang untuk mengembangkan layanan baru, tetapi tetap diwajibkan mematuhi prinsip keamanan, transparansi, akuntabilitas, dan perlindungan konsumen. Konsumen juga harus dilindungi tanpa menghambat manfaat fintech.

Wibowo (2024) menjelaskan bahwa pendekatan adaptive financial regulation dan regulatory sandbox dapat membantu mengatur fintech secara lebih adaptif. Pendekatan ini memberikan ruang bagi inovasi untuk diuji, tetapi tetap berada dalam pengawasan regulator. Dengan demikian, inovasi tidak langsung dibiarkan bebas tanpa kendali, tetapi juga tidak langsung dibatasi secara berlebihan.

Arah pengembangan yang diperlukan adalah menerapkan regulasi berbasis risiko. Layanan fintech dengan risiko tinggi perlu diawasi lebih ketat, sedangkan layanan dengan risiko rendah dapat diberikan ruang inovasi lebih besar. Pendekatan ini dapat membuat regulasi lebih proporsional, efektif, dan tidak menghambat pertumbuhan fintech.

12.6.8 Arah Pengembangan Fintech yang Aman dan Berkelanjutan

Arah pengembangan fintech di Indonesia perlu diarahkan pada ekosistem yang aman, inklusif, inovatif, dan berkelanjutan. Fintech tidak boleh hanya dipahami sebagai alat bisnis, tetapi juga sebagai bagian dari infrastruktur ekonomi digital. Oleh karena itu, fintech harus mendukung pertumbuhan ekonomi, memperluas akses keuangan, melindungi konsumen, dan menjaga kepercayaan publik.

Pengembangan fintech yang aman memerlukan keamanan sistem, pelindungan data pribadi, transparansi informasi, tata kelola risiko, dan mekanisme pengaduan yang efektif. Pengembangan fintech yang inklusif memerlukan layanan yang dapat diakses oleh UMKM, masyarakat daerah, pekerja informal, dan kelompok yang belum terlayani oleh lembaga keuangan konvensional. Pengembangan fintech yang berkelanjutan memerlukan regulasi adaptif, literasi digital, dan kolaborasi antar pemangku kepentingan.

Purborini et al. (2025) menegaskan bahwa regulasi fintech yang baik akan melindungi konsumen, mendorong inovasi, dan menciptakan lingkungan bisnis yang sehat. Dengan demikian, arah pengembangan fintech di Indonesia perlu menggabungkan tiga kepentingan utama, yaitu inovasi layanan, perlindungan konsumen, dan stabilitas sistem keuangan.

Untuk mencapai arah tersebut, Indonesia perlu memperkuat beberapa strategi. Pertama, memperjelas regulasi layanan fintech sesuai jenis risikonya. Kedua, memperkuat pengawasan terhadap fintech ilegal. Ketiga, meningkatkan literasi keuangan digital masyarakat. Keempat, mendorong penggunaan teknologi pengawasan seperti suptech dan regtech. Kelima, memastikan pelindungan data pribadi. Keenam, membangun kerja sama antara regulator, industri, akademisi, dan masyarakat.

Tabel berikut merangkum tantangan dan arah pengembangan fintech di Indonesia.

Tabel 12.6: Tantangan dan Arah Pengembangan Fintech di Indonesia

Tantangan	Dampak	Arah Pengembangan
Regulasi tertinggal dari teknologi	Kekosongan hukum dan ketidakpastian	Regulasi adaptif dan regulatory sandbox
Perlindungan konsumen lemah	Konsumen dirugikan oleh layanan tidak transparan	Transparansi, pengaduan, dan pengawasan
Keamanan siber dan data pribadi	Kebocoran data dan transaksi tidak sah	Standar keamanan sistem dan perlindungan data
Fintech ilegal	Pinjaman ilegal, bunga tinggi, intimidasi	Pemblokiran, penindakan, dan edukasi publik
Literasi digital rendah	Masyarakat mudah tertipu	Edukasi keuangan digital berkelanjutan
Koordinasi lembaga belum optimal	Pengawasan tidak efektif	Kolaborasi antar regulator dan aparat
Inovasi vs pengawasan	Regulasi terlalu longgar atau terlalu ketat	Regulasi berbasis risiko
Keberlanjutan ekosistem fintech	Kepercayaan publik dapat menurun	Tata kelola aman, inklusif, dan akuntabel

Dari tabel tersebut dapat dipahami bahwa pengembangan fintech harus dilakukan secara menyeluruh. Tantangan fintech tidak hanya berasal dari teknologi, tetapi juga dari regulasi, perilaku pelaku usaha, literasi konsumen,

keamanan data, dan koordinasi kelembagaan. Oleh karena itu, arah pengembangan fintech perlu menggabungkan aspek hukum, ekonomi, teknologi, dan perlindungan masyarakat.

Dengan demikian, tantangan dan arah pengembangan fintech di Indonesia harus dilihat sebagai bagian dari pembangunan ekonomi digital nasional. Fintech dapat menjadi sarana penting untuk memperluas inklusi keuangan dan mendorong inovasi, tetapi harus dikembangkan dengan prinsip kehati-hatian, keamanan, transparansi, perlindungan konsumen, dan akuntabilitas. Regulasi yang adaptif, pengawasan yang efektif, literasi masyarakat, serta kolaborasi antarlembaga akan menjadi kunci bagi terciptanya ekosistem fintech yang sehat, aman, dan berkelanjutan.

Bab 13
Kebijakan Nasional dan Internasional tentang Cyber Law

13.1 Konsep Kebijakan Cyber Law Nasional dan Global

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

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

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

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

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

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

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

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

13.2 Kebijakan Nasional Keamanan Siber di Indonesia

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

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

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

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

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

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

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

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

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

13.3 Peran Lembaga Negara dalam Tata Kelola Siber

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

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

1. Badan Siber dan Sandi Negara (BSSN)

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

2. Kementerian Komunikasi dan Digital

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

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

3. Kepolisian Republik Indonesia

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

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

4. Lembaga Sektoral

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

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

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

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

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

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

13.4 Kerja Sama Internasional dalam Penanganan Kejahatan Siber

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

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

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

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

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

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

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

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

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

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

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

2. International Criminal Police Organization (INTERPOL)

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

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

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

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

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

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

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

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

13.5 Perbandingan Kebijakan Cyber Law di Beberapa Negara

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

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

Perkembangan *cyber law* menunjukkan adanya variasi pendekatan antarnegara.

1. Amerika Serikat

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

2. Uni Eropa

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

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

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

3. Singapura

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

4. Indonesia

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

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

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

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

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

13.6 Tantangan Harmonisasi Hukum Siber Internasional

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

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

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

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

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

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

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

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

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

Bab 14
Etika dan Tanggung Jawab dalam Dunia Digital

14.1 Konsep Etika Digital

Etika digital adalah seperangkat nilai, prinsip, dan pedoman perilaku yang digunakan seseorang ketika beraktivitas di ruang digital. Ruang digital tidak hanya mencakup media sosial, tetapi juga layanan pesan instan, platform pembelajaran daring, marketplace, aplikasi keuangan, forum diskusi, gim online, layanan publik elektronik, serta berbagai sistem berbasis internet lainnya. Dalam ruang tersebut, manusia tetap melakukan tindakan sosial, ekonomi, pendidikan, politik, dan budaya. Karena itu, aktivitas digital tidak dapat dilepaskan dari nilai moral, tanggung jawab, dan kesadaran hukum.

Secara sederhana, etika digital dapat dipahami sebagai cara seseorang menggunakan teknologi informasi secara benar, bertanggung jawab, aman, dan menghormati hak orang lain. Etika digital tidak hanya membahas apa yang boleh atau tidak boleh dilakukan di internet, tetapi juga mengajarkan bagaimana seseorang mempertimbangkan dampak dari tindakannya terhadap orang lain. Misalnya, sebelum membagikan informasi, pengguna perlu memastikan kebenaran informasi tersebut. Sebelum mengunggah foto orang lain, pengguna perlu mempertimbangkan izin, privasi, dan akibat sosial dari unggahan tersebut.

Etika digital menjadi penting karena internet memiliki karakter yang berbeda dengan ruang sosial konvensional. Pertama, internet bersifat cepat. Informasi dapat tersebar dalam hitungan detik dan menjangkau banyak orang. Kedua, internet bersifat luas dan lintas batas. Ketiga, internet dapat meninggalkan jejak digital. Komentar, foto, video, riwayat pencarian, dan unggahan dapat tersimpan lama serta digunakan kembali oleh pihak lain. Keempat, internet memungkinkan anonimitas atau identitas semu sehingga sebagian orang merasa bebas melakukan tindakan yang tidak etis, seperti menghina, menyebarkan hoaks, atau melakukan perundungan digital. Karakter ruang digital yang lintas batas ini menjadi salah satu alasan mengapa hukum siber diperlukan untuk mengatur perilaku manusia di dunia virtual (Edrisy, 2019).

Dalam kajian hukum teknologi informasi, etika digital berhubungan erat dengan hukum. Hukum mengatur perilaku manusia melalui norma yang bersifat memaksa dan disertai sanksi, sedangkan etika mengatur perilaku manusia melalui kesadaran moral. Keduanya saling melengkapi. Tidak semua tindakan yang tidak etis langsung menjadi pelanggaran hukum, tetapi tindakan tidak etis dapat berkembang menjadi perbuatan melawan hukum jika menimbulkan kerugian, menyerang kehormatan, menyebarkan informasi palsu, melanggar privasi, atau merugikan konsumen. Oleh sebab itu, etika digital dapat dipandang sebagai langkah awal untuk mencegah penyalahgunaan teknologi.

Dalam konteks Indonesia, pentingnya etika digital dapat dikaitkan dengan perkembangan hukum siber. Aktivitas digital yang dilakukan melalui internet dapat berdampak nyata meskipun berlangsung dalam ruang virtual. Cyber law atau hukum siber mengatur aktivitas yang dilakukan dengan memanfaatkan teknologi informasi, termasuk penggunaan internet, transaksi elektronik, perlindungan hak kekayaan intelektual, dan pencegahan kejahatan siber (Situmeang, 2020). Dengan demikian, etika digital menjadi dasar perilaku yang mendukung terciptanya ruang digital yang aman, tertib, dan bermartabat.

Gambar 14.1: Prinsip Dasar Etika Digital

Etika digital juga berkaitan dengan konsep literasi digital. Literasi digital tidak hanya berarti kemampuan menggunakan perangkat teknologi, tetapi

juga kemampuan memahami informasi, menilai kebenaran sumber, menjaga keamanan data, menghargai privasi, serta berkomunikasi secara sehat di ruang digital. Seseorang yang mahir menggunakan teknologi belum tentu memiliki etika digital yang baik. Misalnya, seseorang dapat menguasai media sosial, tetapi tetap menyebarkan ujaran kebencian, menipu, atau membocorkan data pribadi orang lain. Karena itu, kecakapan teknis harus diimbangi dengan kesadaran etis.

Secara umum, konsep etika digital dapat dijelaskan melalui beberapa prinsip dasar berikut.

1. **Tanggung jawab digital**

   Setiap pengguna teknologi bertanggung jawab atas tindakan yang dilakukan di ruang digital. Komentar, unggahan, pesan, dan konten yang dibagikan dapat berdampak kepada orang lain. Oleh karena itu, pengguna harus mempertimbangkan akibat dari setiap tindakan digitalnya. Dalam ruang siber, suatu tindakan virtual dapat menimbulkan akibat hukum yang nyata sehingga pengguna tidak dapat menganggap aktivitas digital sebagai tindakan tanpa konsekuensi (Edrisy, 2019).

2. **Kejujuran informasi**

   Pengguna digital perlu memastikan bahwa informasi yang dibagikan bukan informasi palsu, menyesatkan, atau belum jelas sumbernya. Kejujuran informasi penting untuk mencegah hoaks, manipulasi opini, dan kepanikan sosial. Penyebaran informasi bohong dan menyesatkan dalam transaksi elektronik dapat menimbulkan kerugian bagi pihak lain dan telah menjadi perhatian dalam pengaturan hukum informasi dan transaksi elektronik di Indonesia (Republik Indonesia, 2016b).

3. **Penghormatan terhadap privasi**

   Etika digital menuntut setiap orang untuk menghormati data pribadi dan ruang privat orang lain. Mengunggah foto, menyebarkan nomor telepon, membagikan alamat, atau membuka percakapan pribadi tanpa izin merupakan tindakan yang tidak etis dan dapat menimbulkan akibat hukum. Perlindungan privasi dalam ruang digital penting karena data pribadi dapat diproses, disebarkan, dan dimanfaatkan secara cepat oleh berbagai pihak (Wibowo, 2023).

4. Kesopanan dalam komunikasi digital

Komunikasi digital tetap harus menjaga bahasa, sikap, dan penghormatan terhadap orang lain. Perbedaan pendapat tidak boleh menjadi alasan untuk menghina, merendahkan, mengancam, atau menyebarkan kebencian. Dalam hukum siber, tindakan seperti pencemaran nama baik, ujaran kebencian, ancaman, dan penyebaran konten melanggar hukum merupakan bagian dari persoalan yang perlu dikendalikan dalam penggunaan teknologi informasi (Rahmawati et al., 2024).

5. Keadilan dan non-diskriminasi

Pengguna ruang digital harus menghindari tindakan yang mendiskriminasi orang lain berdasarkan suku, agama, ras, jenis kelamin, kondisi fisik, status sosial, atau latar belakang tertentu. Prinsip ini penting untuk menjaga ruang digital tetap inklusif. Ruang digital yang sehat menuntut adanya tanggung jawab sosial agar teknologi tidak digunakan untuk memperluas konflik, kebencian, atau perlakuan tidak adil terhadap kelompok tertentu.

6. Keamanan digital

Etika digital juga mencakup kewajiban menjaga keamanan akun, perangkat, dan data. Pengguna perlu menggunakan kata sandi yang kuat, tidak membagikan OTP, berhati-hati terhadap tautan mencurigakan, serta tidak menggunakan data orang lain tanpa izin. Kejahatan siber seperti illegal access, pencurian data, dan penyalahgunaan sistem elektronik menunjukkan bahwa keamanan digital merupakan bagian penting dari perlindungan hukum dan etika pengguna teknologi (Situmeang, 2020).

7. Menghargai karya digital

Konten digital seperti tulisan, gambar, video, musik, desain, perangkat lunak, dan karya kreatif lainnya memiliki nilai dan hak hukum. Mengambil, menyalin, atau menyebarkan karya orang lain tanpa izin dan tanpa atribusi merupakan tindakan tidak etis serta dapat melanggar hak kekayaan intelektual. Perlindungan HAKI dalam cyberspace menjadi salah satu ruang lingkup hukum siber karena karya digital mudah disalin, dimodifikasi, dan disebarkan melalui internet (Rahmawati et al., 2024).

Tabel berikut merangkum hubungan antara prinsip etika digital, contoh perilaku, dan risiko jika prinsip tersebut dilanggar.

Tabel 14.1: Prinsip Etika Digital, Contoh Perilaku Etis, dan Risiko Pelanggaran

Prinsip Etika Digital	Contoh Perilaku Etis	Risiko Jika Dilanggar
Tanggung jawab digital	Memikirkan dampak sebelum mengunggah konten	Merugikan orang lain, konflik sosial, sanksi hukum
Kejujuran informasi	Memeriksa sumber sebelum membagikan berita	Penyebaran hoaks dan informasi menyesatkan
Privasi	Meminta izin sebelum membagikan data/foto orang lain	Pelanggaran privasi, doxing, kebocoran data
Kesopanan komunikasi	Mengkritik tanpa menghina atau mengancam	Cyberbullying, ujaran kebencian, pencemaran nama baik
Non-diskriminasi	Menghargai perbedaan identitas dan pendapat	Diskriminasi, konflik, polarisasi sosial
Keamanan digital	Menjaga password, OTP, dan akun pribadi	Pengambilalihan akun, pencurian identitas
Menghargai karya	Mencantumkan sumber dan tidak membajak karya	Pelanggaran hak cipta dan kerugian pencipta

Etika digital tidak hanya menjadi tanggung jawab individu, tetapi juga tanggung jawab institusi, komunitas, perusahaan teknologi, dan pemerintah. Individu bertanggung jawab menggunakan teknologi secara bijak. Institusi pendidikan bertanggung jawab membangun literasi digital mahasiswa. Perusahaan teknologi bertanggung jawab menyediakan sistem yang aman dan tidak menyesatkan. Pemerintah bertanggung jawab menyusun regulasi, edukasi, dan penegakan hukum. Dalam kerangka hukum siber, pengaturan teknologi informasi diperlukan agar perkembangan teknologi tidak hanya memberi manfaat, tetapi juga tidak merugikan kepentingan hukum masyarakat (Rahmawati et al., 2024).

Dalam praktik sehari-hari, etika digital dapat diterapkan melalui kebiasaan sederhana. Pengguna dapat membiasakan diri untuk membaca ulang

komentar sebelum mengirim, memeriksa kebenaran berita sebelum membagikan, tidak sembarangan mengunggah data pribadi, tidak menggunakan karya orang lain tanpa izin, serta tidak mudah terpancing konflik digital. Sikap ini terlihat sederhana, tetapi sangat penting karena banyak persoalan hukum digital bermula dari perilaku yang tidak hati-hati.

Etika digital juga penting bagi mahasiswa karena mahasiswa adalah pengguna aktif teknologi sekaligus calon profesional di masyarakat. Dalam kegiatan akademik, mahasiswa menggunakan sistem pembelajaran daring, perpustakaan digital, aplikasi konferensi video, media sosial, dan berbagai sumber informasi online. Tanpa etika digital, mahasiswa dapat terlibat dalam plagiarisme, penyebaran informasi palsu, pelanggaran hak cipta, penyalahgunaan data, atau komunikasi akademik yang tidak sopan. Oleh karena itu, etika digital perlu dipahami sebagai bagian dari kompetensi akademik dan profesional.

Dengan demikian, etika digital merupakan konsep dasar yang mengarahkan manusia agar mampu menggunakan teknologi informasi secara bertanggung jawab. Etika digital menekankan bahwa kebebasan di internet harus disertai tanggung jawab, penghormatan terhadap hak orang lain, kesadaran hukum, serta kemampuan menjaga keamanan dan martabat diri sendiri maupun orang lain. Semakin tinggi penggunaan teknologi digital dalam kehidupan masyarakat, semakin penting pula penerapan etika digital dalam setiap aktivitas online.

14.2 Netiket dan Perilaku Bertanggung Jawab di Internet

Netiket atau *netiquette* merupakan gabungan dari kata *network* dan *etiquette*, yang berarti etika atau tata krama dalam berkomunikasi dan berinteraksi melalui jaringan internet. Netiket mengatur bagaimana seseorang seharusnya berperilaku ketika menggunakan media digital, seperti media sosial, forum diskusi, surat elektronik, aplikasi pesan instan, platform pembelajaran daring, ruang komentar, dan komunitas virtual. Netiket penting karena komunikasi di internet sering berlangsung cepat, terbuka, lintas batas, dan melibatkan banyak orang dari latar belakang yang berbeda.

Dalam kehidupan sehari-hari, manusia memiliki tata krama ketika berbicara langsung dengan orang lain. Misalnya, seseorang perlu menggunakan bahasa yang sopan, tidak memotong pembicaraan, tidak menghina, dan tidak

menyebarkan informasi pribadi orang lain. Prinsip yang sama juga berlaku di internet. Walaupun komunikasi digital tidak selalu dilakukan secara tatap muka, pengguna tetap berhadapan dengan manusia lain yang memiliki hak, perasaan, kehormatan, dan privasi. Shea (1994) menegaskan bahwa salah satu prinsip utama netiket adalah mengingat bahwa di balik layar terdapat manusia nyata. Artinya, pengguna internet tidak boleh memperlakukan komunikasi digital sebagai ruang tanpa empati dan tanpa tanggung jawab.

Gambar 14.2: Berpikir Sebelum Bertindak di Internet

Netiket berkaitan erat dengan konsep etika digital. Jika etika digital membahas prinsip umum tentang penggunaan teknologi secara benar dan bertanggung jawab, maka netiket lebih menekankan pada tata cara praktis dalam berkomunikasi di ruang digital. Netiket membantu pengguna memahami bagaimana menulis komentar, membalas pesan, mengirim surel, berdiskusi dalam forum, membagikan konten, serta menanggapi perbedaan pendapat secara pantas. Dalam konteks hukum siber, perilaku di ruang digital dapat menimbulkan akibat nyata karena aktivitas virtual dapat berdampak pada reputasi, keamanan, hubungan sosial, dan hak orang lain (Edrisy, 2019).

Perilaku bertanggung jawab di internet tidak hanya berarti menghindari pelanggaran hukum, tetapi juga menghindari tindakan yang merugikan

orang lain meskipun belum tentu masuk kategori pidana. Misalnya, menyindir seseorang secara kasar di ruang komentar, menyebarkan tangkapan layar percakapan pribadi tanpa izin, membagikan informasi yang belum jelas kebenarannya, atau menggunakan karya digital orang lain tanpa atribusi merupakan tindakan yang tidak etis. Tindakan seperti ini dapat menimbulkan konflik sosial, tekanan psikologis, pencemaran nama baik, pelanggaran privasi, bahkan persoalan hukum apabila menimbulkan kerugian bagi pihak tertentu.

Netiket juga dapat dipahami sebagai bagian dari *digital citizenship* atau kewargaan digital. Ribble (2015) menjelaskan bahwa warga digital yang baik perlu memahami hak, tanggung jawab, etika, komunikasi, literasi, keamanan, dan hukum dalam penggunaan teknologi. Dengan demikian, netiket bukan hanya aturan sopan santun dalam komunikasi daring, tetapi juga bagian dari pembentukan pengguna internet yang sadar terhadap hak dan kewajibannya. Seseorang tidak cukup hanya mampu menggunakan teknologi, tetapi juga harus mampu menggunakan teknologi secara aman, etis, dan bertanggung jawab.

Dalam perspektif etika informasi, penggunaan teknologi digital juga perlu mempertimbangkan dampaknya terhadap manusia dan lingkungan informasi. Floridi (2013) menjelaskan bahwa etika informasi berkaitan dengan bagaimana informasi dibuat, diproses, disebarkan, dan digunakan secara bertanggung jawab. Pandangan ini menunjukkan bahwa perilaku digital tidak dapat hanya dinilai dari aspek teknis, tetapi juga harus dilihat dari aspek moral, sosial, dan hukum. Oleh karena itu, netiket perlu dipahami sebagai pedoman praktis untuk menjaga kualitas komunikasi dan interaksi di ruang digital.

Secara umum, netiket dan perilaku bertanggung jawab di internet dapat dijelaskan melalui beberapa prinsip berikut.

1. Menggunakan bahasa yang sopan dan jelas

Komunikasi digital perlu menggunakan bahasa yang sopan, tidak menghina, tidak merendahkan, dan tidak mengandung ancaman. Pengguna juga perlu menulis pesan secara jelas agar tidak menimbulkan salah paham. Dalam komunikasi tertulis, ekspresi wajah dan intonasi suara sering tidak terlihat, sehingga pilihan kata menjadi sangat penting.

Kalimat yang ditulis secara singkat dan emosional dapat dipahami berbeda oleh penerima pesan.

2. Menghormati privasi orang lain

Pengguna internet tidak boleh menyebarkan data pribadi orang lain tanpa izin, seperti nomor telepon, alamat rumah, foto pribadi, tangkapan layar percakapan, dokumen identitas, atau informasi keluarga. Privasi merupakan bagian penting dari perlindungan individu di ruang digital karena data pribadi dapat disebarkan dan dimanfaatkan secara cepat oleh berbagai pihak (Wibowo, 2023). Tindakan seperti menyebarkan nomor seseorang di media sosial tanpa izin atau membagikan isi percakapan pribadi dapat merugikan korban secara sosial, psikologis, maupun hukum.

3. Memeriksa kebenaran informasi sebelum membagikan

Internet memudahkan penyebaran informasi, tetapi tidak semua informasi yang beredar adalah benar. Pengguna perlu memeriksa sumber, tanggal, konteks, dan kredibilitas informasi sebelum membagikannya. Penyebaran informasi palsu atau menyesatkan dapat menimbulkan keresahan, merugikan pihak lain, dan dalam kondisi tertentu dapat berhubungan dengan pelanggaran hukum informasi dan transaksi elektronik (Republik Indonesia, 2016b). Kemampuan berpikir kritis terhadap informasi menjadi bagian penting dari literasi digital, terutama bagi anak muda dan pelajar yang aktif menggunakan internet (Livingstone & Haddon, 2009).

4. Tidak melakukan perundungan digital

Perundungan digital atau *cyberbullying* dapat berbentuk hinaan, ejekan, ancaman, penyebaran aib, komentar merendahkan, atau serangan berulang kepada seseorang melalui media digital. Perilaku ini dapat berdampak serius terhadap kesehatan mental, reputasi, dan keamanan korban. Dalam kajian hukum siber, penyalahgunaan teknologi untuk menyerang kehormatan atau mengganggu orang lain merupakan bagian dari persoalan yang perlu dicegah melalui etika dan hukum (Rahmawati et al., 2024).

5. Menghargai perbedaan pendapat

Internet mempertemukan pengguna dengan berbagai pandangan, budaya, agama, dan latar belakang sosial. Perbedaan pendapat seharusnya disikapi dengan argumentasi yang rasional, bukan dengan hinaan atau serangan pribadi. Diskusi digital yang sehat menuntut pengguna untuk fokus pada isi pendapat, bukan menyerang identitas atau martabat orang yang berbeda pandangan. Sikap ini penting agar ruang digital tidak berubah menjadi ruang konflik, polarisasi, dan permusuhan.

6. Menghargai hak cipta dan karya digital

Tulisan, gambar, video, musik, desain, dan perangkat lunak yang ditemukan di internet tidak otomatis bebas digunakan tanpa izin. Pengguna perlu mencantumkan sumber, meminta izin jika diperlukan, dan menghindari pembajakan atau plagiarisme. Perlindungan hak kekayaan intelektual dalam ruang siber penting karena karya digital sangat mudah disalin, diubah, dan disebarkan melalui internet (Situmeang, 2020). Dalam lingkungan akademik, prinsip ini berkaitan langsung dengan kejujuran ilmiah dan pencegahan plagiarisme.

7. Menjaga keamanan akun dan perangkat

Perilaku bertanggung jawab di internet juga mencakup keamanan digital. Pengguna perlu memakai kata sandi yang kuat, tidak membagikan OTP, mengaktifkan autentikasi dua faktor, menghindari tautan mencurigakan, dan tidak menggunakan akun orang lain tanpa izin. Keamanan digital penting karena banyak kejahatan siber terjadi melalui kelalaian pengguna, seperti klik tautan palsu, penggunaan kata sandi lemah, atau pemberian kode verifikasi kepada pihak tidak dikenal. Kesadaran keamanan merupakan bagian dari tanggung jawab pengguna dalam ekosistem digital (Ribble, 2015).

8. Berpikir sebelum mengunggah

Setiap unggahan dapat meninggalkan jejak digital. Komentar, foto, video, dan status yang diunggah hari ini dapat tersimpan, disalin, atau digunakan kembali di masa depan. Oleh karena itu, pengguna perlu mempertimbangkan apakah konten yang dibagikan dapat merugikan diri sendiri, orang lain, institusi, atau masyarakat. Prinsip ini penting

karena jejak digital dapat memengaruhi reputasi akademik, profesional, dan sosial seseorang.

Tabel berikut merangkum contoh penerapan netiket dalam aktivitas digital sehari-hari.

Tabel 14.2: Aktivitas Digital, Perilaku Sesuai Netiket, dan Perilaku Tidak Bertanggung Jawab

Aktivitas Digital	Perilaku Sesuai Netiket	Perilaku Tidak Bertanggung Jawab
Mengirim pesan	Menggunakan bahasa sopan dan jelas	Mengirim pesan kasar, spam, atau ancaman
Berkomentar di media sosial	Mengkritik dengan argumentasi	Menghina, mengejek, atau menyerang pribadi
Membagikan informasi	Memeriksa sumber terlebih dahulu	Menyebarkan hoaks atau informasi provokatif
Mengunggah foto	Meminta izin kepada pihak terkait	Mengunggah foto orang lain tanpa izin
Menggunakan karya digital	Mencantumkan sumber dan menghargai hak cipta	Menyalin karya tanpa izin atau plagiarisme
Diskusi daring	Menghargai perbedaan pendapat	Memaksakan pendapat dan melakukan ujaran kebencian
Keamanan akun	Menjaga password dan OTP	Membagikan kode OTP atau memakai akun orang lain

Netiket juga penting dalam lingkungan akademik. Mahasiswa yang mengikuti pembelajaran daring perlu menjaga etika ketika berdiskusi di grup kelas, mengirim tugas melalui sistem informasi akademik, menggunakan sumber digital, dan berkomunikasi dengan dosen atau teman. Contohnya, mahasiswa perlu menulis pesan dengan salam dan identitas yang jelas, tidak mengirim pesan di waktu yang tidak pantas kecuali mendesak, tidak menyalin tugas dari internet tanpa mencantumkan sumber, serta tidak menyebarkan materi kuliah tanpa izin. Kebiasaan tersebut menunjukkan bahwa netiket bukan hanya urusan media sosial, tetapi juga bagian dari budaya akademik digital.

Dalam lingkungan kerja, netiket juga berpengaruh terhadap profesionalisme. Surat elektronik yang ditulis secara sembarangan, pesan kerja yang tidak sopan, penyebaran data perusahaan tanpa izin, atau komentar negatif terhadap rekan kerja di media sosial dapat merusak reputasi seseorang dan institusi. Oleh sebab itu, perilaku bertanggung jawab di internet menjadi kompetensi penting bagi calon tenaga kerja, wirausahawan, pendidik, aparatur pemerintah, dan profesional di berbagai bidang.

Netiket tidak dapat dipisahkan dari kesadaran hukum. Di Indonesia, penggunaan teknologi informasi dan transaksi elektronik telah diatur dalam peraturan perundang-undangan, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya. Regulasi tersebut menunjukkan bahwa aktivitas digital bukan ruang yang bebas dari hukum. Perilaku seperti penyebaran konten melanggar hukum, informasi bohong yang merugikan, pencemaran nama baik, ancaman, dan penyalahgunaan akses elektronik dapat menimbulkan konsekuensi hukum (Republik Indonesia, 2016).

Dengan demikian, netiket dan perilaku bertanggung jawab di internet merupakan bagian penting dari etika digital. Netiket mengajarkan pengguna untuk berkomunikasi secara sopan, menghormati privasi, memeriksa informasi, menghindari perundungan, menghargai karya, menjaga keamanan, dan berpikir sebelum mengunggah. Semakin besar peran internet dalam kehidupan masyarakat, semakin penting pula penerapan netiket agar ruang digital menjadi tempat yang aman, sehat, produktif, dan bermartabat.

14.3 Etika Penggunaan Data dan Informasi Digital

Etika penggunaan data dan informasi digital merupakan prinsip moral yang mengatur bagaimana data dan informasi dikumpulkan, digunakan, disimpan, dibagikan, dianalisis, dan dipublikasikan dalam ruang digital. Pada era teknologi informasi, data tidak lagi hanya menjadi catatan administratif, tetapi telah menjadi sumber daya penting dalam pengambilan keputusan, pelayanan publik, bisnis digital, pendidikan, kesehatan, keamanan, dan komunikasi sosial. Oleh karena itu, penggunaan data dan informasi digital harus dilakukan secara bertanggung jawab agar tidak merugikan individu, kelompok, organisasi, atau masyarakat.

Data digital dapat berupa data pribadi, data transaksi, data lokasi, data akademik, data kesehatan, data keuangan, data perilaku pengguna, dokumen elektronik, foto, video, rekaman suara, maupun jejak aktivitas di internet. Sementara itu, informasi digital adalah hasil pengolahan data yang memiliki makna dan dapat digunakan untuk memahami suatu keadaan, membuat keputusan, atau menyebarkan pengetahuan. Perbedaan sederhana antara data dan informasi adalah bahwa data merupakan bahan mentah, sedangkan informasi merupakan data yang telah diolah sehingga memiliki arti. Namun, keduanya tetap memerlukan perlakuan etis karena dapat memengaruhi hak, reputasi, keamanan, dan kepentingan seseorang.

Gambar 14.3: Prinsip Etika Penggunaan Data dan Informasi Digital"

Dalam perspektif etika informasi, penggunaan data dan informasi tidak boleh hanya dilihat dari sisi teknis, tetapi juga harus mempertimbangkan dampak moral dan sosialnya. Floridi (2013) menjelaskan bahwa etika informasi berkaitan dengan bagaimana informasi dibuat, diproses, disimpan, disebarkan, dan digunakan secara bertanggung jawab. Artinya, seseorang

tidak cukup hanya mampu mengakses data, tetapi juga harus memahami apakah data tersebut boleh digunakan, apakah penggunaannya sesuai tujuan, apakah pemilik data telah memberi izin, dan apakah penyebarannya dapat merugikan pihak lain.

Etika penggunaan data dan informasi digital juga berkaitan erat dengan hukum. Dalam konteks Indonesia, pelindungan data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Regulasi ini menegaskan bahwa data pribadi merupakan data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik atau nonelektronik (Republik Indonesia, 2022). Dengan demikian, penggunaan data pribadi tidak boleh dilakukan secara sembarangan karena menyangkut hak individu atas dirinya.

Selain itu, penggunaan informasi digital juga berhubungan dengan hukum informasi dan transaksi elektronik. Aktivitas seperti menyebarkan informasi palsu, mencemarkan nama baik, mengakses sistem secara tidak sah, atau membagikan dokumen elektronik tanpa hak dapat menimbulkan konsekuensi hukum. Hukum siber hadir untuk mengatur aktivitas manusia di ruang digital agar penggunaan teknologi informasi tidak merugikan masyarakat (Edrisy, 2019). Oleh sebab itu, etika penggunaan data dan informasi digital berfungsi sebagai pedoman awal agar pengguna tidak hanya menghindari pelanggaran hukum, tetapi juga menghindari tindakan yang tidak pantas secara moral.

Secara umum, terdapat beberapa prinsip penting dalam etika penggunaan data dan informasi digital.

1. **Legalitas penggunaan data**

   Data dan informasi digital harus digunakan berdasarkan dasar yang sah. Pengguna tidak boleh mengambil, mengakses, memproses, atau menyebarkan data orang lain tanpa izin atau tanpa kewenangan. Misalnya, mengunduh database pelanggan, menyebarkan data mahasiswa, atau membuka dokumen pribadi orang lain tanpa hak merupakan tindakan yang tidak etis dan dapat melanggar hukum.

2. **Persetujuan pemilik data**

   Penggunaan data pribadi sebaiknya didasarkan pada persetujuan yang jelas dari pemilik data. Persetujuan tidak boleh diperoleh melalui

paksaan, penipuan, atau informasi yang tidak jelas. Pemilik data perlu mengetahui data apa yang dikumpulkan, untuk tujuan apa data digunakan, siapa yang mengelola data, dan apakah data akan dibagikan kepada pihak lain. Prinsip ini penting karena privasi digital berkaitan dengan kendali individu atas informasi tentang dirinya (Solove, 2008).

3. Pembatasan tujuan penggunaan

Data yang dikumpulkan untuk satu tujuan tidak boleh digunakan untuk tujuan lain tanpa dasar yang sah. Misalnya, data mahasiswa yang dikumpulkan untuk administrasi akademik tidak boleh digunakan untuk promosi komersial tanpa izin. Prinsip pembatasan tujuan merupakan bagian penting dalam kerangka perlindungan privasi karena mencegah data digunakan secara berlebihan dan di luar konteks awal pengumpulannya (OECD, 2013).

4. Minimalisasi data

Pengumpulan data harus dibatasi pada data yang benar-benar diperlukan. Organisasi atau pengguna sistem tidak seharusnya meminta data yang tidak relevan dengan layanan yang diberikan. Misalnya, aplikasi sederhana tidak perlu meminta akses ke kontak, lokasi, kamera, dan mikrofon apabila fitur tersebut tidak dibutuhkan. Minimalisasi data membantu mengurangi risiko kebocoran dan penyalahgunaan data.

5. Akurasi informasi

Informasi digital yang digunakan atau disebarkan harus diperiksa kebenarannya. Data yang salah, tidak lengkap, atau tidak terbaru dapat menghasilkan keputusan yang keliru. Dalam konteks akademik, penggunaan informasi yang tidak valid dapat menurunkan kualitas karya ilmiah. Dalam konteks layanan publik atau bisnis, data yang tidak akurat dapat merugikan pengguna layanan. Karena itu, verifikasi sumber, tanggal, konteks, dan kredibilitas informasi menjadi bagian dari etika digital.

6. Keamanan dan kerahasiaan data

Data digital harus disimpan dan dikelola secara aman. Pengguna dan organisasi perlu menjaga kerahasiaan data dengan menggunakan kata sandi yang kuat, enkripsi, pembatasan akses, pencadangan data, serta pengamanan perangkat. Keamanan data penting karena kebocoran data

dapat menyebabkan pencurian identitas, penipuan, pemerasan, diskriminasi, dan kerugian finansial. Dalam hukum siber, keamanan sistem elektronik menjadi unsur penting dalam mencegah penyalahgunaan teknologi informasi (Situmeang, 2020).

7. Transparansi penggunaan informasi

Pihak yang mengumpulkan dan menggunakan data perlu menjelaskan secara terbuka bagaimana data diproses. Transparansi mencakup penjelasan tentang jenis data yang dikumpulkan, tujuan penggunaan, jangka waktu penyimpanan, pihak yang dapat mengakses data, dan mekanisme penghapusan data. Tanpa transparansi, pemilik data sulit mengetahui apakah datanya digunakan secara sah dan bertanggung jawab.

8. Tidak memanipulasi data dan informasi

Etika digital melarang manipulasi data untuk menyesatkan orang lain. Manipulasi dapat berupa mengubah angka, memotong konteks, menyembunyikan fakta tertentu, menggunakan grafik yang menyesatkan, atau menyebarkan informasi palsu. Dalam ruang digital, manipulasi informasi dapat memengaruhi opini publik, keputusan konsumen, reputasi seseorang, bahkan stabilitas sosial.

9. Menghargai hak cipta dan sumber informasi

Informasi digital sering berasal dari karya orang lain, seperti artikel, buku elektronik, laporan penelitian, gambar, video, atau materi pembelajaran. Pengguna harus mencantumkan sumber, menghindari plagiarisme, dan tidak menggunakan karya digital tanpa izin. Perlindungan hak kekayaan intelektual dalam ruang siber penting karena karya digital mudah disalin dan disebarkan (Rahmawati et al., 2024).

10. Akuntabilitas penggunaan data

Setiap pihak yang menggunakan data harus bertanggung jawab atas akibat dari penggunaan data tersebut. Jika terjadi kesalahan, kebocoran, atau penyalahgunaan, pihak yang mengelola data harus dapat menjelaskan penyebab, dampak, serta langkah perbaikan yang dilakukan. Akuntabilitas penting agar penggunaan data tidak hanya menguntungkan pengelola sistem, tetapi juga tetap melindungi hak pemilik data.

Tabel berikut merangkum prinsip etika penggunaan data dan informasi digital.

Tabel 14.3: Prinsip Etika Penggunaan Data dan Informasi Digital

Prinsip Etika	Contoh Penerapan	Risiko Jika Diabaikan
Legalitas	Menggunakan data sesuai izin dan kewenangan	Akses ilegal, pelanggaran hukum
Persetujuan	Meminta izin sebelum memakai data pribadi	Pelanggaran privasi dan kepercayaan
Pembatasan tujuan	Menggunakan data sesuai tujuan awal	Penyalahgunaan data
Minimalisasi data	Mengumpulkan data yang benar-benar perlu	Risiko kebocoran data meningkat
Akurasi	Memeriksa kebenaran data dan informasi	Keputusan keliru dan misinformasi
Keamanan	Melindungi data dengan sandi, enkripsi, dan akses terbatas	Pencurian identitas, penipuan
Transparansi	Menjelaskan cara data digunakan	Ketidakpercayaan pengguna
Anti-manipulasi	Tidak mengubah data untuk menyesatkan	Manipulasi opini dan kerugian publik
Hak cipta	Mencantumkan sumber informasi	Plagiarisme dan pelanggaran HAKI
Akuntabilitas	Bertanggung jawab atas penggunaan data	Sulit menelusuri kesalahan dan kerugian

Dalam lingkungan akademik, etika penggunaan data dan informasi digital sangat penting. Mahasiswa sering menggunakan jurnal, e-book, artikel, data statistik, gambar, video, dan materi dari internet untuk menyusun tugas atau penelitian. Penggunaan sumber digital harus dilakukan dengan mencantumkan sitasi, menghindari plagiarisme, memeriksa kredibilitas sumber, dan tidak memalsukan data. Selain itu, apabila mahasiswa mengumpulkan data responden untuk penelitian, data tersebut harus dijaga kerahasiaannya dan hanya digunakan sesuai tujuan penelitian.

Dalam lingkungan organisasi, penggunaan data juga harus memperhatikan tata kelola yang baik. Perusahaan, lembaga pendidikan, rumah sakit, instansi

pemerintah, dan platform digital mengelola data dalam jumlah besar. Apabila data digunakan tanpa etika, maka dapat terjadi penyalahgunaan seperti penjualan data, pengawasan berlebihan, diskriminasi algoritmik, penargetan iklan yang manipulatif, atau pengambilan keputusan otomatis yang tidak adil. Wibowo (2023) menjelaskan bahwa dalam era globalisasi digital, data dapat menjadi komoditas yang bernilai tinggi sehingga perlu dikendalikan melalui prinsip hukum dan etika.

Penggunaan data dan informasi digital juga harus memperhatikan risiko teknologi baru. Kecerdasan buatan, big data, komputasi awan, dan analitik digital memungkinkan data diproses dalam jumlah besar dan sangat cepat. Teknologi tersebut memberi manfaat, tetapi juga dapat memperbesar risiko apabila data diproses tanpa izin, tanpa transparansi, atau tanpa pengawasan manusia. Oleh karena itu, etika penggunaan data perlu mengikuti perkembangan teknologi agar perlindungan terhadap manusia tetap menjadi prioritas.

Dengan demikian, etika penggunaan data dan informasi digital menekankan bahwa data tidak boleh diperlakukan hanya sebagai objek teknis atau ekonomi. Data sering kali berkaitan dengan manusia, hak, reputasi, keamanan, dan martabat pribadi. Penggunaan data dan informasi digital yang etis harus memperhatikan legalitas, persetujuan, pembatasan tujuan, minimalisasi data, akurasi, keamanan, transparansi, anti-manipulasi, penghargaan terhadap hak cipta, dan akuntabilitas. Semakin besar peran data dalam kehidupan digital, semakin penting pula penerapan etika dalam setiap proses pengelolaan dan pemanfaatannya.

14.4 Etika dalam Media Sosial dan Komunikasi Online

Media sosial dan komunikasi online telah menjadi bagian penting dalam kehidupan masyarakat digital. Melalui media sosial, seseorang dapat berbagi informasi, membangun jejaring sosial, menyampaikan pendapat, mempromosikan usaha, mengikuti pembelajaran, hingga berpartisipasi dalam isu publik. Sementara itu, komunikasi online berlangsung melalui berbagai saluran, seperti aplikasi pesan instan, surat elektronik, forum diskusi, komentar media sosial, ruang rapat virtual, dan platform pembelajaran daring. Perkembangan ini menunjukkan bahwa interaksi manusia tidak lagi terbatas pada ruang fisik, tetapi juga berlangsung secara intensif dalam ruang digital.

Etika dalam media sosial dan komunikasi online diperlukan karena setiap pesan, komentar, unggahan, foto, video, atau tanggapan digital dapat memengaruhi orang lain. Komunikasi online sering kali dilakukan secara cepat dan spontan sehingga pengguna dapat menulis atau membagikan sesuatu tanpa berpikir panjang. Padahal, tindakan sederhana seperti membalas komentar dengan kata kasar, menyebarkan tangkapan layar percakapan pribadi, membagikan berita yang belum jelas kebenarannya, atau mengunggah foto orang lain tanpa izin dapat menimbulkan kerugian sosial, psikologis, bahkan hukum.

Media sosial memiliki karakter yang berbeda dari komunikasi tatap muka. (Boyd, 2014) menjelaskan bahwa media sosial memiliki sifat jaringan, mudah disebarkan, dapat dicari, dan dapat bertahan lama. Artinya, suatu unggahan tidak selalu hilang setelah dibaca. Konten digital dapat disalin, diteruskan, direkam layar, dicari kembali, dan digunakan dalam konteks yang berbeda. Oleh karena itu, pengguna perlu memahami bahwa komunikasi di media sosial bukan hanya percakapan sesaat, melainkan dapat menjadi jejak digital yang memengaruhi reputasi pribadi, akademik, maupun profesional.

Dalam perspektif etika digital, media sosial harus dipahami sebagai ruang sosial yang tetap membutuhkan tanggung jawab. Walaupun pengguna tidak selalu bertemu langsung dengan lawan bicara, di balik akun digital terdapat manusia nyata yang memiliki perasaan, kehormatan, privasi, dan hak hukum. Shea (1994) menekankan bahwa salah satu prinsip dasar netiket adalah mengingat bahwa pengguna sedang berinteraksi dengan manusia, bukan sekadar layar atau akun. Prinsip ini penting agar komunikasi online tidak berubah menjadi ruang penghinaan, permusuhan, manipulasi, dan kekerasan verbal.

Di Indonesia, etika dalam media sosial juga berkaitan dengan hukum siber. Aktivitas digital yang dilakukan melalui internet dapat menimbulkan akibat hukum apabila memuat penghinaan, pencemaran nama baik, ancaman, penyebaran informasi bohong yang merugikan, pelanggaran privasi, atau penyalahgunaan data. Hukum siber diperlukan untuk mengatur perilaku manusia di ruang digital agar perkembangan teknologi informasi tidak menimbulkan kerugian bagi masyarakat (Edrisy, 2019). Karena itu, etika media sosial tidak hanya menjadi persoalan sopan santun, tetapi juga bagian dari pencegahan pelanggaran hukum.

Secara umum, etika dalam media sosial dan komunikasi online dapat dijelaskan melalui beberapa prinsip berikut.

1. **Berpikir sebelum mengunggah**

   Setiap pengguna perlu mempertimbangkan dampak sebelum mengunggah status, komentar, foto, video, atau dokumen digital. Pertanyaan sederhana yang perlu diajukan adalah: apakah unggahan ini benar, bermanfaat, sopan, aman, dan tidak merugikan orang lain? Prinsip ini penting karena unggahan digital dapat meninggalkan jejak yang sulit dihapus sepenuhnya.

2. **Menggunakan bahasa yang sopan dan tidak menyerang pribadi**

   Perbedaan pendapat di media sosial seharusnya disampaikan dengan bahasa yang santun dan argumentatif. Kritik boleh disampaikan, tetapi tidak boleh berubah menjadi hinaan, ejekan, ancaman, atau serangan terhadap identitas pribadi. Komunikasi online yang tidak sopan dapat memicu konflik, perundungan digital, dan pencemaran nama baik.

3. **Menghormati privasi dan data pribadi orang lain**

   Pengguna tidak boleh mengunggah foto, video, nomor telepon, alamat, dokumen, percakapan pribadi, atau informasi keluarga orang lain tanpa izin. Perlindungan privasi penting karena data pribadi di ruang digital dapat dengan mudah disebarkan, disimpan, dan digunakan kembali oleh pihak lain (Wibowo, 2023). Dalam konteks ini, tindakan seperti membocorkan isi percakapan pribadi atau menyebarkan identitas seseorang untuk mempermalukan pihak tertentu merupakan perilaku tidak etis.

4. **Memeriksa kebenaran informasi sebelum membagikan**

   Media sosial sering menjadi tempat penyebaran informasi cepat, tetapi tidak semua informasi benar. Pengguna harus memeriksa sumber, tanggal, konteks, dan kredibilitas informasi sebelum membagikannya. Penyebaran informasi bohong atau menyesatkan dapat merugikan orang lain dan berpotensi menimbulkan konsekuensi hukum dalam ruang informasi dan transaksi elektronik (Republik Indonesia, 2016).

5. **Menghindari ujaran kebencian dan diskriminasi**

   Media sosial tidak boleh digunakan untuk menyerang seseorang atau kelompok berdasarkan suku, agama, ras, gender, kondisi fisik, status

sosial, atau latar belakang tertentu. Ujaran kebencian dapat memperluas konflik, memperkuat prasangka, dan merusak kehidupan sosial. Dalam kajian hukum siber, konten yang menyerang kehormatan, menimbulkan kebencian, atau mengganggu ketertiban digital termasuk persoalan yang perlu dikendalikan melalui etika dan hukum (Rahmawati et al., 2024).

6. Tidak melakukan perundungan digital

Perundungan digital dapat terjadi melalui komentar menghina, pesan ancaman, penyebaran aib, pembuatan akun palsu untuk menyerang seseorang, atau tindakan mempermalukan orang lain secara online. Perilaku ini dapat berdampak serius terhadap kesehatan mental dan reputasi korban. Oleh karena itu, media sosial harus digunakan untuk membangun komunikasi sehat, bukan sebagai alat untuk merendahkan atau menekan orang lain.

7. Menghargai hak cipta dan karya digital

Konten yang beredar di media sosial, seperti tulisan, gambar, video, musik, desain, dan materi pembelajaran, tetap memiliki hak pencipta. Pengguna harus mencantumkan sumber, meminta izin jika diperlukan, dan tidak mengklaim karya orang lain sebagai miliknya. Perlindungan hak kekayaan intelektual dalam ruang siber penting karena karya digital sangat mudah disalin dan disebarkan (Situmeang, 2020).

8. Menjaga keamanan akun dan identitas digital

Pengguna perlu menjaga keamanan akun media sosial dan aplikasi komunikasi online. Hal ini dapat dilakukan dengan menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, tidak membagikan OTP, tidak membuka tautan mencurigakan, dan berhati-hati terhadap akun palsu. Keamanan akun penting karena penyalahgunaan akun dapat menyebabkan penipuan, pencurian identitas, penyebaran konten palsu, dan kerugian reputasi.

9. Tidak mudah terpancing provokasi

Media sosial sering memunculkan perdebatan emosional. Pengguna perlu menahan diri agar tidak langsung membalas komentar yang memancing kemarahan. Komunikasi online yang sehat membutuhkan kemampuan mengendalikan emosi, membaca konteks, dan memilih

kapan harus merespons atau berhenti berdiskusi. Sikap ini penting untuk mencegah konflik digital yang tidak produktif.

10. Membangun komunikasi yang bermanfaat

Media sosial sebaiknya digunakan untuk berbagi informasi yang benar, membangun jejaring positif, mendukung kegiatan akademik, mempromosikan karya, membantu orang lain, dan memperkuat literasi masyarakat. Ribble (2015) menyatakan bahwa warga digital yang baik perlu memahami hak dan tanggung jawab dalam menggunakan teknologi. Dengan demikian, pengguna media sosial tidak hanya dituntut untuk menghindari pelanggaran, tetapi juga mendorong penggunaan internet yang produktif dan bertanggung jawab.

Tabel berikut merangkum contoh perilaku etis dan tidak etis dalam media sosial dan komunikasi online.

Tabel 14.4: Etika dalam Media Sosial dan Komunikasi Online

Aktivitas	Perilaku Etis	Perilaku Tidak Etis
Mengunggah konten	Memastikan konten benar, sopan, dan tidak merugikan	Mengunggah konten provokatif atau mempermalukan orang lain
Berkomentar	Menyampaikan kritik dengan bahasa santun	Menghina, mengejek, atau menyerang pribadi
Membagikan berita	Memeriksa sumber dan konteks informasi	Menyebarkan hoaks atau informasi belum terverifikasi
Menggunakan foto/video	Meminta izin kepada pihak terkait	Mengunggah foto/video orang lain tanpa izin
Diskusi online	Menghargai perbedaan pendapat	Memaksakan pendapat dan menyerang identitas orang lain
Menggunakan karya digital	Mencantumkan sumber dan menghormati hak cipta	Mengambil karya orang lain tanpa atribusi
Keamanan akun	Menjaga password, OTP, dan privasi akun	Membagikan akses akun atau mudah percaya tautan palsu

Etika komunikasi online juga penting dalam lingkungan akademik dan profesional. Dalam lingkungan akademik, mahasiswa perlu menjaga sopan

santun saat mengirim pesan kepada dosen, berdiskusi dalam grup kelas, mengikuti rapat daring, dan menggunakan media sosial kampus. Pesan kepada dosen atau pihak akademik sebaiknya memuat salam, identitas, maksud yang jelas, dan bahasa yang sopan. Dalam forum pembelajaran daring, mahasiswa perlu menghindari komentar yang tidak relevan, menyalin jawaban teman, atau menyebarkan materi kuliah tanpa izin.

Dalam lingkungan profesional, komunikasi online mencerminkan karakter dan kredibilitas seseorang. Surat elektronik yang tidak sopan, komentar negatif tentang tempat kerja, penyebaran dokumen internal, atau candaan yang merendahkan rekan kerja dapat merusak reputasi individu dan organisasi. Karena itu, pengguna perlu memahami batas antara ruang pribadi dan ruang publik dalam media sosial. Turkle (2011) mengingatkan bahwa teknologi komunikasi dapat membuat manusia selalu terhubung, tetapi tidak selalu membuat komunikasi menjadi lebih bijak. Oleh sebab itu, kedekatan digital harus diimbangi dengan kesadaran etis.

Etika dalam media sosial juga berkaitan dengan tanggung jawab terhadap jejak digital. Jejak digital dapat terbentuk dari unggahan, komentar, riwayat interaksi, foto, video, dan data akun. Jejak tersebut dapat digunakan oleh institusi pendidikan, pemberi kerja, komunitas, atau pihak lain untuk menilai reputasi seseorang. Oleh karena itu, pengguna perlu mengelola identitas digital secara bijak. Identitas digital yang sehat dibangun melalui komunikasi yang sopan, konten yang bermanfaat, penghormatan terhadap orang lain, dan kehati-hatian dalam membagikan informasi.

Dengan demikian, etika dalam media sosial dan komunikasi online merupakan bagian penting dari kehidupan digital. Etika ini menekankan pentingnya berpikir sebelum mengunggah, menggunakan bahasa yang sopan, menghormati privasi, memeriksa kebenaran informasi, menghindari ujaran kebencian, tidak melakukan perundungan digital, menghargai hak cipta, menjaga keamanan akun, serta membangun komunikasi yang bermanfaat. Media sosial seharusnya menjadi sarana untuk memperluas pengetahuan, memperkuat hubungan sosial, dan meningkatkan partisipasi masyarakat, bukan menjadi ruang untuk menyebarkan kebencian, manipulasi, atau pelanggaran hak orang lain.

14.5 Tanggung Jawab Individu, Organisasi, dan Platform Digital

Tanggung jawab dalam dunia digital tidak hanya berada pada pengguna individu, tetapi juga melekat pada organisasi dan platform digital. Setiap pihak memiliki peran berbeda dalam membangun ruang digital yang aman, etis, tertib, dan bertanggung jawab. Individu bertanggung jawab atas perilaku dan konten yang dibuat atau dibagikan. Organisasi bertanggung jawab atas tata kelola data, sistem informasi, layanan digital, serta kepatuhan terhadap hukum. Sementara itu, platform digital bertanggung jawab menyediakan ruang interaksi yang aman, transparan, dan tidak merugikan pengguna.

Gambar 14.4: Tanggung Jawab Individu, Organisasi, dan Platform Digital

Perkembangan teknologi informasi membuat batas antara tindakan pribadi, aktivitas organisasi, dan layanan platform semakin saling berhubungan. Seorang individu dapat menyebarkan informasi melalui media sosial. Organisasi dapat mengumpulkan dan mengelola data pelanggan melalui sistem elektronik. Platform digital dapat menentukan bagaimana konten ditampilkan, direkomendasikan, dibatasi, atau dihapus. Oleh karena itu,

tanggung jawab digital harus dilihat sebagai tanggung jawab bersama, bukan hanya beban salah satu pihak.

Dalam perspektif etika informasi, penggunaan teknologi harus mempertimbangkan dampak moral terhadap manusia, data, dan lingkungan informasi. Floridi (2013) menekankan bahwa informasi tidak boleh diperlakukan hanya sebagai objek teknis, tetapi juga sebagai bagian dari kehidupan sosial yang memiliki nilai moral. Artinya, setiap pihak yang menciptakan, memproses, menyebarkan, atau memanfaatkan informasi digital perlu mempertimbangkan akibat dari tindakannya terhadap orang lain.

Dalam konteks hukum siber, aktivitas digital dapat menimbulkan akibat hukum karena tindakan di ruang virtual dapat berdampak nyata pada kehidupan masyarakat. Hukum siber hadir untuk mengatur aktivitas yang menggunakan teknologi informasi, termasuk transaksi elektronik, perlindungan data, kejahatan siber, dan penggunaan sistem elektronik (Edrisy, 2019). Dengan demikian, tanggung jawab digital bukan hanya persoalan moral, tetapi juga berkaitan dengan kewajiban hukum.

14.5.1 Tanggung Jawab Individu

Individu merupakan aktor utama dalam ruang digital. Setiap pengguna internet memiliki kebebasan untuk berkomunikasi, mencari informasi, menyampaikan pendapat, membuat konten, dan menggunakan layanan digital. Namun, kebebasan tersebut harus disertai tanggung jawab. Pengguna tidak boleh menganggap internet sebagai ruang bebas tanpa aturan karena setiap tindakan digital dapat meninggalkan jejak dan menimbulkan konsekuensi sosial maupun hukum.

Tanggung jawab individu dapat dijelaskan melalui beberapa aspek berikut.

1. **Bertanggung jawab atas konten yang dibuat dan dibagikan**

   Individu harus memastikan bahwa konten yang diunggah, dikomentari, atau dibagikan tidak merugikan orang lain. Konten yang mengandung hoaks, fitnah, ujaran kebencian, ancaman, pencemaran nama baik, atau pelanggaran privasi dapat menimbulkan akibat hukum. Dalam hukum informasi dan transaksi elektronik, penyebaran informasi tertentu yang

merugikan pihak lain dapat berhubungan dengan pelanggaran hukum (Republik Indonesia, 2016).

2. Menghormati privasi dan data pribadi orang lain

Individu tidak boleh menyebarkan nomor telepon, alamat, foto pribadi, percakapan, dokumen identitas, atau data pribadi orang lain tanpa izin. Dalam era digital, data pribadi dapat tersebar sangat cepat dan sulit dikendalikan setelah dipublikasikan. Oleh karena itu, pengguna harus menjaga data dirinya dan menghormati data orang lain. Pelindungan data pribadi merupakan bagian penting dari hak individu dalam masyarakat digital (Republik Indonesia, 2022).

3. Menggunakan informasi secara kritis

Individu bertanggung jawab memeriksa kebenaran informasi sebelum membagikannya. Tidak semua informasi yang muncul di internet dapat dipercaya. Pengguna perlu memperhatikan sumber, tanggal, konteks, penulis, dan tujuan informasi. Sikap kritis penting untuk mencegah penyebaran hoaks, manipulasi opini, dan kepanikan sosial.

4. Menjaga keamanan akun dan perangkat

Tanggung jawab individu juga mencakup keamanan digital. Pengguna perlu memakai kata sandi yang kuat, tidak membagikan OTP, mengaktifkan autentikasi dua faktor, memperbarui perangkat lunak, dan berhati-hati terhadap tautan mencurigakan. Banyak kejahatan siber terjadi karena kelalaian pengguna, seperti memberikan kode verifikasi kepada penipu atau menggunakan password yang mudah ditebak.

5. Menghargai hak cipta dan karya digital

Individu tidak boleh mengambil, menyalin, mengunggah ulang, atau mengubah karya digital orang lain tanpa izin. Konten digital seperti tulisan, gambar, video, musik, desain, dan perangkat lunak tetap memiliki hak pencipta. Perlindungan hak kekayaan intelektual dalam ruang siber menjadi penting karena karya digital sangat mudah disebarkan tanpa kontrol (Situmeang, 2020).

6. Berkomunikasi secara sopan dan tidak diskriminatif

Individu perlu menjaga etika komunikasi online. Perbedaan pendapat harus disampaikan dengan argumentasi, bukan dengan hinaan atau serangan pribadi. Shea (1994) menekankan bahwa prinsip utama netiket

adalah menyadari bahwa di balik layar terdapat manusia nyata. Oleh karena itu, komunikasi digital harus tetap mempertahankan empati dan penghormatan terhadap orang lain.

14.5.2 Tanggung Jawab Organisasi

Organisasi dalam konteks digital dapat berupa perusahaan, lembaga pendidikan, instansi pemerintah, rumah sakit, komunitas, lembaga keuangan, maupun badan usaha yang menggunakan sistem elektronik. Organisasi memiliki tanggung jawab lebih besar karena biasanya mengelola data, sistem, layanan, sumber daya manusia, dan relasi dengan banyak pengguna. Jika organisasi lalai, dampaknya dapat merugikan banyak pihak sekaligus.

Tanggung jawab organisasi dapat dijelaskan melalui beberapa aspek berikut.

1. **Membangun tata kelola data yang baik**

   Organisasi harus mengelola data secara sah, transparan, aman, dan sesuai tujuan. Data pelanggan, mahasiswa, pasien, pegawai, atau pengguna layanan tidak boleh digunakan secara sembarangan. Penggunaan data harus memperhatikan prinsip persetujuan, pembatasan tujuan, minimalisasi data, keamanan, dan akuntabilitas. Prinsip-prinsip tersebut sejalan dengan kerangka privasi yang menekankan pembatasan pengumpulan, pembatasan penggunaan, keamanan, keterbukaan, dan tanggung jawab pengelola data (OECD, 2013).

2. **Menjaga keamanan sistem elektronik**

   Organisasi wajib menjaga sistem elektronik agar tidak mudah disusupi, dirusak, atau disalahgunakan. Upaya ini dapat dilakukan melalui pengendalian akses, enkripsi, pencadangan data, audit keamanan, pelatihan pegawai, dan prosedur respons insiden. Dalam hukum siber, keamanan sistem elektronik menjadi bagian penting untuk mencegah kerugian akibat kejahatan digital (Rahmawati et al., 2024).

3. **Memberikan informasi yang transparan kepada pengguna**

   Organisasi perlu menjelaskan kepada pengguna mengenai data apa yang dikumpulkan, untuk tujuan apa digunakan, berapa lama disimpan, siapa yang dapat mengakses, dan bagaimana pengguna dapat menggunakan

haknya. Transparansi penting karena pengguna berhak memahami bagaimana data dan informasinya dikelola.

4. **Mencegah penyalahgunaan wewenang internal**

   Organisasi harus memastikan bahwa pegawai atau pihak internal tidak menyalahgunakan akses terhadap data dan sistem. Misalnya, pegawai tidak boleh membuka data pelanggan tanpa kepentingan kerja, membocorkan dokumen internal, atau menjual data kepada pihak ketiga. Karena itu, organisasi perlu memiliki kebijakan akses, kode etik, dan sanksi internal.

5. **Membangun budaya etika digital**

   Organisasi tidak cukup hanya memiliki sistem teknis yang aman. Organisasi juga perlu membangun budaya etika digital melalui pelatihan, pedoman perilaku, kebijakan penggunaan teknologi, dan mekanisme pelaporan pelanggaran. Budaya etika digital membantu pegawai memahami bahwa data dan informasi bukan sekadar aset organisasi, tetapi juga berkaitan dengan hak dan kepentingan manusia.

6. **Bertanggung jawab atas dampak layanan digital**

   Organisasi harus mempertimbangkan dampak sosial dari layanan digital yang dikembangkan. Misalnya, sistem otomatis, analitik data, dan algoritma keputusan tidak boleh menyebabkan diskriminasi, ketidakadilan, atau kerugian tidak proporsional bagi kelompok tertentu. Dalam era globalisasi digital, data dapat menjadi komoditas bernilai tinggi sehingga pengelolaannya harus dikendalikan dengan prinsip hukum dan etika (Wibowo, 2023).

14.5.3 Tanggung Jawab Platform Digital

Platform digital adalah penyedia ruang, sistem, atau layanan yang memungkinkan pengguna berinteraksi, bertransaksi, membagikan konten, atau menggunakan layanan berbasis teknologi. Contohnya adalah media sosial, marketplace, platform video, aplikasi pesan, layanan transportasi daring, platform pembelajaran, layanan fintech, dan mesin pencari. Platform digital memiliki tanggung jawab besar karena mengatur infrastruktur, aturan komunitas, algoritma, keamanan, dan pengalaman pengguna.

Tanggung jawab platform digital dapat dijelaskan melalui beberapa aspek berikut.

1. **Menyediakan sistem yang aman dan andal**

   Platform digital harus memastikan bahwa sistem yang digunakan memiliki perlindungan keamanan yang memadai. Sistem yang lemah dapat menyebabkan kebocoran data, pencurian identitas, penipuan, dan penyalahgunaan akun. Keamanan platform tidak hanya berdampak pada perusahaan, tetapi juga pada jutaan pengguna yang bergantung pada layanan tersebut.

2. **Melindungi data pribadi pengguna**

   Platform digital mengumpulkan banyak data pengguna, seperti identitas, lokasi, aktivitas, minat, transaksi, komunikasi, dan perangkat. Oleh karena itu, platform harus menerapkan prinsip pelindungan data pribadi, seperti pemrosesan yang sah, pembatasan tujuan, keamanan, transparansi, dan penghormatan terhadap hak subjek data. Undang-Undang Pelindungan Data Pribadi menegaskan adanya kewajiban dalam pemrosesan data pribadi agar hak subjek data tetap terlindungi (Republik Indonesia, 2022).

3. **Menyediakan kebijakan komunitas yang jelas**

   Platform perlu memiliki aturan mengenai konten yang diperbolehkan dan dilarang, seperti hoaks, ujaran kebencian, pornografi ilegal, kekerasan, penipuan, perundungan, atau pelanggaran hak cipta. Kebijakan tersebut harus mudah dipahami, konsisten, dan tidak diterapkan secara sewenang-wenang.

4. **Melakukan moderasi konten secara bertanggung jawab**

   Platform memiliki peran dalam menangani konten yang berbahaya atau melanggar aturan. Namun, moderasi konten harus dilakukan dengan hati-hati agar tidak menimbulkan penyalahgunaan kekuasaan atau pembatasan kebebasan berekspresi secara tidak adil. (Gillespie, 2018) menjelaskan bahwa platform digital tidak hanya menjadi perantara pasif, tetapi juga memiliki peran dalam membentuk ruang publik digital melalui aturan, algoritma, dan moderasi konten.

5. **Mencegah manipulasi, penipuan, dan penyalahgunaan layanan**

   Platform perlu mencegah akun palsu, bot, penipuan, penyebaran malware, phishing, iklan menyesatkan, serta manipulasi algoritmik. Tanggung jawab ini penting karena pengguna sering kali tidak memiliki kemampuan teknis untuk mendeteksi semua risiko dalam platform.

6. **Memberikan mekanisme pelaporan dan pemulihan**

   Pengguna harus memiliki cara untuk melaporkan konten bermasalah, akun palsu, penipuan, pelanggaran privasi, atau penyalahgunaan data. Platform juga perlu menyediakan mekanisme pemulihan akun, penghapusan konten, banding, dan bantuan ketika pengguna mengalami kerugian.

7. **Bersikap transparan terhadap algoritma dan kebijakan data**

   Platform digital menggunakan algoritma untuk menampilkan konten, merekomendasikan produk, menentukan iklan, dan mengatur interaksi pengguna. Transparansi diperlukan agar pengguna memahami bahwa apa yang mereka lihat di platform tidak selalu netral, tetapi dapat dipengaruhi oleh sistem rekomendasi. Zuboff (2019) mengingatkan bahwa ekonomi digital dapat memanfaatkan data perilaku pengguna untuk kepentingan komersial, sehingga diperlukan kontrol etis dan hukum terhadap pemanfaatan data.

Tabel berikut merangkum pembagian tanggung jawab antara individu, organisasi, dan platform digital.

Tabel 14.5: Tanggung Jawab Individu, Organisasi, dan Platform Digital

Pihak	Bentuk Tanggung Jawab	Contoh Penerapan	Risiko Jika Diabaikan
Individu	Bertanggung jawab atas perilaku digital	Tidak menyebarkan hoaks, menjaga privasi, berkomunikasi sopan	Konflik, pencemaran nama baik, sanksi hukum
Individu	Menjaga keamanan akun	Password kuat, tidak membagikan OTP, verifikasi dua langkah	Akun diambil alih, pencurian identitas
Organisasi	Mengelola data secara etis	Persetujuan, pembatasan tujuan, keamanan data	Kebocoran data, hilangnya kepercayaan

Pihak	Bentuk Tanggung Jawab	Contoh Penerapan	Risiko Jika Diabaikan
Organisasi	Menjaga sistem elektronik	Audit keamanan, pembatasan akses, respons insiden	Serangan siber, gangguan layanan
Platform digital	Melindungi pengguna dan data	Kebijakan privasi, moderasi konten, keamanan sistem	Penyalahgunaan data, konten berbahaya
Platform digital	Menyediakan mekanisme pelaporan	Fitur laporan, pemulihan akun, banding konten	Korban sulit memperoleh perlindungan

Tanggung jawab ketiga pihak tersebut saling berkaitan. Individu dapat berperilaku etis, tetapi tetap membutuhkan organisasi dan platform yang menyediakan sistem aman. Organisasi dapat membuat kebijakan internal, tetapi tetap membutuhkan individu yang patuh dan platform yang bertanggung jawab. Platform dapat membuat aturan komunitas, tetapi tetap membutuhkan pengguna yang sadar etika dan organisasi yang mematuhi regulasi. Dengan demikian, tanggung jawab digital bersifat kolektif.

Dalam lingkungan akademik, pembagian tanggung jawab ini dapat dilihat secara sederhana. Mahasiswa bertanggung jawab menggunakan sistem pembelajaran daring secara jujur dan sopan. Perguruan tinggi bertanggung jawab menjaga data mahasiswa dan menyediakan sistem akademik yang aman. Platform pembelajaran bertanggung jawab menyediakan layanan yang stabil, aman, dan menghormati privasi pengguna. Jika salah satu pihak lalai, maka proses pembelajaran digital dapat terganggu.

Dalam lingkungan bisnis, pelanggan bertanggung jawab menjaga akun dan tidak menyalahgunakan layanan. Perusahaan bertanggung jawab mengelola data pelanggan secara aman dan tidak menyesatkan konsumen. Platform e-commerce bertanggung jawab menyediakan sistem transaksi yang aman, mekanisme komplain, perlindungan terhadap penipuan, dan informasi yang jelas. Kerja sama ini penting agar ekonomi digital dapat berjalan dengan kepercayaan.

Dengan demikian, tanggung jawab digital harus dipahami sebagai tanggung jawab bersama antara individu, organisasi, dan platform digital. Individu bertanggung jawab atas perilaku, keamanan, dan komunikasi digitalnya. Organisasi bertanggung jawab atas tata kelola data, keamanan sistem,

kepatuhan hukum, dan budaya etika digital. Platform digital bertanggung jawab atas keamanan layanan, perlindungan data, moderasi konten, transparansi, dan mekanisme perlindungan pengguna. Semakin besar ketergantungan masyarakat terhadap teknologi digital, semakin penting pula pembagian tanggung jawab yang jelas, adil, dan akuntabel.

14.6 Membangun Budaya Digital yang Aman dan Bermartabat

Budaya digital adalah pola pikir, nilai, kebiasaan, dan perilaku masyarakat dalam menggunakan teknologi digital. Budaya digital tidak hanya berkaitan dengan kemampuan menggunakan perangkat, aplikasi, dan internet, tetapi juga berkaitan dengan cara manusia berinteraksi, berbagi informasi, menjaga privasi, menghormati hak orang lain, serta bertanggung jawab terhadap dampak aktivitas digitalnya. Dengan demikian, budaya digital yang baik tidak cukup hanya ditandai oleh tingginya penggunaan teknologi, tetapi juga oleh adanya kesadaran etis, keamanan, literasi, dan penghormatan terhadap martabat manusia.

Membangun budaya digital yang aman dan bermartabat menjadi kebutuhan penting dalam masyarakat modern. Hampir seluruh aspek kehidupan, seperti pendidikan, pekerjaan, perdagangan, pemerintahan, hiburan, kesehatan, dan komunikasi sosial, telah terhubung dengan ruang digital. Kondisi ini membawa banyak manfaat, seperti kemudahan akses informasi, efisiensi layanan, perluasan jejaring, dan terbukanya peluang ekonomi. Namun, perkembangan digital juga membawa risiko, seperti hoaks, ujaran kebencian, perundungan digital, pencurian data, penipuan online, pelanggaran privasi, kecanduan media sosial, serta penyalahgunaan teknologi untuk merugikan orang lain.

Budaya digital yang aman berarti budaya yang mampu melindungi pengguna dari risiko kejahatan, penyalahgunaan data, manipulasi informasi, dan gangguan terhadap keamanan sistem elektronik. Sementara itu, budaya digital yang bermartabat berarti budaya yang menempatkan manusia sebagai subjek yang harus dihormati hak, privasi, kehormatan, kebebasan, dan keselamatannya. Floridi (2013) menjelaskan bahwa etika informasi perlu memperhatikan bagaimana informasi dibuat, diproses, dan digunakan secara bertanggung jawab karena informasi memiliki dampak terhadap kehidupan

manusia. Dengan demikian, pembangunan budaya digital harus memperhatikan dimensi teknis sekaligus dimensi moral.

Gambar 14.5: Budaya Digital yang Aman dan Bermartabat

Dalam konteks hukum siber, ruang digital tidak dapat dipahami sebagai ruang bebas tanpa aturan. Tindakan di internet dapat menimbulkan akibat hukum karena aktivitas virtual dapat berdampak nyata pada individu, organisasi, dan masyarakat (Edrisy, 2019). Oleh karena itu, budaya digital yang aman dan bermartabat perlu dibangun melalui perpaduan antara etika, literasi digital, keamanan teknologi, regulasi, dan tanggung jawab sosial. Hukum berfungsi memberikan batas dan sanksi, sedangkan etika

membentuk kesadaran agar pengguna tidak menyalahgunakan kebebasan digital.

Secara umum, pembangunan budaya digital yang aman dan bermartabat dapat dilakukan melalui beberapa prinsip berikut.

1. **Meningkatkan literasi digital masyarakat**

   Literasi digital adalah kemampuan untuk mengakses, memahami, mengevaluasi, menggunakan, dan menciptakan informasi melalui teknologi digital secara bijak. Literasi digital tidak hanya berarti mampu menggunakan internet, tetapi juga mampu membedakan informasi benar dan salah, memahami risiko privasi, menjaga keamanan akun, serta berkomunikasi dengan etis. Ribble (2015) menegaskan bahwa warga digital yang baik perlu memahami hak, tanggung jawab, etika, komunikasi, literasi, keamanan, dan hukum dalam penggunaan teknologi.

2. **Membiasakan verifikasi informasi**

   Budaya digital yang sehat membutuhkan kebiasaan memeriksa informasi sebelum membagikan. Pengguna perlu membiasakan diri untuk memeriksa sumber, penulis, tanggal, konteks, dan bukti pendukung. Kebiasaan ini penting untuk mencegah penyebaran hoaks, misinformasi, dan disinformasi. Dalam ruang digital, informasi yang salah dapat menyebar sangat cepat dan menimbulkan keresahan sosial. Oleh karena itu, sikap kritis terhadap informasi menjadi bagian penting dari tanggung jawab digital.

3. **Menjaga privasi dan data pribadi**

   Budaya digital yang bermartabat harus menghormati privasi individu. Pengguna tidak boleh sembarangan membagikan data pribadi dirinya maupun orang lain. Organisasi dan platform digital juga harus mengelola data secara sah, aman, transparan, dan bertanggung jawab. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menegaskan bahwa data pribadi merupakan data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung (Republik Indonesia, 2022). Karena itu, pelindungan data pribadi menjadi salah satu fondasi budaya digital yang aman.

4. Membangun komunikasi digital yang santun

Komunikasi digital harus dilakukan dengan bahasa yang sopan, jelas, dan tidak merendahkan orang lain. Perbedaan pendapat seharusnya disampaikan melalui argumentasi, bukan penghinaan, ancaman, atau ujaran kebencian. Shea (1994) mengingatkan bahwa prinsip utama netiket adalah menyadari bahwa di balik layar terdapat manusia nyata. Prinsip ini penting agar pengguna tidak kehilangan empati ketika berkomunikasi melalui media sosial, forum, pesan instan, atau ruang komentar.

5. Menghargai hak dan karya digital

Budaya digital yang bermartabat harus menghargai karya orang lain. Tulisan, gambar, video, musik, desain, perangkat lunak, dan materi pembelajaran yang beredar di internet tetap memiliki hak pencipta. Mengambil atau menyebarkan karya orang lain tanpa izin dan tanpa atribusi merupakan tindakan tidak etis serta dapat melanggar hak kekayaan intelektual. Dalam hukum siber, perlindungan hak kekayaan intelektual menjadi penting karena karya digital sangat mudah disalin, dimodifikasi, dan disebarluaskan (Situmeang, 2020).

6. Menciptakan ruang digital yang inklusif dan non-diskriminatif

Ruang digital harus menjadi tempat yang aman bagi semua pengguna tanpa memandang suku, agama, ras, jenis kelamin, kondisi fisik, status sosial, atau latar belakang tertentu. Budaya digital yang baik menolak perundungan, ujaran kebencian, pelecehan, diskriminasi, dan kekerasan berbasis identitas. Media sosial seharusnya menjadi ruang dialog dan kolaborasi, bukan ruang permusuhan dan perendahan martabat manusia.

7. Menjaga keamanan digital secara kolektif

Keamanan digital bukan hanya tanggung jawab ahli teknologi, tetapi tanggung jawab semua pengguna. Individu harus menjaga akun dan perangkatnya. Organisasi harus menjaga sistem dan data yang dikelola. Platform digital harus menyediakan sistem yang aman dan mekanisme pelaporan yang jelas. Banyak risiko digital muncul karena kelalaian sederhana, seperti membagikan OTP, menggunakan kata sandi lemah, mengklik tautan palsu, atau mengabaikan pembaruan keamanan.

8. Mendorong tanggung jawab organisasi dan platform digital

Budaya digital yang aman tidak mungkin dibangun hanya oleh individu. Organisasi dan platform digital harus menyediakan kebijakan privasi yang jelas, sistem keamanan yang memadai, moderasi konten yang bertanggung jawab, dan mekanisme pemulihan ketika terjadi pelanggaran. Gillespie (2018) menjelaskan bahwa platform digital tidak sekadar menjadi perantara pasif, tetapi ikut membentuk ruang publik digital melalui aturan, algoritma, dan moderasi konten. Oleh karena itu, platform digital memiliki tanggung jawab etis dalam membangun ekosistem digital yang sehat.

9. Menyeimbangkan kebebasan berekspresi dan tanggung jawab

Budaya digital yang bermartabat tetap menghargai kebebasan berekspresi. Namun, kebebasan tersebut tidak boleh digunakan untuk merugikan orang lain, menyebarkan kebencian, memfitnah, mengancam, atau melanggar privasi. Kebebasan di ruang digital harus disertai kesadaran bahwa setiap pengguna memiliki hak dan martabat yang perlu dihormati. Dalam hukum informasi dan transaksi elektronik, aktivitas digital tertentu dapat menimbulkan akibat hukum apabila merugikan pihak lain atau melanggar ketentuan hukum yang berlaku (Republik Indonesia, 2016).

10. Membiasakan refleksi sebelum bertindak di ruang digital

Pengguna perlu membangun kebiasaan bertanya sebelum mengunggah, membagikan, atau merespons konten: apakah informasi ini benar, apakah bahasa yang digunakan sopan, apakah konten ini melanggar privasi, apakah merugikan orang lain, apakah menghargai hak cipta, dan apakah aman bagi diri sendiri maupun orang lain. Kebiasaan reflektif ini membantu mencegah tindakan impulsif yang dapat menimbulkan kerugian sosial maupun hukum.

Tabel berikut merangkum unsur-unsur utama dalam membangun budaya digital yang aman dan bermartabat.

Tabel 14.6: Unsur Budaya Digital yang Aman dan Bermartabat

Unsur Budaya Digital	Bentuk Penerapan	Dampak Positif
Literasi digital	Memahami informasi, teknologi, risiko, dan hak digital	Pengguna lebih kritis dan bijak

Verifikasi informasi	Mengecek sumber sebelum membagikan konten	Mengurangi hoaks dan misinformasi
Perlindungan privasi	Tidak menyebarkan data pribadi tanpa izin	Menjaga keamanan dan martabat individu
Komunikasi santun	Menggunakan bahasa sopan dan argumentatif	Mengurangi konflik dan perundungan digital
Penghargaan karya	Mencantumkan sumber dan menghormati hak cipta	Mencegah plagiarisme dan pelanggaran HAKI
Inklusivitas	Menolak diskriminasi dan ujaran kebencian	Menciptakan ruang digital yang ramah
Keamanan digital	Menjaga akun, perangkat, dan sistem	Mengurangi risiko kejahatan siber
Tanggung jawab platform	Moderasi konten dan perlindungan pengguna	Meningkatkan kepercayaan masyarakat digital

Budaya digital yang aman dan bermartabat perlu dibangun sejak lingkungan keluarga, sekolah, kampus, organisasi, hingga masyarakat luas. Dalam keluarga, orang tua dapat membimbing anak agar menggunakan internet secara sehat. Di sekolah dan kampus, literasi digital dapat dimasukkan dalam pembelajaran dan praktik akademik. Dalam organisasi, budaya digital dapat dibangun melalui kebijakan internal, pelatihan keamanan, kode etik penggunaan teknologi, dan tata kelola data. Dalam masyarakat, budaya digital dapat diperkuat melalui edukasi publik, kampanye antihoaks, perlindungan korban perundungan digital, dan penguatan kesadaran hukum.

Dalam lingkungan akademik, mahasiswa perlu memahami bahwa budaya digital tidak hanya berkaitan dengan penggunaan media sosial, tetapi juga berkaitan dengan integritas akademik. Mahasiswa perlu menghindari plagiarisme, menjaga etika komunikasi dengan dosen dan teman, menggunakan data penelitian secara bertanggung jawab, serta menjaga keamanan akun akademik. Budaya digital yang baik akan mendukung proses pembelajaran yang jujur, aman, dan produktif.

Dalam lingkungan kerja, budaya digital juga menjadi bagian dari profesionalisme. Pegawai perlu menjaga kerahasiaan data organisasi, menggunakan perangkat kerja secara bertanggung jawab, tidak menyebarkan dokumen internal tanpa izin, serta menjaga komunikasi online yang sopan. Organisasi yang memiliki budaya digital baik akan lebih siap

menghadapi risiko keamanan, menjaga kepercayaan pelanggan, dan mematuhi ketentuan hukum.

Dengan demikian, membangun budaya digital yang aman dan bermartabat membutuhkan kesadaran bersama. Individu harus berperilaku etis dan menjaga keamanan dirinya. Organisasi harus membangun tata kelola data dan sistem yang bertanggung jawab. Platform digital harus menyediakan ruang yang aman, transparan, dan adil. Pemerintah perlu menyusun regulasi dan edukasi publik yang mendukung perlindungan masyarakat digital. Apabila semua pihak menjalankan perannya, ruang digital dapat berkembang menjadi lingkungan yang produktif, inklusif, aman, dan menghormati martabat manusia.

Bab 15
Analisis Kasus Hukum Teknologi Informasi di Indonesia

15.1 Pendekatan Analisis Kasus Hukum Teknologi Informasi

Analisis kasus hukum teknologi informasi merupakan kajian terhadap peristiwa hukum yang terjadi akibat penggunaan teknologi digital, sistem elektronik, internet, media sosial, aplikasi, platform digital, dan perangkat teknologi informasi lainnya. Kajian ini penting karena perkembangan teknologi tidak hanya membawa manfaat bagi masyarakat, tetapi juga menimbulkan berbagai persoalan hukum baru. Persoalan tersebut dapat berupa penyalahgunaan data pribadi, pencemaran nama baik melalui media sosial, kejahatan siber, penipuan online, akses ilegal, pembobolan sistem elektronik, penyebaran konten melanggar hukum, pelanggaran hak cipta digital, hingga sengketa transaksi elektronik.

Di Indonesia, kasus hukum teknologi informasi semakin banyak muncul seiring meningkatnya penggunaan internet dan layanan digital. Aktivitas masyarakat yang sebelumnya dilakukan secara langsung kini banyak berpindah ke ruang digital, seperti komunikasi, transaksi perbankan, perdagangan elektronik, pembelajaran, layanan publik, administrasi pemerintahan, dan kegiatan sosial. Perubahan ini membuat hukum harus mampu mengikuti perkembangan teknologi agar tetap dapat memberikan kepastian, perlindungan, dan keadilan bagi masyarakat.

Hukum teknologi informasi di Indonesia banyak bertumpu pada Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE. UU ITE memberikan dasar hukum terhadap informasi elektronik, dokumen elektronik, transaksi elektronik, alat bukti elektronik, serta larangan terhadap perbuatan tertentu dalam ruang digital. Dalam perkembangan berikutnya, pengaturan hukum digital juga diperkuat dengan Undang-Undang Pelindungan Data Pribadi atau UU PDP yang mengatur pelindungan data pribadi, hak subjek data, kewajiban pengendali data, dan sanksi atas

penyalahgunaan data pribadi. Perkembangan ini menunjukkan bahwa hukum Indonesia mulai beradaptasi dengan kebutuhan masyarakat digital.

Analisis kasus hukum teknologi informasi diperlukan agar mahasiswa tidak hanya memahami teori hukum digital, tetapi juga mampu melihat bagaimana hukum diterapkan dalam peristiwa nyata. Melalui analisis kasus, mahasiswa dapat memahami hubungan antara norma hukum, fakta peristiwa, alat bukti, peran aparat penegak hukum, hak korban, tanggung jawab pelaku, serta pertimbangan hakim. Dengan demikian, analisis kasus menjadi jembatan antara konsep hukum dan praktik penegakan hukum.

Dalam konteks kejahatan siber, analisis kasus memiliki peran penting karena cybercrime memiliki karakter yang berbeda dari kejahatan konvensional. Kejahatan siber dapat dilakukan secara lintas batas, menggunakan identitas anonim, memanfaatkan celah keamanan sistem, serta meninggalkan bukti digital yang mudah berubah atau dihapus. Habibi & Liviani (2020) menjelaskan bahwa penegakan hukum cybercrime masih menghadapi hambatan pada perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Hal ini menunjukkan bahwa penyelesaian kasus teknologi informasi memerlukan kemampuan hukum sekaligus pemahaman teknis.

Salah satu aspek penting dalam analisis kasus hukum teknologi informasi adalah pembuktian. Bukti digital berbeda dengan bukti fisik biasa. Bukti digital dapat berupa tangkapan layar, metadata, rekaman percakapan, log akses, file elektronik, akun media sosial, email, data transaksi, rekaman CCTV, atau hasil forensik digital. Bukti tersebut harus dikumpulkan, disimpan, dan diperiksa dengan prosedur yang tepat agar dapat diterima di pengadilan. Oktana (2023) menjelaskan bahwa media sosial dapat berkedudukan sebagai alat bukti elektronik yang sah sepanjang memenuhi syarat formil dan materil sebagaimana diatur dalam UU ITE.

Pembuktian dalam kasus siber juga menghadapi tantangan tersendiri. Aini & Lubis (2024) menyebutkan bahwa tantangan pembuktian kasus kejahatan siber meliputi sifat transnasional, anonimitas pelaku, volatilitas bukti digital, keterbatasan sumber daya, dan keterbatasan keahlian penyidik. Tantangan tersebut membuat proses penyidikan dan pembuktian tidak cukup hanya mengandalkan norma hukum, tetapi juga membutuhkan forensik digital, kerja sama antar lembaga, dan kapasitas teknis aparat penegak hukum.

Selain pembuktian, analisis kasus hukum teknologi informasi juga harus memperhatikan prinsip perlindungan hak. Dalam ruang digital, penegakan hukum tidak boleh mengabaikan hak privasi, kebebasan berekspresi, pelindungan data pribadi, asas praduga tak bersalah, dan prinsip proporsionalitas. Damayanti & Sodikin (2026) menekankan bahwa penegakan hukum teknologi informasi perlu dilakukan secara adaptif, proporsional, dan berorientasi pada perlindungan hak asasi manusia, terutama dalam kasus yang melibatkan penyebaran konten digital dan penggunaan UU ITE.

Kasus kebocoran data pribadi menjadi salah satu contoh penting dalam hukum teknologi informasi. Kebocoran data dapat terjadi pada media sosial, aplikasi kesehatan, e-commerce, layanan publik, lembaga keuangan, maupun sistem pemerintahan. Satrio & Widiatno (2020) menunjukkan bahwa kasus kebocoran data pengguna Facebook di Indonesia memperlihatkan pentingnya perlindungan hukum terhadap data pribadi pengguna media elektronik. Kasus seperti ini tidak hanya berkaitan dengan keamanan teknis, tetapi juga menyangkut hak privasi, kewajiban penyelenggara sistem elektronik, dan upaya hukum bagi korban.

Kasus lain yang banyak terjadi adalah kejahatan siber pada sektor perbankan. Internet banking dan mobile banking memberikan kemudahan bagi nasabah, tetapi juga membuka peluang terjadinya pencurian data, penipuan, pembobolan akun, dan penyalahgunaan informasi keuangan. Ningrum & Robekha (2022) menjelaskan bahwa perkembangan internet banking dapat meningkatkan efisiensi transaksi, tetapi juga menimbulkan risiko kejahatan siber terhadap data dan dana nasabah. Oleh sebab itu, analisis kasus di sektor perbankan perlu memperhatikan tanggung jawab bank, keamanan sistem, perlindungan konsumen, dan kewajiban edukasi kepada nasabah.

Akses ilegal terhadap sistem elektronik juga menjadi kasus penting dalam hukum teknologi informasi. Perbuatan mengakses sistem elektronik orang lain tanpa hak dapat mengancam keamanan data, privasi, dan kepentingan ekonomi korban. Puteri et al. (2025) membahas kasus akses ilegal terhadap sistem DigiPos Telkomsel yang mengakibatkan kerugian finansial dan diproses berdasarkan Pasal 30 jo. Pasal 46 UU ITE. Kasus ini menunjukkan bahwa perlindungan terhadap sistem elektronik merupakan bagian penting dari keamanan digital nasional.

Secara umum, analisis kasus hukum teknologi informasi dapat dilakukan melalui beberapa tahapan berikut.

Gambar 15.1: Alur Analisis Kasus Hukum Teknologi Informas

1. Mengidentifikasi fakta kasus

Tahap pertama adalah memahami peristiwa yang terjadi. Fakta kasus meliputi siapa pelaku, siapa korban, apa tindakan yang dilakukan, media atau teknologi apa yang digunakan, kapan dan di mana peristiwa terjadi, serta akibat yang ditimbulkan. Fakta harus dipisahkan dari opini agar analisis menjadi objektif.

2. Menentukan isu hukum

Setelah fakta dipahami, langkah berikutnya adalah menentukan isu hukum. Isu hukum dapat berupa apakah suatu tindakan termasuk akses ilegal, apakah terjadi penyebaran informasi melanggar hukum, apakah ada pelanggaran data pribadi, apakah bukti elektronik sah, atau apakah platform digital bertanggung jawab atas kerugian pengguna.

3. Mengidentifikasi dasar hukum

Tahap ini dilakukan dengan mencari peraturan yang relevan. Dasar hukum dapat berasal dari UU ITE, UU PDP, KUHP, KUHAP, Undang-Undang Perlindungan Konsumen, Undang-Undang Hak Cipta, peraturan pemerintah, peraturan menteri, atau putusan pengadilan. Pemilihan dasar hukum harus sesuai dengan karakter kasus.

4. Menganalisis unsur perbuatan

Setiap tindak pidana atau pelanggaran hukum memiliki unsur yang harus dibuktikan. Misalnya, dalam akses ilegal perlu dianalisis unsur "tanpa hak", "dengan sengaja", dan "mengakses sistem elektronik".

Dalam penyebaran konten digital, perlu dianalisis unsur kesengajaan, muatan konten, akibat, dan media penyebaran.

5. Menilai alat bukti

Alat bukti dalam kasus teknologi informasi sering berupa bukti elektronik. Analisis perlu melihat apakah bukti diperoleh secara sah, apakah integritasnya terjaga, apakah ada proses forensik digital, dan apakah bukti tersebut dapat menjelaskan hubungan antara pelaku dan perbuatan. Bukti digital harus dijaga agar tidak berubah dan tetap dapat dipertanggungjawabkan.

6. Menganalisis tanggung jawab hukum

Tahap ini menilai siapa yang bertanggung jawab secara hukum. Tanggung jawab dapat berada pada individu, organisasi, penyelenggara sistem elektronik, platform digital, atau pihak lain yang lalai menjaga sistem dan data. Analisis juga perlu membedakan antara tanggung jawab pidana, perdata, administratif, dan etik.

7. Menilai dampak kasus

Kasus hukum teknologi informasi dapat menimbulkan dampak bagi korban, masyarakat, organisasi, dan negara. Dampak dapat berupa kerugian finansial, kerusakan reputasi, kebocoran data, gangguan layanan, hilangnya kepercayaan publik, atau ancaman keamanan digital.

8. Merumuskan rekomendasi penyelesaian

Analisis kasus tidak hanya berhenti pada penilaian hukum, tetapi juga perlu memberikan rekomendasi. Rekomendasi dapat berupa peningkatan keamanan sistem, edukasi pengguna, penguatan regulasi, pelatihan aparat, penguatan forensik digital, perlindungan korban, atau perbaikan tata kelola data.

Tabel berikut merangkum tahapan analisis kasus hukum teknologi informasi.

Tabel 15.1: Tahapan Analisis Kasus Hukum Teknologi Informasi

Tahapan Analisis	Pertanyaan Utama	Contoh Penerapan
Identifikasi fakta	Apa peristiwa yang terjadi?	Kebocoran data, akses ilegal, penipuan online

Tahapan Analisis	Pertanyaan Utama	Contoh Penerapan
Isu hukum	Masalah hukum apa yang muncul?	Pelanggaran privasi, cybercrime, bukti elektronik
Dasar hukum	Aturan apa yang digunakan?	UU ITE, UU PDP, KUHP, KUHAP
Unsur perbuatan	Unsur hukum apa yang harus dibuktikan?	Tanpa hak, sengaja, merugikan, melawan hukum
Alat bukti	Bukti apa yang mendukung kasus?	Log akses, metadata, tangkapan layar, CCTV
Tanggung jawab	Siapa pihak yang bertanggung jawab?	Individu, organisasi, platform digital
Dampak kasus	Kerugian apa yang ditimbulkan?	Kerugian finansial, reputasi, data bocor
Rekomendasi	Apa solusi yang diperlukan?	Forensik digital, literasi, keamanan sistem

Analisis kasus hukum teknologi informasi juga perlu memperhatikan hubungan antara hukum dan etika digital. Tidak semua tindakan tidak etis langsung menjadi pelanggaran hukum, tetapi banyak kasus hukum digital bermula dari perilaku yang tidak etis. Misalnya, menyebarkan data pribadi tanpa izin, menggunakan karya orang lain tanpa atribusi, mengunggah konten yang merendahkan pihak lain, atau menggunakan akses sistem untuk kepentingan pribadi. Fadli et al., (2026) menjelaskan bahwa pelanggaran etika teknologi informasi di Indonesia banyak berkaitan dengan kebocoran data, privasi digital, keamanan informasi, lemahnya regulasi, rendahnya literasi digital, dan kurangnya komitmen organisasi.

Oleh karena itu, analisis kasus hukum teknologi informasi harus dilakukan secara multidisipliner. Kajian ini tidak cukup hanya membaca pasal hukum, tetapi juga perlu memahami teknologi, tata kelola data, keamanan informasi, forensik digital, perilaku pengguna, etika digital, dan dampak sosial. Pendekatan multidisipliner akan membantu menghasilkan analisis yang lebih lengkap dan tidak semata-mata normatif.

Bagi mahasiswa, kemampuan menganalisis kasus hukum teknologi informasi sangat penting karena kasus digital semakin sering terjadi dalam kehidupan sehari-hari. Mahasiswa perlu mampu membaca fakta, menemukan isu hukum, memahami dasar hukum, menilai alat bukti, dan

menyusun argumen hukum secara sistematis. Kemampuan ini bermanfaat untuk kegiatan akademik, penelitian, praktik hukum, kebijakan publik, maupun pengembangan sistem digital yang lebih bertanggung jawab.

Dengan demikian, pengantar analisis kasus hukum teknologi informasi di Indonesia memberikan dasar awal untuk memahami bagaimana peristiwa digital dikaji dari sudut pandang hukum. Analisis kasus membantu menjelaskan hubungan antara teknologi, norma hukum, alat bukti, tanggung jawab, korban, dan penegakan hukum. Semakin kompleks perkembangan teknologi, semakin penting pula kemampuan untuk menganalisis kasus hukum digital secara kritis, objektif, dan berorientasi pada perlindungan hak masyarakat.

15.2 Kasus Penyalahgunaan Data Pribadi

Penyalahgunaan data pribadi dapat diartikan sebagai tindakan memperoleh, mengumpulkan, memakai, menyebarkan, menjual, memindahkan, atau memproses data pribadi seseorang tanpa hak, tanpa persetujuan, atau tidak sesuai dengan tujuan awal pengumpulan data. Bentuknya dapat berupa kebocoran data, pencurian identitas, penjualan database pengguna, penggunaan data untuk pinjaman atau kartu kredit palsu, doxing, profiling komersial tanpa izin, hingga penyebaran data pribadi di forum daring. Penyalahgunaan data pribadi menjadi serius karena korban sering tidak mengetahui sejak awal bahwa datanya telah digunakan oleh pihak lain.

Di Indonesia, pelindungan data pribadi memperoleh dasar hukum yang lebih kuat setelah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang ini mengatur hak subjek data pribadi, kewajiban pengendali data pribadi, pemrosesan data pribadi, larangan penggunaan data tanpa hak, serta sanksi administratif dan pidana. Selain UU PDP, pelindungan data pribadi juga berkaitan dengan Undang-Undang Informasi dan Transaksi Elektronik, terutama dalam penggunaan informasi elektronik yang menyangkut data pribadi seseorang. Sebelum hadirnya UU PDP, pelindungan data pribadi di Indonesia masih tersebar dalam beberapa aturan sektoral sehingga belum sepenuhnya komprehensif (Satrio & Widiatno, 2020).

Salah satu kasus besar yang sering dijadikan contoh adalah kebocoran data Tokopedia pada tahun 2020. Dalam kasus tersebut, data sekitar 91 juta

pengguna Tokopedia diduga bocor dan diperjualbelikan di forum gelap. Data yang disebut bocor meliputi identitas pengguna seperti nama, email, nomor telepon, tanggal lahir, jenis kelamin, dan kata sandi yang telah dienkripsi. Kasus ini menunjukkan bahwa platform e-commerce memiliki tanggung jawab besar sebagai pengendali data pribadi karena mengelola data jutaan pengguna. Anindya & Subiyanto (2025) menjelaskan bahwa kebocoran data Tokopedia menimbulkan persoalan mengenai tanggung jawab hukum platform dalam aspek pencegahan, keamanan sistem, penanganan pasca-insiden, dan perlindungan konsumen sebagai subjek data.

Kasus Tokopedia juga memperlihatkan pentingnya pemberitahuan kepada pengguna ketika terjadi insiden kebocoran data. Pengguna berhak mengetahui data apa yang bocor, risiko apa yang mungkin terjadi, serta langkah apa yang harus dilakukan untuk mengurangi dampak. Dari sisi hukum, platform digital tidak cukup hanya menyatakan bahwa sistem pembayaran aman, tetapi juga harus menunjukkan upaya perlindungan data secara transparan dan akuntabel. Dalam konteks UU PDP, platform digital dapat diposisikan sebagai pengendali data pribadi yang wajib menjaga kerahasiaan, integritas, dan keamanan data pengguna.

Kasus lain yang penting adalah kebocoran data BPJS Kesehatan pada tahun 2021. Dalam kasus ini, sekitar 279 juta data peserta dilaporkan bocor dan dijual secara daring. Data tersebut diduga meliputi nama, nomor induk kependudukan, alamat, nomor telepon, dan data kesehatan. Kasus ini lebih sensitif dibandingkan kebocoran data biasa karena menyangkut data kesehatan dan data kependudukan dalam jumlah sangat besar. Sorisa et al., (2024) menjelaskan bahwa kebocoran data BPJS Kesehatan menunjukkan adanya persoalan serius pada keamanan siber, tata kelola etika, pemantauan keamanan, perlindungan teknis, dan akuntabilitas institusi publik.

Kasus BPJS Kesehatan menunjukkan bahwa penyalahgunaan data pribadi bukan hanya persoalan sektor swasta, tetapi juga dapat terjadi pada sektor publik. Instansi publik yang mengelola data masyarakat memiliki tanggung jawab lebih besar karena data yang dikelola sering kali bersifat wajib diberikan oleh warga negara. Jika data tersebut bocor, masyarakat tidak hanya kehilangan privasi, tetapi juga kehilangan kepercayaan terhadap layanan publik digital. Dalam hal ini, pelindungan data pribadi harus dipandang sebagai bagian dari hak warga negara, bukan sekadar masalah teknis keamanan sistem.

Kasus penyalahgunaan data pribadi juga terjadi dalam sektor perbankan. Dalam salah satu kasus yang dibahas Aritonang et al. (2025), data pribadi nasabah bank diduga disalahgunakan untuk pembuatan kartu kredit tanpa sepengetahuan pemilik data. Korban baru mengetahui masalah tersebut ketika pengajuan Kredit Pemilikan Rumah ditolak karena namanya tercatat bermasalah dalam Sistem Layanan Informasi Keuangan. Kasus ini menunjukkan bahwa kebocoran atau penyalahgunaan data pribadi dapat berdampak langsung pada reputasi keuangan korban, akses kredit, dan status hukum korban sebagai nasabah.

Dalam kasus perbankan, tanggung jawab perlindungan data tidak hanya terletak pada sistem keamanan digital, tetapi juga pada pengawasan internal. Apabila data nasabah disalahgunakan oleh pihak internal, maka bank harus mampu menjelaskan bagaimana akses terhadap data diberikan, siapa yang mengakses data, bagaimana data digunakan, dan mengapa penyalahgunaan dapat terjadi. Aritonang et al. (2025) menegaskan bahwa nasabah yang dirugikan dapat menempuh upaya hukum melalui Otoritas Jasa Keuangan, Kementerian Komunikasi dan Informatika, kepolisian, maupun jalur gugatan perdata.

Kasus kebocoran data pengguna Facebook juga menjadi pelajaran penting dalam perlindungan informasi pribadi. Dalam kasus Cambridge Analytica, data pengguna Facebook digunakan untuk membangun profil psikologis dan preferensi politik tanpa persetujuan yang memadai. Meskipun kasus ini terjadi dalam konteks global, dampaknya relevan bagi Indonesia karena masyarakat Indonesia merupakan pengguna aktif media sosial dalam jumlah besar. Bonggi et al. (2025) menjelaskan bahwa kasus Facebook menimbulkan kerugian pada aspek privasi, kepercayaan pengguna, serta potensi penyalahgunaan data oleh pihak ketiga.

Dalam konteks media sosial, penyalahgunaan data pribadi dapat terjadi melalui berbagai cara. Pengguna sering kali memberikan data secara sukarela ketika membuat akun, mengikuti kuis, mengisi formulir daring, mengunduh aplikasi pihak ketiga, atau memberikan akses terhadap kontak dan lokasi. Masalah muncul ketika data tersebut digunakan untuk tujuan lain tanpa persetujuan, seperti iklan tertarget yang manipulatif, profiling politik, penipuan, doxing, atau penjualan data kepada pihak ketiga. Pertiwi et al. (2020) menegaskan bahwa data pribadi pengguna media sosial merupakan

bagian dari hak privasi yang harus dilindungi karena dapat disalahgunakan untuk kepentingan pribadi pihak lain.

Penyalahgunaan data pribadi di Indonesia juga dapat dilihat dari maraknya kasus pinjaman online ilegal. Dalam praktiknya, sejumlah aplikasi pinjaman online meminta akses berlebihan terhadap kontak, galeri, lokasi, kamera, dan data perangkat pengguna. Data tersebut kemudian dapat dipakai untuk intimidasi, penagihan kasar, mempermalukan korban, atau menyebarkan informasi pribadi kepada kontak korban. Kasus seperti ini menunjukkan bahwa penyalahgunaan data pribadi dapat berubah menjadi tekanan sosial dan psikologis. Karena itu, aspek pelindungan data pribadi harus dikaitkan dengan perlindungan konsumen, perlindungan korban, dan penegakan hukum terhadap pelaku usaha digital ilegal.

Gambar 15.2: Alur Kasus Penyalahgunaan Data Pribadi di Indonesia

Secara umum, kasus penyalahgunaan data pribadi di Indonesia dapat dianalisis melalui beberapa bentuk berikut.

1. **Kebocoran database pengguna**

   Kebocoran terjadi ketika data dalam sistem elektronik dapat diakses oleh pihak yang tidak berwenang. Contohnya adalah kasus Tokopedia dan BPJS Kesehatan. Dalam kasus seperti ini, isu utamanya adalah keamanan sistem, tanggung jawab pengendali data, pemberitahuan kepada subjek data, dan pemulihan korban.

2. **Penjualan data pribadi di forum ilegal**

   Data pribadi yang bocor sering kali diperjualbelikan di forum daring atau dark web. Data tersebut dapat digunakan untuk spam, penipuan, pencurian identitas, atau serangan rekayasa sosial. Perbuatan ini melanggar prinsip legalitas dan persetujuan dalam pemrosesan data pribadi.

3. **Pencurian dan penyalahgunaan identitas**

   Data seperti NIK, nomor kartu keluarga, foto KTP, nomor telepon, dan nama ibu kandung dapat digunakan untuk membuat akun palsu, mengajukan pinjaman, membuka rekening, atau membuat kartu kredit tanpa izin. Kasus penyalahgunaan data nasabah bank menunjukkan bahwa pencurian identitas dapat merugikan korban secara finansial dan reputasional.

4. **Pemrosesan data di luar tujuan awal**

   Data yang awalnya dikumpulkan untuk layanan tertentu digunakan untuk tujuan lain, seperti pemasaran, profiling, penargetan politik, atau analisis perilaku tanpa persetujuan yang jelas. Kasus Facebook dan Cambridge Analytica menjadi contoh penting tentang bahaya pemrosesan data di luar tujuan awal.

5. **Penyalahgunaan akses oleh pihak internal**

   Penyalahgunaan tidak selalu dilakukan oleh peretas dari luar. Dalam beberapa kasus, pihak internal yang memiliki akses ke data dapat menyalahgunakannya untuk kepentingan pribadi. Karena itu, organisasi harus menerapkan pembatasan akses, audit sistem, dan pengawasan internal yang ketat.

6. Penyebaran data pribadi di media sosial

Penyebaran nomor telepon, alamat, foto, dokumen identitas, percakapan pribadi, atau data keluarga tanpa izin dapat menimbulkan doxing, intimidasi, dan perundungan digital. Perbuatan ini berkaitan erat dengan pelanggaran hak privasi dan etika digital.

7. Kelalaian pengendali data

Kelalaian dapat berupa tidak menerapkan enkripsi, tidak memperbarui sistem keamanan, tidak membatasi akses internal, tidak melakukan audit, atau tidak memberi pemberitahuan ketika terjadi insiden. Dalam UU PDP, pengendali data memiliki kewajiban untuk menjaga data pribadi dari akses, pengungkapan, dan pemrosesan yang tidak sah.

Tabel berikut merangkum beberapa kasus penyalahgunaan data pribadi yang relevan di Indonesia.

Tabel 15.2: Contoh Kasus Penyalahgunaan Data Pribadi di Indonesia

Kasus	Bentuk Penyalahgunaan	Data yang Terdampak	Dampak Hukum dan Sosial
Tokopedia 2020	Kebocoran dan dugaan penjualan database pengguna	Nama, email, nomor telepon, tanggal lahir, jenis kelamin, kata sandi terenkripsi	Menimbulkan pertanyaan tanggung jawab platform, keamanan e-commerce, dan perlindungan konsumen
BPJS Kesehatan 2021	Kebocoran data peserta dalam jumlah besar	NIK, nama, alamat, nomor telepon, dan data kesehatan	Mengancam privasi, kepercayaan publik, dan keamanan data sektor publik
Facebook/Cambridge Analytica	Pemrosesan data pengguna untuk profiling tanpa persetujuan memadai	Data akun, preferensi, jejaring pertemanan, profil perilaku	Menurunkan kepercayaan pengguna dan menunjukkan risiko manipulasi informasi

Kasus	Bentuk Penyalahgunaan	Data yang Terdampak	Dampak Hukum dan Sosial
Perbankan/BRI	Penyalahgunaan data nasabah untuk kartu kredit tanpa sepengetahuan korban	Identitas nasabah dan data keuangan	Merugikan reputasi keuangan korban dan dapat menghambat akses kredit
Pinjaman online ilegal	Akses berlebihan dan penyebaran data pribadi	Kontak, foto, lokasi, identitas, data perangkat	Intimidasi, tekanan psikologis, pencemaran reputasi, dan pelanggaran privasi
Media sosial	Penyebaran data pribadi tanpa izin	Foto, nomor telepon, alamat, percakapan pribadi	Doxing, perundungan digital, ancaman keamanan pribadi

Dari beberapa kasus tersebut, tampak bahwa penyalahgunaan data pribadi tidak hanya terjadi karena serangan teknis, tetapi juga karena lemahnya tata kelola organisasi. Organisasi yang mengelola data harus menerapkan prinsip perlindungan data sejak tahap perancangan sistem. Prinsip ini mencakup pengumpulan data secara terbatas, pemrosesan sesuai tujuan, transparansi, keamanan, pembatasan akses, dan akuntabilitas. OECD (2013) juga menekankan pentingnya prinsip pembatasan pengumpulan, kualitas data, pembatasan penggunaan, keamanan, keterbukaan, partisipasi individu, dan akuntabilitas dalam perlindungan privasi.

Dalam pembuktian kasus penyalahgunaan data pribadi, bukti digital menjadi unsur yang sangat penting. Bukti dapat berupa log akses, metadata, riwayat perubahan data, tangkapan layar, email, laporan forensik digital, bukti transaksi, rekaman percakapan, atau dokumen pemberitahuan insiden. Aini dan Lubis (2024) menjelaskan bahwa bukti digital memiliki sifat mudah berubah, mudah dihapus, dan sering tersebar dalam berbagai sistem. Oleh karena itu, bukti digital harus dikumpulkan dan disimpan dengan prosedur yang benar agar dapat digunakan dalam proses hukum.

Tanggung jawab hukum dalam kasus penyalahgunaan data pribadi dapat dibagi ke dalam beberapa bentuk. Pertama, tanggung jawab pidana dapat dikenakan kepada pihak yang secara sengaja memperoleh, menggunakan, menjual, atau mengungkapkan data pribadi secara melawan hukum. Kedua,

tanggung jawab perdata dapat muncul apabila korban mengalami kerugian dan mengajukan ganti rugi. Ketiga, tanggung jawab administratif dapat dikenakan kepada pengendali data yang melanggar kewajiban perlindungan data. Keempat, tanggung jawab etik muncul ketika organisasi atau profesional teknologi gagal menjalankan prinsip kehati-hatian, keamanan, dan tanggung jawab dalam mengelola data.

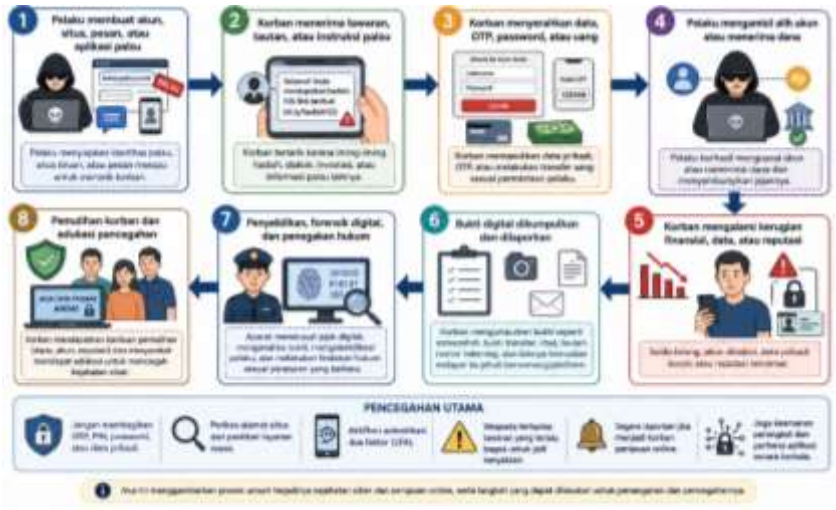
Korban penyalahgunaan data pribadi dapat mengalami beberapa dampak. Dampak finansial dapat berupa kerugian uang, tagihan palsu, pinjaman ilegal, atau transaksi tanpa izin. Dampak psikologis dapat berupa stres, rasa takut, tekanan akibat intimidasi, dan hilangnya rasa aman. Dampak sosial dapat berupa rusaknya reputasi, tersebarnya informasi pribadi, atau hilangnya kepercayaan dari lingkungan. Dampak hukum dapat berupa korban dianggap memiliki kewajiban atau catatan buruk akibat tindakan yang sebenarnya dilakukan oleh pelaku penyalahgunaan data.

Upaya pencegahan harus dilakukan oleh pengguna, organisasi, platform digital, dan pemerintah. Pengguna perlu berhati-hati dalam membagikan data, membaca izin aplikasi, menggunakan kata sandi kuat, mengaktifkan autentikasi dua faktor, dan tidak mudah memberikan OTP. Organisasi perlu menerapkan enkripsi, audit keamanan, pembatasan akses, pelatihan pegawai, kebijakan privasi yang jelas, dan respons insiden yang cepat. Platform digital harus transparan dalam pemrosesan data dan menyediakan mekanisme pelaporan. Pemerintah perlu memperkuat pengawasan, literasi digital, penegakan UU PDP, dan kerja sama antarlembaga.

Dengan demikian, kasus penyalahgunaan data pribadi di Indonesia menunjukkan bahwa perlindungan data bukan lagi isu tambahan, melainkan kebutuhan utama dalam masyarakat digital. Kasus Tokopedia, BPJS Kesehatan, Facebook, perbankan, pinjaman online ilegal, dan media sosial memperlihatkan bahwa data pribadi dapat disalahgunakan dalam berbagai bentuk. Analisis hukum terhadap kasus-kasus tersebut perlu memperhatikan fakta peristiwa, jenis data yang terdampak, dasar hukum, tanggung jawab pengendali data, bukti digital, dampak bagi korban, dan upaya pemulihan. Pelindungan data pribadi yang efektif hanya dapat tercapai apabila regulasi, keamanan sistem, tata kelola organisasi, literasi pengguna, dan penegakan hukum berjalan secara bersama.

15.3 Kasus Kejahatan Siber dan Penipuan Online

Kejahatan siber dan penipuan online merupakan salah satu bentuk penyalahgunaan teknologi informasi yang paling sering terjadi dalam kehidupan digital masyarakat Indonesia. Perkembangan internet, media sosial, mobile banking, e-commerce, dompet digital, dan layanan komunikasi daring telah memberikan kemudahan dalam bertransaksi dan berinteraksi. Namun, kemudahan tersebut juga membuka ruang bagi pelaku kejahatan untuk melakukan tindakan melawan hukum dengan memanfaatkan sistem elektronik, identitas palsu, rekayasa sosial, dan kelemahan keamanan digital.



Gambar 15.3: Kasus Kejahatan Siber dan Penipuan Online

Kejahatan siber atau cybercrime dapat dipahami sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan komputer, jaringan internet, sistem elektronik, atau perangkat digital, baik sebagai alat maupun sebagai sasaran kejahatan. Dalam praktiknya, kejahatan siber dapat berupa akses ilegal, pencurian data, peretasan, penyebaran malware, penipuan online, pencemaran nama baik digital, penyebaran berita bohong, pemerasan digital, hingga penyalahgunaan identitas. Habibi & Liviani (2020) menjelaskan bahwa cybercrime di Indonesia masih menjadi persoalan serius karena sistem hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer

forensik belum sepenuhnya mampu menjawab kompleksitas kejahatan berbasis teknologi.

Penipuan online merupakan salah satu bentuk kejahatan siber yang paling dekat dengan masyarakat. Penipuan ini dilakukan melalui media digital untuk memperoleh keuntungan secara tidak sah dari korban. Modusnya dapat berupa toko online palsu, investasi bodong, hadiah palsu, phishing, penipuan melalui WhatsApp, penipuan marketplace, lowongan kerja palsu, social engineering, penipuan QRIS, hingga pengambilalihan akun mobile banking. Dalam banyak kasus, korban tertipu bukan hanya karena kelemahan sistem, tetapi karena pelaku menggunakan manipulasi psikologis yang membuat korban percaya dan menyerahkan data, uang, atau akses akun secara sukarela.

Di Indonesia, dasar hukum penanganan kejahatan siber dan penipuan online dapat dikaitkan dengan Undang-Undang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, Undang-Undang Pelindungan Data Pribadi, Undang-Undang Perlindungan Konsumen, serta aturan sektoral lain seperti peraturan Otoritas Jasa Keuangan untuk transaksi keuangan digital. UU ITE mengatur berbagai perbuatan yang sering terjadi dalam ruang digital, seperti distribusi konten melanggar hukum, penyebaran berita bohong yang merugikan konsumen, akses ilegal, intersepsi ilegal, gangguan sistem elektronik, dan manipulasi informasi elektronik.

Salah satu karakter penting dalam kejahatan siber adalah sifatnya yang tidak selalu tampak secara fisik. Pelaku dapat beroperasi dari lokasi berbeda, menggunakan akun palsu, menyembunyikan identitas, memakai jaringan anonim, atau memanfaatkan perangkat korban dari jarak jauh. Aini & Lubis (2024) menjelaskan bahwa pembuktian dalam kejahatan siber menghadapi tantangan karena adanya sifat transnasional, anonimitas pelaku, volatilitas bukti digital, serta keterbatasan sumber daya dan keahlian penyidik. Kondisi ini menyebabkan penanganan kasus kejahatan siber membutuhkan kemampuan hukum sekaligus kemampuan teknis digital.

Dalam konteks Indonesia, kasus kejahatan siber banyak terjadi pada sektor perbankan dan layanan keuangan digital. Layanan internet banking dan mobile banking memberikan kemudahan bagi nasabah untuk melakukan transfer, pembayaran, pembelian, dan transaksi lainnya. Namun, layanan tersebut juga menjadi sasaran pelaku kejahatan melalui phishing, pencurian OTP, pemalsuan aplikasi, pesan palsu yang mengatasnamakan bank, dan

pengambilalihan akun. Ningrum dan Robekha (2022) menjelaskan bahwa internet banking dan mobile banking memiliki risiko kejahatan siber karena data dan dana nasabah dapat menjadi target pelaku yang memanfaatkan celah keamanan maupun kelengahan pengguna.

Modus phishing merupakan salah satu bentuk penipuan online yang paling sering digunakan. Dalam modus ini, pelaku membuat pesan, situs, tautan, atau aplikasi palsu yang menyerupai layanan resmi. Korban diarahkan untuk memasukkan data seperti username, password, PIN, OTP, nomor kartu, atau data pribadi. Setelah data diperoleh, pelaku dapat mengambil alih akun korban dan melakukan transaksi tanpa izin. Dalam analisis hukum, phishing dapat dikaitkan dengan penipuan, akses ilegal, pencurian data pribadi, dan penyalahgunaan sistem elektronik.

Selain phishing, penipuan online juga banyak terjadi dalam transaksi e-commerce dan marketplace. Pelaku dapat membuat toko palsu, menawarkan barang dengan harga tidak wajar, meminta pembayaran di luar platform resmi, atau mengirim bukti transaksi palsu. Korban biasanya mengalami kerugian karena barang tidak dikirim, barang tidak sesuai, atau uang tidak dapat dikembalikan. Dalam kasus seperti ini, analisis hukum perlu melihat apakah terdapat unsur tipu muslihat, identitas palsu, transaksi elektronik, kerugian konsumen, serta bukti komunikasi antara korban dan pelaku.

Penipuan online juga sering dilakukan melalui media sosial. Pelaku menggunakan akun palsu untuk menawarkan investasi, pekerjaan, bantuan sosial, hadiah, atau layanan tertentu. Media sosial memudahkan pelaku membangun kepercayaan dengan korban karena komunikasi berlangsung cepat dan terlihat personal. Pertiwi et al. (2020) menjelaskan bahwa media sosial rentan terhadap penyalahgunaan data pribadi dan tindakan yang merugikan pengguna, terutama karena data pribadi sering diberikan secara mudah ketika seseorang menggunakan layanan digital.

Kasus lain yang relevan adalah akses ilegal terhadap sistem elektronik. Akses ilegal terjadi ketika seseorang masuk ke sistem elektronik milik orang lain tanpa hak atau melawan hukum. Puteri et al. (2025) membahas kasus akses ilegal terhadap sistem DigiPos Telkomsel yang menyebabkan kerugian finansial dan diproses berdasarkan Pasal 30 jo. Pasal 46 UU ITE. Kasus ini memperlihatkan bahwa kejahatan siber tidak hanya berupa

penipuan komunikasi, tetapi juga dapat berupa peretasan sistem untuk memperoleh keuntungan ekonomi secara tidak sah.

Dalam kejahatan siber, bukti digital memiliki peran sangat penting. Bukti dapat berupa tangkapan layar percakapan, riwayat transfer, alamat email, nomor telepon, tautan phishing, alamat IP, metadata, log akses, rekaman CCTV, bukti transaksi, file digital, akun media sosial, atau hasil forensik digital. Oktana (2023) menjelaskan bahwa media sosial dapat berkedudukan sebagai alat bukti elektronik yang sah sepanjang memenuhi syarat formil dan materil sebagaimana diatur dalam UU ITE. Artinya, bukti digital tidak cukup hanya ada, tetapi harus diperoleh, disimpan, dan diajukan dengan prosedur yang dapat dipertanggungjawabkan.

Virdayanti & Mahendrayana (2025) juga menjelaskan bahwa teknologi dapat membantu investigasi tindak pidana melalui penggunaan CCTV, forensik digital, pengenalan wajah, pengenalan suara, analisis data, dan kecerdasan buatan. Namun, penggunaan teknologi dalam investigasi juga harus memperhatikan privasi, keamanan data, dan hak asasi manusia. Dengan demikian, pembuktian kejahatan siber harus menjaga keseimbangan antara efektivitas penegakan hukum dan perlindungan hak warga negara.

Dalam menganalisis kasus kejahatan siber dan penipuan online, terdapat beberapa unsur penting yang perlu diperhatikan.

1. **Identitas pelaku dan korban**

   Analisis dimulai dengan mengidentifikasi siapa pelaku dan siapa korban. Dalam kejahatan siber, pelaku sering menggunakan identitas palsu, nomor sementara, akun anonim, atau nama orang lain. Oleh sebab itu, identifikasi pelaku membutuhkan bukti digital yang menghubungkan akun, perangkat, nomor, rekening, atau alamat IP dengan tindakan kejahatan.

2. **Media atau sistem yang digunakan**

   Penipuan online dapat dilakukan melalui WhatsApp, Telegram, Instagram, Facebook, marketplace, email, situs web palsu, aplikasi palsu, atau sistem perbankan digital. Media yang digunakan penting untuk menentukan jenis bukti dan pihak yang dapat dimintai keterangan.

3. **Modus operandi**

   Modus operandi menjelaskan cara pelaku melakukan kejahatan. Contohnya, mengirim tautan palsu, berpura-pura sebagai pegawai bank, menawarkan investasi palsu, membuat toko online fiktif, mengambil alih akun, atau mengakses sistem elektronik tanpa izin.

4. **Unsur tipu muslihat atau akses tanpa hak**

   Dalam penipuan online, perlu dianalisis apakah pelaku menggunakan kebohongan, manipulasi, janji palsu, atau identitas palsu untuk membuat korban menyerahkan uang atau data. Dalam akses ilegal, perlu dianalisis apakah pelaku masuk ke sistem elektronik tanpa hak.

5. **Kerugian korban**

   Kerugian dapat berupa uang hilang, akun diambil alih, data pribadi bocor, reputasi rusak, atau tekanan psikologis. Kerugian harus dibuktikan melalui dokumen transaksi, laporan rekening, bukti percakapan, atau keterangan korban.

6. **Bukti digital**

   Bukti digital menjadi dasar penting dalam membuktikan hubungan antara pelaku, perbuatan, dan kerugian. Bukti harus dijaga agar tidak diubah, dihapus, atau dipalsukan.

7. **Dasar hukum yang digunakan**

   Dasar hukum dapat berupa UU ITE, KUHP, UU PDP, UU Perlindungan Konsumen, atau aturan khusus lain. Pemilihan dasar hukum harus disesuaikan dengan fakta kasus dan bentuk perbuatan.

8. **Upaya pemulihan korban**

   Penanganan kasus tidak hanya bertujuan menghukum pelaku, tetapi juga memulihkan korban. Pemulihan dapat berupa pengembalian dana, pemblokiran akun pelaku, pemulihan akun korban, penghapusan data yang disalahgunakan, atau rehabilitasi nama baik.

Tabel berikut merangkum bentuk-bentuk kejahatan siber dan penipuan online yang sering terjadi.

Tabel 15.3: Bentuk Kejahatan Siber dan Penipuan Online

Bentuk Kasus	Modus yang Digunakan	Contoh Dampak bagi Korban	Aspek Hukum yang Relevan
Phishing	Tautan atau situs palsu menyerupai layanan resmi	Akun diambil alih, saldo hilang, data bocor	Akses ilegal, penipuan, perlindungan data
Penipuan marketplace	Toko palsu, pembayaran di luar platform, bukti transfer palsu	Uang hilang, barang tidak diterima	Penipuan online, perlindungan konsumen
Penipuan mobile banking	OTP dicuri, aplikasi palsu, pesan mengatasnamakan bank	Rekening terkuras, akun diambil alih	Cybercrime perbankan, UU ITE, perlindungan nasabah
Investasi online palsu	Janji keuntungan tinggi dan cepat	Kerugian finansial besar	Penipuan, perlindungan konsumen, regulasi keuangan
Akses ilegal	Masuk ke sistem elektronik tanpa hak	Kerugian sistem, pencurian data, gangguan layanan	Pasal 30 jo. Pasal 46 UU ITE
Doxing dan pemerasan digital	Penyebaran data pribadi atau ancaman penyebaran data	Tekanan psikologis, reputasi rusak	Pelindungan data pribadi, pemerasan
Malware dan aplikasi palsu	Aplikasi berisi program berbahaya	Data dicuri, perangkat dikendalikan	Gangguan sistem elektronik, akses ilegal
Penipuan lowongan kerja	Biaya administrasi palsu, identitas perusahaan palsu	Kerugian uang dan data pribadi	Penipuan, penyalahgunaan identitas

Kejahatan siber dan penipuan online juga perlu dilihat dari sudut perlindungan korban. Banyak korban tidak segera melapor karena malu, tidak tahu prosedur hukum, atau menganggap kerugian sulit dipulihkan.

Padahal, laporan cepat dapat membantu pemblokiran rekening, pelacakan transaksi, pengamanan bukti, dan pencegahan korban lain. Oleh karena itu, literasi hukum digital perlu ditingkatkan agar masyarakat memahami cara menyimpan bukti, melapor ke pihak berwenang, dan menghindari penghapusan bukti digital.

Langkah awal yang dapat dilakukan korban penipuan online adalah menyimpan seluruh bukti komunikasi, tangkapan layar, nomor rekening pelaku, tautan yang dikirim, nomor telepon, bukti transfer, dan kronologi kejadian. Korban juga dapat segera menghubungi bank atau penyedia layanan keuangan untuk meminta pemblokiran transaksi atau rekening tujuan apabila memungkinkan. Setelah itu, korban dapat membuat laporan kepada pihak kepolisian dan melaporkan akun, situs, atau nomor pelaku kepada platform terkait.

Dari sisi pencegahan, masyarakat perlu memahami bahwa penipuan online sering memanfaatkan rasa takut, tergesa-gesa, serakah, atau percaya berlebihan. Karena itu, pengguna harus berhati-hati terhadap pesan yang meminta OTP, PIN, password, atau data pribadi. Bank, marketplace, dan platform resmi umumnya tidak meminta kode rahasia melalui pesan pribadi. Pengguna juga perlu memeriksa alamat situs, menggunakan aplikasi resmi, tidak mengklik tautan mencurigakan, dan mengaktifkan autentikasi dua faktor.

Organisasi dan platform digital juga memiliki tanggung jawab penting. Mereka harus menyediakan sistem keamanan yang memadai, mekanisme pelaporan yang mudah, edukasi kepada pengguna, verifikasi akun, deteksi transaksi mencurigakan, serta respons cepat terhadap insiden. Dalam konteks e-commerce, platform perlu mencegah transaksi di luar sistem, memblokir toko palsu, dan memperkuat mekanisme penyelesaian sengketa. Dalam konteks perbankan, bank perlu memperkuat autentikasi, monitoring transaksi, edukasi nasabah, dan respons terhadap laporan kejahatan digital.

Aparat penegak hukum juga perlu terus meningkatkan kapasitas dalam menangani kejahatan siber. Penanganan kasus tidak cukup hanya memahami hukum pidana konvensional, tetapi juga memerlukan kemampuan membaca bukti digital, memahami sistem elektronik, melakukan koordinasi dengan platform, dan menggunakan forensik digital. Habibi dan Liviani (2020) menegaskan bahwa hambatan penegakan hukum

cybercrime di Indonesia masih berkaitan dengan perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Oleh karena itu, penguatan sumber daya manusia dan sarana forensik digital menjadi kebutuhan penting.

Dengan demikian, kasus kejahatan siber dan penipuan online menunjukkan bahwa perkembangan teknologi informasi harus disertai dengan kesiapan hukum, keamanan sistem, literasi digital, dan etika penggunaan teknologi. Penipuan online tidak hanya merugikan korban secara finansial, tetapi juga dapat mengancam privasi, reputasi, dan kepercayaan masyarakat terhadap layanan digital. Analisis kasus kejahatan siber harus memperhatikan fakta, modus, media yang digunakan, bukti digital, dasar hukum, kerugian korban, serta upaya pemulihan. Semakin meningkat penggunaan teknologi digital, semakin penting pula perlindungan hukum terhadap masyarakat dari kejahatan siber dan penipuan online.

15.4 Kasus Pelanggaran Hak Cipta Digital

Pelanggaran hak cipta digital merupakan salah satu persoalan hukum yang semakin sering terjadi seiring berkembangnya teknologi informasi. Karya yang dahulu hanya beredar dalam bentuk fisik, seperti buku, musik, film, foto, desain, dan karya seni, kini banyak tersedia dalam bentuk digital. Perubahan ini memberikan kemudahan bagi masyarakat untuk mengakses dan menikmati karya cipta. Namun, pada saat yang sama, teknologi digital juga memudahkan pihak tertentu untuk menggandakan, mengunggah ulang, menyebarkan, memodifikasi, atau memperjualbelikan karya cipta tanpa izin dari pencipta atau pemegang hak cipta.

Hak cipta pada dasarnya memberikan hak eksklusif kepada pencipta atau pemegang hak cipta atas ciptaannya. Hak eksklusif tersebut meliputi hak moral dan hak ekonomi. Hak moral berkaitan dengan hak pencipta untuk tetap diakui sebagai pembuat karya, sedangkan hak ekonomi berkaitan dengan hak untuk memperoleh manfaat ekonomi dari karya tersebut. Dalam konteks digital, pelanggaran hak cipta dapat merugikan pencipta karena karya dapat disebarluaskan secara cepat tanpa izin, tanpa atribusi, dan tanpa pembayaran royalti.

Di Indonesia, perlindungan hak cipta diatur dalam Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Undang-undang ini memberikan

perlindungan terhadap berbagai ciptaan di bidang ilmu pengetahuan, seni, dan sastra, termasuk karya tulis, musik, film, fotografi, program komputer, desain, dan karya digital lainnya. Dalam era digital, pelanggaran hak cipta tidak hanya terjadi melalui penjualan barang bajakan secara fisik, tetapi juga melalui situs web, media sosial, layanan streaming ilegal, kanal video, aplikasi berbagi file, dan platform digital lainnya.

Gambar 15.4: Alur Kasus Pelanggaran Hak Cipta Digital

Pelanggaran hak cipta digital menjadi lebih kompleks karena karya digital sangat mudah disalin dan disebarkan. Satu file digital dapat digandakan berkali-kali tanpa mengurangi kualitas aslinya. Film, lagu, e-book, foto, video, dan software dapat diunggah ke internet dan diakses oleh banyak orang dalam waktu singkat. Wulandari (2024) menjelaskan bahwa pelanggaran hak cipta di era digital meningkat karena kemudahan distribusi dan penggunaan konten digital tanpa izin. Hal ini menimbulkan kerugian bagi pencipta dan pemegang hak cipta, baik secara ekonomi maupun secara moral.

Salah satu bentuk pelanggaran hak cipta digital yang banyak terjadi adalah pembajakan karya digital. Pembajakan ini dapat berupa penyebaran e-book tanpa izin, pengunggahan film ke situs ilegal, pembagian software bajakan, pengunggahan ulang konten video, atau distribusi musik tanpa lisensi. Syafi'iyah et al. (2026) menjelaskan bahwa pembajakan karya digital di Indonesia masih terjadi karena rendahnya kesadaran hukum masyarakat,

lemahnya penegakan hukum, dan sulitnya pengawasan terhadap platform digital.

Kasus situs streaming ilegal menjadi contoh nyata pelanggaran hak cipta digital. Melalui situs tersebut, film atau karya sinematografi dapat ditonton atau diunduh secara gratis tanpa izin dari pencipta atau pemegang hak cipta. Padahal, film merupakan karya sinematografi yang dilindungi oleh Undang-Undang Hak Cipta. Novia et al., (2022) menjelaskan bahwa pembajakan karya sinematografi melalui situs streaming ilegal merupakan bentuk pelanggaran hak cipta karena karya film digandakan dan disebarkan tanpa izin. Perbuatan ini merugikan pencipta, produser, rumah produksi, distributor, dan pihak lain yang memiliki hak ekonomi atas film tersebut.

Pelanggaran hak cipta melalui situs streaming ilegal juga berdampak pada industri kreatif. Ketika masyarakat lebih memilih menonton film melalui situs ilegal, pendapatan dari bioskop, layanan streaming resmi, dan distribusi legal dapat menurun. Hal ini mengurangi potensi royalti dan keuntungan yang seharusnya diterima oleh pencipta atau pemegang hak cipta. Jika praktik ini terus berlangsung, maka pencipta dan pelaku industri kreatif dapat kehilangan motivasi untuk menghasilkan karya baru.

Selain film, pelanggaran hak cipta digital juga sering terjadi pada konten kreator media sosial. Konten berupa video, foto, ilustrasi, musik, ulasan, tutorial, atau karya kreatif lain sering diunggah ulang oleh akun lain tanpa izin. Dalam beberapa kasus, konten tersebut digunakan untuk kepentingan komersial, seperti iklan, promosi produk, peningkatan engagement, atau monetisasi akun. Abya et al., (2024) membahas kasus re-upload video konten kreator media sosial untuk kegiatan komersial berdasarkan Putusan Mahkamah Agung Nomor 41 PK/Pdt.Sus-HKI/2021. Kasus ini menunjukkan bahwa konten digital yang dibuat oleh kreator tetap dilindungi oleh hak cipta meskipun diunggah melalui platform media sosial.

Re-upload konten tanpa izin dapat melanggar hak moral dan hak ekonomi pencipta. Hak moral dilanggar apabila nama pencipta tidak dicantumkan atau karya diklaim sebagai milik orang lain. Hak ekonomi dilanggar apabila karya digunakan untuk memperoleh keuntungan tanpa izin. Misalnya, seseorang mengunduh video dari akun kreator asli, lalu mengunggahnya kembali ke akun lain untuk menarik penonton dan memperoleh pendapatan iklan. Perbuatan ini tidak dapat dibenarkan hanya karena konten tersebut tersedia secara terbuka di internet.

Dalam konteks media sosial, masih banyak masyarakat yang salah memahami bahwa semua konten yang tersedia di internet dapat digunakan secara bebas. Padahal, keterbukaan akses tidak sama dengan kebebasan menggunakan. Konten yang diunggah di internet tetap memiliki pencipta dan tetap dilindungi oleh hak cipta. Penggunaan ulang harus memperhatikan izin, lisensi, tujuan penggunaan, atribusi, serta batasan penggunaan wajar. Jika konten digunakan untuk tujuan komersial tanpa izin, maka potensi pelanggaran hak cipta menjadi lebih kuat.

Pelanggaran hak cipta digital juga dapat terjadi dalam bentuk pembajakan software. Software merupakan salah satu objek hak cipta yang memiliki nilai ekonomi tinggi. Penggunaan software tanpa lisensi, penyebaran crack, aktivator ilegal, atau salinan program berbayar secara gratis merupakan bentuk pelanggaran hak cipta. Praktik ini merugikan pengembang software dan dapat menimbulkan risiko keamanan bagi pengguna karena software bajakan sering mengandung malware atau celah keamanan.

Selain itu, pelanggaran hak cipta digital dapat terjadi pada karya tulis dan e-book. Buku digital sangat mudah disebarkan melalui grup pesan instan, media sosial, situs berbagi file, atau marketplace tidak resmi. Banyak karya tulis diperbanyak dalam bentuk PDF dan dibagikan tanpa izin dari penulis atau penerbit. Meskipun tampak sederhana, praktik ini tetap merugikan penulis karena menghilangkan potensi pendapatan dari penjualan legal. Di sisi lain, tindakan tersebut juga melemahkan penghargaan masyarakat terhadap karya intelektual.

Kasus pelanggaran hak cipta digital perlu dianalisis melalui beberapa unsur. Pertama, harus dilihat apakah karya tersebut merupakan ciptaan yang dilindungi. Kedua, perlu diketahui siapa pencipta atau pemegang hak cipta. Ketiga, perlu dianalisis apakah ada tindakan penggandaan, distribusi, pengumuman, modifikasi, atau penggunaan komersial tanpa izin. Keempat, perlu dibuktikan apakah tindakan tersebut menimbulkan kerugian bagi pencipta atau pemegang hak cipta. Kelima, perlu ditentukan apakah penyelesaian dilakukan melalui jalur perdata, pidana, administratif, atau mekanisme platform digital.

Dalam kasus pelanggaran hak cipta digital, bukti elektronik memiliki peran penting. Bukti dapat berupa tangkapan layar unggahan, tautan situs, riwayat upload, metadata file, informasi akun pelaku, laporan platform, bukti

monetisasi, bukti transaksi, dan dokumen kepemilikan hak cipta. Bukti tersebut harus dikumpulkan dengan hati-hati agar dapat menunjukkan hubungan antara karya asli, tindakan pelanggaran, pelaku, dan kerugian. Dalam praktiknya, pencipta atau pemegang hak cipta sering kali perlu menyimpan dokumentasi karya, tanggal publikasi, lisensi, dan bukti bahwa karya tersebut merupakan hasil ciptaannya.

Secara hukum, pelanggaran hak cipta digital dapat menimbulkan akibat bagi pelaku. Pelaku dapat diminta menghentikan penggunaan karya, menghapus unggahan, membayar ganti rugi, atau menghadapi sanksi pidana apabila memenuhi unsur tertentu dalam Undang-Undang Hak Cipta. Dalam konteks platform digital, pemegang hak cipta juga dapat mengajukan laporan pelanggaran melalui mekanisme takedown atau penghapusan konten. Mekanisme ini penting untuk mencegah penyebaran karya bajakan secara lebih luas.

Pelanggaran hak cipta digital juga dapat dianalisis dari sudut etika digital. Menggunakan karya orang lain tanpa izin merupakan tindakan yang tidak menghargai proses kreatif pencipta. Dalam ruang digital, etika penggunaan karya mencakup mencantumkan sumber, meminta izin, menggunakan karya sesuai lisensi, tidak mengklaim karya orang lain, dan tidak mengambil keuntungan dari karya yang bukan miliknya. Oleh karena itu, pendidikan mengenai etika digital dan literasi hak cipta menjadi bagian penting dalam pencegahan pelanggaran.

Pencegahan pelanggaran hak cipta digital membutuhkan kerja sama berbagai pihak. Pemerintah perlu memperkuat pengawasan dan penegakan hukum. Platform digital perlu menyediakan mekanisme pelaporan pelanggaran yang mudah dan efektif. Pencipta perlu memahami cara melindungi karya digitalnya, misalnya melalui watermark, dokumentasi publikasi, lisensi, dan pendaftaran hak cipta apabila diperlukan. Masyarakat perlu diedukasi agar tidak mengunduh, menyebarkan, atau menggunakan karya bajakan.

Tabel berikut merangkum beberapa bentuk pelanggaran hak cipta digital dan akibat hukumnya.

Tabel 15.4: Bentuk Pelanggaran Hak Cipta Digital dan Akibat Hukumnya

Bentuk Pelanggaran	Contoh Perbuatan	Objek yang Dilanggar	Akibat Hukum dan Dampak
Streaming ilegal	Mengunggah film ke situs ilegal	Film atau karya sinematografi	Kerugian ekonomi bagi pencipta dan pemegang hak cipta
Re-upload konten	Mengunggah ulang video kreator tanpa izin	Video, foto, musik, konten media sosial	Pelanggaran hak moral dan hak ekonomi
Pembajakan software	Menggunakan software tanpa lisensi	Program komputer	Kerugian pengembang dan risiko keamanan digital
Pembajakan e-book	Membagikan file PDF buku tanpa izin	Karya tulis digital	Hilangnya royalti penulis dan penerbit
Distribusi musik ilegal	Membagikan lagu melalui situs atau aplikasi ilegal	Karya musik	Kerugian royalti dan pelanggaran lisensi
Modifikasi karya tanpa izin	Mengubah desain, foto, atau video lalu mengunggah ulang	Karya visual dan audiovisual	Pelanggaran atribusi dan integritas karya
Penggunaan komersial tanpa izin	Memakai konten orang lain untuk iklan atau promosi	Konten digital kreator	Potensi gugatan ganti rugi dan penghapusan konten

Dalam menganalisis kasus pelanggaran hak cipta digital, terdapat beberapa langkah yang dapat dilakukan.

1. **Mengidentifikasi karya yang dilindungi**

   Langkah pertama adalah memastikan bahwa objek yang dipersoalkan merupakan ciptaan yang dilindungi oleh hukum hak cipta, seperti film, musik, video, foto, desain, e-book, atau software.

2. **Menentukan pencipta atau pemegang hak cipta**

   Analisis perlu menjelaskan siapa pencipta, pemegang hak cipta, produser, penerbit, atau pihak yang memiliki hak ekonomi atas karya tersebut.

3. **Menelusuri bentuk pelanggaran**

   Pelanggaran dapat berupa penggandaan, pengumuman, distribusi, re-upload, modifikasi, atau penggunaan komersial tanpa izin.

4. **Menilai izin atau lisensi**

   Perlu diperiksa apakah penggunaan karya dilakukan dengan izin, lisensi, atau ketentuan penggunaan tertentu. Jika tidak ada izin, maka tindakan tersebut berpotensi melanggar hak cipta.

5. **Mengumpulkan bukti digital**

   Bukti dapat berupa tautan situs, tangkapan layar, bukti upload, metadata, informasi akun, bukti transaksi, atau bukti monetisasi.

6. **Menilai kerugian pencipta atau pemegang hak cipta**

   Kerugian dapat berupa hilangnya royalti, penurunan pendapatan, reputasi karya yang rusak, atau hilangnya kontrol atas distribusi karya.

7. **Menentukan jalur penyelesaian**

   Penyelesaian dapat dilakukan melalui pelaporan ke platform, somasi, gugatan perdata, laporan pidana, atau penyelesaian alternatif.

8. **Merumuskan pencegahan**

   Pencegahan dapat berupa edukasi hak cipta, penguatan sistem pelaporan, penggunaan watermark, perlindungan teknologi, dan peningkatan kesadaran masyarakat.

Pelanggaran hak cipta digital menunjukkan bahwa perkembangan teknologi harus diimbangi dengan kesadaran hukum dan etika. Masyarakat perlu memahami bahwa karya digital bukan barang bebas yang dapat digunakan sesuka hati. Setiap karya memiliki pencipta, nilai ekonomi, dan perlindungan hukum. Oleh karena itu, penggunaan karya digital harus dilakukan secara bertanggung jawab, baik untuk kepentingan pribadi, pendidikan, hiburan, maupun komersial.

Dengan demikian, kasus pelanggaran hak cipta digital di Indonesia memperlihatkan adanya tantangan besar dalam melindungi karya kreatif pada era internet. Situs streaming ilegal, pembajakan e-book, penggunaan software bajakan, re-upload konten kreator, dan distribusi musik ilegal merupakan bentuk nyata pelanggaran yang harus mendapat perhatian serius. Analisis kasus pelanggaran hak cipta digital perlu memperhatikan jenis

karya, bentuk pelanggaran, bukti elektronik, kerugian pencipta, dasar hukum, serta upaya penyelesaian. Perlindungan hak cipta digital hanya dapat berjalan efektif apabila regulasi, penegakan hukum, platform digital, pencipta, dan masyarakat bekerja bersama untuk menghargai karya intelektual.

15.5 Kasus Sengketa Transaksi Elektronik

Sengketa transaksi elektronik merupakan persoalan hukum yang muncul akibat hubungan hukum yang dilakukan melalui sistem elektronik. Transaksi elektronik dapat terjadi dalam bentuk jual beli online, penggunaan dompet digital, layanan marketplace, transaksi mobile banking, langganan aplikasi, kontrak digital, pembayaran cash on delivery, maupun penggunaan layanan berbasis platform. Dalam praktiknya, transaksi elektronik memberikan kemudahan bagi masyarakat karena dapat dilakukan secara cepat, fleksibel, dan tanpa pertemuan langsung antara para pihak. Namun, kemudahan tersebut juga membuka peluang munculnya sengketa, terutama ketika salah satu pihak tidak memenuhi kewajibannya.

Sengketa transaksi elektronik dapat terjadi antara konsumen dan pelaku usaha, pengguna dan platform digital, penjual dan pembeli, nasabah dan penyedia jasa keuangan digital, atau antara para pihak dalam kontrak elektronik. Sengketa dapat timbul karena barang tidak dikirim, barang tidak sesuai pesanan, keterlambatan pengiriman, saldo digital hilang, akun diblokir, pembayaran gagal, kesalahan sistem, penipuan toko online, wanprestasi, perbuatan melawan hukum, atau penyalahgunaan data dalam transaksi digital.

Di Indonesia, transaksi elektronik diatur dalam Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE. Dalam UU ITE, transaksi elektronik dipahami sebagai perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Pengaturan ini menunjukkan bahwa transaksi yang dilakukan secara digital tetap memiliki akibat hukum sebagaimana transaksi konvensional. Oleh sebab itu, para pihak yang membuat transaksi elektronik tetap terikat oleh hak dan kewajiban hukum.

Secara perdata, transaksi elektronik juga berkaitan dengan ketentuan umum perjanjian dalam Kitab Undang-Undang Hukum Perdata. Suatu perjanjian

dianggap sah apabila memenuhi syarat kesepakatan para pihak, kecakapan hukum, objek tertentu, dan sebab yang halal. Dalam transaksi elektronik, kesepakatan dapat muncul melalui klik persetujuan, pemesanan barang, konfirmasi pembayaran, penggunaan tanda tangan elektronik, atau persetujuan terhadap syarat dan ketentuan layanan. Anami et al. (2025) menjelaskan bahwa kontrak digital memiliki kesamaan dengan kontrak konvensional dan tetap mengikat para pihak sepanjang memenuhi unsur sahnya perjanjian sebagaimana diatur dalam Pasal 1320 KUH Perdata.

Sengketa transaksi elektronik sering terjadi dalam transaksi e-commerce. Konsumen dapat mengalami kerugian karena barang tidak sesuai deskripsi, barang rusak, barang tidak dikirim, pembayaran sudah dilakukan tetapi pesanan tidak diproses, atau pelaku usaha tidak bertanggung jawab. Sugara dan Sugara & Az-Zahra (2024) menjelaskan bahwa kegiatan jual beli melalui e-commerce merupakan bentuk perjanjian yang diatur dalam hukum perdata, tetapi pelaksanaannya sering menimbulkan masalah yang merugikan para pihak, khususnya konsumen.

Salah satu contoh sengketa yang sering terjadi adalah wanprestasi dalam jual beli online. Wanprestasi terjadi ketika salah satu pihak tidak melaksanakan kewajiban sebagaimana yang telah disepakati. Misalnya, pembeli telah membayar harga barang, tetapi penjual tidak mengirimkan barang. Contoh lain adalah penjual mengirim barang yang berbeda dari deskripsi, kualitas barang tidak sesuai, atau barang cacat. Dalam kondisi seperti ini, konsumen dapat menuntut pemenuhan prestasi, penggantian barang, pengembalian uang, atau ganti rugi.

Selain wanprestasi, sengketa transaksi elektronik juga dapat berbentuk perbuatan melawan hukum. Perbuatan melawan hukum terjadi apabila seseorang melakukan tindakan yang melanggar hukum dan menimbulkan kerugian bagi orang lain. Dalam e-commerce, perbuatan melawan hukum dapat berupa penipuan toko online, penggunaan identitas palsu, manipulasi bukti transaksi, penyebaran data pembeli, atau penggunaan sistem elektronik untuk merugikan pihak lain. Sugara dan Az-Zahra (2024) menjelaskan bahwa perbuatan melawan hukum dalam transaksi e-commerce dapat menimbulkan kesulitan dalam menuntut kerugian material dan immaterial apabila hanya dipandang sebagai perbuatan pidana.

Kasus lain yang penting adalah sengketa dalam pembayaran cash on delivery atau COD. COD pada dasarnya memberi kemudahan karena pembeli

membayar barang ketika barang diterima. Namun, dalam praktiknya, transaksi COD juga dapat menimbulkan sengketa. Pembeli dapat menolak membayar setelah barang sampai, menolak paket karena merasa tidak memesan, atau melakukan komplain kepada kurir padahal kesalahan berasal dari penjual atau platform. Di sisi lain, penjual juga dapat mengalami kerugian karena barang dikembalikan, biaya pengiriman meningkat, atau barang rusak dalam proses pengiriman. Rosid & Musadad (2025) menjelaskan bahwa transaksi COD dalam e-commerce dapat menimbulkan sengketa dan perlu diselesaikan melalui mekanisme di luar pengadilan seperti mediasi, konsiliasi, atau arbitrase.

Sengketa transaksi elektronik juga terjadi dalam layanan dompet digital. Salah satu contoh yang dibahas dalam literatur adalah sengketa saldo DANA. Dalam kasus seperti ini, persoalan dapat berkaitan dengan saldo yang hilang, transaksi yang tidak dikenali pengguna, kesalahan sistem, atau ketidakjelasan tanggung jawab penyedia layanan. Anami et al. (2025) menjelaskan bahwa studi kasus sengketa saldo DANA menunjukkan bahwa meskipun regulasi terkait kontrak digital telah tersedia, implementasi perlindungan hukum bagi para pihak masih perlu diperkuat. Hal ini menunjukkan pentingnya mekanisme pengaduan, verifikasi transaksi, pembuktian elektronik, dan tanggung jawab penyedia sistem elektronik.

Dalam sengketa transaksi elektronik, alat bukti elektronik memiliki peran sangat penting. Bukti dapat berupa invoice digital, bukti transfer, tangkapan layar percakapan, riwayat pesanan, resi pengiriman, email konfirmasi, log transaksi, syarat dan ketentuan platform, rekaman percakapan layanan pelanggan, atau dokumen elektronik lainnya. UU ITE mengakui informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah. Oleh karena itu, konsumen dan pelaku usaha perlu menyimpan bukti digital setiap kali melakukan transaksi.

Penyelesaian sengketa transaksi elektronik dapat dilakukan melalui jalur litigasi maupun nonlitigasi. Jalur litigasi dilakukan melalui pengadilan, misalnya gugatan perdata atau gugatan class action apabila kerugian dialami oleh banyak orang. Widjaja et al. (2018) menjelaskan bahwa Pasal 38 dan Pasal 39 UU ITE membuka ruang bagi setiap orang untuk mengajukan gugatan terhadap pihak yang menyelenggarakan sistem elektronik atau menggunakan teknologi informasi yang menimbulkan kerugian. Selain

gugatan perdata, masyarakat juga dapat mengajukan gugatan perwakilan apabila kerugian menimpa masyarakat luas.

Penyelesaian sengketa secara nonlitigasi dapat dilakukan melalui negosiasi, mediasi, konsiliasi, arbitrase, atau lembaga penyelesaian sengketa alternatif. Jalur ini sering dianggap lebih sesuai untuk sengketa transaksi elektronik karena lebih cepat, fleksibel, dan biaya relatif lebih rendah dibandingkan proses pengadilan. Widjaja et al. (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun nonlitigasi, termasuk mediasi, negosiasi, dan arbitrase. Dalam konteks perlindungan konsumen, penyelesaian di luar pengadilan juga dapat dilakukan melalui Badan Penyelesaian Sengketa Konsumen atau BPSK.

Junior et al., (2021) menjelaskan bahwa penyelesaian sengketa dalam transaksi bisnis e-commerce dapat dilakukan melalui litigasi maupun nonlitigasi. Litigasi dilakukan melalui pengadilan, sedangkan nonlitigasi dapat dilakukan melalui penyelesaian di luar pengadilan. Dalam praktiknya, banyak sengketa e-commerce diselesaikan terlebih dahulu melalui mekanisme internal platform, seperti pusat bantuan, komplain pesanan, pengembalian dana, retur barang, atau mediasi antara penjual dan pembeli oleh pihak platform.

Secara umum, sengketa transaksi elektronik dapat dianalisis melalui beberapa unsur berikut.

1. **Identifikasi para pihak**

   Analisis dimulai dengan menentukan siapa saja pihak yang terlibat, misalnya konsumen, penjual, marketplace, penyedia dompet digital, bank, jasa ekspedisi, atau penyelenggara sistem elektronik.

2. **Bentuk transaksi elektronik**

   Perlu dilihat apakah transaksi berupa jual beli online, pembayaran digital, kontrak elektronik, COD, pemesanan jasa, langganan aplikasi, atau transaksi perbankan digital.

3. **Kesepakatan dan syarat transaksi**

   Analisis harus memperhatikan syarat dan ketentuan platform, deskripsi produk, bukti pemesanan, harga, metode pembayaran, kebijakan retur, dan kesepakatan lain yang berlaku.

4. **Bentuk pelanggaran atau sengketa**

   Sengketa dapat berupa wanprestasi, perbuatan melawan hukum, barang tidak sesuai, saldo hilang, pembayaran gagal, barang tidak dikirim, atau akun pengguna bermasalah.

5. **Kerugian yang dialami**

   Kerugian dapat berupa kerugian finansial, hilangnya barang, hilangnya saldo, rusaknya reputasi, waktu yang terbuang, atau kerugian immaterial lainnya.

6. **Bukti elektronik**

   Bukti elektronik menjadi dasar penting untuk membuktikan hubungan hukum dan kerugian. Bukti dapat berupa riwayat transaksi, bukti transfer, invoice, chat, email, log sistem, atau resi pengiriman.

7. **Dasar hukum penyelesaian**

   Dasar hukum dapat berasal dari KUH Perdata, UU ITE, UU Perlindungan Konsumen, PP PSTE, UU PDP, atau ketentuan platform.

8. **Mekanisme penyelesaian**

   Penyelesaian dapat dilakukan melalui komplain platform, negosiasi, mediasi, BPSK, arbitrase, gugatan perdata, atau laporan pidana apabila terdapat unsur penipuan.

Tabel berikut merangkum bentuk sengketa transaksi elektronik dan mekanisme penyelesaiannya.

Tabel 15.5: Bentuk Sengketa Transaksi Elektronik dan Mekanisme Penyelesaiannya

Bentuk Sengketa	Contoh Kasus	Bukti yang Diperlukan	Mekanisme Penyelesaian
Barang tidak dikirim	Pembeli sudah membayar tetapi barang tidak sampai	Invoice, bukti transfer, chat, resi	Komplain platform, mediasi, gugatan perdata
Barang tidak sesuai	Produk berbeda dari deskripsi atau cacat	Foto barang, deskripsi produk, riwayat pesanan	Retur, refund, mediasi platform
Sengketa COD	Pembeli menolak bayar atau menolak paket	Bukti pesanan, resi, bukti pengiriman	Mediasi platform, negosiasi, BPSK

Bentuk Sengketa	Contoh Kasus	Bukti yang Diperlukan	Mekanisme Penyelesaian
Saldo digital hilang	Saldo dompet digital berkurang tanpa transaksi yang diakui	Riwayat transaksi, log akun, laporan aplikasi	Pengaduan platform, OJK/BI, gugatan
Kontrak digital bermasalah	Persetujuan elektronik dipersoalkan	Syarat dan ketentuan, bukti klik, tanda tangan elektronik	Mediasi, arbitrase, pengadilan
Penipuan toko online	Penjual palsu menerima uang lalu menghilang	Bukti transfer, chat, akun pelaku	Laporan platform, kepolisian, gugatan
Data transaksi disalahgunakan	Data pembeli dipakai tanpa izin	Kebijakan privasi, bukti penggunaan data	Pengaduan, UU PDP, gugatan
Gagal pengembalian dana	Refund tidak diproses meskipun syarat terpenuhi	Bukti komplain, status pesanan, kebijakan refund	Komplain platform, BPSK, gugatan perdata

Dalam menganalisis sengketa transaksi elektronik, penting untuk membedakan antara sengketa perdata dan tindak pidana. Tidak semua masalah transaksi online langsung merupakan pidana. Jika sengketa muncul karena keterlambatan pengiriman, barang cacat, atau ketidaksesuaian prestasi, maka persoalan dapat dianalisis sebagai wanprestasi atau sengketa perdata. Namun, apabila sejak awal terdapat niat menipu, identitas palsu, manipulasi sistem, atau pengambilan uang secara melawan hukum, maka perkara dapat berkembang menjadi tindak pidana penipuan atau kejahatan siber.

Penyelesaian sengketa elektronik yang ideal sebaiknya dimulai dari mekanisme yang paling sederhana. Pertama, konsumen dapat menghubungi penjual atau penyedia layanan. Kedua, konsumen dapat mengajukan komplain melalui fitur resmi platform. Ketiga, para pihak dapat melakukan negosiasi atau mediasi. Keempat, jika tidak selesai, sengketa dapat dibawa ke BPSK, lembaga arbitrase, atau pengadilan. Kelima, apabila terdapat unsur pidana, korban dapat membuat laporan kepada aparat penegak hukum.

Perlindungan konsumen dalam transaksi elektronik juga menuntut tanggung jawab pelaku usaha dan platform digital. Pelaku usaha wajib memberikan informasi yang benar, jelas, dan jujur mengenai produk atau layanan.

Platform digital perlu menyediakan sistem pengaduan yang mudah diakses, kebijakan pengembalian dana yang transparan, serta mekanisme verifikasi penjual. Konsumen juga harus berhati-hati dengan membaca deskripsi produk, memeriksa reputasi penjual, tidak bertransaksi di luar platform, dan menyimpan bukti digital.

Sengketa transaksi elektronik menunjukkan bahwa perkembangan teknologi harus diikuti dengan pemahaman hukum digital. Masyarakat perlu memahami bahwa klik persetujuan, bukti pembayaran, riwayat chat, invoice elektronik, dan dokumen digital lainnya dapat memiliki nilai hukum. Di sisi lain, pelaku usaha harus memahami bahwa transaksi online tetap menimbulkan kewajiban hukum yang harus dipenuhi. Oleh karena itu, literasi hukum digital menjadi penting agar para pihak tidak hanya mampu menggunakan teknologi, tetapi juga memahami konsekuensi hukumnya.

Dengan demikian, kasus sengketa transaksi elektronik di Indonesia menunjukkan bahwa hubungan hukum digital tetap memerlukan kepastian, perlindungan, dan mekanisme penyelesaian yang efektif. Sengketa dapat terjadi dalam e-commerce, dompet digital, kontrak digital, COD, maupun layanan platform lainnya. Analisis sengketa harus memperhatikan para pihak, bentuk transaksi, kesepakatan elektronik, bukti digital, kerugian, dasar hukum, serta jalur penyelesaian. Penyelesaian sengketa yang cepat, adil, dan mudah diakses akan memperkuat kepercayaan masyarakat terhadap ekosistem transaksi elektronik.

15.6 Pembelajaran Hukum dari Kasus Teknologi Informasi di Indonesia

Kasus-kasus hukum teknologi informasi di Indonesia memberikan banyak pembelajaran penting bagi perkembangan hukum, penegakan hukum, tata kelola digital, serta perilaku masyarakat dalam menggunakan teknologi. Berbagai kasus seperti penyalahgunaan data pribadi, kebocoran data, kejahatan siber, penipuan online, pelanggaran hak cipta digital, dan sengketa transaksi elektronik menunjukkan bahwa teknologi tidak hanya membawa kemudahan, tetapi juga menghadirkan risiko hukum yang kompleks. Oleh karena itu, pembelajaran dari kasus-kasus tersebut penting untuk memahami bagaimana hukum harus merespons perubahan sosial akibat perkembangan teknologi.

Gambar 15.5: Pembelajaran Hukum dari Kasus Teknologi Informasi di Indonesia

Pembelajaran pertama adalah bahwa hukum harus mampu mengikuti perkembangan teknologi. Perkembangan teknologi informasi berlangsung sangat cepat, sedangkan pembentukan dan penerapan hukum sering berjalan lebih lambat. Akibatnya, muncul celah antara praktik digital di masyarakat dan aturan hukum yang tersedia. Sebelum hadirnya Undang-Undang Pelindungan Data Pribadi, pelindungan data pribadi di Indonesia masih tersebar dalam berbagai peraturan sektoral. Hal ini terlihat dalam kasus-kasus kebocoran data pengguna media sosial, e-commerce, dan layanan publik digital yang menunjukkan belum kuatnya pengaturan dan pengawasan perlindungan data pada masa sebelumnya (Satrio & Widiatno, 2020).

Pembelajaran kedua adalah pentingnya pelindungan data pribadi sebagai bagian dari hak warga negara. Kasus kebocoran data Tokopedia, BPJS Kesehatan, media sosial, dan sektor perbankan menunjukkan bahwa data pribadi memiliki nilai ekonomi dan dapat disalahgunakan untuk berbagai kepentingan. Data seperti nama, nomor telepon, alamat, NIK, data kesehatan, dan data keuangan tidak boleh dipandang sebagai informasi biasa. Data tersebut melekat pada hak privasi seseorang dan harus dikelola secara hati-hati. Anindya & Subiyanto (2025) menjelaskan bahwa

kebocoran data Tokopedia menimbulkan pertanyaan mengenai tanggung jawab platform dalam menjaga data pengguna. Sementara itu, Sorisa et al., (2024) menunjukkan bahwa kebocoran data BPJS Kesehatan berdampak pada kepercayaan publik terhadap institusi pengelola data.

Pembelajaran ketiga adalah bahwa pengelola sistem elektronik harus bertanggung jawab secara hukum dan etik. Platform digital, marketplace, bank, dompet digital, lembaga publik, dan penyedia layanan online tidak cukup hanya menyediakan layanan yang mudah digunakan. Mereka juga harus memastikan keamanan sistem, transparansi pemrosesan data, mekanisme pengaduan, serta perlindungan bagi pengguna. Dalam konteks pelindungan data pribadi, pengendali data wajib menjaga keamanan data, membatasi akses, menggunakan data sesuai tujuan, dan memberi pemberitahuan apabila terjadi insiden. Fadli et al., (2026) menegaskan bahwa pelanggaran etika teknologi informasi di Indonesia banyak dipengaruhi oleh lemahnya keamanan informasi, rendahnya literasi digital, dan kurangnya komitmen organisasi.

Pembelajaran keempat adalah bahwa pembuktian digital menjadi aspek kunci dalam penegakan hukum. Dalam kasus kejahatan siber, penipuan online, akses ilegal, sengketa transaksi elektronik, dan pelanggaran hak cipta digital, bukti yang digunakan sering kali berbentuk elektronik. Bukti tersebut dapat berupa tangkapan layar, riwayat transaksi, log akses, metadata, email, chat, rekaman CCTV, invoice digital, tautan situs, data akun, atau hasil forensik digital. Aini & Lubis (2024) menjelaskan bahwa pembuktian dalam kasus kejahatan siber menghadapi tantangan karena bukti digital bersifat mudah berubah, mudah dihapus, dan sering tersebar pada berbagai sistem. Oleh karena itu, penanganan bukti digital harus dilakukan secara cepat, hati-hati, dan sesuai prosedur.

Pembelajaran kelima adalah pentingnya peningkatan kapasitas aparat penegak hukum. Kejahatan teknologi informasi tidak dapat ditangani hanya dengan pendekatan hukum konvensional. Aparat penegak hukum perlu memahami teknologi, sistem elektronik, keamanan siber, forensik digital, dan pola kejahatan online. Habibi & Liviani (2020) menjelaskan bahwa penegakan hukum cybercrime di Indonesia masih menghadapi hambatan pada perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Hal ini menunjukkan perlunya pelatihan berkelanjutan,

penguatan laboratorium forensik digital, dan kerja sama antara aparat hukum, ahli teknologi, akademisi, serta penyelenggara sistem elektronik.

Pembelajaran keenam adalah bahwa masyarakat membutuhkan literasi hukum digital. Banyak kasus teknologi informasi terjadi karena rendahnya pemahaman masyarakat mengenai hak dan kewajiban di ruang digital. Korban penipuan online sering tidak memahami cara menyimpan bukti dan melapor. Pengguna media sosial sering tidak menyadari bahwa menyebarkan data pribadi orang lain dapat melanggar hukum. Masyarakat juga sering menganggap konten di internet bebas digunakan, padahal karya digital tetap dilindungi hak cipta. Wulandari (2024) menjelaskan bahwa pelanggaran hak cipta di era digital meningkat karena kemudahan distribusi dan penggunaan konten digital tanpa izin. Oleh sebab itu, literasi hukum digital harus mencakup pelindungan data pribadi, keamanan transaksi, etika komunikasi, hak cipta, dan penggunaan bukti elektronik.

Pembelajaran ketujuh adalah perlunya memperkuat perlindungan konsumen digital. Sengketa transaksi elektronik menunjukkan bahwa konsumen dapat mengalami kerugian akibat barang tidak dikirim, barang tidak sesuai, saldo digital hilang, pembayaran gagal, akun diblokir, atau pelaku usaha tidak bertanggung jawab. Sugara & Az-Zahra (2024) menjelaskan bahwa transaksi e-commerce merupakan bentuk perjanjian yang diatur dalam hukum perdata, tetapi pelaksanaannya sering menimbulkan masalah yang merugikan para pihak. Dengan demikian, perlindungan konsumen digital memerlukan mekanisme pengaduan yang mudah, sistem refund yang jelas, verifikasi penjual, serta penyelesaian sengketa yang cepat dan adil.

Pembelajaran kedelapan adalah pentingnya penyelesaian sengketa yang tidak hanya bergantung pada pengadilan. Dalam kasus transaksi elektronik, penyelesaian melalui pengadilan sering membutuhkan waktu dan biaya. Oleh karena itu, penyelesaian nonlitigasi seperti negosiasi, mediasi, konsiliasi, arbitrase, dan penyelesaian melalui platform digital menjadi penting. Widjaja et al., (2018) menjelaskan bahwa sengketa transaksi elektronik dapat diselesaikan melalui pengadilan maupun di luar pengadilan. Rosid & Musadad (2025) juga menekankan pentingnya penyelesaian sengketa konsumen e-commerce di luar pengadilan, terutama agar penyelesaian dapat dilakukan lebih cepat dan efisien.

Pembelajaran kesembilan adalah bahwa etika digital harus berjalan bersama hukum. Tidak semua tindakan buruk di dunia digital langsung diproses

sebagai tindak pidana, tetapi perilaku tidak etis sering menjadi awal dari pelanggaran hukum. Misalnya, menggunakan data orang lain tanpa izin, mengunggah ulang konten kreator, menyebarkan informasi pribadi, membuat toko online palsu, atau memberikan informasi produk yang menyesatkan. Etika digital membantu membangun kesadaran agar pengguna teknologi tidak hanya bertanya "apakah ini boleh secara hukum?", tetapi juga "apakah ini adil, aman, dan bertanggung jawab?"

Pembelajaran kesepuluh adalah perlunya tanggung jawab bersama antara individu, organisasi, platform, dan negara. Individu bertanggung jawab menjaga data pribadi, tidak mudah membagikan OTP, tidak menyebarkan konten ilegal, dan menghormati hak cipta. Organisasi bertanggung jawab mengelola data dan sistem secara aman. Platform bertanggung jawab menyediakan mekanisme perlindungan pengguna dan pelaporan pelanggaran. Negara bertanggung jawab membentuk regulasi, melakukan pengawasan, dan menegakkan hukum. Tanpa kerja sama semua pihak, kasus-kasus teknologi informasi akan terus berulang.

Dari berbagai kasus yang telah dibahas dalam bab ini, dapat ditarik beberapa pelajaran hukum utama.

1. **Pelindungan data pribadi harus menjadi prioritas**

   Data pribadi merupakan bagian dari hak privasi dan memiliki nilai ekonomi. Kebocoran atau penyalahgunaan data dapat menimbulkan kerugian finansial, reputasional, psikologis, dan sosial.

2. **Keamanan sistem elektronik adalah kewajiban hukum**

   Platform digital, instansi publik, bank, dan penyelenggara sistem elektronik harus memastikan sistemnya aman, diaudit, dan dikelola secara bertanggung jawab.

3. **Bukti digital harus dijaga sejak awal**

   Dalam kasus teknologi informasi, bukti elektronik menjadi dasar penting untuk membuktikan peristiwa hukum. Bukti harus disimpan dengan baik agar tidak hilang atau berubah.

4. **Literasi digital masyarakat perlu diperkuat**

   Masyarakat harus memahami risiko phishing, penipuan online, penyalahgunaan data, transaksi ilegal, dan pelanggaran hak cipta digital.

5. **Penegakan hukum memerlukan kemampuan teknis**

   Aparat penegak hukum membutuhkan kemampuan forensik digital, pemahaman sistem elektronik, dan kerja sama lintas lembaga.

6. **Platform digital harus lebih akuntabel**

   Platform tidak hanya menjadi perantara layanan, tetapi juga memiliki tanggung jawab dalam mencegah penyalahgunaan sistem dan melindungi pengguna.

7. **Penyelesaian sengketa harus mudah diakses**

   Konsumen digital membutuhkan mekanisme penyelesaian yang cepat, murah, transparan, dan adil, baik melalui platform, BPSK, mediasi, arbitrase, maupun pengadilan.

8. **Hak cipta digital tetap harus dihormati**

   Karya digital yang mudah diakses tidak berarti bebas digunakan tanpa izin. Konten kreator, penulis, musisi, pembuat film, dan pengembang software tetap memiliki hak moral dan hak ekonomi.

Tabel berikut merangkum pembelajaran hukum dari beberapa jenis kasus teknologi informasi di Indonesia.

Tabel 15.6: Pembelajaran Hukum dari Kasus Teknologi Informasi di Indonesia

Jenis Kasus	Contoh Permasalahan	Pembelajaran Hukum
Penyalahgunaan data pribadi	Kebocoran data Tokopedia, BPJS Kesehatan, media sosial, perbankan	Data pribadi harus dilindungi sebagai hak privasi dan aset digital
Kejahatan siber dan penipuan online	Phishing, akses ilegal, penipuan marketplace, pencurian OTP	Masyarakat perlu literasi keamanan digital dan bukti digital harus disimpan
Pelanggaran hak cipta digital	Streaming ilegal, re-upload konten, pembajakan e-book dan software	Karya digital tetap dilindungi hak cipta meskipun mudah diakses
Sengketa transaksi elektronik	Barang tidak dikirim, saldo digital hilang, sengketa COD	Transaksi digital tetap merupakan hubungan hukum yang menimbulkan hak dan kewajiban
Pembuktian digital	Screenshot, metadata, log akses, invoice, rekaman CCTV	Bukti elektronik harus dikumpulkan dan dijaga integritasnya

Jenis Kasus	Contoh Permasalahan	Pembelajaran Hukum
Tanggung jawab platform	Kegagalan keamanan, lemahnya pengaduan, lambatnya respons	Platform perlu transparansi, akuntabilitas, dan mekanisme perlindungan pengguna
Perlindungan konsumen digital	Barang tidak sesuai, refund gagal, penjual tidak bertanggung jawab	Konsumen membutuhkan mekanisme penyelesaian sengketa yang cepat dan adil

Pembelajaran dari kasus teknologi informasi juga menunjukkan bahwa hukum tidak boleh hanya bersifat reaktif. Hukum tidak cukup bekerja setelah terjadi kerugian, tetapi harus mampu mencegah terjadinya pelanggaran. Pencegahan dapat dilakukan melalui desain sistem yang aman, edukasi pengguna, standar keamanan informasi, audit berkala, perlindungan data sejak awal, dan penguatan kebijakan platform. Dalam konteks ini, pendekatan preventif menjadi sama pentingnya dengan pendekatan represif.

Selain itu, kasus-kasus teknologi informasi mengajarkan bahwa kepastian hukum harus berjalan bersama keadilan dan kemanfaatan. Hukum perlu memberikan kepastian bagi korban, pelaku usaha, platform, dan masyarakat. Namun, hukum juga harus adil agar tidak hanya menghukum, tetapi juga memulihkan hak korban. Hukum juga harus bermanfaat dengan mendorong ekosistem digital yang aman, produktif, dan dipercaya masyarakat.

Bagi mahasiswa, pembelajaran hukum dari kasus teknologi informasi dapat digunakan untuk mengembangkan kemampuan analisis. Mahasiswa tidak hanya perlu menghafal pasal, tetapi juga harus mampu membaca fakta, mengidentifikasi isu hukum, menentukan dasar hukum, menilai bukti digital, memahami dampak sosial, dan merumuskan rekomendasi. Kemampuan ini penting karena kasus teknologi informasi sering melibatkan hubungan antara hukum, teknologi, bisnis, etika, dan masyarakat.

Dengan demikian, kasus teknologi informasi di Indonesia memberikan pelajaran bahwa transformasi digital harus diikuti dengan transformasi hukum, tata kelola, dan kesadaran masyarakat. Pelindungan data pribadi, keamanan transaksi, perlindungan konsumen, hak cipta digital, pembuktian elektronik, dan tanggung jawab platform merupakan bagian penting dari hukum teknologi informasi. Semakin besar ketergantungan masyarakat pada teknologi, semakin besar pula kebutuhan terhadap hukum yang adaptif, penegakan yang kuat, etika digital, dan literasi masyarakat.

Daftar Pustaka

Abya, J., Abas, M., Rahmatiar, Y., & Lubis, A. (2024). Penegakan Hukum Terhadap Pelanggaran Hak Cipta: Studi Kasus Re-Upload Video Konten Kreator Sosial Media Untuk Kegiatan Komersial (Studi Putusan Mahkamah Agung Nomor 41 PK/Pdt.Sus-HKI/2021). *Jurnal Ilmu Hukum, Humaniora Dan Politik*, *4*(6), 2306–2318. https://doi.org/10.38035/jihhp

ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence* (5th ed.).

Affandi, Y., & Iskandar, C. L. (Eds.). (2025). *Ekonomi Dan Keuangan Digital: Konsep Dan Implementasi Di Indonesia* (1st ed.). BI Institute.

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(2), 55–63. https://doi.org/10.54209/judge.v5i02.566

Al Kautsar, I., & Muhammad, D. W. (2022). Sistem Hukum Modern Lawrance M. Friedman: Budaya Hukum dan Perubahan Sosial Masyarakat dari Industrial ke Digital. *SAPIENTIA ET VIRTUS*, *7*(2), 84–99. https://doi.org/10.37477/sev.v7i2.358

Amelia, S. P. (2025). Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna. *Studia: Journal of Humanities and Education Studies*, *1*(2), 132–141. https://edukastra.com/studia/article/view/22

Anami, M. K., Lidowati, A. M., Panjaitan, R. N., Fadhila, R. A., Purba, D. F. N., & Surahmad. (2025). Analisis Hukum Perdata Pada Perlindungan Hukum Bagi Para Pihak Dalam Kontrak Digital: Studi Kasus Sengketa Saldo DANA. *Media Hukum Indonesia*, *2*(5), 338–344. https://doi.org/10.5281/zenodo.15260235

Anindya, R. P., & Subiyanto, A. E. (2025). Tanggung Jawab Platform Tokopedia Dalam Kasus Kebocoran Data Menurut Undang-Undang Tentang Perlindungan Data Pribadi. *Journal of Artificial Intelligence and Digital Business*, *4*(3), 1105–1112. https://doi.org/10.31004/riggs.v4i3.2105

Arief, H. (2016). *Pengantar Hukum Indonesia*. PT LKiS Pelangi Aksara.

Aritonang, L. M., Zyetwill, & Handayani, R. (2025). Analisis Hukum Terhadap Kebocoran Data Pribadi Dan Penyalahgunaan Identitas

Dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Ranah Research: Journal of Multidisciplinary Research and Development*, *7*(5), 3146–3158. https://doi.org/10.38035/rrj.v7i5

Attidhira, S. W., & Permana, Y. S. (2022). Review of Personal Data Protection Legal Regulations in Indonesia. *Awang Long Law Review*, *5*(1), 280–294. https://doi.org/10.56301/awl.v5i1.562

Attorney-General's Chambers of Singapore. (2018). *Cybersecurity Act 2018*. https://sso.agc.gov.sg/Act/CA2018

Attorney-General's Chambers of Singapore. (2021). *Personal Data Protection Act 2012, 2020 Revised Edition*. https://sso.agc.gov.sg/Act/PDPA2012

Azi, S., Priatni, R. D., Pujiati, I., Wijaya, A., Rahmani, A. D., Gumanti, J., Kustiawan, W., & Ruslina, E. (2024). Peran UU ITE dalam Regulasi E-Commerce di Era Digital. *Jurnal Ilmu Hukum, Humaniora Dan Politik*, *5*(1), 258–267. https://doi.org/10.38035/jihhp.v5i1.2900

Bainbridge, D. I. (2008). *Introduction to Information Technology Law* (6th ed.). Pearson Education.

Bonggi, R. I. A., Rachman, M., Ramadhan, R. D., Fikri, M. A., & Augustia, A. E. (2025). Studi Kasus Kebocoran Data Facebook Dan Perlindungan Informasi Pribadi. *TEKNOBIS: Teknologi, Bisnis Dan Pendidikan*, *3*(2), 283–287.

Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.

Brownsword, R., & Goodwin, M. (2012). *Law And The Technologies Of The Twenty-First Century: Text And Materials*. Cambridge University Press.

BSSN. (2024). *Peraturan Badan Siber Dan Sandi Negara Nomor 1 Tahun 2024 Tentang Pengelolaan Insiden Siber*. Badan Siber dan Sandi Negara. https://peraturan.bpk.go.id/Download/350527/2024_perbanbssn_001.pdf

Casey, E. (2011). *Digital Evidence And Computer Crime: Forensic Science, Computers, And The Internet* (3rd ed.). Academic Press.

Castells, M. (2010). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture (Vol. 1)* (2nd ed.). Wiley-Blackwell.

CISA. (2022). *Implementing Phishing-Resistant MFA*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

CISA. (2025). *StopRansomware Guide*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/stopransomware/ransomware-guide

CISA. (2026). *Malware, Phishing, And Ransomware*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Council of Europe. (2001). *Convention On Cybercrime*. Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Creative Commons. (2024). *Creative Commons Public Licenses*. https://creativecommons.org/licenses/

Cyber Security Agency of Singapore. (2021). *The Singapore Cybersecurity Strategy 2021*. https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021/

Damayanti, P. N., & Sodikin. (2026). Analisis Perkembangan Hukum Teknologi Informasi Dan Kaitannya Terhadap Penetapan Tersangka Roy Suryo Notodiprojo Cs. *Ranah Research: Journal of Multidisciplinary Research and Development*, *8*(2), 1188–1194. https://doi.org/10.38035/rrj.v8i2

Data Privacy Framework Program. (2026). *Overview of the EU-U.S. Data Privacy Framework Program*. https://www.dataprivacyframework.gov/framework-article/OVERVIEW

Dikdik, Mansur, M. A., & Gultom, E. (2009). *Cyber Law: Aspek Hukum Teknologi Informasi* (A. Gunarsa (Ed.); 2nd ed.). Refika Aditama.

DJKI. (2026). *Langkah 5 Menit Catatkan Hak Cipta Melalui POP HC*. Direktorat Jenderal Kekayaan Intelektual. https://www.dgip.go.id/index.php/artikel/detail-artikel-berita/langkah-5-menit-catatkan-hak-cipta-melalui-pop-hc

Edrisy, I. F. (2019). *Pengantar Hukum Siber* (Kamilatun (Ed.)). Sai Wawai Publishing.

European Commission and High Representative of the Union for Foreign

Affairs and Security Policy. (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade

European Parliament and Council of the European Union. (2016a). *Regulation (EU) 2016/679 (General Data Protection Regulation)* (Issue L119).

European Parliament and Council of the European Union. (2016b). *Regulation (EU) 2016/679 of the European Parliament and of the Council: General Data Protection Regulation*.

European Parliament and Council of the European Union. (2022a). *Directive (EU) 2022/2555 of the European Parliament and of the Council*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Parliament and Council of the European Union. (2022b). *Regulation (EU) 2022/1925 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

European Parliament and Council of the European Union. (2022c). *Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act)*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Fadillah, R. N., & Pasundan, U. (2024). Perlindungan Hak Atas Kekayaan Intelektual Artificial Intelligence (AI) dari Perspektif Hak Cipta dan Paten. *Dassollen*, *2023*, 1–16. https://doi.org/10.11111/dassollen.xxxxxxx

Fadli, Hardiansyah, S. A., & Sutabri, T. (2026). Analisis Pelanggaran Etika Teknologi Informasi Di Indonesia: Studi Kasus Kebocoran Data. *Jurnal Ilmiah Penelitian Mahasiswa*, *4*(1), 666–676. https://doi.org/10.61722/jipm.v4i1.1951

Fahmi, T. (2024). Transformasi Digital dan Pengaruhnya Terhadap Budaya Organisasi: Tinjauan Literatur Sistematis. *Jurnal Manajemen*

Akuntansi Dan Ilmu Ekonomi, *1*(2), 101–109. https://doi.org/10.70585/jumali.v1i2.46

Fairuzabadi, M., Pangaribuan, J. J., Moedjahedy, J. H., Sihotang, J. I., Simarmata, J., Andryanto, A., Jaya, A. K., Sasongko, D., Turnip, T. N. S., Suardinata, S., others, A, A., Jaya, A. K., Sasongko, D., Turnip, T. N. S., Yasir, F. N., Gustiana, Z., Rizal, M., & Pungus, S. R. (2023). *Keamanan Sistem Informasi dan Kriptografi*.

Febriharini, M. P. (2016). Eksistensi Hak Atas Kekayaan Intelektual Terhadap Hukum Siber. *Serat Acitya: Jurnal Ilmiah UNTAG Semarang*, *5*(1), 15–22. https://download.garuda.kemdikbud.go.id/article.php?article=403616&title=EKSISTENSI+HAK+ATAS+KEKAYAAN+INTELEKTUAL+TERHADAP+HUKUM+SIBER&val=6017

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

Gharibi, W. (2012). Some Recommended Protection Technologies For Cyber Crime Based On Social Engineering Techniques: Phishing. *ArXiv Preprint*. https://arxiv.org/abs/1202.2404

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426.

Hardjaloka, L. (2015). Studi Pengaturan Keamanan Siber di Indonesia dan Perbandingannya dengan Negara Lain. *Jurnal Legislasi Indonesia*, *12*(3), 299–318.

Hutahaean, E., Fitria, Y. Z. N., Rozikin, I., Sihombing, A., Arisandi, N. P., Suherman, J., Prayuti, Y., Bagaskoro, M. R., Iqbal, D. I., Khumaeroh, I. N., Anggraeni, H. Y., Oktavianto, H., Prasetia, A. R., & Rahman, Y. M. (2026). *Hukum Bisnis Modern: Tantangan, Risiko, dan Peluang di Era Disrupsi*. Penerbit Widina.

ICANN. (2020). *Uniform Domain-Name Dispute-Resolution Policy*. Internet Corporation for Assigned Names and Numbers. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-

domain-name-dispute-resolution-policy-01-01-2020-en

ICPO-INTERPOL. (2024). *Constitution of the ICPO-INTERPOL*. https://www.interpol.int/

INTERPOL. (2026). *Cybercrime*. International Criminal Police Organization. https://www.interpol.int/en/Crimes/Cybercrime

ISO/IEC. (2012). *ISO/IEC 27037:2012 Information Technology -- Security Techniques -- Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. https://www.iso.org/standard/44381.html

Junior, A. A. B. S., Dewi, A. A. S. L., & Arini, D. G. D. (2021). Penyelesaian Sengketa Transaksi Bisnis Electronic Commerce Melalui Internet. *Jurnal Konstruksi Hukum*, *2*(2), 218–222. https://doi.org/10.22225/jkh.2.2.3209.218-222

Kaffah, A. F., & Badriyah, S. M. (2024). Legal Aspects of Business Protection in Indonesia's Digital Era: Aspek Hukum Dalam Perlindungan Bisnis Era Digital Di Indonesia. *Lex Renaissance*, *9*(1), 203–228. https://doi.org/10.20885/JLR.vol9.iss1.art10

Kementerian Kominfo RI. (2020). *Waspada Kejahatan Siber: Kominfo Imbau Jangan Bagikan Kode Rahasia OTP Fraud*. Kementerian Komunikasi dan Informatika Republik Indonesia. https://www.komdigi.go.id/berita/pengumuman/detail/siaran-pers-no-118-hm-kominfo-09-2020-tentang-waspada-kejahatan-siber-kominfo-imbau-jangan-bagikan-kode-rahasia-otp-fraud

Kementerian Komunikasi dan Informatika Republik Indonesia. (2013). *Peraturan Menteri Komunikasi dan Informatika Nomor 23 Tahun 2013 tentang Pengelolaan Nama Domain*. https://peraturan.bpk.go.id/Details/155401/permenkominfo-no-23-tahun-2013

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (Issues 800–86). https://csrc.nist.gov/pubs/sp/800/86/final

Khasanah, D. D., Iftitah, A., Kasiani, Abas, M., Sipayung, B., Hastarini, A., Arifuddin, Q., Dewi, S. R., Anita, A. A., Dewi, N., Jenar, S., Bhakti, I. S. G., Faried, F. S., Tarmizi, R., Ningtyas, M. A., Puspandari, R. Y., & Rohmah, A. N. (2023). *Hukum Perdata*. Sada Kurnia Pustaka.

Koops, B.-J. (2010). The Internet and Its Opportunities for Cybercrime. In

M. Herzog-Evans (Ed.), *Transnational Criminology Manual* (Vol. 1, pp. 735–754). Wolf Legal Publishers.

Koswara, W. (2022). Implementasi Aturan Perlindungan Data Pribadi oleh Penyelenggara Sistem Elektronik Dikaitkan dengan Teori Keadilan dan Kepastian Hukum. *Jurnal Paradigma Hukum Pembangunan*, *7*(2), 86–103. https://doi.org/10.25170/paradigma.v7i2.3681

Koto, I., Hanifah, I., Perdana, S., Tarmizi, & Nadirah, I. (2023). Perlindungan Hukum Atas Kekayaan Intelektual Perspektif Hukum Islam. *Jurnal Yuridis*, *10*(2), 66–73. https://doi.org/10.35586/jyur.v10i2.7142

Kristanto, & Baihaki, R. (2025). *Tindak Pidana Siber di Indonesia: Regulasi, Tantangan, dan Penegakan Hukum*. PT Media Penerbit Indonesia.

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Livingstone, S., & Haddon, L. (2009). *Kids Online: Opportunities and Risks for Children*. Policy Press.

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen oleh Penyelenggara Sistem Elektronik dalam Transaksi Digital. *Jurnal USM Law Review*, *7*(1), 333–347. https://doi.org/10.26623/julr.v7i1.8705

Mantili, R., & Dewi, P. E. T. (2020). Prinsip Kehati-hatian dalam Penyelenggaraan Sistem Elektronik dalam Upaya Perlindungan Data Pribadi di Indonesia. *Jurnal Aktual Justice*, *5*(2), 132–145. https://doi.org/10.47329/aktualjustice.v5i2.549

Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Rineka Cipta.

Murray, A. (2019). *Information Technology Law: The Law And Society* (4th ed.). Oxford University Press.

Ningrum, D. P. S., & Robekha, J. (2022). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia. *Journal Evidence of Law*, *1*(1), 112–128.

NIST. (2024a). *Cybersecurity Framework 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NIST. (2024b). *The NIST Cybersecurity Framework (CSF) 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Novia, A. A., Rahmadani, D. A., & Hidayati, M. N. (2022). Pelanggaran Hak Cipta Melalui Situs Streaming Ilegal. *Artikel Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Al Azhar Indonesia*.

Nurse, J. R. C. (2018). Cybercrime And You: How Criminals Attack And The Human Factors That They Seek To Exploit. *ArXiv Preprint*. https://arxiv.org/abs/1811.06624

OECD. (2003). *Privacy Online: OECD Guidance on Policy and Practice*. Organisation for Economic Co-Operation and Development.

OECD. (2013). *The OECD Privacy Framework*. OECD Publishing.

OECD. (2016). *Consumer Protection In E-Commerce: OECD Recommendation*. OECD Publishing.

OJK. (2024). *Panduan Strategi Anti Fraud Penyelenggara Inovasi Teknologi Sektor Keuangan*. Otoritas Jasa Keuangan. https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/ITSK/Documents/PANDUAN STRATEGI ANTI FRAUD %28ITSK%29 2024.pdf

OKJ. (2015). *Bijak Ber-Electronic Banking*. Otoritas Jasa Keuangan. https://www.ojk.go.id/Files/box/buku bijak ber-ebanking.pdf

Oktana, R. (2023). *Analisis Hukum Terhadap Media Sosial Dalam Pembuktian Tindak Pidana Informasi Dan Transaksi Elektronik*. Universitas Hasanuddin.

Open Source Initiative. (2026). *Open Source Licenses*. https://opensource.org/licenses

Pertiwi, E., Nuraldini, D. D., Buana, G. T., & Arthacerses, A. (2020). Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *2*(1), 1–7.

Pratiwi, M. D., & Erniwati. (2022). *Upaya Pemerintah Dalam Memberikan Perlindungan Hukum Terhadap Nasabah Fintech Peer To Peer Lending*.

Purborini, V. S., Suryanatha, I. B., & Kasmin. (2025). Hukum Dan Ekonomi Digital: Regulasi Fintech Di Indonesia. *J-CEKI: Jurnal Cendekia Ilmiah*, *4*(3), 956–964.

Puteri, C. B., Subaidi, J., & Bahreisy, B. (2025). Analisis Putusan Hakim Terhadap Tindak Pidana Dalam Mengakses Sistem Elektronik Orang

Lain Tanpa Hak: Studi Putusan Nomor 9/Pid.Sus/2021/PN Pli. *Jurnal Ilmiah Mahasiswa Fakultas Hukum*, *8*(2).

R. Lina Sinaulan, Sugeng, & Marsha Angelina Utoyo S. (2025). *Buku Ajar: Etika dan Hukum Bisnis*. PT Penerbit Qriset Indonesia.

Raharjo, A. (2002). *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. PT Citra Aditya Bakti.

Raharjo, B. (2021). *Fintech: Teknologi Finansial Perbankan Digital* (J. T. Santoso (Ed.)). Yayasan Prima Agus Teknik bekerja sama dengan Universitas Sains \& Teknologi Komputer (Universitas STEKOM).

Rahmawati, C., Watkat, F. X., Siburian, H. K., Mulyadi, D., Abas, M., & Dwirananingsih, Y. (2024). *Hukum Siber* (Y. Novita (Ed.)). Getpress Indonesia.

Ramadhani, W. K. S., & Wiraguna, S. A. (2025). Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan. *Perspektif Administrasi Publik Dan Hukum*, *2*(2), 158–175. https://doi.org/10.62383/perspektif.v2i2.248

Ramli, A. M. (2004). *Cyber Law Dan HAKI Dalam Sistem Hukum Indonesia*. Refika Aditama.

Reed, C. (2012). *Making Laws For Cyberspace*. Oxford University Press.

Remmelink, J. (2003). *Hukum Pidana: Komentar Atas Pasal-Pasal Terpenting Dari Kitab Undang-Undang Hukum Pidana Belanda Dan Padanannya Dalam Kitab Undang-Undang Hukum Pidana Indonesia*. Gramedia Pustaka Utama.

Republik Indonesia. (1979). *Undang-Undang Nomor 1 Tahun 1979 tentang Ekstradisi*.

Republik Indonesia. (1999a). *Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia*.

Republik Indonesia. (1999b). *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*.

Republik Indonesia. (2002a). *Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia*.

Republik Indonesia. (2002b). *Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara*.

Republik Indonesia. (2004). *Undang-Undang Nomor 34 Tahun 2004*

tentang Tentara Nasional Indonesia.

Republik Indonesia. (2006). *Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana*.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. Republik Indonesia. https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Republik Indonesia. (2011). *Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan*.

Republik Indonesia. (2014a). *Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta*.

Republik Indonesia. (2014b). *Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan*.

Republik Indonesia. (2016a). *Undang-Undang Nomor 13 Tahun 2016 tentang Paten*. https://peraturan.bpk.go.id/Details/37536/uu-no-13-tahun-2016

Republik Indonesia. (2016b). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2016c). *Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis*. https://peraturan.bpk.go.id/Details/37595/uu-no-20-tahun-2016

Republik Indonesia. (2017). *Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara*. https://peraturan.bpk.go.id/Home/Details/72920/perpres-no-53-tahun-2017

Republik Indonesia. (2019a). *Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik*. Republik Indonesia. https://peraturan.bpk.go.id/Details/126143/pp-no-80-tahun-2019

Republik Indonesia. (2019b). *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Republik Indonesia. https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

Republik Indonesia. (2021). *Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara*. https://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021

Republik Indonesia. (2022a). *Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*.

Republik Indonesia. (2022b). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Pemerintah Republik Indonesia. https://peraturan.bpk.go.id/Home/Details/203629/uu-no-27-tahun-2022

Republik Indonesia. (2023a). *Peraturan Presiden Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional Dan Manajemen Krisis Siber*. Republik Indonesia. https://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023

Republik Indonesia. (2023b). *Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan*.

Republik Indonesia. (2024a). *Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital*. https://peraturan.bpk.go.id/Details/306884/perpres-no-174-tahun-2024

Republik Indonesia. (2024b). *Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. Republik Indonesia. https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024

Republik Indonesia. (2024c). *Undang-Undang Nomor 65 Tahun 2024 tentang Perubahan Ketiga atas Undang-Undang Nomor 13 Tahun 2016 tentang Paten*.

Republik Indonesia. (2025a). *Undang-Undang Nomor 20 Tahun 2025 Tentang Kitab Undang-Undang Hukum Acara Pidana*. Republik Indonesia. https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025

Republik Indonesia. (2025b). *Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia*. https://peraturan.bpk.go.id/Details/319166/uu-no-3-tahun-2025

Republik Indonesia. (2026). *Undang-Undang Nomor 5 Tahun 2026 tentang Perubahan Ketiga atas Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia*. https://peraturan.bpk.go.id/Details/350096/uu-no-5-tahun-2026

Ribble, M. (2015). *Digital Citizenship In Schools: Nine Elements All Students Should Know* (3rd ed.). International Society for Technology in Education.

Rizkia, N. D., Hidaya, W. A., Kaemirawati, D. T., Novianty, R. R., & Febrianty, Y. (2024). Legal Protection of Consumers in Electronic Transactions: Challenges and Future Prospects. *Journal Equity of Law and Governance*, *4*(2), 307–315. https://www.ejournal.warmadewa.ac.id/index.php/elg

Rosid, A., & Musadad, A. (2025). Upaya Hukum Penyelesaian Sengketa Konsumen Dalam Transaksi E-Commerce Di Luar Pengadilan. *Pemuliaan Keadilan*, *2*(1), 50–59. https://doi.org/10.62383/pk.v2i1.400

Salim, A., Susilowati, T., & Sejati, H. (2024). Consumer Data Protection in Electronic Transaction Practices in E-Commerce. *Journal of Economics, Technology, and Business (JETBIS)*, *3*(8), 451–460. https://doi.org/10.57185/jetbis.v3i8.128

Satrio, M. B., & Widiatno, M. W. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik: Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia. *JCA of Law*, *1*(1), 49–61.

Schmitt, M., & Flechais, I. (2023). Digital Deception: Generative Artificial Intelligence In Social Engineering And Phishing. *ArXiv Preprint*. https://arxiv.org/abs/2310.13715

Setyananda, A. F., & Israhadi, E. I. (2025). The Urgency of Legal Roles in The Development and Advancement of Indonesia's Digital Economy. *Jurnal Greenation Sosial Dan Politik*, *3*(4), 795–805. https://doi.org/10.38035/jgsp.v3i4.501

Shea, V. (1994). *Netiquette*. Albion Books.

Siber Polri. (2026). *Patroli Siber*. https://patrolisiber.id/contact-us/

Sitompul, J. (2024). *Wajah Baru UU ITE*. Kementerian Komunikasi dan Informatika Republik Indonesia. https://jdih.setwan-dprd.lampungprov.go.id/web/document/attachment/1734089492-----1729219799-Wajah_Baru_UU_ITE_04_03_2024.pdf

Situmeang, S. M. T. (2020). *Cyber Law* (1st ed.). Penerbit Cakra.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.

Solove, D. J., & Schwartz, P. M. (2020). *Information Privacy Law* (7th ed.). Wolters Kluwer.

Sorisa, C., Kiareni, C. L., & Parhusip, J. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan Di Indonesia. *Jurnal Sains Student Research*, *2*(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996

Suadi, I. P. (2021). Tinjauan Yuridis Subjek Hukum dalam Transaksi Jual Beli Online/E-Commerce Ditinjau dari Kitab Undang-Undang Hukum Perdata. *E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha*, *4*(2), 671.

Subekti, R. (2008). *Kitab Undang-Undang Hukum Perdata*. Pradnya Paramita.

Sugara, M. V. L., & Az-Zahra, A. R. (2024). Penyelesaian Sengketa Konsumen Dalam Transaksi Elektronik (E-Commerce) Berdasarkan Hukum Perdata. *Jurnal Kewarganegaraan*, *8*(1), 873–879.

Surachman, D., Rato, D., & Ohoiwutun, Y. A. T. (2026). Transformasi Konsep Law as a Tool of Social Engineering dalam Pembangunan Hukum di Indonesia. *Jurnal Supremasi: Jurnal Ilmiah Ilmu Hukum*, *16*(1), 1–14. https://ejournal.unisbablitar.ac.id/index.php/supremasi

Suwardi. (2015). *Hukum Dagang: Suatu Pengantar*. Deepublish.

Syafi'iyah, R. F., Afifah, S. N., Lailiyah, Z. S. N., Salsabila, S., Iqbal, M., & Prakoso, F. A. (2026). Perlindungan Hukum Hak Cipta Terhadap Pembajakan Karya Digital Di Indonesia. *Mahkamah: Jurnal Riset Ilmu Hukum*, *3*(1), 106–116. https://doi.org/10.62383/mahkamah.v3i1.1467

Tandon, R. (2020). A Survey Of Distributed Denial Of Service Attacks And Defenses. *ArXiv Preprint*. https://arxiv.org/abs/2008.01345

The European Parliament and The Council of the European Union. (2016). *General Data Protection Regulation*.

Turban, E., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2015). *Electronic Commerce: A Managerial And Social Networks Perspective* (8th ed.). Springer.

Turkle, S. (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books.

United Nations. (2005). *Tunis Agenda for the Information Society*.

International Telecommunication Union. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

United Nations. (2015). *United Nations Guidelines For Consumer Protection*. United Nations.

United Nations General Assembly. (2018). *Resolution 73/27: Developments in the Field of Information and Telecommunications in the Context of International Security*. https://docs.un.org/en/a/res/73/27

United Nations General Assembly. (2019). *Resolution 74/247: Countering the Use of Information and Communications Technologies for Criminal Purposes*. https://docs.un.org/en/a/res/74/247

United Nations General Assembly. (2024). *Resolution 79/243: United Nations Convention against Cybercrime*. https://docs.un.org/en/a/res/79/243

United Nations Office on Drugs and Crime. (2024). *United Nations Convention against Cybercrime*. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

UNODC. (2013). *Comprehensive Study On Cybercrime*. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC. (2026). *Cybercrime Module 2: General Types Of Cybercrime*. United Nations Office on Drugs and Crime. https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-2/key-issues/intro.html

UU PDP Pelindungan Data Pribadi (2022).

Virdayanti, N. P. S., & Mahendrayana, I. M. D. D. (2025). Analisis Konseptual Terhadap Penggunaan Teknologi Dalam Investigasi Tindak Pidana Di Indonesia. *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, *1*(3), 333–339.

Wibowo, A. (2023). *Hukum di Era Globalisasi Digital* (J. T. Santoso (Ed.)). Yayasan Prima Agus Teknik bekerja sama dengan Universitas Sains \& Teknologi Komputer.

Wibowo, A. (2024). *Layanan Fintech Dalam Perspektif Hukum, Ekonomi, Teknologi*. Yayasan Prima Agus Teknik bekerja sama dengan Universitas Sains \& Teknologi Komputer (Universitas STEKOM).

Widjaja, G., Prestika, A., Hartanti, O. P., & Fazrin, A. (2018). Penyelesaian Sengketa Transaksi Elektronik. *Cross-Border*, *1*(1), 229–251.

WIPO. (2025). *WIPO Copyright Treaty (WCT)*. World Intellectual Property Organization. https://www.wipo.int/en/web/treaties/ip/wct/index

Wirogioto, A. J., & Belgradoputra, J. S. (2026). *Memahami Hukum Siber* (S. I. Nurani (Ed.)). CV. Intelektual Writer.

Wulandari, F. (2024). Problematika Pelanggaran Hak Cipta Di Era Digital. *Journal of Contemporary Law Studies*, *2*(2), 99–114. https://doi.org/10.47134/lawstudies.v2i2.2261

Wulandari, Y. S. (2018). Perlindungan Hukum bagi Konsumen terhadap Transaksi Jual Beli E-Commerce. *Ajudikasi: Jurnal Ilmu Hukum*, *2*(2), 199–210. https://doi.org/10.30656/ajudikasi.v2i2.687

Xu, S., Gao, Y., Fan, L., Liu, Z., Liu, Y., & Ji, H. (2022). LiDetector: License Incompatibility Detection for Open Source Software. *Unknown Journal*.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Biodata Penulis

Ir. Mila Jumarlis, S.Pt., S.Kom., M.Kom.,IPP. Lulus S-1 di program Studi Sosial Ekonomi Peternakan Universitas Hasanuddin tahun 2009, S-1 Teknik Informatika Universitas pejuang Republik Indonesia Tahun 2016, S-2 Sistem Komputer STMIK Handayani Tahun 2015, Program Profesi Insinyur Universitas Muslim Indonesia tahun 2021. Saat ini adalah Dosen Tetap di STAIN Majene dan menjabat sebagai Kepala Unit Teknologi Informasi dan Pangkalan Data. Aktif dibeberapa organisasi yaitu Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM), Ikatan Ahli Informatika Indonesia (IAII), Perkumpulan Dosen Indonesia Semesta (DIS) dan Persatuan Insinyur Indonesia (PII) bidang pemberdayaan Perempuan.

Menhya Snae, M.Kom. lahir di Kupang pada 25 Mei 1979. Ia menyelesaikan pendidikan Sarjana Komputer di STMIK Indonesia, Jakarta, pada tahun 2002. Pendidikan Magister Komputer diselesaikannya di Universitas Diponegoro, Semarang, pada tahun 2014.

Sejak tahun 2002 hingga sekarang, ia mengabdikan diri sebagai dosen pada Program Studi Sistem Informasi, STIKOM Uyelindo Kupang. Selain melaksanakan kegiatan pendidikan dan pengajaran, ia aktif menulis buku dalam bidang teknologi informasi, kecerdasan buatan, dan pemanfaatan teknologi dalam pendidikan.

Beberapa buku yang telah ditulisnya antara lain Mixed Reality dalam Pendidikan Inklusif, The Rise of Smart Machines: Membedah Otak Digital di Era AI, serta From Prompt to Project: Panduan Mahasiswa Menggunakan Generative AI.

Saat ini, ia berdomisili di Kota Kupang, Provinsi Nusa Tenggara Timur. Penulis dapat dihubungi melalui surel menhyasnae@gmail.com atau nomor telepon +62 852-5334-0195.

Dr. Andi Firmansyah, S.H., M.H., C.QAP. merupakan akademisi, praktisi hukum, dan peneliti yang lahir di Bulukumba, Sulawesi Selatan, pada 23 Maret 1994. Pendidikan hukumnya ditempuh mulai dari Program Sarjana Hukum di UIN Alauddin Makassar, Program Magister Hukum di Universitas Muslim Indonesia, hingga Program Doktor Hukum di UIN Alauddin Makassar.

Sejak mengikuti Pendidikan Khusus Profesi Advokat pada tahun 2015, ia aktif berkarier sebagai advokat dan tenaga ahli kebijakan publik. Pengalamannya mencakup penanganan perkara litigasi dan nonlitigasi, konsultasi hukum, penyusunan kajian hukum, serta rekomendasi kebijakan daerah. Ia juga pernah bertugas sebagai Tenaga Ahli Profesional pada DPRD Provinsi Sulawesi Selatan.

Sejak tahun 2018, ia mengabdi sebagai dosen tetap di Yayasan Amkop Business School. Selain mengajar, ia aktif dalam pengembangan kurikulum, penelitian, dan pengabdian kepada masyarakat. Keahliannya meliputi analisis hukum, kebijakan publik, kajian regulasi, dan pendidikan tinggi.

Komitmennya terhadap mutu pendidikan ditunjukkan melalui sertifikasi **Certified Quality Assurance Practitioner (C.QAP.)** dalam bidang penjaminan mutu perguruan tinggi. Ia juga aktif dalam HMI, KNPI, dan ICMI serta berkontribusi dalam advokasi, pendidikan hukum, dan pemberdayaan generasi muda.

Melalui karya-karya tulisnya, Andi Firmansyah berupaya menjembatani dunia akademik dan praktik hukum agar bermanfaat bagi mahasiswa, akademisi, praktisi, pembuat kebijakan, dan masyarakat.

Email: andifirman23.af@gmail.com

Vidya Devia Ardania, S.H., M.Kn. lahir di Bantul, Daerah Istimewa Yogyakarta, pada 8 September 1996. Meraih gelar Sarjana Hukum dari Fakultas Hukum Universitas Gadjah Mada (UGM) Yogyakarta pada tahun 2019 dan menyelesaikan program Magister Kenotariatan di Universitas Gadjah Mada pada tahun 2021. Saat ini, bekerja sebagai dosen pada Program Studi Hukum Bisnis, Fakultas Bisnis dan Hukum, Universitas PGRI Yogyakarta (UPY). Bidang keilmuan yang ditekuni meliputi hukum agraria, hukum perdata, dan hukum kenotariatan. Sebagai dosen, mengampu berbagai mata kuliah, antara lain Hukum Agraria, Hukum Perdata, Filsafat Hukum, dan Hukum dan Teknologi. Pada mata kuliah Hukum dan Teknologi, secara khusus mengembangkan materi mengenai *Artificial Intelligence* (AI), transformasi digital, perlindungan data pribadi, tata kelola teknologi, serta berbagai isu hukum yang muncul akibat perkembangan teknologi digital. Selain menjalankan tugas pendidikan, aktif melaksanakan penelitian dan pengabdian kepada masyarakat dengan fokus pada hukum agraria, hukum pertanahan, hukum bisnis, regulasi teknologi, dan AI. Berbagai karya ilmiah telah dipublikasikan pada jurnal nasional dan juga prosiding ilmiah.

Email: vidya.devia@upy.ac.id

Dr. Azry Yusuf, S.H., M.H. lahir di Tanaberu, Kabupaten Bulukumba, pada 4 April 1972. Ia merupakan dosen tetap pada Fakultas Hukum Universitas Handayani Makassar, advokat, mediator bersertifikat, serta konsultan hukum yang memiliki pengalaman panjang dalam bidang hukum tata negara, hukum pemilu, hukum administrasi, dan penyelesaian sengketa publik.

Penulis menyelesaikan pendidikan Sarjana Hukum dan Magister Hukum di Universitas Muslim Indonesia. Pendidikan Doktor Ilmu Hukum dengan konsentrasi Hukum Tata Negara juga diselesaikannya di Universitas Muslim Indonesia pada tahun 2021. Selain menjalankan profesi sebagai dosen, sejak tahun 1998 ia berpraktik sebagai advokat dan saat ini menjadi Managing Partner pada Kantor Hukum AY & Rekan di Makassar. Sejak tahun 2021, ia juga berprofesi sebagai mediator bersertifikat Universitas Gadjah Mada.

Pengalaman penulis dalam bidang demokrasi dan penyelenggaraan pemilu dimulai ketika menjabat sebagai Ketua Panitia Pengawas Pemilu Kecamatan Bontobahari, Kabupaten Bulukumba, pada tahun 2004–2005. Selanjutnya, ia dipercaya menjadi Ketua Panitia Pengawas Pemilu Kabupaten Bulukumba pada tahun 2007–2009, Anggota Komisi Pemilihan Umum Kabupaten Bulukumba pada tahun 2009–2013, serta Pimpinan Badan Pengawas Pemilihan Umum Provinsi Sulawesi Selatan selama dua periode, yakni tahun 2013–2023.

Sejak tahun 2023, penulis tercatat sebagai dosen tetap pada Fakultas Hukum Universitas Handayani Makassar. Selain itu, sejak tahun 2024 ia menjadi Pengajar Utama pada Akasa Law Students di Kota Tangerang, Banten. Dalam menjalankan tugas akademik dan profesinya, penulis aktif memberikan pendidikan, pelatihan, konsultasi, pendampingan hukum, serta pemikiran akademik dalam bidang hukum dan demokrasi.

Bidang keahlian utama penulis meliputi Hukum Tata Negara, Hukum Pemilu, Hukum Pidana Pemilu, Hukum Administrasi Pemilu, Hukum Acara Mahkamah Konstitusi, Penyelesaian Sengketa Administrasi Publik, *legal drafting*, serta *legislative review*. Berbekal pengalaman sebagai akademisi, advokat, mediator, dan mantan penyelenggara pemilu, penulis berkomitmen untuk mengembangkan ilmu hukum yang berintegritas, responsif terhadap perkembangan masyarakat, dan berorientasi pada tegaknya demokrasi, kepastian hukum, serta keadilan.

Jimmy Herawan Moedjahedy adalah seorang akademisi yang lahir di Jayapura dan dibesarkan di Manado. Ketertarikannya pada bidang komputer telah tumbuh sejak menempuh pendidikan di bangku sekolah menengah. Ia menyelesaikan pendidikan Sarjana (S1) Ilmu Komputer di Universitas Klabat, kemudian melanjutkan studi Magister (S2) Manajemen di Universitas Klabat, serta Magister (S2) Teknik Informatika di Universitas Amikom Yogyakarta.

Saat ini, ia berkarier sebagai dosen di Fakultas Ilmu Komputer, Universitas Klabat, Airmadidi, Sulawesi Utara. Selain menjalankan tugas sebagai dosen, ia juga aktif sebagai instruktur Cisco Networking Academy sejak tahun 2014 hingga sekarang. Dalam perjalanan karier profesionalnya, ia pernah menjabat sebagai Kepala Sistem Informasi dan IT.

Saat ini, ia aktif menulis buku serta mempublikasikan karya ilmiah pada jurnal dan konferensi, baik nasional maupun internasional. Ia juga berperan sebagai reviewer di beberapa jurnal nasional.

Andi Ismayana Wahid, S.H., M.H. lahir di Bulukumba, Sulawesi Selatan, pada 23 Desember 1983. Meraih gelar Sarjana Hukum dari Fakultas Hukum Universitas Muslim Indonesia (UMI) Makassar, pada tahun 2005 dan menyelesaikan program Magister Hukum di Pascasarjana Universitas Muslim Indonesia, pada tahun 2010. Saat ini, bekerja sebagai dosen pada Program Studi Hukum, Fakultas Hukum dan Ilmu Sosial Universitas Handayani Makassar (UHM), Mulai tahun 2023 sampai Sekarang. Telah menulis beberapa buku dan berbagai publikasi telah dimuat dalam jurnal nasional.

Email: andiismayanawahid@gmail.com

Karman Jaya, S.H., M.H. dilahirkan di Sinjai, Sulawesi Selatan, pada 14 Juli 1997. Sejak tahun 2022 hingga saat ini, ia mengabdi sebagai Dosen Tetap pada Program Studi Hukum, Fakultas Hukum dan Sosial, Universitas Handayani Makassar. Ia menyelesaikan studi Strata Satu (S1) Ilmu Hukum di Fakultas Syariah dan Hukum Universitas Islam Negeri Alauddin Makassar pada tahun 2018, kemudian melanjutkan studi Strata Dua (S2) dan berhasil menyelesaikan Program Magister Hukum di Universitas Hasanuddin pada tahun 2021.

Selain menjalankan tugas utama dalam pengajaran, ia aktif dalam kegiatan penelitian dan pengabdian kepada masyarakat dengan fokus keahlian pada Hukum Pidana, Hukum Administrasi Negara, dan Hukum Ketenagakerjaan. Untuk menunjang kompetensi praktisnya di bidang hukum, ia telah menyelesaikan Pendidikan Khusus Profesi Advokat (PKPA) dan saat ini sedang mempersiapkan proses penyumpahan advokat dalam waktu dekat.

Email: karmanjy97@gmail.com

Dr. Ir. Mirfan., S.Kom., M.T., M.Kom., IPM., ASEAN Eng. lulus S-1 pada Program Studi Teknik Informatika STMIK Handayani tahun 2005, S-2 Teknik Elektro di Universitas Hasanuddin tahun 2015, S-2 Sistem Komputer STMIK Handayani tahun 2016, Program Profesi Insinyur di Universitas Muslim Indonesia tahun 2021, serta menyelesaikan Program Doktor (S-3) Pendidikan pada tahun 2026. Saat ini sebagai dosen tetap di Universitas Handayani Makassar sekaligus Wakil Rektor III Bidang Kemahasiswaan dan Kerja Sama. Aktif dalam berbagai organisasi profesi, di antaranya Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM), Ikatan Ahli Informatika Indonesia Nusantara (IAIIN), dan Forum Dosen Indonesia (FDI). Selain itu, juga aktif sebagai pengurus Badan Kejuruan Informatika Persatuan Insinyur Indonesia (PII) serta Majelis Uji Kompetensi Badan Kejuruan Informatika PII.

Email: mirfan@handayani.ac.id

Fatri Sagita, S.HI., M.H. Lahir di Ujung Pandang pada 16 Desember 1989. Lulus S-1 di Program Studi Perbandingan Mazhab dan Hukum Universitas Islam Negeri Alauddin Makassar tahun 2012 dan S-2 Ilmu Hukum Universitas Muslim Indonesia Makassar Tahun 2017. Saat ini adalah Dosen Tetap di STAIN Majene dan berdomisili di Majene Sulawesi Barat.

Menjadi Editor pada Jurnal Qisthosia: Jurnal Syariah dan Hukum STAIN Majene dan Menjadi anggota Persatuan Dosen Hukum Keluarga Islam (PDHKI) sejak 2021 – sekarang.

Febria Gupita, S.H., M.H. lahir di Kota Yogyakarta, DIY, pada 21 Februari 1998. Meraih gelar Sarjana Hukum dari Fakultas Hukum Universitas Gadjah Mada (UGM) Yogyakarta pada tahun 2020 dan menyelesaikan program Magister Hukum Bisnis di Universitas Gadjah Mada pada tahun 2022. Saat ini, bekerja sebagai dosen pada Program Sarjana Hukum Bisnis Fakultas Bisnis dan Hukum Universitas PGRI Yogyakarta (UPY). Selain berperan sebagai pengajar, aktif dalam penelitian dan pengabdian kepada masyarakat dengan fokus pada Hukum Perdata, Hukum Bisnis dan Hukum Ketenagakerjaan.

Email: febria.gupita@upy.ac.id

Adv. Dr. Sigit Handoko, S.H., M.H.,C. Me
Lahir di Sleman, 10 November 1965. Beliau adalah Dosen Tetap Yayasan di Universitas PGRI Yogyakarta (UPY). Meraih gelar Sarjana (S-1) dari Fakultas Hukum Universitas PGRI Yogyakarta (1989). Meraih gelar Master (S-2) dari Fakultas Hukum Universitas Islam Indonesia , dan meraih Doktor (S-3) pada Program Doktor Fakultas Hukum Universitas Islam Indonesia Yogyakarta (UII). Selain sebagai Dosen Tetap di UPY beliau juga menjadi Dosen Tidak Tetap beberapa tahun di STIE SBI Yogyakarta, dan menjadi Tutor di Universitas Terbuka sejak 2007 sampai sekarang.

Pernah menerbitkan beberapa buku diantaranya Character Education Based on Local Wisdom for The Prisoner (2018), Revitalisasi Pancasila (Kreasi Total Media, 2020). Etika & Hukum Dalam Pemasaran (2024), Etika dan Hukum Bisnis di Era Digital (2024), Hukum Pidana (2025), Hukum dan HAM (2025), Hukum Lingkungan (2025), Hukum Acara Pidana (2026). Aktif juga melakukan penelitian dan mengikuti berbagai forum ilmiah. Karir pekerjaannya, pernah menjabat sebagai Sekretaris Jurusan PMP-Kn (1990-1992), Ketua Jurusan PMP-Kn (1992-1996), Pembantu Dekan I FKIP (1996-2001), Pjs Dekan FKIP (2021 beberapa bulan), Ketua Program Studi PPKn (2001-2005), Wakil Rektor 3 UPY (2009-2013), Wakil Dekan 3 FKIP (2013-2017), Kepala LKK (2017-2021), Kepala Unit LKKP (2021 beberapa bulan), Kepala Humas Protokoler UPY (2022-2024), Kaprodi Hukum Bisnis (2024-2025) dan (2025-2029).

Aktifitas lain di luar kampus Universitas PGRI Yogyakarta, menjadi Advokat dan Mediator. Di samping itu juga aktif di beberapa organisasi maupun ormas. Ketua ICMI Orda Bantul (2022-2026), Wakil Ketua I Komnasdik DIY (2025-2030), Pembina POKDARKAMTIBMAS Bantul, Anggota Lembaga Cegah Kejahatan Indonesia DIY (2016-2020), Kasubdit Komite Investigasi Negara (KIN-RI) periode 2018-2019, Anggota International Police Organization (IPO) 2019-2021, Penasehat Pengurus Besar Shirote-Do DIY, Anggota ADVOKAI DPD DIY, Anggota Lawyer J'lamb (Jaringan Lembaga Advokai Masyarakat Berkeadilan), Anggota LBH JOXZIN Lawas Indonesia Yogyakarta. Email : sigit@upy.ac.id.

Suci Damayanti, S.H., M.H. lahir di Bantaeng, 04 Desember 1998. Meraih gelar Sarjana Hukum (S.H.) dan Magister Hukum (M.H.) dari Fakultas Hukum Universitas Gadjah Mada. Saat ini bekerja sebagai dosen tetap pada Program Studi Hukum Bisnis, Fakultas Bisnis dan Hukum, Universitas PGRI Yogyakarta (UPY). Selain menjalankan tugas sebagai pengajar, Ia juga aktif dalam berbagai kegiatan penelitian dan pengabdian kepada masyarakat di bidang hukum bisnis, hukum pajak, hukum dan teknologi, serta perlindungan hukum di era digital. Fokus kajian yang ditekuni meliputi hukum pajak, tata kelola hukum bisnis, perlindungan data pribadi, keamanan siber, dan transformasi digital. Berbagai karya ilmiah telah dipublikasikan pada jurnal nasional, *bookchapter*, dan prosiding ilmiah.

Email: sucidamayanti@upy.ac.id

Muh. Fachrur Razy Mahka, S.H.I., M.H. lahir di Makassar Pada Tanggal 03 Juni 1993. Anak Pertama dari tiga bersaudara, pasangan Bapak Mahyuddin Jamsih dan Ibu Kawaidah Alham. Penulis menyelesaikan Pendidikan Strata Satu (S1) di Jurusan Hukum Pidana dan Ketatanegaraan Fakultas Syari'ah & Hukum UIN Alauddin Makassar Tahun 2014, Pendidikan Strata Dua (S2) di Hukum Islam UIN Alauddin Makassar Tahun 2020. Saat ini penulis adalah Dosen Tetap Pada Universitas Handayani Makassar dan menjabat sebagai Ketua Program Studi Hukum. Penulis aktif di Organisasi Profesi Dosen Dewan Pengurus Daerah (DPD) Dosen Indonesia Semesta (DIS) Provinsi Sulawesi Selatan dan Organisasi Perakan Pemuda Ansor Kabupaten Gowa Provinsi Sulawesi Selatan

Sufriaman, S.H., M.H., Lahir di Kota Bulukumba, Sulawesi Selatan, pada 24 September 1990. Meraih gelar Sarjana Hukum di Fakultas Syariah dan Hukum Universitas Islam Negeri Alauddin Makassar pada tahun 2012, menyelesaikan Program Studi Magister Hukum di Universitas Muslim Indonesia Makassar pada tahun 2019 dan saat ini sedang menempuh studi Program Doktor di Universitas Muslim Indonesia Makassar. Saat ini bekerja sebagai Dosen pada Program Studi Hukum di Fakultas Hukum dan Ilmu Sosial di Universitas Handayani Makassar, selain berperan sebagai pengajar, aktif dalam penelitian dan pengabdian pada masyarakat dengan fokus pada hukum perdata, hukum bisnis dan hukum ketenagakerjaan.

Email: sufriamanshmh@gmail.com & sufriaman@handayani.ac.id

PENGANTAR HUKUM TEKNOLOGI INFORMASI

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

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

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

yash media.
Follow Us:
yashmedia.id
IKAPI
IKATAN PENERBIT INDONESIA

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