Cyber Law

Dr. Dian Eka Kusuma Wardani, SH.,MH

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 28 TAHUN 2014
TENTANG HAK CIPTA

PASAL 113
KETENTUAN PIDANA

(1) Setiap orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp. 100.000.000,00 (seratus juta rupiah).
(2) Setiap orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf g untuk Penggunaan Secara Komerial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah).
(3) Setiap orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
(4) Setiap orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah)

CYBER LAW

Dr. Dian Eka Kusuma Wardani, SH.,MH

2024

PENERBIT AGMA

Penulis:
Dr. Dian Eka Kusuma Wardani, SH.,MH.

ISBN: 978-634-7063-34-2

Editor:
Aqramawardana, SH., MH.

Perancang Sampul:
Ahmad Sidiq

Penata Letak:
Ahmad Sidiq

Sumber Sampul:
Freepik.com

IKAPI Member No: 054/SSL/2023

Diterbitkan Oleh:
AGMA

Redaksi:
PT. AGMA KREATIF INDONESIA
Jl. Dirgantara, Kel. Mangalli, Kec. Pallangga,
Kab. Gowa, Sulawesi Selatan. 92161
Telp: (0411) 8201421, HP/WA: 08114489177
Web: www.penerbitagma.com
Email: agma.myteam@gmail.com

Edisi Pertama, Desember 2024

Dian Eka Kusuma Wardani, 2024. Cyber Law. Gowa: Penerbit Agma
viii + 140; 15,5 x 23 cm

ISBN 978-634-7063-34-2 (PDF)

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya buku berjudul Cyber Law: Hukum di Era Digital ini. Buku ini disusun sebagai bahan ajar dan referensi komprehensif dalam memahami dinamika hukum di ruang siber, yang semakin kompleks seiring dengan perkembangan teknologi informasi dan komunikasi.

Transformasi digital telah membawa perubahan signifikan dalam hampir seluruh aspek kehidupan—termasuk dalam bidang hukum. Munculnya berbagai fenomena seperti kejahatan siber, penyalahgunaan data pribadi, transaksi elektronik, hingga penyebaran ujaran kebencian di media sosial, menuntut pemahaman baru yang melampaui hukum konvensional. Oleh karena itu, kehadiran Cyber Law menjadi sangat penting sebagai landasan normatif, etis, dan teknis dalam mengatur perilaku manusia di dunia maya.

Buku ini disusun berdasarkan kurikulum pembelajaran yang sistematis dan aplikatif. Setiap bab memuat topik-topik penting seperti karakteristik dunia maya, regulasi hukum siber di Indonesia, investigasi digital forensik, perlindungan data pribadi, tanggung jawab platform digital, hingga cyber war dalam konteks hukum internasional. Metode pembelajaran seperti ceramah, studi kasus, debat, presentasi kelompok, dan simulasi dirancang untuk membangun pemahaman yang kritis, kolaboratif, dan kontekstual bagi pembaca, khususnya mahasiswa dan praktisi hukum.

Kami berharap buku ini dapat menjadi sumber pengetahuan yang bermanfaat tidak hanya bagi kalangan akademisi, tetapi juga bagi masyarakat luas yang ingin memahami bagaimana hukum bekerja di tengah realitas digital

yang terus berubah. Ucapan terima kasih kami sampaikan kepada semua pihak yang telah memberikan kontribusi, baik dalam bentuk masukan akademis maupun dukungan moral, dalam proses penyusunan buku ini.

Akhir kata, kami menyadari bahwa buku ini masih memiliki keterbatasan. Oleh karena itu, kami terbuka terhadap kritik dan saran konstruktif untuk penyempurnaan edisi berikutnya.

Makassar, Desember 2024

Penulis

DAFTAR ISI

BAB 1

Pendahuluan

A. Pengantar

1. Definisi Cyber Law

Cyber Law, atau yang dalam Bahasa Indonesia disebut sebagai hukum siber, merupakan suatu cabang ilmu hukum yang secara khusus mengatur, mengawasi, dan memberikan kerangka normatif terhadap berbagai aktivitas manusia yang berlangsung melalui media teknologi informasi dan komunikasi (TIK), khususnya internet dan jaringan komputer. Cyber Law hadir sebagai respons terhadap perkembangan teknologi digital yang begitu pesat dan telah mengubah pola interaksi sosial, ekonomi, dan budaya manusia secara signifikan.

Menurut pandangan akademik, Cyber Law tidak hanya sebatas aturan hukum yang berlaku di dunia digital, tetapi juga mencerminkan adaptasi dari prinsip-prinsip hukum konvensional ke dalam konteks baru yang ditandai oleh ruang virtual (cyberspace), batas yurisdiksi yang kabur, serta identitas digital yang sering kali anonim. Oleh karena itu, Cyber Law sering dipandang sebagai hukum lintas disiplin yang mencakup elemen-elemen dari hukum perdata, pidana, administrasi negara, internasional, hingga hukum hak asasi manusia.

Definisi menurut para ahli:

a. Dikdik M. Arief Mansur mendefinisikan hukum siber sebagai "sekumpulan norma hukum yang mengatur dan melindungi berbagai aktivitas manusia dalam ruang digital."

b. Danrivanto Budhijanto menyebut Cyber Law sebagai instrumen hukum yang dirancang untuk menjamin keadilan, keamanan, dan ketertiban dalam penyelenggaraan sistem informasi dan komunikasi berbasis digital.
c. Dalam konteks internasional, UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific) mendefinisikan Cyber Law sebagai "the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware, and information systems."

2. Tujuan Cyber Law

1. Melindungi Hak-Hak Pengguna Internet

Dalam konteks hukum siber, perlindungan terhadap hak-hak pengguna internet merupakan aspek fundamental yang harus dijamin oleh regulasi. Hak-hak tersebut meliputi hak atas privasi, perlindungan data pribadi, kebebasan berekspresi, dan hak untuk tidak mengalami diskriminasi atau pelecehan di ruang digital. Perlindungan ini bertujuan memastikan bahwa pengguna dapat menggunakan teknologi informasi dengan aman dan tanpa rasa takut akan pelanggaran terhadap hak-hak pribadinya.

Contoh:

Seorang pengguna media sosial yang mengalami penyalahgunaan data pribadinya, seperti foto atau informasi identitas yang digunakan tanpa izin, dapat mengajukan tuntutan hukum berdasarkan undang-undang perlindungan data pribadi dan peraturan terkait penyalahgunaan informasi di Indonesia.

2. Memberikan Kepastian Hukum dalam Aktivitas Digital

Cyber Law menyediakan kerangka hukum yang jelas dan sistematis untuk mengatur berbagai aktivitas yang dilakukan secara elektronik, sehingga memberikan kepastian hukum bagi

pelaku dan penerima layanan digital. Kepastian hukum ini sangat penting dalam mengurangi risiko hukum dan sengketa, sekaligus mendukung perkembangan ekonomi digital secara berkelanjutan.

Contoh:

Transaksi jual beli melalui platform e-commerce diatur dalam peraturan mengenai transaksi elektronik dan perlindungan konsumen digital, sehingga jika terjadi sengketa, seperti barang tidak sesuai pesanan, kedua pihak memiliki landasan hukum yang jelas untuk menyelesaikannya secara adil.

3. Menanggulangi Kejahatan Siber (Cybercrime)

Salah satu fungsi utama Cyber Law adalah sebagai instrumen penegakan hukum terhadap tindakan kriminal yang memanfaatkan teknologi informasi. Kejahatan siber meliputi berbagai bentuk tindakan ilegal seperti peretasan, penyebaran malware, penipuan daring, pencurian identitas, serta penyebaran konten ilegal atau merugikan pihak lain. Regulasi ini bertujuan untuk memberikan sanksi tegas dan efek jera, sekaligus meningkatkan keamanan digital nasional.

Contoh:

Kasus peretasan pada sistem perbankan yang mengakibatkan pencurian data nasabah dapat ditindaklanjuti dengan penegakan hukum berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan terkait keamanan siber.

4. Menjaga Integritas dan Keamanan Sistem Elektronik

Cyber Law juga berperan penting dalam menetapkan standar dan kewajiban hukum bagi penyelenggara sistem elektronik untuk melindungi integritas dan keamanan data serta sistem yang digunakan. Aspek ini mencakup pengelolaan risiko

keamanan siber, perlindungan terhadap akses tidak sah, serta pengamanan data agar tetap utuh dan dapat dipercaya. Dengan demikian, hukum siber berkontribusi pada terciptanya ekosistem digital yang aman dan andal.

Contoh:

Perusahaan teknologi informasi diwajibkan menerapkan protokol keamanan seperti enkripsi dan firewall untuk melindungi data pelanggan dari ancaman peretasan. Apabila terjadi pelanggaran, perusahaan dapat dikenai sanksi administratif atau pidana sesuai dengan peraturan yang berlaku.

5. Mengatur Transaksi dan Komunikasi Elektronik

Cyber Law memberikan dasar hukum yang mengatur validitas dan keabsahan transaksi elektronik serta komunikasi yang terjadi di dunia maya. Hal ini mencakup penggunaan tanda tangan elektronik, pengakuan bukti elektronik di pengadilan, serta pengaturan kontrak digital. Regulasi ini memfasilitasi pertukaran informasi dan transaksi secara efisien dan aman, sekaligus memberikan perlindungan hukum bagi semua pihak yang terlibat.

Contoh:

Penggunaan tanda tangan elektronik dalam kontrak kerja sama antara perusahaan dan klien diakui sebagai alat bukti yang sah secara hukum, sehingga apabila terjadi pelanggaran kontrak, penyelesaian dapat dilakukan melalui mekanisme hukum yang berlaku.

3. Ruang Lingkup Cyber Law

Cyber Law atau hukum siber merupakan cabang hukum yang mengatur berbagai aspek hukum yang muncul akibat pemanfaatan teknologi informasi dan komunikasi, khususnya internet. Ruang lingkup Cyber Law sangat luas dan multidisipliner, mencakup berbagai bidang hukum dan

teknologi. Secara umum, ruang lingkup Cyber Law dapat diklasifikasikan sebagai berikut:

1. Cybercrime (Kejahatan Siber)

   Merupakan tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer dan jaringan internet. Kejahatan ini meliputi peretasan (hacking), penyebaran virus atau malware, penipuan daring (online fraud), pencurian data, hingga penyebaran konten ilegal seperti pornografi dan ujaran kebencian. Cyber Law menetapkan aturan untuk pencegahan, penindakan, dan penegakan hukum terhadap kejahatan tersebut.

2. Perlindungan Data Pribadi

   Mengatur hak-hak individu terkait data pribadi yang dikumpulkan, disimpan, dan diproses oleh pihak ketiga. Regulasi ini bertujuan untuk menjaga privasi pengguna internet dan memastikan bahwa data pribadi diperlakukan secara etis dan sesuai hukum.

3. Transaksi Elektronik dan E-Commerce

   Mengatur validitas kontrak elektronik, mekanisme tanda tangan digital, perlindungan konsumen dalam transaksi online, serta aspek legal lainnya yang berkaitan dengan perdagangan dan transaksi yang berlangsung secara elektronik.

4. Hak Kekayaan Intelektual Digital

   Meliputi perlindungan atas karya cipta, paten, merek dagang, dan rahasia dagang yang berbentuk digital. Cyber Law melindungi hak-hak tersebut dari pembajakan, penggandaan ilegal, dan pelanggaran lainnya di dunia maya.

5. Keamanan Siber (Cybersecurity)

   Mengatur kewajiban dan standar teknis bagi penyelenggara sistem elektronik untuk menjaga keamanan informasi dan infrastruktur teknologi dari ancaman, gangguan, atau akses ilegal.

6. Etika dan Kebebasan Digital

Mencakup aturan dan norma yang mengatur perilaku pengguna di dunia maya, termasuk kebebasan berekspresi, hak atas informasi, serta batasan terhadap penyebaran konten yang melanggar hukum atau norma sosial.

7. Hukum Internasional dan Cyber War

Mengatur hubungan antarnegara dalam ranah siber, termasuk kerja sama internasional untuk menangani kejahatan siber lintas negara serta aspek hukum terkait konflik siber (cyber war).

B. Urgensi Hukum Siber

Hukum siber, atau cyber law, merupakan cabang hukum yang mengatur aktivitas dan interaksi manusia dalam ruang digital yang tercipta melalui teknologi informasi dan komunikasi, khususnya internet. Istilah ini mencakup berbagai aspek hukum yang berkaitan dengan dunia maya, termasuk namun tidak terbatas pada kejahatan siber (cybercrime), transaksi elektronik, perlindungan data pribadi, dan hak kekayaan intelektual digital .

Di Indonesia, pengembangan hukum siber bertujuan untuk memberikan kerangka hukum yang jelas dalam menghadapi dinamika dan tantangan yang muncul akibat perkembangan teknologi digital. Hal ini mencakup penyusunan dan penegakan regulasi yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) .

Perkembangan teknologi informasi dan komunikasi (TIK) telah mengubah secara fundamental cara manusia berinteraksi, bertransaksi, bekerja, hingga menjalankan pemerintahan. Internet dan jaringan digital telah menciptakan ruang baru yang dikenal sebagai dunia maya (cyberspace), di mana interaksi tidak lagi dibatasi oleh sekat-sekat geografis atau waktu. Transformasi

digital ini membawa dampak positif dalam berbagai sektor, namun pada saat yang sama menimbulkan tantangan baru dalam aspek hukum, keamanan, etika, dan hak-hak sipil. Di sinilah urgensi hukum siber (cyber law) menjadi sangat penting untuk diangkat dan dikembangkan secara serius.

1. Pertumbuhan dan Kompleksitas Kejahatan Siber

Salah satu alasan utama urgensinya hukum siber adalah meningkatnya insiden kejahatan siber (cybercrime). Bentuk-bentuk kejahatan siber sangat beragam dan terus berkembang, mulai dari penipuan daring (online fraud), peretasan sistem (hacking), penyebaran virus, ransomware, pencurian data pribadi (data breach), hingga kejahatan yang lebih kompleks seperti manipulasi sistem keuangan dan serangan terhadap infrastruktur digital negara.

Karakteristik dunia maya yang bersifat anonim, lintas batas, dan cepat membuat penegakan hukum terhadap kejahatan ini menjadi lebih kompleks dibandingkan dengan kejahatan konvensional. Tanpa kerangka hukum yang kuat, kejahatan digital akan sulit ditangani secara efektif, dan korban akan semakin tidak terlindungi.

Contoh: Kasus peretasan data BPJS Kesehatan yang terjadi di Indonesia menunjukkan bagaimana data pribadi jutaan warga negara dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, sementara kerangka regulasi saat itu masih belum cukup memadai untuk menangani dampak dan menindak pelakunya secara optimal.

2. Perlindungan Data Pribadi sebagai Hak Konstitusional

Dalam konteks negara hukum, hak atas privasi merupakan bagian dari hak asasi manusia yang dilindungi. Di era digital, data pribadi menjadi komoditas yang sangat berharga dan rentan

disalahgunakan, baik oleh pelaku kejahatan siber, perusahaan teknologi, maupun institusi negara.

Hukum siber dibutuhkan untuk mengatur mekanisme pengumpulan, penyimpanan, pengolahan, dan distribusi data pribadi agar tidak disalahgunakan. Hal ini sejalan dengan berkembangnya prinsip perlindungan data global seperti General Data Protection Regulation (GDPR) di Uni Eropa, serta Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia.

Contoh: Platform digital seperti marketplace dan media sosial mengumpulkan banyak informasi sensitif dari pengguna. Tanpa hukum yang tegas, data tersebut bisa bocor atau digunakan tanpa persetujuan pemiliknya untuk kepentingan komersial atau politik.

3. Menjamin Kepastian Hukum dalam Transaksi Digital

E-commerce, perbankan digital, kontrak elektronik, dan tanda tangan digital kini menjadi bagian tak terpisahkan dari kehidupan masyarakat modern. Namun, tanpa kerangka hukum yang jelas, transaksi elektronik dapat menimbulkan konflik antara pelaku usaha dan konsumen, khususnya jika terjadi penipuan, ketidaksesuaian produk, atau pelanggaran kontrak.

Hukum siber berperan dalam memberikan landasan hukum yang sah atas aktivitas digital, termasuk legalitas dokumen elektronik, validitas perjanjian digital, serta prosedur penyelesaian sengketa online.

Contoh: Dalam transaksi e-commerce, apabila terjadi pengiriman produk yang tidak sesuai deskripsi, konsumen berhak atas perlindungan dan kompensasi sebagaimana diatur dalam peraturan perlindungan konsumen digital.

4. Menjaga Kedaulatan dan Keamanan Siber Nasional

Aspek yang tidak kalah penting adalah perlunya hukum siber untuk menjaga kedaulatan digital dan keamanan nasional. Ancaman siber terhadap sistem informasi pemerintah, militer, dan infrastruktur kritis seperti energi, transportasi, dan kesehatan dapat menyebabkan ketidakstabilan negara.

Dalam kerangka ini, hukum siber berfungsi sebagai perangkat regulatif dan preventif untuk mencegah serangan siber, memperkuat sistem pertahanan digital nasional, serta mengatur batasan dan tanggung jawab aktor-aktor internasional dalam ruang siber.

Contoh: Serangan siber terhadap data kependudukan atau sistem e-voting dapat membahayakan proses demokrasi dan kepercayaan publik terhadap negara.

5. Menyediakan Dasar Etika dan Norma Digital

Hukum siber tidak hanya berfungsi sebagai perangkat koersif, tetapi juga sebagai panduan etis dalam menggunakan teknologi informasi. Dalam dunia maya yang sangat terbuka, penyebaran konten ilegal seperti ujaran kebencian, pornografi anak, atau hoaks, harus diatur agar tidak mengganggu tatanan sosial dan moral masyarakat.

Urgensi ini semakin relevan dengan meningkatnya jumlah pengguna internet muda yang membutuhkan edukasi hukum digital dan pedoman etika dalam bermedia sosial.

Contoh: Hukum siber dapat mengatur batasan kebebasan berekspresi di internet agar tetap dalam koridor yang menghormati hak asasi manusia dan nilai-nilai kemasyarakatan.

Cyber Law hadir sebagai respons hukum terhadap tantangan baru yang muncul akibat perkembangan teknologi informasi. Dunia maya memiliki karakteristik khas—tanpa batas, anonim, cepat, dan berbasis teknologi—yang tidak dapat diatur

sepenuhnya oleh hukum konvensional. Oleh karena itu, Cyber Law dibutuhkan untuk mengatur aktivitas digital secara adil, memberikan perlindungan hukum, serta menciptakan ruang siber yang aman dan etis bagi seluruh pengguna.

Keberadaan Cyber Law merupakan respons terhadap perubahan zaman yang ditandai oleh dominasi teknologi dalam kehidupan manusia. Dalam konteks akademik, hukum siber tidak dapat dipisahkan dari dinamika sosial global dan nasional, serta menuntut pendekatan yang komprehensif dan multidisipliner. Di Indonesia, urgensi pengembangan hukum siber terletak pada upaya untuk memberikan kepastian hukum, melindungi hak digital masyarakat, dan menjaga keamanan nasional dari ancaman dunia maya. Oleh karena itu, penguatan regulasi, peningkatan literasi hukum digital, serta kolaborasi antar sektor merupakan kunci menuju tata kelola ruang digital yang inklusif, aman, dan adil.

BAB 2

Karakteristik Dunia Maya

Dunia maya (cyberspace) telah menjadi entitas sosial, ekonomi, dan hukum baru yang menyatu dalam kehidupan masyarakat global modern. Tidak seperti ruang fisik yang dibatasi oleh teritorial, dunia maya hadir sebagai ruang virtual tanpa batas yang memungkinkan interaksi dan aktivitas digital melampaui hambatan geografis dan politik. Fenomena ini memunculkan dimensi hukum baru, yakni hukum siber (cyber law), yang bertujuan memberikan regulasi terhadap berbagai bentuk perilaku dan transaksi yang terjadi di ranah digital. Untuk memahami tantangan dan urgensi penataan hukum di dunia maya, penting untuk mengkaji karakteristik mendasar dari ruang siber itu sendiri.

Berikut beberapa karakteristik dari Dunia Maya

1. Tanpa Batas Geografis (Borderless Jurisdiction)

Dunia maya bersifat transnasional, artinya aktivitas yang dilakukan oleh individu atau entitas di satu negara dapat berdampak langsung pada sistem atau individu lain di berbagai belahan dunia. Hal ini mengaburkan prinsip-prinsip dasar dalam hukum konvensional, khususnya terkait yurisdiksi negara. Ketika seseorang mengunggah konten atau melakukan transaksi daring, tindakan tersebut dapat melibatkan hukum dari berbagai negara sekaligus, menciptakan kompleksitas dalam aspek penegakan hukum.

Contoh: Kasus pencemaran nama baik di media sosial yang dilakukan oleh pengguna di Indonesia terhadap seseorang

di Singapura dapat menimbulkan konflik yurisdiksi terkait hukum mana yang berlaku dan pengadilan mana yang berwenang mengadili.

2. Identitas Digital dan Anonimitas

Di dunia maya, identitas fisik tidak lagi menjadi syarat utama untuk berpartisipasi dalam interaksi sosial maupun transaksi ekonomi. Individu dapat menciptakan identitas digital, baik dengan nama asli maupun anonim, melalui akun media sosial, alamat surel, atau profil daring lainnya. Kemampuan untuk menyembunyikan atau memalsukan identitas ini menciptakan kebebasan, tetapi juga meningkatkan risiko penyalahgunaan.

Konsekuensi hukum: Dalam hukum konvensional, pelaku tindak pidana dapat dengan mudah diidentifikasi melalui data kependudukan. Namun di ruang digital, keberadaan identitas palsu atau akun anonim mempersulit upaya penegakan hukum, khususnya dalam kasus seperti cyberbullying, penipuan daring, dan peretasan.

Contoh: Seorang peretas yang menyerang situs pemerintah menggunakan jaringan proxy dan identitas palsu akan sulit dilacak tanpa teknik investigasi digital forensik yang mendalam.

3. Replikasi dan Persistensi Informasi Digital

Informasi yang dipublikasikan di internet memiliki sifat mudah direplikasi dan cenderung bersifat permanen. Sekali suatu data atau konten tersebar di dunia maya, sangat sulit untuk menghapusnya secara total, terutama jika telah disimpan atau dibagikan ulang oleh banyak pihak.

Contoh: Sebuah video yang bocor ke publik dapat tetap tersebar di berbagai situs mirror bahkan setelah dihapus dari platform utama, menimbulkan kerugian jangka panjang bagi pemilik data atau subjek dalam video tersebut.

4. Kecepatan Interaksi dan Skala Global

Salah satu kekuatan utama dunia maya adalah kemampuannya memfasilitasi komunikasi secara real-time. Informasi dapat disebarluaskan dalam hitungan detik ke jutaan pengguna di seluruh dunia. Sifat ini membawa dampak positif dalam efisiensi komunikasi dan transaksi, tetapi juga mempercepat penyebaran hoaks, ujaran kebencian, dan berbagai bentuk gangguan siber.

Contoh: Sebuah kampanye disinformasi politik yang diluncurkan melalui platform media sosial dapat memengaruhi opini publik secara masif sebelum ada kesempatan untuk mengklarifikasi atau menindaklanjuti secara hukum.

5. Ketergantungan pada Infrastruktur Teknologi

Semua aktivitas di dunia maya sangat bergantung pada sistem teknologi informasi dan komunikasi, termasuk perangkat keras (hardware), perangkat lunak (software), serta jaringan internet global. Kerentanan teknis terhadap gangguan atau serangan dapat menyebabkan konsekuensi yang luas terhadap berbagai sektor, termasuk ekonomi, pendidikan, dan layanan publik.

Contoh: Serangan siber pada sistem perbankan nasional dapat mengakibatkan lumpuhnya transaksi keuangan dan berdampak pada kepercayaan publik terhadap stabilitas ekonomi.

6. Multidimensi dan Interdisipliner

Karakteristik dunia maya tidak hanya bersifat teknis, tetapi juga memuat dimensi sosial, ekonomi, budaya, dan politik. Oleh karena itu, pengaturan dunia maya membutuhkan pendekatan hukum yang tidak bersifat sektoral, melainkan lintas disiplin. Hukum siber harus bersinergi dengan prinsip-prinsip HAM, kebebasan berpendapat, perlindungan konsumen, hingga keamanan nasional.

Identitas Digital

Seiring dengan transformasi digital yang kian masif, identitas manusia tidak lagi hanya dibatasi oleh keberadaan fisik dan data kependudukan konvensional. Munculnya ruang maya (cyberspace) telah melahirkan konsep baru yang dikenal sebagai identitas digital (digital identity), yaitu representasi individu, kelompok, atau entitas hukum dalam bentuk data yang digunakan untuk mengakses dan berinteraksi di dunia digital. Identitas digital memainkan peran sentral dalam hampir seluruh aktivitas daring, baik dalam konteks sosial, ekonomi, politik, maupun hukum. Dalam perkembangan hukum siber, pengakuan dan perlindungan terhadap identitas digital menjadi isu strategis yang berkaitan langsung dengan hak asasi manusia, privasi, keamanan, dan integritas sistem hukum itu sendiri.

Secara umum, identitas digital dapat didefinisikan sebagai kumpulan data elektronik yang merepresentasikan karakteristik atau atribut dari seseorang atau suatu entitas yang digunakan untuk mengenali, mengotentikasi, dan mengotorisasi keberadaan mereka di dunia maya. Identitas digital ini dapat berupa nama pengguna, kata sandi, alamat email, metadata, identitas biometrik, hingga jejak digital yang terbentuk dari aktivitas daring.

Dalam konteks hukum, identitas digital memiliki dimensi ganda:

- Sebagai alat autentikasi hukum, yang digunakan dalam transaksi elektronik atau akses terhadap layanan publik.
- Sebagai subjek hukum virtual, yang memiliki hak dan kewajiban serta dapat dikenai tanggung jawab hukum atas tindakannya di dunia maya.

Komponen Identitas Digital

Identitas digital merupakan elemen kunci dalam interaksi manusia di dunia maya. Dalam berbagai konteks digital—baik administratif, sosial, maupun komersial—identitas digital digunakan sebagai representasi elektronik dari subjek hukum. Untuk membangun sistem identitas digital yang aman, sah, dan dapat diandalkan, dibutuhkan pemahaman menyeluruh mengenai komponen-komponen utama yang menyusun identitas tersebut. Masing-masing komponen memiliki peran spesifik dalam proses pengenalan, autentikasi, otorisasi, dan pengelolaan data pribadi dalam ekosistem digital.

1. Data Identifikasi Pribadi (Personally Identifiable Information / PII)

Merupakan data-data dasar yang secara unik dapat digunakan untuk mengidentifikasi individu. PII sering kali menjadi fondasi utama dari sistem identitas digital.

Contoh Komponen:

- Nama lengkap
- Tanggal lahir
- Nomor identitas nasional (seperti NIK di Indonesia)
- Nomor paspor atau SIM
- Alamat tempat tinggal
- Nomor telepon dan alamat email

Contoh Kasus:

Ketika seseorang mendaftar untuk layanan perbankan digital, ia harus memasukkan PII sebagai verifikasi awal, seperti mencantumkan NIK dan mengunggah foto KTP.

2. Kredensial Akses (Authentication Credentials)

Kredensial ini digunakan untuk memverifikasi bahwa pengguna adalah pemilik sah dari identitas digital tersebut.

Jenis Kredensial:

- Username dan password

- PIN
- Sertifikat digital
- Token keamanan (security tokens)
- Autentikasi dua faktor (2FA), seperti SMS OTP atau aplikasi autentikator

Contoh Kasus:

Saat mengakses akun email atau e-wallet, pengguna diminta untuk memasukkan kombinasi username dan password, serta kode OTP yang dikirimkan ke nomor terdaftar untuk autentikasi ganda.

3. Informasi Biometrik (Biometric Identifiers)

Data biometrik adalah jenis data pribadi yang berkaitan dengan karakteristik fisik atau perilaku seseorang, yang unik dan tidak mudah direplikasi.

Contoh Biometrik:

- Sidik jari
- Pengenalan wajah
- Pemindaian retina
- Suara
- Pola ketikan (keystroke dynamics)

Contoh Kasus:

Layanan perbankan dan pemerintah kini banyak mengintegrasikan biometrik ke dalam proses verifikasi, misalnya e-KTP di Indonesia yang menggunakan sidik jari dan pemindaian iris.

4. Atribut Sosial dan Ekonomi

Atribut yang menggambarkan status, preferensi, dan aktivitas seseorang dalam dunia digital, biasanya terekam melalui interaksi dengan platform tertentu.

Contoh:

- Riwayat pembelian dalam e-commerce
- Aktivitas media sosial (likes, komentar, unggahan)

- Preferensi browsing dan lokasi
- Riwayat pendidikan dan pekerjaan (seperti di LinkedIn)

Contoh Kasus:

Platform e-commerce seperti Tokopedia atau Shopee menggunakan histori pembelian untuk memverifikasi keaslian akun dan mendeteksi aktivitas penipuan.

5. Metadata dan Jejak Digital (Digital Footprint)

Definisi:

Merupakan informasi tidak langsung yang dihasilkan oleh aktivitas daring seseorang dan direkam secara otomatis oleh sistem atau platform.

Contoh Metadata:

- Alamat IP
- Waktu dan lokasi login
- Jenis perangkat dan browser yang digunakan
- Cookies yang tersimpan di perangkat pengguna

Contoh Kasus:

Jejak digital ini sangat berguna dalam investigasi siber, misalnya melacak lokasi IP terakhir dari pelaku kejahatan siber yang menggunakan akun anonim.

6. Identitas Hukum Digital (Legal Digital Identity)

Identitas digital yang secara resmi diakui oleh negara atau lembaga hukum sebagai representasi sah dari individu dalam sistem digital.

Contoh:

- Tanda tangan digital tersertifikasi
- Sertifikat elektronik dari otoritas sertifikasi

Sistem identitas elektronik nasional seperti e-KTP (Indonesia), e-ID (Estonia), atau MyKad (Malaysia)

Contoh Kasus:

Di Estonia, warga negara dapat melakukan voting, akses perbankan, bahkan menandatangani kontrak hukum hanya dengan menggunakan satu identitas digital yang disahkan secara hukum oleh negara.

7. Mekanisme Otorisasi dan Hak Akses

Definisi:

Setelah proses identifikasi dan autentikasi, komponen ini menentukan sejauh mana akses yang dimiliki pengguna terhadap layanan atau data tertentu.

Contoh:

- Role-based access control (RBAC)
- Attribute-based access control (ABAC)

Contoh Kasus:

Dalam sistem e-learning kampus, mahasiswa hanya memiliki akses ke materi kuliah, sedangkan dosen memiliki akses tambahan untuk mengunggah bahan ajar dan memberi nilai.

Identitas digital terdiri atas berbagai komponen yang saling melengkapi, mulai dari data identifikasi pribadi, kredensial akses, informasi biometrik, hingga metadata aktivitas daring. Komponen-komponen tersebut tidak hanya berfungsi secara teknis untuk memastikan keabsahan pengguna dalam sistem digital, tetapi juga memiliki implikasi hukum yang signifikan. Dalam era digital yang sarat dengan ancaman keamanan dan penyalahgunaan data, pemahaman terhadap struktur identitas digital menjadi kunci dalam menciptakan ekosistem digital yang aman, terpercaya, dan berkeadilan

Yurisdiksi dalam Dunia Maya

Yurisdiksi merupakan prinsip dasar dalam ilmu hukum yang menentukan kewenangan suatu negara atau lembaga hukum dalam membuat, menegakkan, dan mengadili suatu peristiwa hukum. Dalam konteks konvensional, yurisdiksi

ditentukan berdasarkan batas-batas geografis suatu negara atau wilayah. Namun, kehadiran dunia maya (cyberspace) telah mengaburkan batas-batas fisik tersebut. Internet memungkinkan aktivitas lintas negara tanpa harus berpindah tempat secara fisik, sehingga menciptakan tantangan yuridis yang kompleks mengenai siapa yang berwenang menangani kasus hukum yang terjadi di ruang digital.

Dalam dunia maya, yurisdiksi dapat didefinisikan sebagai hak dan kewenangan hukum suatu negara atau entitas untuk menerapkan aturan, melakukan penyelidikan, mengadili pelanggaran hukum, serta menegakkan putusan terhadap aktivitas yang dilakukan melalui jaringan internet. Yurisdiksi ini bisa bersifat:

1. Yurisdiksi Teritorial

Yurisdiksi teritorial mengacu pada kewenangan suatu negara untuk menerapkan hukum terhadap peristiwa atau perbuatan yang terjadi di dalam batas-batas wilayah geografisnya. Dalam konteks siber, konsep ini diperluas untuk mencakup lokasi fisik dari server, data center, atau sistem jaringan yang terlibat dalam suatu aktivitas digital.

Jika sebuah server yang digunakan untuk melakukan penipuan online berada di Indonesia, maka Indonesia dapat mengklaim yurisdiksi berdasarkan lokasi infrastruktur teknologinya, meskipun pelaku atau korban mungkin berada di negara lain.

Salah satu tantangan utama dalam penerapan yurisdiksi teritorial di dunia maya adalah ketiadaan batas geografis yang jelas. Tidak seperti ruang fisik yang memiliki garis batas negara yang dapat diukur dan ditentukan secara hukum, dunia maya bersifat virtual dan lintas batas. Informasi dan aktivitas digital dapat mengalir bebas dari satu negara ke negara lain tanpa kendala fisik. Selain itu, keberadaan teknologi cloud computing

memperumit persoalan yurisdiksi karena data dan server yang digunakan untuk menjalankan layanan internet dapat tersebar di berbagai lokasi global secara dinamis. Misalnya, sebuah aplikasi digital yang diakses oleh pengguna di Indonesia bisa saja disimpan di server yang berpindah-pindah antara Singapura, Amerika Serikat, dan Eropa dalam hitungan detik, sehingga sulit untuk menentukan di wilayah hukum mana aktivitas digital tersebut sebenarnya terjadi. Kondisi ini menimbulkan ambiguitas dalam penegakan hukum dan memerlukan pendekatan yurisdiksi yang fleksibel dan kolaboratif lintas negara.

2. Yurisdiksi Personal (*Personal Jurisdiction*)

Yurisdiksi personal adalah kewenangan hukum yang dimiliki suatu negara terhadap individu atau entitas hukum berdasarkan kewarganegaraan, domisili, atau tempat kedudukan hukum mereka, terlepas dari lokasi peristiwa digital yang terjadi.

Seorang warga negara Indonesia yang melakukan kejahatan siber terhadap sistem informasi bank di negara lain tetap dapat dikenai hukum Indonesia berdasarkan yurisdiksi personal. Sebaliknya, seseorang yang berdomisili di AS namun melakukan pencemaran nama baik terhadap individu di Indonesia melalui media sosial, dapat dikenai hukum AS berdasarkan prinsip yang sama.

Dalam konteks yurisdiksi personal dalam dunia maya, tantangan besar yang dihadapi adalah kesulitan dalam mengidentifikasi pelaku kejahatan siber secara akurat. Identitas pelaku sering kali disamarkan melalui berbagai teknik seperti penggunaan VPN, proxy server, atau identitas palsu yang membuat mereka sulit dilacak oleh aparat penegak hukum. Bahkan dalam banyak kasus, pelaku dapat beroperasi secara anonim dan tersembunyi di balik infrastruktur digital yang kompleks. Selain itu, ketika pelaku berhasil diidentifikasi dan ternyata berada di luar negeri, proses ekstradisi menjadi

hambatan tersendiri, terutama jika negara asal pelaku tidak memiliki perjanjian kerja sama hukum internasional dengan negara korban. Tanpa mekanisme ekstradisi dan mutual legal assistance yang kuat antarnegara, penegakan hukum lintas yurisdiksi terhadap pelaku kejahatan siber menjadi sangat terbatas dan lambat, sehingga memperlemah efek jera serta mengurangi efektivitas hukum siber secara global.

3. Yurisdiksi Subjektif (Subjective or Effects-based Jurisdiction)

Yurisdiksi subjektif merujuk pada prinsip bahwa suatu negara dapat mengeklaim yurisdiksi atas tindakan digital yang meskipun dilakukan di luar wilayahnya, namun menimbulkan dampak langsung dan nyata (real effect) di dalam wilayah hukum negara tersebut.

Jika suatu situs web asing menyebarkan konten hoaks yang menimbulkan keresahan di masyarakat Indonesia, pemerintah Indonesia dapat mengklaim yurisdiksi berdasarkan dampak sosial dan keamanan yang ditimbulkan, meskipun konten tersebut diunggah dari luar negeri.

Prinsip ini dikenal juga sebagai "effects doctrine" dan sering dipakai dalam hukum siber internasional, khususnya dalam kasus pelanggaran hak cipta, penyebaran malware lintas negara, dan serangan siber terhadap infrastruktur kritikal.

Dalam penerapan yurisdiksi subjektif di ranah dunia maya, salah satu tantangan utama adalah potensi terjadinya overlapping yurisdiksi, yaitu ketika dua atau lebih negara secara bersamaan mengklaim kewenangan hukum atas suatu kasus siber yang sama. Hal ini umumnya terjadi karena tindakan digital yang dilakukan di satu negara dapat menimbulkan dampak nyata di negara lain, sehingga masing-masing merasa memiliki dasar hukum untuk mengambil tindakan. Situasi ini dapat memicu konflik hukum internasional, terutama jika tidak terdapat kesepakatan atau

pengakuan bersama atas batas-batas yurisdiksi antara negara-negara yang terlibat. Tanpa adanya kerangka hukum internasional yang disepakati secara luas, seperti konvensi atau perjanjian bilateral, maka penanganan kasus siber lintas negara menjadi rumit, berisiko menciptakan ketegangan antarnegara, dan menghambat proses keadilan bagi korban kejahatan digital.

Ketiga jenis yurisdiksi—teritorial, personal, dan subjektif—pada dasarnya saling melengkapi dan sering kali diterapkan secara bersamaan dalam penanganan kasus-kasus siber yang melibatkan berbagai negara. Meskipun begitu, keberhasilan penegakan hukum di ruang digital sangat bergantung pada beberapa faktor krusial.

Pertama, diperlukan kerja sama internasional yang kuat, baik melalui perjanjian ekstradisi maupun mekanisme bantuan hukum timbal balik (mutual legal assistance) untuk memastikan pelaku kejahatan dapat ditindak secara hukum lintas batas negara.

Kedua, pemanfaatan teknologi forensik digital sangat penting dalam melacak jejak pelaku, mengidentifikasi perangkat yang digunakan, dan mengumpulkan bukti elektronik yang sah secara hukum.

Ketiga, peran aktif platform digital global, seperti media sosial dan penyedia layanan internet, juga dibutuhkan dalam mematuhi dan mendukung pelaksanaan yurisdiksi hukum dari berbagai negara tempat mereka beroperasi. Dengan pemahaman yang mendalam terhadap perbedaan dan peran masing-masing jenis yurisdiksi, para pembuat kebijakan dan penegak hukum di seluruh dunia dapat merumuskan regulasi dan strategi penegakan hukum yang lebih adaptif dan efektif dalam menghadapi kompleksitas dunia maya yang dinamis dan lintas batas.

BAB 3

Regulasi Cyber Law di Indonesia

Regulasi Cyber Law di Indonesia merupakan bentuk respons negara terhadap dinamika dan kompleksitas dunia digital yang semakin berkembang. Seiring dengan pesatnya kemajuan teknologi informasi dan komunikasi, berbagai aktivitas masyarakat—baik dalam ranah sosial, ekonomi, maupun hukum—telah bertransformasi ke dalam ruang siber yang tidak lagi dibatasi oleh wilayah geografis. Hal ini menuntut adanya kerangka hukum yang adaptif, komprehensif, dan progresif guna melindungi hak-hak warga negara, menjaga keamanan siber nasional, serta menegakkan keadilan dalam menghadapi kejahatan siber.

Oleh karena itu, studi terhadap regulasi Cyber Law di Indonesia menjadi penting sebagai upaya untuk memahami fondasi normatif yang digunakan negara dalam menata dan mengatur ruang digital, serta menganalisis sejauh mana efektivitas regulasi tersebut dalam menjawab tantangan hukum di era transformasi digital.

Beberapa acuan yang digunakan hukum siber di Indonesia:

1. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian diperbarui melalui UU No. 19

Tahun 2016, merupakan pilar utama dalam regulasi aktivitas digital di Indonesia. Undang-undang ini mencakup berbagai aspek, termasuk pengakuan atas dokumen dan tanda tangan elektronik, serta pengaturan mengenai transaksi elektronik. Selain itu, UU ITE menetapkan sanksi pidana untuk berbagai pelanggaran, seperti penyebaran konten asusila, perjudian online, pencemaran nama baik, penyebaran berita bohong, ujaran kebencian, akses ilegal ke sistem elektronik, dan penyadapan tanpa izin.

2. Peraturan Pelaksana dan Pendukung

Dalam rangka memperkuat implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), pemerintah Indonesia telah menetapkan sejumlah peraturan pelaksana dan kebijakan teknis yang bertujuan untuk mengatur aspek-aspek teknis dan operasional dari aktivitas digital.

Salah satu peraturan kunci yang mendasari penyelenggaraan sistem elektronik adalah Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Peraturan ini menggantikan PP No. 82 Tahun 2012 dan memperluas cakupan pengaturan terhadap seluruh penyelenggara sistem elektronik, baik sektor publik maupun privat, termasuk platform digital global yang menyediakan layanan kepada masyarakat Indonesia.

PP No. 71 Tahun 2019 memuat ketentuan mengenai kewajiban pendaftaran sistem elektronik, tata kelola keamanan sistem informasi, hingga persyaratan perlindungan data pribadi pengguna. Misalnya, setiap penyelenggara sistem elektronik diwajibkan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan data yang dikelola, serta melapor kepada otoritas apabila terjadi insiden kebocoran data atau gangguan sistem. Peraturan ini juga menekankan pentingnya interoperabilitas antar

sistem elektronik, serta lokalisasi data untuk jenis data strategis tertentu yang dinilai penting bagi kedaulatan nasional.

3. Undang-Undang Perlindungan Data Pribadi (UU PDP)

UU PDP merupakan regulasi penting yang dirancang untuk memberikan perlindungan hukum terhadap hak-hak subjek data, yaitu individu yang memiliki data pribadi yang diproses oleh pihak-pihak tertentu. Di Indonesia, UU PDP resmi disahkan pada tahun 2022 dengan tujuan utama untuk mengatur pengumpulan, penyimpanan, penggunaan, dan pengungkapan data pribadi secara adil, transparan, dan aman.

UU PDP hadir sebagai respons terhadap pesatnya perkembangan teknologi informasi dan komunikasi yang membawa dampak signifikan terhadap pengelolaan data pribadi di ranah digital. Dalam konteks digitalisasi layanan publik, transaksi elektronik, dan interaksi sosial yang semakin luas melalui internet, perlindungan data pribadi menjadi sangat krusial untuk mencegah penyalahgunaan data, pelanggaran privasi, dan kejahatan siber seperti pencurian identitas dan penipuan online.

Secara substansial, UU PDP menetapkan sejumlah prinsip dasar yang harus dipenuhi oleh setiap pengendali data dan pemroses data, antara lain prinsip keadilan, transparansi, tujuan terbatas, keamanan data, serta hak akses dan koreksi oleh subjek data. Misalnya, pengendali data wajib mendapatkan persetujuan yang jelas dan eksplisit dari subjek data sebelum mengumpulkan dan memproses data pribadi, serta harus memastikan bahwa data yang disimpan terlindungi dari akses tidak sah atau kebocoran.

Selain itu, UU PDP juga membentuk sebuah lembaga independen yang bertugas mengawasi pelaksanaan perlindungan data pribadi, yaitu Otoritas Perlindungan Data Pribadi (PDP Authority). Lembaga ini memiliki fungsi untuk melakukan audit kepatuhan, menerima laporan pelanggaran

data, serta memberikan edukasi kepada masyarakat dan pelaku usaha mengenai pentingnya perlindungan data pribadi.

Implementasi UU PDP juga mendorong organisasi dan perusahaan untuk menerapkan kebijakan keamanan informasi yang ketat, termasuk enkripsi data dan audit berkala terhadap sistem keamanan. Dalam hal terjadi pelanggaran data, pengendali data diwajibkan untuk segera melaporkan insiden tersebut kepada otoritas terkait dan, jika perlu, kepada subjek data yang terdampak.

Secara global, UU PDP menempatkan Indonesia dalam koridor perlindungan data yang sejalan dengan standar internasional seperti General Data Protection Regulation (GDPR) di Uni Eropa, sehingga juga mendukung kelancaran kerja sama internasional dalam perdagangan elektronik dan keamanan siber lintas negara.

Dengan demikian, UU PDP bukan hanya sekadar regulasi teknis, melainkan juga fondasi bagi pengembangan ekosistem digital yang sehat, etis, dan berkeadilan, yang menghormati hak privasi individu sekaligus mendukung inovasi dan pertumbuhan ekonomi digital nasional.

BAB 4

Hukum dan Teknologi Informasi

Kemajuan teknologi informasi telah membawa dampak yang sangat besar bagi kehidupan manusia modern. Perkembangan pesat dalam bidang teknologi digital dan komunikasi telah mengubah cara manusia berinteraksi, bekerja, belajar, dan bahkan bertransaksi. Informasi kini dapat diakses dengan mudah dan cepat melalui jaringan internet yang menghubungkan berbagai belahan dunia tanpa batasan geografis.

Namun, di balik kemudahan dan manfaat tersebut, muncul berbagai tantangan yang berkaitan dengan aspek hukum. Hal ini mendorong lahirnya bidang hukum khusus yang mengatur penggunaan teknologi informasi, yang dikenal sebagai hukum teknologi informasi.

Hukum teknologi informasi merupakan cabang hukum yang mengatur tentang tata cara, hak, dan kewajiban dalam penggunaan teknologi digital serta internet. Bidang hukum ini bertujuan untuk melindungi kepentingan pengguna teknologi sekaligus menjaga keamanan dan keadilan dalam dunia digital.

Definisi Hukum Teknologi Informasi

Hukum teknologi informasi adalah kumpulan aturan dan regulasi yang dirancang untuk mengatur segala aktivitas yang berkaitan dengan penggunaan teknologi informasi dan

komunikasi. Hal ini meliputi aspek-aspek seperti penyebaran informasi secara elektronik, perlindungan data pribadi, transaksi elektronik, hingga penyelesaian sengketa yang terjadi di ranah digital.

Secara garis besar, hukum ini bertujuan untuk memastikan bahwa penggunaan teknologi informasi dilakukan secara sah, aman, dan bertanggung jawab, serta mencegah penyalahgunaan teknologi yang dapat merugikan individu atau institusi.

Perkembangan Hukum Teknologi Informasi

Seiring dengan meluasnya penggunaan internet dan perangkat digital, kebutuhan akan regulasi yang mengatur interaksi di dunia maya menjadi semakin penting. Negara-negara di seluruh dunia mulai merumuskan dan mengimplementasikan undang-undang yang mengatur penggunaan teknologi informasi agar tetap dalam koridor hukum.

Contohnya, regulasi mengenai perlindungan data pribadi yang mengatur bagaimana data seseorang dikumpulkan, disimpan, dan digunakan oleh berbagai pihak. Selain itu, muncul juga peraturan yang mengakui keabsahan transaksi dan kontrak yang dilakukan secara elektronik, memberikan kepastian hukum bagi pelaku bisnis dan konsumen di era digital.

Di Indonesia, salah satu regulasi penting yang mengatur bidang ini adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang memberikan landasan hukum bagi penggunaan teknologi informasi dan transaksi elektronik.

Ciri Khas Dunia Digital dan Implementasi Hukum

Dunia digital memiliki sifat dan karakteristik yang sangat berbeda jika dibandingkan dengan dunia fisik yang sudah lama dikenal dalam praktik hukum konvensional. Perbedaan ini bukan hanya terletak pada aspek teknis atau teknologi, tetapi juga pada

aspek sosial, budaya, serta hukum yang menyertainya. Oleh karena itu, penerapan hukum di dunia digital harus memperhatikan karakteristik khusus agar dapat efektif, relevan, dan adil. Berikut ini adalah penjelasan lebih rinci mengenai karakteristik utama dunia digital beserta dampaknya terhadap penegakan hukum.

1. Skala Global dan Keterbatasan Batas Wilayah

Internet adalah jaringan global yang menghubungkan jutaan perangkat dan pengguna dari seluruh dunia tanpa memandang batas negara. Aktivitas digital yang dilakukan di satu tempat secara fisik bisa berdampak di tempat lain yang secara geografis sangat jauh. Hal ini menimbulkan kompleksitas hukum yang besar karena hukum nasional yang berlaku di satu negara belum tentu sama atau sesuai dengan hukum yang berlaku di negara lain.

Misalnya, sebuah konten yang dianggap legal dan boleh disebarluaskan di satu negara mungkin dianggap melanggar hukum di negara lain. Begitu pula dalam kasus kejahatan siber seperti penipuan atau pencurian data, pelaku dan korban dapat berada di negara berbeda, sehingga koordinasi antar aparat penegak hukum lintas negara menjadi sangat penting namun juga penuh tantangan.

Karakteristik ini menuntut adanya kerja sama internasional yang kuat, pembentukan perjanjian bilateral atau multilateral, serta harmonisasi hukum di bidang teknologi informasi untuk menjembatani perbedaan regulasi antarnegara. Tanpa adanya kesepakatan dan koordinasi ini, proses hukum sering kali menemui kebuntuan karena masalah yurisdiksi yang tidak jelas.

2. Anonimitas dan Identitas Virtual

Salah satu ciri khas dunia digital adalah kemampuan pengguna untuk beroperasi secara anonim atau menggunakan identitas virtual yang tidak selalu merefleksikan identitas asli

mereka. Pengguna bisa membuat akun palsu, menyembunyikan lokasi, atau menggunakan berbagai teknik untuk menyamarkan keberadaan aslinya.

Sifat anonim ini memberikan kebebasan yang lebih besar bagi pengguna untuk berekspresi, berkomunikasi, dan mengakses informasi tanpa takut dikenali atau dihakimi secara langsung. Namun, di sisi lain, anonimitas ini juga membuka peluang bagi tindakan yang tidak bertanggung jawab dan bahkan ilegal, seperti penipuan online, peretasan, penyebaran berita palsu (hoaks), ujaran kebencian, hingga tindakan kriminal lainnya yang sulit untuk dilacak pelakunya.

Dampak hukum dari anonimitas ini adalah perlunya regulasi dan teknologi pendukung untuk memastikan bahwa aktivitas digital tetap dapat dipertanggungjawabkan. Contohnya adalah kewajiban platform digital untuk melakukan verifikasi identitas pengguna tertentu, mekanisme pelaporan dan penanganan konten ilegal, serta pengembangan teknik forensik digital untuk mengungkap identitas pelaku kejahatan siber.

3. Kecepatan dan Volume Transaksi Digital yang Sangat Tinggi

Transaksi dan pertukaran informasi di dunia digital berlangsung dalam hitungan detik dan dalam jumlah yang sangat besar. Aktivitas e-commerce, komunikasi digital, transfer data, hingga transaksi finansial bisa terjadi secara simultan dan terus-menerus tanpa henti.

Kecepatan dan volume yang tinggi ini menjadi tantangan tersendiri bagi sistem hukum dan penegakan hukum. Kasus pelanggaran atau kejahatan digital harus dapat direspons dengan cepat agar tidak menyebabkan kerugian yang lebih besar. Misalnya, dalam kasus peretasan atau penyebaran malware, tindakan cepat sangat diperlukan untuk meminimalkan dampak dan mencegah kerusakan lebih luas.

Selain itu, volume data yang sangat besar menuntut penggunaan teknologi dan sumber daya yang memadai untuk mengumpulkan, menganalisis, dan menyimpan bukti digital. Hal ini berarti aparat penegak hukum harus memiliki kemampuan teknologi informasi yang memadai agar dapat menangani bukti digital secara efektif dan sah di mata hukum.

4. Aktif 24 Jam Nonstop, Tanpa Henti

Salah satu karakteristik paling unik dari dunia digital adalah bahwa ia tidak pernah berhenti beroperasi. Internet bekerja secara kontinu, 24 jam sehari, 7 hari dalam seminggu, tanpa mengenal waktu, hari kerja, atau hari libur. Tidak seperti aktivitas di dunia fisik yang umumnya dibatasi oleh waktu operasional tertentu, aktivitas di ruang digital berlangsung secara konstan, dengan pengguna dari berbagai zona waktu yang terus terhubung dan berinteraksi kapan pun mereka menginginkannya.

Kondisi ini menciptakan lingkungan yang sangat dinamis, fleksibel, dan penuh peluang. Namun, di sisi lain, sifat nonstop ini juga menghadirkan tantangan besar dalam konteks penegakan hukum dan regulasi. Potensi pelanggaran hukum di dunia digital tidak mengenal waktu—kejahatan atau penyimpangan bisa saja terjadi di tengah malam, akhir pekan, bahkan saat hari besar nasional berlangsung. Misalnya, peretasan situs pemerintahan bisa terjadi pada dini hari, penyebaran konten pornografi anak bisa dilakukan ketika petugas pengawas sedang tidak aktif, atau aksi penipuan online bisa menyasar korban dari berbagai negara secara serentak.

Implikasi Hukum

Karakteristik unik dari dunia digital—mulai dari skala global, anonimitas pengguna, kecepatan serta volume data yang tinggi, hingga sifat operasional yang berlangsung tanpa henti—menimbulkan tantangan besar bagi sistem hukum modern.

Hukum yang awalnya dirancang untuk mengatur interaksi dalam ruang fisik kini harus menghadapi kompleksitas ruang maya yang terus berkembang secara dinamis. Oleh karena itu, sistem hukum perlu menyesuaikan diri dan mengadopsi pendekatan baru untuk menjawab tantangan yang muncul di era digital ini. Beberapa implikasi hukum yang signifikan dapat diidentifikasi sebagai berikut:

1. Kebutuhan Akan Harmonisasi dan Kerja Sama Internasional

Dunia digital bersifat lintas batas dan transnasional. Aktivitas di satu negara bisa berdampak langsung pada negara lain, terutama dalam kasus seperti peretasan, penipuan daring lintas negara, pelanggaran hak kekayaan intelektual, hingga penyebaran konten ilegal yang bersifat global. Dalam konteks ini, yurisdiksi hukum menjadi kabur dan rumit. Apakah hukum negara asal pelaku berlaku? Ataukah hukum negara tempat korban berada yang harus diterapkan?

Masalah ini hanya bisa diselesaikan melalui kerja sama internasional yang erat dan sistematis, baik secara bilateral, regional, maupun multilateral. Negara-negara perlu membentuk perjanjian internasional yang mencakup aspek-aspek hukum siber, seperti Konvensi Budapest tentang Kejahatan Siber, serta memperkuat peran organisasi internasional seperti:

- INTERPOL, dalam penyelidikan dan pelacakan pelaku kejahatan lintas negara,
- ITU (International Telecommunication Union) dalam penyusunan standar teknis dan regulasi komunikasi digital,
- ASEAN, Uni Eropa, atau organisasi regional lainnya untuk membentuk kerangka hukum regional yang harmonis.

Tanpa adanya harmonisasi hukum, pelaku kejahatan siber dapat memanfaatkan celah hukum antar negara untuk

menghindari tanggung jawab hukum, menciptakan safe haven digital yang sulit dijangkau hukum nasional.

2. Pengembangan Regulasi Khusus yang Responsif

Hukum konvensional, yang dirancang untuk mengatur interaksi di dunia fisik, tidak lagi memadai dalam menangani persoalan kompleks di ruang digital. Dunia digital menimbulkan fenomena-fenomena baru seperti:

- Transaksi elektronik (e-commerce),
- Mata uang kripto dan teknologi blockchain,
- Perlindungan data pribadi dan metadata,
- Platform media sosial dan moderasi konten,
- Kecerdasan buatan dan algoritma pengambilan keputusan otomatis.

Hal ini menuntut pengembangan kerangka hukum baru yang secara khusus dirancang untuk dunia digital, atau biasa dikenal sebagai cyber law atau hukum teknologi informasi. Beberapa prinsip penting dalam regulasi ini antara lain:

- Perlindungan data pribadi dan keamanan informasi digital,
- Keabsahan dokumen dan transaksi elektronik,
- Kewajiban platform digital dalam menghapus konten ilegal,
- Perlindungan konsumen digital,
- Penanggulangan kejahatan siber (cybercrime) seperti hacking, phishing, dan distribusi malware.

Regulasi yang responsif juga harus bersifat fleksibel dan adaptif, karena teknologi berkembang sangat cepat. Regulasi yang kaku dan lamban akan segera usang dan tidak relevan lagi dengan situasi yang berkembang.

3. Penguatan Kapasitas dan Kompetensi Penegak Hukum

Salah satu tantangan terbesar dalam penegakan hukum digital adalah keterbatasan kapasitas sumber daya manusia dan

infrastruktur hukum. Kejahatan di ruang siber membutuhkan metode penanganan yang berbeda dari kejahatan konvensional. Oleh karena itu, aparat penegak hukum perlu dilengkapi dengan keahlian dan peralatan yang sesuai.

Beberapa langkah penting yang harus dilakukan antara lain:

- Pelatihan intensif dalam forensik digital, agar aparat mampu melacak jejak digital, menganalisis sistem komputer, dan mengamankan bukti elektronik.
- Penguasaan atas teknologi keamanan siber, seperti enkripsi, blockchain, cloud security, dan sistem keamanan jaringan.
- Kolaborasi dengan pakar teknologi dan akademisi, guna memperkaya pendekatan investigatif dan penyusunan kebijakan hukum.
- Peningkatan anggaran dan dukungan teknologi, agar lembaga penegak hukum memiliki akses terhadap perangkat lunak, laboratorium digital, dan sistem pemantauan otomatis.

Penegak hukum juga perlu memahami dimensi etika dan HAM dalam penegakan hukum digital, agar perlindungan hukum tidak justru merugikan hak privasi dan kebebasan berekspresi masyarakat.

4. Peningkatan Kesadaran dan Literasi Digital Masyarakat

Hukum tidak akan efektif jika masyarakat tidak mengetahui dan memahami hak serta kewajibannya di ruang digital. Oleh karena itu, pendidikan hukum dan literasi digital menjadi aspek krusial dalam mendukung penegakan hukum yang efektif. Masyarakat perlu dibekali dengan:

- Pemahaman tentang etika penggunaan teknologi, termasuk sopan santun digital, keamanan siber, dan tanggung jawab bermedia sosial.
- Kesadaran akan hak privasi dan perlindungan data pribadi, sehingga mereka tahu bagaimana cara menjaga data dan menghindari penyalahgunaannya.
- Pengetahuan mengenai mekanisme hukum yang tersedia, seperti cara melaporkan konten ilegal, mengadukan penipuan daring, atau menyelesaikan sengketa konsumen digital.
- Keterampilan untuk mendeteksi informasi palsu (hoaks), serta cara mengecek validitas sumber informasi di internet.

Program literasi hukum digital dapat dilakukan melalui berbagai saluran, mulai dari pendidikan formal, kampanye publik, pelatihan komunitas, hingga penyuluhan di media sosial. Pemerintah juga perlu bekerja sama dengan sektor swasta dan organisasi masyarakat sipil untuk menjangkau kelompok rentan seperti anak-anak, lansia, dan masyarakat pedesaan.

Aspek Kontrak dan Transaksi Elektronik

Transformasi digital telah mengubah hampir seluruh aspek kehidupan manusia, termasuk cara berinteraksi secara hukum dan ekonomi. Salah satu dampak yang paling nyata dari revolusi teknologi informasi adalah munculnya kontrak dan transaksi elektronik. Konsep ini tidak hanya merevolusi praktik perdagangan, tetapi juga menantang paradigma hukum yang selama ini dibangun berdasarkan interaksi fisik, dokumen kertas, dan tanda tangan manual.

Dalam konteks hukum, kontrak dan transaksi elektronik memunculkan berbagai isu penting, mulai dari validitas hukum,

pembuktian, perlindungan konsumen, hingga penyelesaian sengketa. Dengan adanya perangkat hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, keberadaan kontrak elektronik kini telah memperoleh pengakuan formal, meskipun pelaksanaannya di lapangan masih menghadapi berbagai tantangan.

Kontrak dan transaksi elektronik merupakan fenomena hukum yang semakin dominan dalam era digital saat ini. Kontrak elektronik dapat diartikan sebagai suatu perjanjian yang dibuat dan disepakati oleh dua pihak atau lebih melalui sistem elektronik. Meskipun tidak terjadi tatap muka atau penandatanganan dokumen fisik, kontrak ini tetap memiliki kekuatan hukum asalkan memenuhi syarat-syarat sahnya perjanjian menurut hukum perdata.

Pasal 1 angka 17 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) secara tegas mendefinisikan kontrak elektronik sebagai perjanjian yang dilakukan para pihak melalui sistem elektronik. Dalam praktiknya, kontrak ini dapat berupa tindakan klik tombol "setuju" pada sebuah situs web, konfirmasi melalui surat elektronik (email), atau kontrak otomatis berbasis teknologi blockchain yang dikenal dengan smart contract.

Sementara itu, transaksi elektronik mengacu pada setiap kegiatan hukum yang dilakukan dengan bantuan sistem elektronik, seperti jual beli barang, penyediaan jasa, transfer dana, atau layanan administrasi berbasis digital. Pasal 1 angka 2 UU ITE menyatakan bahwa transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Baik kontrak maupun transaksi elektronik memerlukan pengaturan hukum yang jelas karena pelaksanaannya menimbulkan tantangan baru terkait pembuktian, validitas, hingga perlindungan hukum bagi pihak-pihak yang terlibat.

Untuk diakui secara sah, kontrak elektronik harus memenuhi empat syarat sebagaimana diatur dalam Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata), yaitu adanya kesepakatan para pihak, kecakapan hukum, objek yang jelas, dan sebab yang halal. Kesepakatan dalam konteks digital bisa diwakili oleh tindakan klik tombol "I Agree", pengiriman pesan konfirmasi, otorisasi melalui kode OTP, maupun tanda tangan elektronik. Meskipun demikian, tantangan utamanya adalah pembuktian bahwa persetujuan tersebut benar-benar diberikan secara sadar dan sukarela.

Unsur kecakapan hukum mengharuskan bahwa pihak-pihak dalam kontrak adalah mereka yang secara hukum dianggap cakap. Namun, dalam transaksi elektronik, sulit untuk memastikan usia atau status hukum pihak karena keterbatasan dalam verifikasi identitas. Oleh karena itu, validasi data pribadi menjadi aspek yang sangat penting. Selain itu, objek kontrak harus jelas dan dapat ditentukan, baik berupa barang fisik maupun digital, seperti perangkat lunak, lisensi, atau data. Terakhir, sebab dari kontrak tidak boleh bertentangan dengan hukum atau norma yang berlaku. Kontrak untuk kegiatan ilegal tetap dianggap tidak sah, meskipun dibuat secara daring.

Dalam praktiknya, terdapat berbagai model kontrak elektronik yang umum digunakan. Pertama, click-wrap agreement, yaitu model di mana pengguna secara eksplisit harus menyatakan persetujuan dengan mengklik tombol tertentu sebelum dapat melanjutkan. Kedua, browse-wrap agreement, di mana pengguna dianggap setuju hanya dengan mengakses situs, meskipun tanpa klik persetujuan eksplisit—model ini cenderung lebih lemah dari sisi legalitas. Ketiga, shrink-wrap agreement, yang umum digunakan dalam distribusi perangkat lunak dan mulai berlaku begitu kemasan dibuka atau perangkat lunak diinstal. Keempat, smart contracts, yaitu kontrak yang dijalankan

secara otomatis dalam jaringan blockchain ketika syarat yang telah ditentukan terpenuhi. Meskipun teknologi ini belum secara eksplisit diatur dalam hukum nasional, konsepnya semakin relevan untuk masa depan transaksi digital yang otomatis dan terpercaya.

Dari sisi pembuktian, UU ITE memberikan legitimasi terhadap informasi dan dokumen elektronik sebagai alat bukti hukum yang sah dan setara dengan dokumen tertulis lainnya. Agar dokumen elektronik dapat diterima dalam proses hukum, ia harus otentik, tidak dimanipulasi, dapat ditelusuri asal-usulnya, tersimpan dengan aman, dan dihasilkan dari sistem elektronik yang andal.

Salah satu aspek penting lainnya adalah tanda tangan elektronik, yang berfungsi sebagai pengesahan dan pengakuan suatu dokumen. UU ITE membedakan antara tanda tangan elektronik biasa dan tanda tangan elektronik tersertifikasi. Yang terakhir memiliki tingkat validasi dan keamanan lebih tinggi karena menggunakan layanan pihak ketiga yang tersertifikasi.

Dalam konteks transaksi elektronik, konsumen seringkali berada dalam posisi yang lebih rentan dibanding penyedia layanan. Oleh karena itu, perlindungan konsumen menjadi aspek penting yang harus diakomodasi hukum. Prinsip-prinsip seperti transparansi informasi, keamanan transaksi, hak untuk membatalkan, dan kompensasi atas kegagalan layanan menjadi landasan dalam upaya melindungi hak konsumen. UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, bersama dengan UU ITE, menjadi kerangka hukum yang menjamin perlindungan konsumen digital di Indonesia.

Adapun sengketa dalam transaksi elektronik dapat timbul dari berbagai hal, seperti penipuan, barang tidak sesuai dengan deskripsi, pelanggaran data, hingga ketidaksesuaian identitas pelaku. Penyelesaian sengketa ini dapat dilakukan melalui

beberapa jalur, antara lain melalui litigasi di pengadilan dengan penggunaan bukti elektronik, alternatif penyelesaian sengketa seperti mediasi atau arbitrase online, serta mekanisme internal dari platform digital seperti layanan pelanggan dan sistem pengaduan. Selain itu, penerapan sistem peradilan elektronik (e-Court) oleh Mahkamah Agung merupakan langkah positif dalam mendigitalisasi proses hukum dan mempermudah akses masyarakat terhadap keadilan.

Dengan demikian, aspek kontrak dan transaksi elektronik merupakan isu sentral dalam perkembangan hukum di era digital. Perlu adanya sinergi antara regulasi, teknologi, dan kesadaran publik agar sistem hukum mampu merespons dinamika yang terus berkembang dengan tetap menjamin kepastian dan perlindungan hukum bagi seluruh pihak.

BAB 5

Cybercrime

Cybercrime atau kejahatan siber merupakan bentuk kejahatan yang menggunakan komputer, jaringan internet, atau perangkat digital lainnya sebagai alat, target, atau tempat terjadinya tindak pidana. Perkembangan teknologi informasi yang pesat telah menciptakan ruang digital baru bagi manusia dalam berkomunikasi, bekerja, dan bertransaksi, tetapi juga membuka peluang bagi pelaku kejahatan untuk mengeksploitasi kerentanan sistem dan pengguna.

Kejahatan siber tidak hanya mencakup pencurian data atau peretasan sistem komputer, tetapi juga meliputi tindakan seperti penipuan daring, penyebaran virus, perdagangan ilegal di dark web, pencemaran nama baik melalui media sosial, hingga eksploitasi seksual berbasis teknologi.

Karakteristik utama cybercrime adalah sifatnya yang lintas batas (borderless), anonim, cepat, dan bersifat disruptif. Dalam banyak kasus, pelaku dan korban tidak berada di wilayah yurisdiksi yang sama, sehingga menimbulkan tantangan besar dalam hal penegakan hukum dan pembuktian.

Anonimitas pengguna internet juga membuat identifikasi pelaku menjadi sulit, terlebih jika mereka menggunakan teknologi enkripsi, virtual private network (VPN), atau metode spoofing untuk menyembunyikan identitas dan lokasi. Selain itu, cybercrime dapat terjadi dalam hitungan detik, dengan dampak yang luas dan merugikan secara ekonomi, sosial, maupun psikologis.

Secara umum, cybercrime dapat diklasifikasikan ke dalam tiga kategori besar: (1) kejahatan terhadap komputer (misalnya: hacking, penyebaran malware, dan DDoS attack), (2) kejahatan dengan menggunakan komputer sebagai sarana (misalnya: penipuan online, pemalsuan identitas, dan transaksi ilegal), dan (3) kejahatan di dunia maya terhadap individu atau masyarakat (misalnya: pencemaran nama baik, penyebaran konten pornografi, dan ujaran kebencian). Penggolongan ini menunjukkan bahwa cybercrime dapat berdimensi teknis maupun sosial.

Di Indonesia, cybercrime diatur dalam berbagai instrumen hukum, terutama dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah beberapa kali mengalami revisi untuk menyesuaikan dengan dinamika teknologi.

Beberapa pasal penting dalam UU ITE mengatur larangan terhadap akses ilegal ke sistem elektronik (Pasal 30), gangguan terhadap integritas data (Pasal 32), serta penyebaran informasi yang bersifat penghinaan, pencemaran nama baik, atau berita bohong (Pasal 27 dan 28). Selain itu, KUHP dan beberapa peraturan pelaksana juga digunakan untuk menjerat pelaku kejahatan siber, tergantung pada tindak pidana yang dilakukan.

Penanggulangan kejahatan siber tidak hanya bergantung pada perangkat hukum, tetapi juga pada kesiapan aparat penegak hukum, kesadaran masyarakat, serta kerja sama lintas negara. Aparat penegak hukum dituntut memiliki kapasitas dalam melakukan digital forensics, pelacakan IP address, hingga pengumpulan bukti digital yang sah secara hukum. Di sisi lain, masyarakat perlu diedukasi mengenai ancaman cybercrime dan cara melindungi diri, seperti tidak mudah membagikan data pribadi, menggunakan sistem keamanan ganda (two-factor authentication), dan menghindari klik tautan yang mencurigakan.

Secara internasional, kerja sama antarnegara sangat diperlukan dalam menghadapi cybercrime, terutama melalui mekanisme mutual legal assistance (MLA), perjanjian ekstradisi, dan partisipasi dalam konvensi internasional seperti Budapest Convention on Cybercrime. Konvensi ini menjadi instrumen hukum internasional pertama yang mengatur penanggulangan kejahatan siber secara komprehensif, dengan mendorong harmonisasi hukum pidana, peningkatan kapasitas penegakan hukum, dan kerja sama lintas negara.

Dalam konteks masa depan, tantangan kejahatan siber diprediksi akan semakin kompleks dengan berkembangnya teknologi baru seperti kecerdasan buatan (AI), Internet of Things (IoT), blockchain, dan metaverse. Serangan siber dapat bersifat lebih terstruktur, masif, dan bahkan digunakan untuk tujuan geopolitik, seperti cyber warfare atau spionase digital antarnegara. Oleh karena itu, hukum harus terus berinovasi, baik dari sisi substansi, prosedur, maupun kelembagaan, agar mampu menjawab tantangan tersebut dan memberikan perlindungan yang memadai bagi warga negara.

Jenis – Jenis Kejahatan Siber

Kejahatan siber, atau yang lebih dikenal dengan istilah cybercrime, merupakan salah satu tantangan besar dalam era digital yang terus mengalami transformasi pesat. Seiring dengan meningkatnya ketergantungan masyarakat pada teknologi informasi dan komunikasi—baik dalam bidang ekonomi, pendidikan, sosial, pemerintahan, maupun kehidupan sehari-hari—risiko terjadinya pelanggaran hukum di ruang siber pun turut meningkat secara signifikan.

Fenomena ini tidak hanya berdampak pada individu, tetapi juga pada institusi publik dan swasta, bahkan dapat mengancam keamanan nasional. Kejahatan siber bersifat lintas

batas (borderless), dilakukan secara tersembunyi (invisible), serta dapat berlangsung dalam waktu yang sangat singkat namun menimbulkan kerugian besar dalam bentuk materi, psikologis, bahkan reputasi.

Dengan sifat dunia maya yang sangat terbuka dan dinamis, pelaku kejahatan dapat memanfaatkan berbagai celah keamanan digital untuk melakukan tindak kriminal tanpa harus hadir secara fisik. Hal ini membuat pelacakan dan penegakan hukum menjadi semakin kompleks, terutama karena yurisdiksi hukum antarnegara yang belum sepenuhnya harmonis dalam menghadapi kejahatan lintas wilayah ini.

Oleh karena itu, upaya klasifikasi jenis-jenis kejahatan siber menjadi sangat krusial, baik dari sisi akademik, hukum, maupun praktis. Klasifikasi ini membantu dalam mengidentifikasi pola-pola kejahatan digital, memahami modus operandi yang digunakan oleh para pelaku, serta menyusun strategi pencegahan dan penindakan yang efektif.

Secara umum, kejahatan siber dapat dikelompokkan berdasarkan berbagai aspek, seperti sasaran serangan (individu, institusi, negara), cara atau teknik yang digunakan (hacking, malware, phishing), dan dampak yang ditimbulkan (finansial, reputasi, keamanan nasional). Selain itu, kejahatan siber juga dapat dibagi menjadi kejahatan yang murni menggunakan teknologi sebagai alat utama kejahatan, dan kejahatan yang menggunakan teknologi sebagai sarana pendukung. Dalam banyak kasus, batas antar jenis kejahatan siber bisa sangat kabur dan saling tumpang tindih, mengingat pelaku sering kali menggabungkan berbagai teknik untuk mencapai tujuannya.

Lebih jauh lagi, penting bagi para penegak hukum, akademisi, praktisi teknologi, dan masyarakat umum untuk memahami klasifikasi ini sebagai landasan dalam membangun sistem keamanan informasi yang tangguh. Pemahaman yang

komprehensif terhadap jenis-jenis kejahatan siber akan mempermudah dalam menyusun regulasi, mengembangkan teknologi deteksi dan pencegahan, serta membentuk budaya digital yang aman dan bertanggung jawab.

Dalam konteks pendidikan hukum dan teknologi informasi, pengkajian mendalam terhadap berbagai tipe cybercrime ini juga menjadi pijakan awal untuk menghasilkan kebijakan yang adaptif dan sistem perlindungan hukum yang memadai di tengah derasnya arus digitalisasi global.

Kejahatan siber dapat diklasifikasikan ke dalam beberapa kategori berdasarkan sasaran, modus operandi, dan tujuan dari pelaku kejahatan. Klasifikasi ini bertujuan untuk mempermudah identifikasi bentuk pelanggaran serta pengembangan strategi pencegahan dan penanganan. Berikut adalah jenis-jenis kejahatan siber yang umum dijumpai:

1. Unauthorized Access (Akses Tanpa Izin)

Jenis kejahatan Unauthorized Access (Akses Tanpa Izin) merupakan salah satu bentuk kejahatan siber yang paling mendasar dan umum terjadi. Kejahatan ini terjadi ketika seseorang dengan sengaja dan tanpa otorisasi mengakses sistem komputer, jaringan, atau perangkat digital milik orang lain. Tindakan ini melanggar hak privasi dan keamanan informasi, serta dapat menimbulkan kerugian besar, baik secara finansial maupun reputasional.

Pelaku akses tanpa izin sering kali memiliki tujuan tertentu, seperti mencuri data pribadi, mengakses informasi rahasia perusahaan, merusak sistem, atau sekadar menunjukkan kemampuan teknisnya dalam mengeksplorasi celah keamanan sistem. Aktivitas ini dapat dilakukan melalui berbagai metode, seperti membobol kata sandi, mengeksploitasi kelemahan perangkat lunak, atau menyusup melalui jaringan nirkabel yang tidak terlindungi.

Contoh nyata dari unauthorized access meliputi peretasan akun media sosial, penyusupan ke dalam server internal perusahaan tanpa izin, hingga pembobolan jaringan Wi-Fi pribadi yang diamankan dengan kata sandi. Meskipun dalam beberapa kasus pelaku mungkin tidak berniat merusak sistem, tindakan ini tetap dikategorikan sebagai kejahatan karena dilakukan tanpa persetujuan pemilik sistem dan berpotensi membahayakan integritas data dan privasi pengguna.

2. Data Theft and Information Espionage (Pencurian Data dan Spionase Digital)

Pencurian Data dan Spionase Digital adalah bentuk kejahatan siber yang bertujuan untuk memperoleh informasi penting atau sensitif secara ilegal. Kejahatan ini menyasar data milik individu, organisasi bisnis, hingga lembaga pemerintahan, dengan maksud untuk menyalahgunakannya demi keuntungan ekonomi, politik, atau strategis.

Informasi yang dicuri bisa berupa database pelanggan, rincian kartu kredit, rahasia dagang, strategi bisnis, hingga komunikasi rahasia antar pejabat negara. Dalam dunia korporasi, pencurian data sering kali dilakukan oleh pesaing bisnis yang ingin mendapatkan keunggulan kompetitif secara tidak sah. Sementara dalam ranah geopolitik, spionase digital digunakan oleh aktor negara atau kelompok tertentu untuk mendapatkan informasi intelijen yang bersifat rahasia.

Metode yang digunakan dalam kejahatan ini cukup beragam, mulai dari pengiriman malware untuk menyusup ke sistem target, hingga teknik social engineering seperti phishing untuk mengelabui korban agar memberikan akses ke data sensitif. Contoh nyata dari kejahatan ini mencakup pembobolan sistem keamanan perusahaan untuk mencuri data pelanggan, penyadapan komunikasi digital antar pejabat pemerintah, atau pengambilalihan informasi strategis dari server internal sebuah

lembaga riset. Dampaknya tidak hanya merugikan korban secara finansial, tetapi juga dapat mengancam reputasi, keamanan nasional, serta stabilitas politik dan ekonomi suatu negara.

3. Malware Attacks (Serangan Perangkat Lunak Berbahaya)

Malware Attacks merupakan salah satu bentuk kejahatan siber yang paling merusak dan beragam. Malware, singkatan dari malicious software, adalah program atau kode berbahaya yang dirancang secara khusus untuk menyusup, merusak, mencuri data, atau mengambil alih kendali atas sistem komputer dan jaringan tanpa sepengetahuan atau izin pengguna.

Serangan ini dapat menyasar individu, perusahaan, maupun instansi pemerintahan, dan sering kali dilakukan untuk tujuan sabotase, pemerasan, pencurian data, atau pengintaian. Jenis-jenis malware yang umum meliputi virus yang menyebar dengan menyisipkan diri ke file atau program lain, worm yang dapat menggandakan dirinya dan menyebar melalui jaringan, trojan yang menyamar sebagai aplikasi sah namun mengandung muatan berbahaya, ransomware yang mengenkripsi data korban dan meminta tebusan untuk memulihkan akses, serta spyware yang memantau aktivitas pengguna dan mencuri informasi pribadi secara diam-diam.

Contoh konkret dari serangan ini termasuk ransomware yang mengunci seluruh sistem komputer rumah sakit hingga tidak dapat digunakan, atau spyware yang diam-diam merekam data login dan aktivitas pengguna untuk kemudian dikirimkan ke pelaku. Akibat dari serangan malware bisa sangat serius, mulai dari kehilangan data penting, gangguan operasional, kebocoran informasi rahasia, hingga kerugian finansial yang besar. Oleh karena itu, perlindungan terhadap malware menjadi aspek krusial dalam keamanan siber.

4. Phishing dan Social Engineering

Phishing dan Social Engineering merupakan dua metode kejahatan siber yang mengandalkan manipulasi psikologis dan penipuan untuk memperoleh informasi pribadi atau memicu tindakan tertentu dari korban. Phishing adalah bentuk penipuan digital di mana pelaku menyamar sebagai entitas tepercaya—seperti bank, institusi pemerintah, atau perusahaan teknologi—dan mengirimkan email, pesan teks, atau tautan palsu yang dirancang untuk mengelabui korban agar memberikan informasi sensitif.

Informasi yang biasanya ditargetkan meliputi nama pengguna (username), kata sandi, nomor kartu kredit, atau data identitas lainnya. Serangan phishing seringkali tampak meyakinkan, menggunakan logo dan bahasa yang menyerupai institusi resmi, sehingga banyak korban tidak menyadari bahwa mereka sedang ditipu.

Sementara itu, social engineering adalah pendekatan yang lebih luas dan bersifat interpersonal, di mana pelaku menggunakan manipulasi emosional dan kepercayaan untuk mengecoh korban. Contohnya termasuk pelaku yang berpura-pura menjadi teman atau anggota keluarga dalam keadaan darurat dan meminta uang, atau mengaku sebagai teknisi IT perusahaan dan meminta akses ke sistem. Berbeda dengan serangan teknis seperti malware, social engineering memanfaatkan kelemahan manusia sebagai celah utama.

Contoh konkret dari kedua metode ini antara lain adalah email palsu yang tampak berasal dari bank dan meminta pengguna untuk mengklik tautan dan memasukkan informasi login, atau pesan WhatsApp dari "teman" yang mengaku kehilangan dompet dan membutuhkan transfer uang segera. Kedua jenis kejahatan ini berbahaya karena dapat terjadi dengan cepat dan sulit dilacak, serta dapat menyebabkan kerugian yang

signifikan jika data sensitif jatuh ke tangan yang salah. Oleh karena itu, penting bagi pengguna untuk selalu waspada, memverifikasi sumber informasi, dan tidak sembarangan memberikan data pribadi di internet.

5. Cyber Fraud and Online Scams (Penipuan dan Skema Daring)

Cyber Fraud and Online Scams (Penipuan dan Skema Daring) adalah bentuk kejahatan siber yang bertujuan untuk memperoleh keuntungan secara tidak sah dengan memanfaatkan kelemahan pengguna melalui tipu daya di dunia maya. Penipuan jenis ini sangat beragam dan sering kali memanfaatkan kredibilitas, harapan, atau kebutuhan ekonomi korban untuk menciptakan skema yang tampak sah, padahal palsu. Dalam banyak kasus, pelaku menawarkan produk, jasa, investasi, atau hadiah yang menjanjikan keuntungan besar dalam waktu singkat, namun pada akhirnya korban mengalami kerugian finansial, kehilangan data, atau bahkan menjadi korban pemerasan.

Beberapa contoh umum dari kejahatan ini antara lain adalah toko online palsu yang menawarkan barang dengan harga sangat murah namun tidak pernah mengirimkan produk setelah pembayaran dilakukan; undian atau hadiah yang meminta korban membayar "biaya administrasi" untuk mengklaim hadiah fiktif; skema investasi berbasis kripto yang menjanjikan imbal hasil tinggi tetapi ternyata adalah penipuan (scam); hingga arisan online yang ternyata merupakan skema ponzi di mana uang dari peserta baru digunakan untuk membayar peserta lama, sampai akhirnya sistem runtuh.

Penipuan daring ini sangat merugikan karena selain menyebabkan kerugian finansial, juga dapat menurunkan kepercayaan publik terhadap ekosistem digital. Oleh karena itu, edukasi dan kewaspadaan masyarakat sangat penting agar tidak mudah tergiur oleh tawaran yang terlalu bagus untuk menjadi

kenyataan, serta selalu melakukan verifikasi atas setiap transaksi dan entitas digital yang ditemui.

6. Cyberbullying dan Online Harassment

Cyberbullying dan Online Harassment adalah bentuk kejahatan siber yang melibatkan tindakan intimidasi, pelecehan, penghinaan, atau ancaman yang dilakukan terhadap seseorang melalui media digital, seperti media sosial, aplikasi pesan instan, forum daring, dan platform komunikasi lainnya. Kejahatan ini tidak hanya menyasar anak-anak dan remaja, tetapi juga orang dewasa, termasuk tokoh publik dan profesional.

Bentuk-bentuknya sangat beragam, mulai dari komentar kebencian yang berulang, pengiriman pesan ancaman, penyebaran foto atau video tanpa izin, hingga doxing, yaitu tindakan membocorkan data pribadi korban ke publik tanpa persetujuan dengan tujuan mempermalukan atau mengintimidasi.

Cyberbullying berdampak serius pada kesehatan mental dan emosional korban. Banyak kasus menunjukkan bahwa korban mengalami stres berat, kecemasan, depresi, bahkan sampai pada tindakan menyakiti diri sendiri atau bunuh diri. Berbeda dengan bullying konvensional yang terbatas ruang dan waktu, cyberbullying bisa terjadi kapan saja dan di mana saja, selama korban terhubung ke internet. Karakteristik digital juga membuat penyebaran konten negatif berlangsung cepat dan sulit dihentikan.

Untuk mengatasi kejahatan ini, dibutuhkan pendekatan hukum yang tegas serta dukungan dari platform digital dalam memfasilitasi pelaporan dan penindakan terhadap pelaku. Selain itu, peningkatan kesadaran masyarakat tentang etika berkomunikasi di dunia maya, pentingnya empati digital, serta literasi digital menjadi kunci utama dalam mencegah dan menangani kasus cyberbullying dan pelecehan daring.

7. Defacing dan Sabotase Situs Web

Defacing dan Sabotase Situs Web merupakan bentuk kejahatan siber yang menargetkan tampilan dan fungsi suatu situs web atau sistem digital. Defacing adalah tindakan merusak atau mengganti konten halaman situs web tanpa izin, biasanya dengan tujuan menyampaikan pesan tertentu, mempermalukan pemilik situs, atau menunjukkan kemampuan teknis pelaku.

Aksi ini sering dikaitkan dengan hacktivism, yaitu peretasan yang bermotif ideologis atau politik, di mana pelaku ingin menyampaikan protes terhadap kebijakan, institusi, atau negara. Sementara itu, sabotase situs web bisa mencakup tindakan yang lebih luas, seperti penghapusan data, pengubahan konfigurasi sistem, atau pengenalan bug yang merusak operasional situs.

Contoh dari kejahatan ini adalah ketika tampilan situs web lembaga pemerintah atau perusahaan besar diganti oleh peretas dengan gambar, pesan propaganda, atau sindiran. Tidak hanya mengganggu reputasi institusi, tindakan ini juga dapat menyebabkan gangguan layanan, kehilangan kepercayaan publik, dan kerugian ekonomi.

Dalam konteks keamanan siber, defacing dan sabotase menunjukkan pentingnya penerapan sistem pertahanan yang kuat, seperti firewall, enkripsi, dan pemantauan sistem secara berkala, guna mencegah dan mendeteksi akses tidak sah yang dapat mengarah pada kerusakan sistem atau pencurian informasi penting.

8. Identity Theft (Pencurian Identitas)

Identity Theft (Pencurian Identitas) adalah jenis kejahatan siber di mana pelaku menggunakan informasi pribadi milik orang lain secara ilegal untuk melakukan tindakan penipuan atau kejahatan lainnya atas nama korban. Informasi yang dicuri bisa berupa nomor KTP, nomor kartu kredit, data akun media sosial,

alamat email, hingga informasi sensitif lain yang memungkinkan pelaku untuk mengakses berbagai layanan dan fasilitas digital atau finansial. Kejahatan ini sangat berbahaya karena dapat merusak reputasi dan keuangan korban secara serius, serta menimbulkan kesulitan hukum bagi mereka.

Contoh konkret dari pencurian identitas adalah ketika pelaku menggunakan data pribadi korban untuk membuka rekening bank baru, mengambil pinjaman online, atau melakukan transaksi keuangan tanpa sepengetahuan korban. Selain itu, pelaku juga dapat memanfaatkan identitas tersebut untuk mengajukan dokumen resmi, melakukan pembelian, atau bahkan melakukan aktivitas kriminal lainnya yang mengatasnamakan korban.

Oleh karena itu, perlindungan data pribadi dan kewaspadaan dalam membagikan informasi secara daring sangat penting untuk mencegah terjadinya pencurian identitas. Sistem keamanan digital dan regulasi perlindungan data juga harus terus ditingkatkan agar mampu mengantisipasi dan menindak pelaku kejahatan ini secara efektif.

9. Cyber Terrorism

Cyber Terrorism adalah tindakan teror yang memanfaatkan teknologi informasi dan komunikasi untuk mencapai tujuan yang bersifat mengintimidasi, menimbulkan ketakutan, atau merusak keamanan nasional dan masyarakat. Pelaku cyber terrorism menggunakan serangan digital untuk menyabotase infrastruktur penting seperti jaringan listrik, sistem kontrol bandara, fasilitas rumah sakit, dan sarana transportasi, sehingga dapat menimbulkan gangguan besar dan kekacauan.

Selain itu, cyber terrorism juga mencakup penyebaran propaganda ekstremis dan radikalisme secara masif di internet untuk merekrut anggota baru, memprovokasi kekerasan, atau menyebarkan ideologi teroris.

Contoh nyata dari cyber terrorism adalah serangan yang menargetkan sistem kontrol bandara yang dapat mengganggu jadwal penerbangan, serangan terhadap rumah sakit yang menyebabkan sistem kesehatan lumpuh, atau penyebaran konten radikal yang menimbulkan keresahan dan perpecahan sosial.

Dampak dari cyber terrorism sangat serius karena selain kerusakan fisik dan ekonomi, juga menimbulkan ketidakstabilan sosial dan rasa takut yang meluas di masyarakat. Oleh karena itu, upaya pencegahan dan penanggulangan cyber terrorism memerlukan koordinasi antar lembaga keamanan, pemerintah, dan sektor swasta, serta penguatan regulasi dan teknologi keamanan siber yang canggih.

10. Child Exploitation Online

Child Exploitation Online merupakan salah satu bentuk kejahatan siber yang paling mengkhawatirkan karena melibatkan korban yang sangat rentan, yaitu anak-anak. Kejahatan ini mencakup berbagai tindakan eksploitasi seksual terhadap anak melalui media digital, seperti penyebaran dan perdagangan materi pornografi anak, pemerasan seksual daring (sextortion), serta grooming, yaitu proses manipulatif di mana pelaku secara bertahap membangun hubungan kepercayaan dengan anak dengan tujuan akhirnya adalah pelecehan atau eksploitasi seksual.

Para pelaku kerap menggunakan media sosial, platform gim, atau aplikasi pesan untuk mendekati anak-anak, sering kali dengan menyamar sebagai teman sebaya agar lebih mudah mendapatkan kepercayaan korban.

Salah satu contoh kasus adalah ketika pelaku berpura-pura menjadi anak remaja di media sosial, membangun percakapan intens, lalu membujuk atau memaksa anak untuk mengirimkan foto-foto tidak pantas. Setelah mendapatkan materi tersebut, pelaku dapat menggunakannya untuk memeras korban agar mengirimkan lebih banyak foto atau bahkan melakukan tindakan yang lebih ekstrem.

Kejahatan semacam ini tidak hanya merusak masa depan korban secara psikologis, tetapi juga dapat menyebabkan trauma jangka panjang. Oleh karena itu, penting bagi orang tua, pendidik, dan masyarakat untuk meningkatkan literasi digital dan pengawasan terhadap aktivitas daring anak-anak, serta bagi negara untuk memiliki kerangka hukum dan sistem pelaporan yang efektif dalam menangani eksploitasi anak di dunia maya.

BAB 6

Investigasi Digital Forensik

Perkembangan teknologi informasi dan komunikasi telah menciptakan transformasi besar dalam berbagai aspek kehidupan manusia, termasuk dalam bidang hukum. Seiring dengan meningkatnya ketergantungan terhadap perangkat digital dan sistem informasi, muncul pula berbagai bentuk kejahatan siber yang menuntut pendekatan penegakan hukum yang baru. Dalam konteks inilah Investigasi Digital Forensik (Digital Forensic Investigation) menjadi elemen kunci untuk memastikan bahwa hukum tetap dapat ditegakkan di dunia maya.

Digital forensik merupakan cabang ilmu forensik yang berfokus pada identifikasi, pelestarian, analisis, dan penyajian bukti digital yang sah secara hukum. Aktivitas ini sangat penting dalam pengungkapan kasus kejahatan siber seperti peretasan (hacking), pencurian identitas, penyebaran malware, pelanggaran hak cipta digital, hingga penipuan berbasis daring.

Secara akademik, digital forensik dapat didefinisikan sebagai proses ilmiah dan sistematis yang digunakan untuk memperoleh, menjaga, menganalisis, dan menyajikan data elektronik dari berbagai perangkat dan sistem digital guna digunakan sebagai bukti dalam proses hukum. Data elektronik yang dimaksud dapat berasal dari komputer, ponsel, perangkat IoT (Internet of Things), server, jaringan internet, hingga layanan cloud.

Investigasi ini melibatkan pemahaman mendalam tentang arsitektur sistem informasi, teknik pengumpulan bukti digital

tanpa mengubah data asli, serta kemampuan menafsirkan temuan teknis dalam kerangka hukum yang dapat diterima di pengadilan.

A. Prosedur Investigasi Digital Forensik

Investigasi digital forensik merupakan proses ilmiah dan metodologis yang digunakan untuk memperoleh, menganalisis, dan menyajikan bukti digital dalam konteks penegakan hukum. Proses ini penting dalam menghadapi kejahatan siber yang seringkali meninggalkan jejak digital yang tersembunyi, bersifat volatil, dan tersebar di berbagai perangkat atau sistem jaringan. Oleh karena itu, prosedur investigasi forensik digital harus dilakukan secara hati-hati, terstruktur, dan sesuai standar hukum agar hasilnya dapat diterima di pengadilan.

1. Identifikasi Awal dan Perencanaan Investigasi

Langkah pertama dalam proses investigasi adalah identifikasi insiden atau dugaan kejahatan digital. Investigasi biasanya dimulai atas dasar laporan pelanggaran, temuan sistem keamanan, atau perintah pengadilan. Dalam tahap ini, investigator menentukan ruang lingkup penyelidikan, termasuk jenis kejahatan, target sistem, serta potensi perangkat atau media penyimpan data yang relevan. Perencanaan awal ini juga mencakup pembentukan tim, distribusi tugas, serta pertimbangan hukum dan etika yang berkaitan dengan privasi data.

Salah satu contoh mengenai hal tersebut yaitu dalam kasus pencurian data pelanggan pada perusahaan e-commerce, tim forensik akan terlebih dahulu mengidentifikasi sistem yang dicurigai diretas, seperti server basis data atau sistem manajemen pengguna.

2. Akuisisi dan Pengamanan Bukti Digital

Tahap ini merupakan inti dari proses investigasi, yakni pengumpulan dan pengamanan bukti digital dari perangkat keras (komputer, laptop, USB, ponsel), perangkat lunak (sistem operasi, aplikasi), hingga lalu lintas jaringan. Pengamanan dilakukan dengan metode imaging forensik—yakni menyalin data secara bit-per-bit untuk mempertahankan integritas aslinya.

- Chain of custody (rantai kendali barang bukti) diterapkan untuk memastikan setiap bukti dicatat asal-usul, waktu, dan orang yang menangani.
- Pengumpulan bukti dilakukan menggunakan alat khusus seperti FTK Imager, EnCase, atau Guymager.

Sebuah contoh dalam kasus penyebaran konten ilegal, penyidik mengambil image dari hard disk pelaku dan menyimpannya di media penyimpanan aman dengan tanda tangan digital (hash value) sebagai verifikasi integritas.

3. Analisis Forensik Data Digital

Analisis forensik data digital merupakan tahap krusial dalam proses investigasi forensik digital yang bertujuan untuk mengungkap, menginterpretasi, dan mengekstrak informasi relevan dari bukti elektronik. Tahapan ini dilakukan setelah proses akuisisi atau pencitraan data, dan membutuhkan keahlian teknis serta ketelitian tinggi agar hasilnya valid secara hukum dan akurat secara teknis.

Dalam dunia digital yang kompleks, pelaku kejahatan siber kerap memanfaatkan teknik penyamaran, enkripsi, atau penghapusan data untuk mengaburkan jejak mereka. Oleh karena itu, proses analisis tidak hanya bersifat teknis, melainkan juga strategis, karena penyidik harus mampu memahami konteks dari data yang diperoleh, baik yang tampak maupun tersembunyi (hidden artifacts). Setelah bukti dikumpulkan, proses berlanjut ke tahap analisis, yang bertujuan untuk menemukan informasi yang

relevan secara hukum, teknis, atau investigatif. Analisis dapat dilakukan terhadap:

(1) File System

Analisis file system melibatkan pemeriksaan terhadap struktur penyimpanan file dalam sebuah perangkat digital, seperti komputer, hard disk, atau flash drive. Fokus utama terletak pada:

a) File tersembunyi: File yang sengaja disembunyikan oleh sistem atau pengguna, sering kali oleh pelaku kejahatan untuk mengaburkan bukti.
b) Log aktivitas: Catatan penggunaan sistem, termasuk program yang dijalankan, file yang diakses, dan kesalahan sistem.
c) Timestamp: Informasi waktu pada file, mencakup kapan file dibuat (created), diubah (modified), dan terakhir diakses (accessed).

Dalam kasus penyebaran konten ilegal, forensik menemukan folder tersembunyi berisi file gambar yang diberi timestamp palsu. Namun metadata sistem menunjukkan adanya aktivitas pengubahan tanggal file, yang memperkuat dugaan manipulasi bukti.

(2) Email, Chat, dan Metadata Komunikasi

Pesan digital seperti email dan chat sering digunakan dalam kejahatan siber, baik untuk menipu, memeras, atau berkoordinasi. Analisis mencakup:

a) Isi pesan: Untuk menelusuri niat, perintah, atau instruksi ilegal.
b) Lampiran: File yang dikirim, bisa berisi malware atau bukti transaksi.
c) Metadata: Informasi teknis seperti alamat IP pengirim, waktu pengiriman, dan ID perangkat.

Dalam penipuan online, email yang dikirim pelaku menyertakan dokumen palsu. Metadata menunjukkan IP pengirim berasal dari negara berbeda dengan yang diklaim pelaku, serta waktu pengiriman menunjukkan pola otomatisasi.

(3) Artefak Browser dan Cache

Browser menyimpan banyak data jejak aktivitas pengguna, yang disebut artefak digital, antara lain:

a) Riwayat pencarian dan situs dikunjungi
b) Cache: Salinan lokal dari halaman yang pernah dibuka
c) Cookie dan login session: Untuk pelacakan akun yang digunakan

Dalam investigasi pencurian data, ditemukan artefak browser yang menunjukkan pelaku mengakses situs pastebin.com dan mengunggah file data korban, meskipun browser sudah dibersihkan secara manual

(4) Log Sistem dan Jejak Penggunaan Jaringan

Sistem operasi dan perangkat jaringan menyimpan berbagai log aktivitas, termasuk:

a) Login/logout user
b) Koneksi jaringan masuk dan keluar
c) Alamat IP yang terhubung
d) Event log (Windows), syslog (Linux)

Dalam serangan ransomware, log sistem menunjukkan koneksi RDP (Remote Desktop Protocol) dari IP yang tidak dikenal pada pukul 2 pagi. Serangan kemudian terjadi beberapa menit setelah login tersebut.

(5) Volatile Memory (RAM)

RAM menyimpan data yang aktif digunakan sistem saat komputer menyala. Berbeda dengan penyimpanan permanen, data di RAM akan hilang setelah perangkat dimatikan. Oleh karena itu, analisis volatile memory dilakukan sesegera mungkin.

Yang dapat ditemukan di RAM antara lain:

a) Proses aktif
b) Password yang tersimpan sementara
c) Perintah terminal/command prompt
d) Kehadiran malware dalam bentuk proses runtime.

Dalam analisis serangan zero-day, investigator menggunakan Volatility Framework untuk mengekstrak dump RAM dan menemukan proses mencurigakan yang menyuntikkan skrip PowerShell ke browser pengguna. Bukti ini memperjelas teknik pelaku menghindari deteksi antivirus.

4. Dokumentasi dan Pelaporan

Dalam ranah digital forensik, proses dokumentasi dan pelaporan merupakan aspek krusial yang menentukan validitas serta akuntabilitas seluruh temuan investigatif. Tidak seperti investigasi tradisional, analisis data digital sangat rentan terhadap perubahan yang tidak disengaja maupun manipulasi, sehingga setiap tindakan yang diambil oleh analis forensik harus terekam secara sistematis, terstruktur, dan dapat diaudit.

Dokumentasi bukan hanya berfungsi sebagai catatan kerja, tetapi juga menjadi instrumen legal yang dapat digunakan dalam proses pembuktian hukum di pengadilan. Setiap langkah dalam proses forensik harus didokumentasikan secara sistematis. Laporan forensik mencakup:

a) Deskripsi temuan teknis dan metode akuisisi
b) Hasil analisis dan interpretasi teknis
c) Verifikasi integritas data (melalui hash value)
d) Bukti visual seperti tangkapan layar atau rekaman aktivitas
e) Pendapat ahli jika diperlukan

Laporan ini nantinya akan digunakan dalam proses peradilan, baik sebagai bukti maupun referensi untuk kesaksian ahli.

5. Penyajian Bukti dan Keterangan Ahli di Pengadilan

Bukti digital yang telah diverifikasi kemudian diajukan ke pengadilan bersama keterangan ahli digital forensik. Tujuannya adalah menjelaskan relevansi, integritas, serta metode forensik yang digunakan. Dalam banyak kasus, penyidik juga harus mampu menjelaskan kepada hakim atau jaksa tentang bagaimana bukti tersebut dapat dihubungkan langsung dengan pelaku.

Dalam kasus pencemaran nama baik melalui media sosial, forensik membuktikan bahwa akun yang digunakan pelaku login dari IP rumahnya pada waktu yang bersamaan dengan unggahan fitnah.

B. Alat dan Perangkat Lunak Digital Forensik

Dalam praktik digital forensik, keberhasilan proses investigasi sangat bergantung pada penggunaan alat dan perangkat lunak (tools) yang andal, terstandarisasi, dan mampu memberikan hasil akurat tanpa mengubah data asli.

Berbeda dengan investigasi konvensional, analisis digital melibatkan pemrosesan data dalam jumlah besar yang bersifat volatile, tersembunyi, dan tersebar di berbagai sistem dan jaringan. Oleh karena itu, pemilihan tools yang tepat menjadi krusial untuk akuisisi, analisis, verifikasi, dan pelaporan forensik yang sah secara hukum.

1. Alat Akuisisi (Acquisition Tools)

Akuisisi adalah proses pengambilan atau penyalinan data digital dari perangkat target (hard disk, SSD, perangkat mobile, dll.) tanpa mengubah data aslinya. Alat ini harus menjamin integritas data selama proses berlangsung.

a) FTK Imager: Digunakan untuk membuat image forensik dari media penyimpanan. Dikenal karena kecepatan dan kemampuannya membaca berbagai sistem file.
b) dd / dc3dd (Linux-based): Merupakan utilitas command-line untuk membuat bit-by-bit copy dari storage device, sering digunakan dalam lingkungan open-source.
c) Guymager: Alat akuisisi open-source di Linux yang mendukung berbagai format output dan verifikasi hash.

2. Alat Analisis File System dan Artefak

Setelah akuisisi, penyidik harus melakukan analisis terhadap file system, artefak pengguna, dan log sistem untuk menemukan bukti digital.

a) Autopsy (GUI dari Sleuth Kit): Platform open-source yang populer untuk menganalisis partisi, artefak browser, recent files, registry, dan metadata file.
b) X-Ways Forensics: Alat komersial dengan performa tinggi, mendukung analisis kompleks seperti rekonstruksi aktivitas pengguna dan timeline forensik.
c) EnCase Forensic: Salah satu tool industri yang paling banyak digunakan oleh lembaga penegak hukum. Memiliki fitur lengkap untuk akuisisi, analisis, indexing, dan pelaporan.

3. Alat Analisis Komunikasi dan Metadata

Alat ini digunakan untuk menelusuri komunikasi pengguna melalui email, pesan instan, dan file komunikasi lainnya, termasuk metadata tersembunyi.

a) MailXaminer: Dirancang khusus untuk memproses dan menganalisis data dari platform email (Outlook, Gmail, Yahoo), serta mendeteksi spam, malware, atau upaya penipuan.

b) Belkasoft Evidence Center: Menyediakan kemampuan analisis chat, history browser, dan artefak dari aplikasi komunikasi seperti WhatsApp, Telegram, Skype.

4. Alat Analisis Memori dan Sistem Langsung

Forensik memori (volatile memory) penting untuk mengungkap aktivitas saat serangan berlangsung, seperti proses yang aktif, koneksi jaringan, atau malware yang sedang berjalan.

a) Volatility Framework: Tool open-source berbasis Python untuk analisis memori RAM (dump), seperti proses berjalan, file DLL, koneksi jaringan aktif, dan keylogger.
b) Rekall: Alternatif dari Volatility dengan arsitektur modular dan dokumentasi lengkap.

5. Alat Analisis Jaringan (Network Forensics Tools)

Alat ini digunakan untuk mengumpulkan dan menganalisis lalu lintas jaringan, memantau intrusi, dan melacak aktivitas mencurigakan secara real-time.

a) Wireshark: Tool analisis paket jaringan yang sangat populer. Dapat mendeteksi komunikasi mencurigakan, seperti serangan man-in-the-middle atau transmisi data ilegal.
b) NetworkMiner: Tool forensik pasif yang dapat mengekstraksi informasi seperti file transfer, kredensial login, dan metadata komunikasi.

6. Alat Deteksi dan Analisis Malware

Seringkali, investigasi digital juga melibatkan identifikasi dan pembongkaran kode jahat (malware) yang digunakan untuk serangan.

a) Cuckoo Sandbox: Alat automated malware analysis yang dapat menjalankan sampel di lingkungan virtual dan menganalisis perilakunya.

b) IDA Pro / Ghidra: Digunakan untuk reverse engineering dan analisis kode binari dari malware atau perangkat lunak yang dicurigai.

7. Alat Hashing dan Validasi Integritas

Untuk memastikan bahwa data tidak berubah sejak proses akuisisi, alat hash digunakan pada awal dan akhir proses.

a) HashCalc / MD5Summer: Alat yang menghasilkan nilai hash dari file untuk memastikan integritas.
b) WinHex: Selain sebagai hex editor, juga berfungsi untuk menghitung hash dan memeriksa struktur file mentah.

8. Platform Integratif dan Suite Forensik Lengkap

Beberapa perangkat lunak menyediakan platform lengkap mulai dari akuisisi hingga pelaporan dalam satu lingkungan kerja.

a) Cellebrite UFED: Digunakan oleh penegak hukum di seluruh dunia untuk akuisisi dan analisis data dari perangkat seluler.
b) Oxygen Forensic Suite: Menyediakan ekstraksi mendalam dari perangkat Android dan iOS, termasuk aplikasi pihak ketiga dan data cloud.

Pemilihan dan penggunaan alat forensik digital tidak hanya ditentukan oleh kecanggihan teknis, tetapi juga oleh konteks hukum, jenis kasus, dan tujuan investigasi. Keandalan alat, rekam jejak penggunaannya di pengadilan, dan tingkat dokumentasi hasil analisis merupakan pertimbangan utama.

Oleh karena itu, praktisi forensik digital harus memiliki keahlian multidisiplin yang mencakup aspek teknis, hukum, dan etika untuk menjamin kredibilitas bukti yang dikumpulkan melalui perangkat tersebut.

C. Pembuktian dalam Investigasi Digital Forensik

Pembuktian dalam investigasi digital forensik merupakan proses sistematis yang bertujuan untuk mengidentifikasi, memperoleh, memverifikasi, menganalisis, dan menyajikan bukti digital secara sah di hadapan hukum.

Dalam era digital saat ini, di mana banyak aktivitas kriminal maupun perdata terjadi dalam ruang maya, pembuktian berbasis teknologi informasi menjadi salah satu komponen penting dalam proses penegakan hukum. Investigasi digital forensik tidak hanya melibatkan aspek teknis, tetapi juga harus tunduk pada prinsip-prinsip hukum acara dan tata cara pembuktian yang diakui secara legal.

1. Prinsip-Prinsip Pembuktian Forensik Digital

Agar hasil investigasi dapat diterima di pengadilan, bukti digital harus memenuhi sejumlah prinsip hukum, antara lain:

a) Authenticity (Keaslian): Bukti harus dapat diverifikasi sebagai asli, tidak dimodifikasi sejak diambil dari sumbernya.
b) Integrity (Integritas): Harus dipastikan tidak ada intervensi atau perubahan terhadap data sejak diperoleh hingga dianalisis.
c) Chain of Custody: Harus ada catatan lengkap tentang siapa saja yang menangani bukti, kapan, di mana, dan dalam kondisi apa, untuk menjaga keabsahan proses.
d) Repeatability: Proses investigasi dan hasilnya harus bisa diulang oleh pihak lain dengan hasil yang sama (prinsip ilmiah).
e) Legality: Bukti harus dikumpulkan melalui cara yang sah, tanpa melanggar hak asasi atau privasi seseorang.

2. Tahapan Pembuktian dalam Investigasi Digital Forensik

a) Identifikasi Bukti Digital

Mengenali perangkat, akun, atau sistem yang berpotensi menyimpan bukti. Contoh: hard disk, ponsel, akun email, file log serve

b) Pengumpulan (Acquisition)

Melakukan pencatatan dan pengambilan data menggunakan perangkat forensik untuk menjaga integritas. Biasanya dilakukan dengan metode disk imaging dan disertai dengan hash (MD5/SHA256) sebagai verifikasi.

c) Analisis dan Interpretasi

Tahap ini melibatkan pembacaan metadata, rekonstruksi aktivitas pengguna, pencarian file tersembunyi, artefak sistem, serta hubungan antara perangkat dan aktivitas kriminal.

d) Pelaporan

Menyusun laporan forensik yang sah dan jelas, lengkap dengan dokumentasi setiap langkah dan temuan yang akan digunakan di proses hukum.

3. Alat Pembuktian dalam Digital Forensik

Beberapa alat yang umum digunakan untuk mendukung pembuktian forensik digital:

a) EnCase Forensic: Untuk imaging dan analisis data disk.
b) FTK (Forensic Toolkit): Untuk mengekstrak, menganalisis, dan merekonstruksi file.
c) Autopsy dan Sleuth Kit: Open-source tools untuk memeriksa sistem file, log, artefak digital.
d) Wireshark: Untuk menganalisis trafik jaringan.
e) Volatility Framework: Untuk menganalisis memori (RAM) dan menemukan jejak aktivitas temporer.

4. Bentuk dan Contoh Bukti Digital

Bukti digital dapat berupa:

a) Log file: Catatan akses sistem (misalnya, log login gagal).
b) Metadata: Informasi tersembunyi dalam file seperti tanggal pembuatan dokumen, lokasi pengambilan foto.
c) Pesan email dan chat: Bukti komunikasi antar pelaku.
d) Jejak browser: Situs yang dikunjungi, waktu akses, cache.
e) Volatile memory (RAM): Untuk mendeteksi malware aktif, proses berjalan saat serangan.

Dalam kasus pencurian data karyawan oleh mantan pegawai, investigator menemukan log aktivitas USB yang menunjukkan pencurian file sensitif dua hari sebelum pengunduran diri.

5. Pembuktian di Pengadilan

Agar bukti digital dapat diterima dan bernilai di hadapan hukum, pembuktian harus memenuhi standar yuridis dan teknis, antara lain:

a) Validitas Prosedural: Bukti dikumpulkan oleh penyidik resmi atau ahli yang memiliki sertifikasi.
b) Verifikasi Hash: Disampaikan ke pengadilan sebagai jaminan data tidak berubah.
c) Pendapat Ahli: Diperlukan jika data bersifat kompleks dan membutuhkan interpretasi teknis.
d) Visualisasi dan Reproduksi: Bukti dapat ditunjukkan dalam bentuk tangkapan layar, grafik hubungan file, atau animasi kronologis aktivitas.

6. Tantangan dalam Pembuktian Digital
    a) Volatilitas Bukti: Bukti bisa hilang jika sistem mati (contoh: RAM).
    b) Enkripsi dan Anti-Forensik: Pelaku bisa menggunakan software enkripsi, wiping tools, atau obfuscation.
    c) Yurisdiksi Internasional: Jika data berada di server luar negeri, proses hukum bisa rumit tanpa perjanjian internasional.
    d) Overload Data: Investigator harus menyaring ratusan ribu file untuk menemukan jejak bukti yang relevan.

Pembuktian dalam investigasi digital forensik adalah proses ilmiah yang kompleks dan memerlukan sinergi antara keahlian teknis dan pemahaman hukum. Keberhasilannya sangat bergantung pada integritas prosedur, kemampuan penyidik, serta kesiapan hukum nasional untuk menerima dan menilai bukti berbasis teknologi.

Di masa depan, kebutuhan akan standar pembuktian digital yang terintegrasi secara internasional akan menjadi semakin mendesak seiring globalisasi kejahatan digital.

BAB 7

Perlindungan Data Pribadi

Dalam era transformasi digital yang berkembang pesat, data pribadi telah bergeser dari sekadar informasi individu menjadi komoditas bernilai tinggi di berbagai sektor seperti ekonomi, sosial, politik, dan keamanan. Data ini menjadi dasar dalam pengambilan keputusan berbasis data, pemasaran digital, kebijakan publik, hingga pengembangan teknologi kecerdasan buatan. Akibatnya, banyak pihak—baik negara maupun korporasi—secara masif mengumpulkan dan memanfaatkan data pribadi, menjadikannya elemen sentral dalam ekosistem digital global.

Namun, kemudahan pertukaran informasi melalui internet dan layanan cloud menimbulkan risiko serius terhadap hak privasi. Ketiadaan batas yurisdiksi yang jelas serta munculnya praktik seperti pencurian identitas, pengintaian digital, dan pengambilan data tanpa izin memperparah kerentanan individu. Dalam konteks ini, hukum siber (cyber law) memiliki peran penting untuk melindungi data pribadi tidak hanya secara teknis, tetapi juga dalam kerangka hukum yang menjamin hak-hak dasar warga negara.

Perlindungan data pribadi juga merupakan bagian dari penghormatan terhadap hak asasi manusia, khususnya hak atas privasi, sebagaimana diatur dalam instrumen internasional. Di Indonesia, hal ini diwujudkan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menjadi dasar hukum penting dalam menjamin kendali individu

atas datanya. Maka, perlindungan data pribadi bukan hanya isu legal-formal, melainkan juga kebutuhan etis dan sosial dalam mewujudkan ruang digital yang aman dan adil bagi seluruh pengguna.

A. Definisi Data Pribadi

Menurut Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data pribadi adalah setiap data tentang seseorang yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik.

Data pribadi dibedakan menjadi dua kategori:

1. Data pribadi umum

Data pribadi umum mencakup informasi dasar yang sering kali digunakan dalam administrasi atau pelayanan publik, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, alamat, serta nomor telepon. Meskipun tampak sederhana, data ini tetap memiliki nilai strategis dalam konteks identifikasi individu dan dapat menimbulkan risiko penyalahgunaan jika tidak dilindungi dengan baik.

2. Data pribadi spesifik.

Data pribadi spesifik mencakup informasi yang secara hukum dan etika dianggap lebih sensitif, karena dapat mengungkapkan aspek mendalam dan intim dari kehidupan seseorang. Jenis data ini meliputi data dan informasi kesehatan (rekam medis), data biometrik (sidik jari, retina, wajah), data genetika, keyakinan agama atau kepercayaan, kondisi disabilitas, orientasi seksual, pandangan politik, dan data keuangan. Kategori ini mendapatkan perlindungan yang lebih ketat karena

penyalahgunaannya dapat menimbulkan dampak yang serius terhadap privasi, martabat, dan keamanan individu.

Dengan demikian, pemahaman yang jelas mengenai definisi dan klasifikasi data pribadi menjadi landasan fundamental dalam perumusan kebijakan perlindungan privasi dan pengembangan sistem keamanan informasi. Hal ini tidak hanya berkaitan dengan kepatuhan hukum, tetapi juga dengan penghormatan terhadap hak asasi manusia di era digital yang semakin kompleks.

B. Prinsip – Prinsip Privasi

Dalam kerangka hukum perlindungan data pribadi, baik pada tataran internasional maupun nasional, terdapat prinsip-prinsip mendasar yang menjadi fondasi dalam pengelolaan informasi pribadi seseorang. Di tingkat global, prinsip-prinsip ini tercermin dalam instrumen seperti General Data Protection Regulation (GDPR) di Uni Eropa maupun OECD Privacy Guidelines, sementara di Indonesia dituangkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Prinsip-prinsip tersebut dirancang untuk melindungi hak privasi individu dalam menghadapi kompleksitas pemrosesan data di era digital. Selain memberikan landasan hukum, prinsip ini juga berfungsi sebagai pedoman etis bagi institusi publik maupun swasta dalam mengumpulkan, menyimpan, menggunakan, dan mendistribusikan data pribadi.

Beberapa prinsip utama yang diatur mencakup keabsahan dan keadilan (lawfulness and fairness), transparansi, pembatasan tujuan (purpose limitation), minimalisasi data, akurasi, pembatasan penyimpanan (storage limitation), integritas dan kerahasiaan, serta akuntabilitas. Setiap prinsip memiliki implikasi praktis, seperti keharusan memberikan pemberitahuan kepada

subjek data, membatasi penggunaan data hanya untuk keperluan yang sah dan disetujui, serta menjamin keamanan data dari akses tidak sah. Dengan berlandaskan prinsip-prinsip ini, penyelenggaraan sistem elektronik dan pemrosesan data pribadi diharapkan berjalan secara legal, proporsional, dan menghormati hak asasi manusia, khususnya hak atas privasi dalam ruang digital.

1. Prinsip Kesahihan dan Keabsahan (Lawfulness and Fairness)

Setiap kegiatan pengumpulan, pemrosesan, dan penyimpanan data pribadi harus dilakukan secara sah, berkeadilan, dan sesuai dengan hukum yang berlaku. Pemrosesan data tidak boleh dilakukan secara sembunyi-sembunyi atau tanpa dasar hukum yang jelas.

Sebuah perusahaan e-commerce tidak dapat mengumpulkan data lokasi pengguna tanpa izin atau pemberitahuan terlebih dahulu. Hal tersebut melanggar prinsip lawfulness karena tidak ada dasar yang sah.

2. Prinsip Transparansi (Transparency)

Subjek data (pemilik data) berhak mengetahui bagaimana data pribadinya dikumpulkan, untuk tujuan apa, siapa yang mengaksesnya, dan berapa lama data tersebut akan disimpan. Informasi ini harus disampaikan secara jelas, mudah dipahami, dan tidak menyesatkan.

Aplikasi mobile wajib menyertakan kebijakan privasi (privacy policy) yang menjelaskan secara rinci cara penggunaan dan penyimpanan data pengguna.

3. Prinsip Tujuan yang Spesifik (Purpose Limitation)

Data pribadi hanya boleh dikumpulkan untuk tujuan tertentu yang sah dan eksplisit, dan tidak boleh diproses lebih lanjut untuk tujuan yang tidak sesuai dengan tujuan awal pengumpulan.

Data pelanggan yang dikumpulkan oleh rumah sakit untuk keperluan medis tidak boleh digunakan oleh pihak lain untuk iklan tanpa persetujuan eksplisit.

4. Prinsip Minimalisasi Data (Data Minimization)

Data pribadi yang dikumpulkan harus relevan, terbatas, dan proporsional terhadap tujuan pengolahan. Tidak diperkenankan meminta data yang tidak diperlukan. Situs web berita yang hanya meminta email untuk pengiriman buletin mingguan tidak boleh meminta nomor KTP atau alamat lengkap pengguna.

5. Prinsip Akurasi (Accuracy)

Data pribadi harus dijaga keakuratannya dan diperbarui jika diperlukan. Setiap pihak yang memproses data wajib menyediakan mekanisme bagi subjek data untuk memperbaiki atau memperbarui data pribadinya.

Layanan perbankan online harus menyediakan fitur bagi pengguna untuk memperbarui alamat atau nomor telepon mereka jika terjadi perubahan.

6. Prinsip Penyimpanan Terbatas (Storage Limitation)

Prinsip penyimpanan terbatas mengatur bahwa data pribadi hanya boleh disimpan selama diperlukan untuk memenuhi tujuan spesifik dari pengumpulannya. Setelah tujuan tersebut tercapai, data wajib dihapus, dimusnahkan, atau dianonimkan agar tidak lagi dapat dikaitkan dengan individu terkait. Prinsip ini bertujuan untuk mencegah penyimpanan data secara berlebihan, yang berisiko terhadap kebocoran atau penyalahgunaan data dalam jangka panjang.

Sebagai contoh, perusahaan yang mengumpulkan data pelamar kerja memiliki kewajiban untuk menghapus data pelamar yang tidak lolos seleksi dalam jangka waktu yang wajar, sesuai dengan kebijakan retensi data perusahaan. Menyimpan data pribadi tersebut tanpa dasar hukum atau kepentingan sah setelah

proses seleksi selesai dianggap melanggar prinsip ini. Dengan menerapkan prinsip penyimpanan terbatas, organisasi menunjukkan kepatuhan terhadap praktik perlindungan data yang etis dan sesuai dengan ketentuan perundang-undangan yang berlaku.

7. Prinsip Integritas dan Kerahasiaan (Integrity and Confidentiality)

Prinsip integritas dan kerahasiaan menekankan bahwa data pribadi harus dijaga agar tetap akurat, utuh, dan tidak dapat diakses oleh pihak yang tidak berwenang. Perlindungan terhadap data pribadi mencakup pencegahan terhadap risiko kehilangan, kebocoran, manipulasi, atau perusakan data, baik yang disebabkan oleh kesalahan manusia, kerusakan sistem, maupun serangan siber. Untuk itu, penyelenggara sistem elektronik dan pihak pemroses data wajib menerapkan langkah-langkah keamanan teknis dan organisasi yang sesuai dengan tingkat risiko, seperti penggunaan firewall, sistem otentikasi berlapis, kontrol akses, serta audit keamanan berkala.

Sebagai contoh konkret, dalam sektor perbankan, data transaksi keuangan nasabah harus dilindungi menggunakan sistem enkripsi yang kuat, sehingga meskipun data tersebut disadap atau dicuri selama proses transmisi, informasi yang terkandung di dalamnya tetap tidak dapat dibaca atau dimanfaatkan oleh pihak yang tidak memiliki otorisasi. Penerapan prinsip ini menjadi landasan penting dalam membangun kepercayaan publik terhadap sistem digital dan menjamin perlindungan hak privasi individu secara menyeluruh.

8. Prinspi Akuntabilitas (Accountability)

Prinsip akuntabilitas menegaskan bahwa setiap pihak yang mengumpulkan, menyimpan, atau memproses data pribadi wajib bertanggung jawab atas kepatuhan mereka terhadap seluruh prinsip perlindungan data yang berlaku. Tidak cukup

hanya mengikuti aturan secara pasif, namun mereka harus secara proaktif menerapkan kebijakan, prosedur, dan langkah-langkah pengamanan yang memadai untuk memastikan perlindungan data secara konsisten. Selain itu, pihak pengelola data harus mampu mendokumentasikan dan menunjukkan bukti kepatuhan tersebut ketika diminta oleh otoritas pengawas atau regulator.

Sebagai contoh, sebuah perusahaan yang mengelola data pribadi pelanggan harus memiliki catatan terperinci mengenai setiap aktivitas pengolahan data, mulai dari pengumpulan, penyimpanan, hingga penghapusan data. Catatan ini harus disusun dengan baik agar dapat diaudit oleh lembaga pengawas seperti Komisi Perlindungan Data Pribadi (Komisi PDP) di Indonesia. Dengan menerapkan prinsip akuntabilitas, organisasi tidak hanya memenuhi kewajiban hukum, tetapi juga membangun kepercayaan publik melalui transparansi dan tanggung jawab dalam pengelolaan data pribadi.

C. GDPR VS UU PDP

GDPR (General Data Protection Regulation) diberlakukan oleh Uni Eropa pada 25 Mei 2018 sebagai tanggapan atas semakin kompleksnya ekosistem digital dan maraknya pelanggaran privasi yang melibatkan data pribadi. GDPR menggantikan Data Protection Directive 95/46/EC dan memiliki karakter mengikat secara langsung (binding regulation) terhadap seluruh negara anggota Uni Eropa dan entitas bisnis internasional yang memproses data warga Uni Eropa.

UU PDP (Perlindungan Data Pribadi) disahkan oleh pemerintah Indonesia pada 20 September 2022. Ini adalah regulasi komprehensif pertama yang secara khusus mengatur pengumpulan, penyimpanan, pemrosesan, dan penghapusan data pribadi. Regulasi ini didorong oleh kebutuhan akan

perlindungan hukum dalam ekonomi digital, meningkatnya kasus kebocoran data, serta harmonisasi standar internasional.

1. Ruang Lingkup dan Wilayah Berlaku
- GDPR: Berlaku secara ketat untuk semua entitas yang mengumpulkan atau memproses data pribadi warga Uni Eropa, baik yang beroperasi di dalam maupun di luar wilayah UE, selama data tersebut berasal dari warga UE.
- UU PDP: Berlaku untuk penyelenggara sistem elektronik dan pengendali data yang beroperasi di Indonesia, serta untuk entitas yang menggunakan data pribadi warga negara Indonesia, dengan fokus pada wilayah nasional.

2. Definisi Data Pribadi
- GDPR: Mendefinisikan data pribadi sebagai segala informasi yang dapat mengidentifikasi individu secara langsung maupun tidak langsung, termasuk data biometrik, genetika, dan data sensitif lainnya.
- UU PDP: Definisi serupa, mengkategorikan data pribadi menjadi data umum dan data spesifik (sensitif) seperti biometrik, rekam medis, dan data keuangan.

3. Prinsip-Prinsip Perlindungan Data
- GDPR: Memuat prinsip-prinsip seperti legalitas, transparansi, pembatasan tujuan, minimisasi data, akurasi, penyimpanan terbatas, integritas dan kerahasiaan, serta akuntabilitas yang ketat.
- UU PDP: Prinsip-prinsip serupa yang menekankan pengelolaan data yang adil, transparan, tujuan terbatas, akurasi, dan keamanan data, serta kewajiban akuntabilitas bagi pengendali data.

4. Hak Subjek Data
- GDPR: Memberikan hak luas kepada individu, termasuk hak akses, hak untuk dilupakan (right to erasure), hak untuk

memperbaiki data, hak membatasi pemrosesan, hak portabilitas data, dan hak menolak pemrosesan.

- UU PDP: Memberikan hak kepada pemilik data untuk mengakses, memperbaiki, menghapus, dan membatasi penggunaan data, meskipun beberapa hak masih dalam tahap implementasi lebih lanjut melalui peraturan pelaksana.

5. Persetujuan dan Dasar Hukum Pemrosesan

- GDPR: Menetapkan persetujuan eksplisit sebagai salah satu dasar pemrosesan data, dengan standar tinggi agar persetujuan jelas, spesifik, dan dapat dibuktikan. Selain itu, pemrosesan dapat didasarkan pada kepentingan sah, kontrak, kewajiban hukum, dan lain-lain.
- UU PDP: Persetujuan juga menjadi dasar utama pemrosesan data, dengan ketentuan agar persetujuan diberikan secara sadar dan sukarela. Selain itu, UU juga mengatur dasar hukum lain seperti kepentingan publik dan perjanjian.

6. Pengawasan dan Penegakan Hukum

- GDPR: Mengatur pembentukan otoritas pengawas nasional di setiap negara anggota, dengan kewenangan untuk melakukan investigasi, memberikan sanksi administratif berat (denda hingga 20 juta Euro atau 4% dari omzet global), serta tindakan korektif.
- UU PDP: Otoritas pengawas utama adalah Komisi Perlindungan Data Pribadi (Komisi PDP) yang memiliki kewenangan melakukan pengawasan, audit, dan pemberian sanksi administratif maupun pidana, walaupun implementasi dan mekanisme penegakan masih terus dikembangkan.

7. Sanksi dan Hukuman

- GDPR: Memberikan sanksi yang sangat berat bagi pelanggaran serius, termasuk denda administratif hingga 4% dari total pendapatan tahunan global perusahaan.

- UU PDP: Menetapkan sanksi administratif, denda, dan bahkan pidana bagi pelanggaran tertentu, namun besaran dan penegakan sanksi masih relatif lebih terbatas dibandingkan GDPR.

Meskipun UU PDP Indonesia mengambil banyak inspirasi dan prinsip dari GDPR sebagai standar global, terdapat perbedaan dalam cakupan yurisdiksi, implementasi hak-hak subjek data, serta intensitas penegakan hukum.

UU PDP masih dalam tahap pengembangan dan penyesuaian praktik, sedangkan GDPR sudah lebih mapan dan diterapkan secara ketat di seluruh wilayah Uni Eropa. Namun, keduanya sama-sama bertujuan memberikan perlindungan yang kuat terhadap hak-hak individu atas data pribadi di era digital.

BAB 8

Kebijakan Siber Nasional

Kebijakan Siber Nasional merupakan sebuah kerangka strategis, normatif, dan regulatif yang disusun secara sistematis oleh suatu negara sebagai bentuk respons terhadap tantangan dan dinamika yang berkembang dalam ekosistem digital global. Kebijakan ini berfungsi sebagai pedoman utama dalam merancang, mengelola, dan melindungi ruang siber nasional guna menjamin keamanan dan ketahanan negara, menjunjung tinggi hak asasi warga negara, serta mendukung pertumbuhan ekonomi digital yang inklusif dan berkelanjutan.

Dalam konteks ini, ruang siber tidak lagi dipandang sekadar sebagai medium komunikasi dan informasi, melainkan telah menjadi bagian integral dari infrastruktur kritis nasional yang mempengaruhi sektor-sektor vital seperti pertahanan dan keamanan, pemerintahan elektronik (e-government), sistem perbankan dan keuangan, layanan kesehatan, pendidikan, serta logistik dan transportasi.

Di era digital yang ditandai oleh ketergantungan tinggi terhadap teknologi informasi dan komunikasi, ancaman terhadap ruang siber—seperti peretasan, sabotase digital, pencurian data pribadi, penyebaran disinformasi, dan serangan siber berskala besar—dapat berdampak sistemik terhadap stabilitas nasional. Oleh karena itu, keberadaan kebijakan siber nasional menjadi elemen fundamental dalam menjaga kedaulatan negara di ranah digital, sekaligus membangun kepercayaan masyarakat terhadap penyelenggaraan layanan publik berbasis digital.

Dengan demikian, kebijakan siber nasional tidak hanya mencerminkan kapasitas negara dalam mengelola risiko teknologi, tetapi juga menjadi instrumen strategis dalam mengarahkan transformasi digital yang beretika, berkeadilan, dan berlandaskan pada prinsip-prinsip demokrasi.

Dalam era transformasi digital yang berkembang pesat, data pribadi telah bergeser dari sekadar informasi individu menjadi komoditas bernilai tinggi di berbagai sektor seperti ekonomi, sosial, politik, dan keamanan. Data ini menjadi dasar dalam pengambilan keputusan berbasis data, pemasaran digital, kebijakan publik, hingga pengembangan teknologi kecerdasan buatan. Akibatnya, banyak pihak—baik negara maupun korporasi—secara masif mengumpulkan dan memanfaatkan data pribadi, menjadikannya elemen sentral dalam ekosistem digital global.

A. BSSN (Badan Siber dan Sandi Negara)

Badan Siber dan Sandi Negara (BSSN) adalah lembaga pemerintah nonkementerian di Indonesia yang memiliki mandat utama untuk melaksanakan tugas-tugas teknis di bidang keamanan siber dan persandian. Lembaga ini dibentuk berdasarkan Peraturan Presiden (Perpres) Nomor 53 Tahun 2017, yang kemudian diperbarui melalui Perpres Nomor 28 Tahun 2021. Pembentukan BSSN merupakan langkah strategis pemerintah Indonesia dalam menanggapi dinamika ancaman di ruang siber yang kian kompleks, serta sebagai bentuk komitmen dalam membangun ketahanan siber nasional yang terkoordinasi dan terintegrasi.

Secara fungsi, BSSN bertugas untuk merumuskan dan melaksanakan kebijakan teknis nasional di bidang keamanan siber, termasuk pengamanan informasi yang bersifat strategis, pengawasan terhadap sistem elektronik nasional, serta

pembinaan dan pengawasan terhadap keamanan sistem informasi di instansi pemerintah, sektor vital nasional, dan penyelenggara sistem elektronik. BSSN juga berwenang mengoordinasikan respons terhadap insiden siber skala nasional, termasuk dengan membentuk Computer Security Incident Response Team (CSIRT) di berbagai sektor.

Kewenangan BSSN mencakup:

- Pengelolaan dan perlindungan informasi strategis nasional;
- Pengawasan dan penilaian keamanan sistem elektronik, baik milik pemerintah maupun sektor swasta;
- Pelatihan dan sertifikasi tenaga profesional di bidang keamanan siber;
- Penyusunan standar, pedoman, dan tata kelola keamanan informasi serta infrastruktur siber;
- Kerja sama internasional di bidang keamanan siber dan kriptografi.

Sebagai contoh konkret, BSSN berperan dalam menyusun dan mensosialisasikan pedoman teknis perlindungan infrastruktur informasi kritis nasional (IIKN), seperti sektor energi, keuangan, transportasi, dan pemerintahan. BSSN juga memiliki sistem pemantauan siber nasional (National Cyber Monitoring Center), yang berfungsi untuk mendeteksi, menganalisis, dan merespons ancaman serta insiden siber secara real-time.

Dalam menjalankan tugasnya, BSSN tidak bekerja sendiri, tetapi bersinergi dengan instansi lain seperti Kementerian Komunikasi dan Informatika, Polri, TNI, BIN, serta lembaga non-pemerintah dan sektor privat. BSSN juga menjadi penghubung utama Indonesia dalam berbagai kerja sama internasional di bidang siber, seperti dengan ASEAN, ITU, dan lembaga-lembaga keamanan siber dunia.

Keberadaan BSSN sangat penting dalam era digital yang ditandai oleh tingginya ketergantungan pada sistem elektronik,

munculnya serangan siber yang semakin canggih (seperti Advanced Persistent Threat/APT dan ransomware), serta meningkatnya kebutuhan akan perlindungan data pribadi dan privasi warga negara. Dengan memperkuat peran dan kapasitas BSSN, pemerintah Indonesia berharap dapat menciptakan ekosistem ruang siber nasional yang aman, tangguh, dan berdaulat.

B. Computer Emergency Response Team (CERT)

Computer Emergency Response Team (CERT) merupakan satuan teknis yang didirikan secara khusus untuk menangani berbagai insiden keamanan siber, seperti serangan peretasan, malware, kebocoran data, dan gangguan sistem elektronik yang dapat mengancam integritas, ketersediaan, serta kerahasiaan infrastruktur digital, baik di tingkat organisasi maupun negara.

Dalam kerangka kebijakan siber nasional, peran CERT menjadi sangat strategis sebagai garda terdepan dalam mendeteksi, merespons, menanggulangi, hingga memulihkan kondisi pasca-insiden siber, terutama yang berdampak pada layanan publik, pemerintahan, dan sektor strategis nasional.

Di Indonesia, fungsi CERT dijalankan oleh berbagai entitas, termasuk Indonesia CERT (ID-CERT) dan tim-tim tanggap insiden sektor tertentu yang beroperasi di bawah koordinasi Badan Siber dan Sandi Negara (BSSN). CERT memiliki mandat utama antara lain:

- Melakukan pemantauan ancaman siber secara berkelanjutan (real-time monitoring) untuk mendeteksi potensi serangan, baik dari aktor domestik maupun internasional.
- Menjalin koordinasi antarinstansi, termasuk dengan penyelenggara jasa internet (ISP), kementerian/lembaga,

BUMN, dan sektor swasta, untuk merespons secara cepat dan efektif terhadap insiden.

- Menghimpun dan menganalisis informasi teknis mengenai kerentanan sistem, pola serangan terkini, serta langkah-langkah pencegahan dan mitigasi.
- Meningkatkan kapasitas tanggap nasional melalui penyelenggaraan pelatihan, simulasi penanggulangan insiden (cyber drill), dan pengembangan protokol standar respons insiden.
- Menjalin kemitraan internasional, baik dalam lingkup regional maupun global, guna memperkuat pertukaran informasi, kerja sama teknis, dan solidaritas global menghadapi kejahatan siber lintas batas negara.

Contoh konkret dari peran CERT (Computer Emergency Response Team) dapat terlihat secara nyata dalam penanganan insiden serius, seperti serangan ransomware terhadap sistem rumah sakit, infrastruktur publik, atau instansi pemerintahan. Ketika insiden semacam ini terjadi, tim CERT akan segera bergerak untuk melakukan identifikasi awal terhadap sumber dan vektor serangan, mengisolasi sistem yang terdampak, serta membatasi penyebaran kerusakan ke sistem-sistem lainnya.

Selanjutnya, CERT juga berperan dalam proses pemulihan sistem, baik melalui restorasi data, perbaikan kerentanan, maupun pemulihan layanan publik yang terganggu. Tidak kalah penting, tim ini juga menyusun rekomendasi jangka panjang untuk peningkatan sistem pertahanan siber dan prosedur keamanan guna mencegah insiden serupa di masa mendatang.

Seiring dengan meningkatnya volume, kompleksitas, dan sifat transnasional dari ancaman siber, keberadaan dan profesionalisme CERT menjadi komponen strategis dalam membangun ekosistem digital nasional yang resilien, adaptif, dan tangguh. CERT tidak hanya berfungsi sebagai unit reaksi cepat

yang menangani serangan setelah terjadi, tetapi juga berkembang menjadi pusat unggulan (center of excellence) dalam pengembangan intelijen ancaman siber (cyber threat intelligence). Mereka mengidentifikasi tren serangan, pola-pola ancaman baru, dan teknik mitigasi mutakhir yang dapat digunakan oleh sektor publik maupun swasta.

Dengan pendekatan yang tidak hanya reaktif, tetapi juga preventif dan kolaboratif, peran CERT menjadi semakin esensial dalam menjaga stabilitas nasional di era digital. CERT juga membangun jejaring kerja sama lintas sektor, baik di dalam negeri maupun dengan entitas internasional, untuk memastikan bahwa penanggulangan insiden siber dilakukan secara terintegrasi dan berbasis data intelijen yang mutakhir. Oleh karena itu, penguatan kapasitas dan dukungan kebijakan terhadap keberlangsungan operasional CERT menjadi bagian penting dalam agenda keamanan siber nasional.

C. Literasi Digital

Literasi digital merupakan seperangkat kemampuan yang sangat penting dalam era informasi dan teknologi saat ini. Secara konseptual, literasi digital merujuk pada kapasitas individu untuk mengakses, memahami, menggunakan, mengevaluasi, dan menciptakan informasi melalui perangkat dan platform digital secara aman, etis, dan bertanggung jawab.

Dalam konteks kebijakan siber nasional, literasi digital dipandang tidak hanya sebagai keterampilan teknis, tetapi juga sebagai fondasi pembentukan warga negara digital (digital citizens) yang cerdas, kritis, serta tangguh terhadap ancaman informasi dan manipulasi di dunia maya.

Literasi digital berperan penting dalam menanggulangi berbagai tantangan siber kontemporer, mulai dari penyebaran

informasi palsu (hoaks), penipuan daring (online scam), hingga serangan berbasis rekayasa sosial seperti phishing dan baiting.

Masyarakat yang memiliki literasi digital rendah akan lebih rentan menjadi korban eksploitasi data pribadi, penyalahgunaan informasi, dan bahkan disinformasi politik yang dapat menggoyahkan stabilitas sosial. Oleh karena itu, penguatan literasi digital menjadi elemen strategis dalam menciptakan ekosistem digital yang resilien, inklusif, dan aman bagi seluruh lapisan masyarakat. Empat komponen utama literasi digital yang menjadi fokus pengembangan nasional antara lain:

1. **Keamanan Digital (Digital Security)**

Keamanan digital mengacu pada serangkaian kemampuan dan pengetahuan yang memungkinkan individu untuk melindungi diri dan datanya saat beraktivitas di ruang digital. Aspek ini mencakup pemahaman tentang pentingnya kata sandi yang kuat, penggunaan autentikasi dua faktor (2FA) untuk meningkatkan lapisan keamanan, serta kemampuan untuk mengenali dan mencegah ancaman seperti perangkat lunak berbahaya (malware), phishing, dan ransomware. Selain itu, keamanan digital juga mencakup penerapan teknologi seperti enkripsi untuk melindungi komunikasi dan transaksi daring, serta pemahaman mengenai hak atas privasi dan perlindungan data pribadi sesuai dengan prinsip-prinsip hukum yang berlaku.

2. **Etika Digital (Digital Ethics)**

Etika digital merujuk pada kesadaran dan sikap tanggung jawab dalam berinteraksi di dunia maya. Individu yang beretika digital memahami pentingnya menghormati hak orang lain, termasuk hak privasi dan kebebasan berekspresi. Mereka menghindari perilaku negatif seperti penyebaran ujaran kebencian, cyberbullying, plagiarisme, serta penyebaran informasi yang tidak benar atau menyesatkan. Etika digital juga mencakup pemahaman akan norma hukum dan sosial yang

mengatur interaksi digital, serta kemampuan untuk bersikap adil, sopan, dan empatik dalam setiap aktivitas daring.

3. Kecakapan Informasi (Information Literacy)

Kecakapan informasi merupakan kemampuan untuk mencari, mengevaluasi, dan menggunakan informasi digital secara efektif dan bertanggung jawab. Dalam konteks meningkatnya disinformasi, hoaks, dan manipulasi opini publik di ruang maya, kemampuan untuk memverifikasi sumber informasi, menilai kredibilitas dan objektivitas konten, serta memahami konteks penyebaran informasi menjadi sangat krusial. Kecakapan ini juga mendukung pembentukan masyarakat yang berpikir kritis, tidak mudah terprovokasi, dan mampu membedakan antara fakta dan opini, serta informasi yang sahih dan yang menyesatkan.

4. Kewargaan Digital (Digital Citizenship)

Kewargaan digital menekankan pada partisipasi aktif dan konstruktif dalam kehidupan digital sebagai bagian dari masyarakat dan warga negara. Hal ini mencakup keterlibatan dalam demokrasi digital, seperti e-voting, e-participation, dan penggunaan layanan publik berbasis digital (e-government) secara cerdas dan bertanggung jawab. Warga digital yang baik juga berperan dalam menciptakan lingkungan daring yang sehat dengan menyebarkan konten positif, melaporkan pelanggaran, dan berkontribusi pada diskusi publik yang informatif dan inklusif.

Keempat aspek ini saling melengkapi dan memperkuat, sehingga harus dikembangkan secara seimbang melalui kebijakan pendidikan, program pelatihan, dan inisiatif sosial yang kolaboratif. Literasi digital bukan hanya alat untuk bertahan dalam era informasi, melainkan juga fondasi strategis bagi ketahanan nasional di ranah siber.

BAB 9

Tanggung Jawab Platform Digital

Platform digital—seperti media sosial, mesin pencari, marketplace, aplikasi komunikasi, dan layanan daring lainnya—menjadi tulang punggung ekosistem digital modern. Dalam dunia yang semakin tergantung pada teknologi informasi, platform-platform ini tidak hanya menjadi sarana interaksi dan transaksi, tetapi juga sebagai ruang publik baru yang memiliki dampak luas terhadap aspek sosial, ekonomi, dan politik masyarakat.

Oleh karena itu, tanggung jawab platform digital tidak bisa dianggap remeh dan harus dikelola secara serius demi menciptakan ekosistem digital yang aman, adil, dan berkelanjutan. Beberapa bentuk tanggung jawab platform digital:

1. Perlindungan Data dan Privasi Pengguna

Salah satu tanggung jawab utama platform digital adalah melindungi data pribadi dan informasi pengguna. Dengan besarnya volume data yang dikumpulkan, diproses, dan disimpan, risiko kebocoran, penyalahgunaan, dan akses tidak sah menjadi ancaman nyata. Platform harus menerapkan standar keamanan teknis yang kuat, seperti enkripsi data, autentikasi dua faktor, dan sistem deteksi anomali untuk mencegah kebocoran data.

Selain itu, mereka harus transparan dalam menginformasikan kepada pengguna bagaimana data mereka

digunakan, serta mematuhi regulasi perlindungan data yang berlaku, seperti GDPR di Eropa dan UU Perlindungan Data Pribadi (UU PDP) di Indonesia. Transparansi dan pilihan kontrol bagi pengguna atas data pribadi mereka menjadi landasan penting dalam membangun kepercayaan dan menjaga hak privasi.

2. Pengelolaan Konten dan Penanganan Pelanggaran

Platform digital wajib menyediakan mekanisme yang efektif untuk mengelola konten yang beredar di ruang digital mereka. Ini mencakup pemantauan, moderasi, dan penghapusan konten yang melanggar hukum atau norma sosial, seperti ujaran kebencian, konten pornografi, berita palsu, serta penyebaran hoaks dan disinformasi.

Penyedia platform harus menyediakan sistem pelaporan yang mudah diakses oleh pengguna dan merespons keluhan dengan cepat dan transparan. Selain itu, platform perlu menerapkan kebijakan yang jelas terkait aturan komunitas dan etika penggunaan, guna menciptakan ruang digital yang kondusif dan nyaman bagi seluruh pengguna.

3. Transparansi dan Akuntabilitas

Transparansi menjadi kunci bagi platform digital dalam membangun kepercayaan publik. Platform perlu mengungkapkan secara terbuka bagaimana algoritma bekerja dalam menyajikan konten, iklan, dan rekomendasi kepada pengguna. Informasi terkait moderasi konten, kebijakan privasi, serta kerjasama dengan pihak ketiga juga harus dapat diakses oleh publik.

Selain itu, platform wajib bertanggung jawab secara akuntabel atas praktik operasionalnya dan harus siap diaudit oleh otoritas pengawas atau lembaga regulasi sesuai dengan ketentuan hukum. Dengan akuntabilitas yang jelas, platform dapat mengurangi risiko penyalahgunaan kekuasaan digital serta menjamin perlindungan hak pengguna.

4. Edukasi dan Literasi Digital

Platform digital memiliki peran penting dalam meningkatkan kesadaran dan literasi digital masyarakat. Mereka dapat berkontribusi dengan menyediakan materi edukasi tentang keamanan siber, privasi data, etika digital, serta cara mengenali dan menangkal informasi palsu atau penipuan online.

Edukasi ini penting untuk membentuk pengguna yang cerdas, kritis, dan bertanggung jawab dalam menggunakan teknologi digital. Inisiatif ini juga membantu memperkuat ekosistem digital yang sehat dan tahan terhadap ancaman siber serta manipulasi informasi.

5. Kerjasama dengan Pemerintah dan Pemangku Kepentingan

Dalam menghadapi tantangan yang kompleks di dunia digital, platform tidak dapat bekerja sendiri. Kerjasama yang erat dengan pemerintah, lembaga pengawas, organisasi masyarakat sipil, dan sektor swasta sangat diperlukan untuk menciptakan lingkungan digital yang aman dan berintegritas. Platform harus berpartisipasi aktif dalam pertukaran informasi intelijen ancaman siber, penanganan insiden keamanan, dan pengembangan kebijakan yang adaptif terhadap perkembangan teknologi dan ancaman baru. Kolaborasi lintas sektor ini juga membantu dalam penegakan hukum dan penyelesaian sengketa terkait konten digital secara lebih efektif.

Tanggung jawab platform digital adalah aspek fundamental dalam pembangunan ekosistem digital yang inklusif, aman, dan berkelanjutan. Dengan menjaga perlindungan data pribadi, mengelola konten secara bertanggung jawab, menjalankan transparansi dan akuntabilitas, serta berkontribusi pada literasi digital dan kolaborasi lintas pemangku kepentingan, platform digital dapat menjadi pilar utama dalam mendorong kemajuan teknologi sekaligus menjaga hak dan keamanan

pengguna di dunia maya. Mengingat peran dan dampak yang sangat besar, regulasi dan pengawasan yang tepat dari pemerintah dan masyarakat pun menjadi sangat krusial untuk memastikan bahwa tanggung jawab ini dipenuhi dengan sebaik-baiknya.

Kebijakan Siber Nasional merupakan sebuah kerangka strategis, normatif, dan regulatif yang disusun secara sistematis oleh suatu negara sebagai bentuk respons terhadap tantangan dan dinamika yang berkembang dalam ekosistem digital global. Kebijakan ini berfungsi sebagai pedoman utama dalam merancang, mengelola, dan melindungi ruang siber nasional guna menjamin keamanan dan ketahanan negara, menjunjung tinggi hak asasi warga negara, serta mendukung pertumbuhan ekonomi digital yang inklusif dan berkelanjutan.

Intermediary Liability

Intermediary Liability (Kewajiban Perantara) adalah konsep hukum yang mengatur sejauh mana penyedia layanan perantara digital—seperti platform media sosial, penyedia layanan hosting, ISP, marketplace, dan mesin pencari—bertanggung jawab atas konten atau aktivitas yang dilakukan oleh pengguna di platform mereka. Konsep ini menjadi sangat krusial di era digital, di mana jutaan konten dan transaksi terjadi setiap saat dan platform berperan sebagai "tempat" utama interaksi tersebut berlangsung

A. Konsep Dasar Intermediary Liability

Dalam ekosistem digital yang semakin kompleks, peran penyedia layanan perantara (intermediaries) menjadi krusial sebagai jembatan antara pengguna dengan berbagai layanan dan konten daring. Namun, pertanyaan penting yang muncul adalah: sejauh mana platform-platform ini bertanggung jawab

atas aktivitas yang dilakukan oleh penggunanya? Untuk menjawab hal tersebut, konsep intermediary liability atau kewajiban perantara hadir sebagai kerangka hukum yang mengatur batas tanggung jawab serta kewajiban hukum dari para penyedia layanan digital terhadap konten yang disebarkan melalui sistem mereka.

Konsep ini menjadi fondasi penting dalam menjaga keseimbangan antara kebebasan berekspresi, inovasi teknologi, dan perlindungan terhadap konten ilegal maupun merugikan.

1. Perlindungan bagi Intermediaries

Dalam banyak yurisdiksi, penyedia layanan perantara—seperti platform media sosial, penyedia hosting, mesin pencari, dan marketplace—diberikan perlindungan hukum khusus agar mereka tidak secara otomatis dianggap bertanggung jawab atas konten ilegal atau merugikan yang diunggah oleh pengguna. Perlindungan ini berakar pada prinsip bahwa intermediaries hanya menyediakan infrastruktur teknis atau akses, tanpa keterlibatan langsung dalam produksi atau penyebaran isi tersebut.

Dengan demikian, selama platform tidak secara aktif memoderasi, mengedit, atau mengontrol isi yang diunggah pengguna secara substantif, mereka tidak diperlakukan sebagai penerbit atau penyebar langsung, melainkan hanya sebagai fasilitator. Hal ini membedakan antara tanggung jawab pasif dan aktif.

Misalnya, jika sebuah platform menjadi tempat penyebaran ujaran kebencian atau pelanggaran hak cipta, maka mereka tidak serta-merta dianggap bersalah—kecuali jika mereka telah diberi tahu secara resmi (misalnya melalui notice and takedown) dan gagal bertindak secara proporsional.

Perlindungan ini bertujuan untuk:

- Mendorong inovasi digital, dengan memberikan ruang bagi pengembangan teknologi dan layanan baru tanpa ancaman hukum yang berlebihan.
- Menjaga keseimbangan kepentingan, antara kebebasan berekspresi pengguna dan tanggung jawab hukum atas konten yang merugikan.
- Menghindari penyensoran berlebihan, karena tanpa perlindungan ini, platform mungkin akan memilih untuk menghapus konten secara berlebihan demi menghindari risiko hukum.

Namun, perlindungan ini umumnya bersyarat. Platform tetap dituntut untuk memiliki mekanisme respons yang andal, seperti proses penanganan laporan pelanggaran, dan harus bertindak cepat saat mengetahui adanya konten ilegal. Di berbagai negara, kegagalan untuk merespons laporan ini dapat membatalkan perlindungan hukum yang dimiliki dan membuat platform bertanggung jawab secara langsung.

Contoh perlindungan serupa terlihat dalam:

- Section 230 Communications Decency Act (AS), yang memberikan perlindungan luas bagi platform selama mereka tidak terlibat dalam pembuatan konten.
- E-Commerce Directive (Uni Eropa), yang mengatur tanggung jawab terbatas penyedia layanan informasi, selama mereka bertindak pasif dan netral.

Dengan demikian, perlindungan bagi intermediaries adalah elemen penting dalam membangun ekosistem digital yang seimbang, di mana inovasi dapat berkembang tanpa mengorbankan perlindungan hukum bagi masyarakat luas.

B. Notice and Takedown (Pemberitahuan dan Penghapusan)

Notice and takedown adalah mekanisme hukum yang dirancang untuk menangani konten ilegal atau melanggar ketentuan pada platform digital melalui proses berbasis pelaporan. Dalam mekanisme ini, pihak yang merasa dirugikan atau otoritas yang berwenang dapat mengirimkan pemberitahuan resmi kepada penyedia layanan perantara (intermediary), meminta agar konten tertentu segera dihapus atau dinonaktifkan aksesnya.

Begitu pemberitahuan diterima, platform diwajibkan untuk menilai validitas laporan tersebut dan bertindak cepat—biasanya dengan menghapus konten atau membatasi akses dalam jangka waktu tertentu. Kewajiban ini menciptakan bentuk tanggung jawab terbatas: platform tidak bertanggung jawab atas konten sebelum diberi tahu, tetapi dapat dimintai pertanggungjawaban jika tidak mengambil tindakan setelah pemberitahuan diterima.

Mekanisme ini mencerminkan upaya menyeimbangkan dua prinsip yang seringkali berseberangan:

1. Kebebasan berekspresi: Memberikan ruang kepada pengguna untuk menyampaikan pendapat, berekspresi, dan berbagi informasi tanpa penyensoran yang berlebihan dari pihak platform.
2. Penegakan hukum dan perlindungan hak: Memastikan bahwa konten yang melanggar hukum—seperti ujaran kebencian, pelanggaran hak cipta, pornografi anak, atau penipuan—dapat dihapus secara cepat dan efektif.

Proses notice and takedown umumnya memiliki elemen-elemen sebagai berikut:

- Pemberitahuan tertulis: Harus mencantumkan informasi yang jelas tentang konten yang dianggap melanggar,

termasuk tautan, alasan pelanggaran, dan bukti yang relevan.

- Tindakan platform: Platform harus mengevaluasi pemberitahuan dan mengambil langkah penghapusan atau penonaktifan dalam waktu yang wajar.
- Mekanisme banding: Beberapa sistem hukum juga mengharuskan adanya proses pemulihan jika penghapusan dilakukan secara keliru, untuk melindungi hak pengguna.

Mekanisme ini telah diadopsi di berbagai negara, dengan variasi implementasi. Misalnya:

- Digital Millennium Copyright Act (DMCA) di AS menerapkan notice and takedown secara spesifik untuk pelanggaran hak cipta.
- Digital Services Act (DSA) di Uni Eropa mengharuskan platform besar memiliki sistem transparan dan efisien dalam menangani pelaporan konten ilegal.
- Peraturan Menteri Kominfo di Indonesia juga memuat ketentuan serupa, terutama untuk konten bermuatan negatif.

Meski efektif dalam banyak kasus, mekanisme ini juga menghadapi tantangan, seperti potensi penyalahgunaan untuk membungkam kritik sah (abusive takedown) dan kesulitan dalam verifikasi konten secara cepat. Oleh karena itu, sistem notice and takedown harus dijalankan dengan prinsip kehati-hatian, transparansi, serta akuntabilitas guna memastikan keadilan dan perlindungan hak semua pihak yang terlibat.

C. Kewajiban Proaktif

Seiring meningkatnya kompleksitas dan volume konten digital, banyak negara mulai mengadopsi pendekatan regulatif yang menuntut platform digital—terutama yang beroperasi dalam

skala besar—untuk tidak hanya bersikap reaktif terhadap konten ilegal, tetapi juga menjalankan tanggung jawab secara proaktif. Artinya, platform diharapkan dapat secara aktif memantau, menyaring, dan mencegah penyebaran konten berbahaya atau ilegal bahkan sebelum adanya laporan dari pengguna atau otoritas.

Kewajiban proaktif ini umumnya meliputi:

- Penggunaan teknologi deteksi otomatis: Seperti algoritma pembelajaran mesin dan kecerdasan buatan (AI) yang dirancang untuk mengenali ujaran kebencian, kekerasan ekstrem, pornografi anak, misinformasi, atau pelanggaran hak cipta.
- Moderasi konten skala besar: Platform diwajibkan memiliki sistem dan tim moderasi yang mampu menangani konten dalam jumlah besar, dalam waktu cepat, dan dalam berbagai bahasa serta konteks budaya.
- Penilaian risiko sistematis: Platform besar seperti media sosial dan marketplace diminta untuk secara berkala melakukan audit internal dan menilai dampak sistem mereka terhadap hak pengguna dan keamanan digital secara keseluruhan.

Pendekatan ini telah diwujudkan dalam beberapa regulasi internasional, seperti:

- Digital Services Act (DSA) di Uni Eropa, yang mewajibkan platform sangat besar (VLOPs) untuk menilai dan mengurangi risiko sistemik dari algoritma mereka, termasuk dampaknya terhadap disinformasi, ujaran kebencian, dan hak fundamental pengguna.
- Online Safety Bill di Inggris yang mewajibkan platform untuk melindungi pengguna dari konten ilegal dan berbahaya secara proaktif.

- Regulasi Kominfo di Indonesia, yang mulai mengarah ke kewajiban pelaporan dan penghapusan konten negatif secara berkala berdasarkan klasifikasi tertentu.

Namun, penerapan kewajiban proaktif ini menimbulkan sejumlah tantangan dan dilema:

1. Kebebasan Berekspresi
   Moderasi yang terlalu agresif atau berbasis algoritma bisa menyebabkan konten sah—terutama yang bersifat kritik politik atau diskusi sensitif—dihapus secara keliru (false positives), yang berpotensi mengancam kebebasan berekspresi.
2. Privasi Pengguna
   Pemantauan aktif atas komunikasi daring, termasuk pesan pribadi, dapat mengganggu privasi individu dan menimbulkan kekhawatiran etis dan hukum, terutama jika dilakukan tanpa pengawasan independen.
3. Beban Teknis dan Keuangan
   Kewajiban ini memberikan tekanan besar kepada platform, khususnya perusahaan kecil dan menengah, untuk membangun infrastruktur deteksi konten yang canggih dan mempekerjakan tim moderasi dalam skala besar, yang mungkin tidak sebanding dengan sumber daya yang mereka miliki.
4. Risiko Overblocking
   Ketika platform lebih memilih untuk menghindari risiko hukum dengan menghapus konten yang "meragukan", ini bisa berujung pada pemblokiran berlebihan (overblocking) yang merugikan keberagaman opini dan kebebasan digital.

Oleh karena itu, meskipun kewajiban proaktif bertujuan untuk menciptakan ruang digital yang lebih aman dan bertanggung jawab, penerapannya harus disertai dengan

mekanisme transparansi, akuntabilitas, dan perlindungan hak asasi manusia. Diperlukan juga kerja sama antara pemerintah, masyarakat sipil, dan industri teknologi untuk memastikan regulasi ini tidak berubah menjadi bentuk penyensoran yang merugikan demokrasi digital.

D. Contoh Regulasi Intermediary Liability

- Amerika Serikat (Section 230, Communications Decency Act)

Memberikan perlindungan yang sangat luas bagi platform agar tidak bertanggung jawab atas konten yang diunggah pengguna, selama platform tersebut tidak ikut memproduksi konten tersebut. Ini menjadi fondasi utama pertumbuhan media sosial dan platform digital di AS.

- Uni Eropa (Digital Services Act - DSA)

Mewajibkan platform besar melakukan moderasi konten lebih ketat, menerapkan transparansi algoritma, dan melindungi hak pengguna. Namun, perlindungan bagi intermediaries tetap diberikan selama mereka mematuhi aturan.

- Indonesia

UU ITE dan aturan turunannya mengatur bahwa intermediaries wajib menghapus konten bermuatan negatif atau ilegal setelah mendapat pemberitahuan. Namun, regulasi ini masih berkembang mengikuti dinamika teknologi dan tantangan baru di dunia digital.

Intermediary liability merupakan fondasi hukum yang krusial dalam membentuk ekosistem digital yang sehat, dinamis, dan bertanggung jawab. Konsep ini penting karena memungkinkan terciptanya keseimbangan antara perlindungan terhadap kebebasan berekspresi dan kebutuhan untuk menanggulangi penyebaran konten berbahaya atau ilegal seperti ujaran kebencian, hoaks, penipuan, serta kejahatan siber lainnya. Dengan adanya kerangka intermediary liability yang jelas,

platform digital dapat memahami batas tanggung jawab mereka, sehingga tidak terbebani dengan kewajiban moderasi yang berlebihan yang justru dapat menimbulkan risiko penyensoran serta pelanggaran privasi pengguna. Di sisi lain, mekanisme ini juga memberikan perlindungan hukum kepada pengguna dan masyarakat, serta mendorong akuntabilitas platform dalam memastikan ruang digital tetap aman dan inklusif.

BAB 10

Hukum Internasional dan Cyber War

Dalam konteks hukum internasional, perang siber (cyber war) menimbulkan tantangan normatif yang signifikan karena karakteristik unik dunia maya: tanpa batas teritorial, sulitnya atribusi pelaku, serta ambiguitas dalam klasifikasi "serangan" dan "kerusakan." Meskipun belum ada instrumen hukum internasional khusus yang secara eksplisit mengatur serangan siber antarnegara, prinsip-prinsip hukum internasional yang ada—seperti kedaulatan negara, larangan penggunaan kekerasan, dan hak untuk membela diri—tetap berlaku dan menjadi rujukan utama dalam menilai legalitas tindakan tersebut.

Prinsip non-intervensi melarang campur tangan negara lain dalam urusan dalam negeri suatu negara, termasuk melalui serangan siber terhadap sistem pemilu, pemerintahan, atau infrastruktur penting. Jika dampak serangan siber setara dengan serangan bersenjata konvensional (misalnya mengakibatkan kerusakan fisik, korban jiwa, atau lumpuhnya layanan publik), maka berdasarkan Pasal 51 Piagam PBB, negara korban memiliki hak untuk melakukan pembelaan diri, baik dalam bentuk respons siber maupun konvensional, selama memenuhi prinsip proporsionalitas dan kebutuhan mendesak (necessity).

Untuk membantu interpretasi hukum ini, para ahli menyusun Tallinn Manual, sebuah panduan non-resmi yang menjelaskan bagaimana hukum humaniter dan hukum damai internasional dapat diterapkan dalam konflik siber. Dokumen ini

menegaskan bahwa perlindungan terhadap warga sipil, larangan serangan terhadap infrastruktur sipil, dan keharusan membedakan target militer tetap berlaku dalam konflik siber.

Namun, penerapan prinsip-prinsip tersebut menghadapi berbagai kendala: kesulitan dalam atribusi (menentukan secara pasti siapa pelaku serangan), kurangnya kesepakatan internasional tentang batasan dan definisi serangan siber, serta minimnya mekanisme akuntabilitas yang efektif. Oleh karena itu, meskipun hukum internasional memberikan kerangka awal untuk menilai dan mengatur perang siber, tantangan faktual dan teknis di lapangan masih memerlukan penguatan melalui perjanjian internasional khusus dan kerja sama antarnegara yang lebih erat.

Platform digital—seperti media sosial, mesin pencari, marketplace, aplikasi komunikasi, dan layanan daring lainnya—menjadi tulang punggung ekosistem digital modern. Dalam dunia yang semakin tergantung pada teknologi informasi, platform-platform ini tidak hanya menjadi sarana interaksi dan transaksi, tetapi juga sebagai ruang publik baru yang memiliki dampak luas terhadap aspek sosial, ekonomi, dan politik masyarakat. Bagaimana hukum internasional mengatur tindakan semacam itu?

1. Hukum Humaniter Internasional

Dalam konteks konflik bersenjata, hukum humaniter internasional (IHL)—seperti yang tercantum dalam Konvensi Jenewa 1949 dan protokol-protokol tambahannya—berfungsi untuk memberikan perlindungan terhadap pihak-pihak yang tidak berpartisipasi langsung dalam permusuhan, terutama warga sipil, serta mengatur cara dan alat yang sah dalam berperang (means and methods of warfare).

Walaupun hukum ini awalnya disusun untuk mengatur konflik konvensional bersenjata secara fisik, dalam perkembangannya prinsip-prinsip IHL juga diadaptasi untuk

menjawab tantangan baru dalam domain siber. Serangan siber yang ditujukan pada infrastruktur kritis yang mendukung kehidupan masyarakat sipil, seperti rumah sakit, pembangkit listrik, sistem air bersih, atau jaringan komunikasi, jika terjadi dalam kerangka konflik antarnegara, dapat dianggap sebagai pelanggaran terhadap IHL karena menimbulkan penderitaan langsung terhadap populasi sipil.

Oleh karena itu, tindakan semacam itu harus tunduk pada prinsip-prinsip dasar IHL, termasuk prinsip pembedaan (distinction), proporsionalitas (proportionality), dan kehati-hatian (precaution). Penerapan hukum humaniter dalam dunia siber menegaskan bahwa hukum internasional tetap relevan dan harus ditaati, meskipun bentuk peperangan telah mengalami transformasi teknologi.

2. Tallinn Manual

Tallinn Manual merupakan suatu dokumen non-binding (tidak mengikat secara hukum) yang disusun oleh sekelompok ahli hukum internasional atas prakarsa NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) di Tallinn, Estonia. Manual ini hadir sebagai respons terhadap kebutuhan mendesak akan interpretasi yang sistematis mengenai bagaimana norma dan prinsip hukum internasional dapat diterapkan pada konteks operasi siber, khususnya dalam situasi konflik antarnegara.

Versi awalnya, Tallinn Manual 1.0 (2013), berfokus pada penerapan hukum humaniter internasional (international humanitarian law) dan hukum konflik bersenjata terhadap serangan siber. Sementara itu, Tallinn Manual 2.0 (2017) memperluas cakupan pembahasannya hingga meliputi situasi di luar konflik bersenjata, termasuk hak asasi manusia, prinsip non-intervensi, penggunaan kekuatan (use of force), serta yurisdiksi negara dalam ruang siber.

Meskipun tidak memiliki kekuatan hukum formal layaknya traktat atau konvensi internasional, Tallinn Manual memiliki nilai otoritatif dan akademik yang tinggi karena disusun berdasarkan konsensus para pakar hukum internasional. Manual ini digunakan secara luas oleh pembuat kebijakan, praktisi militer, akademisi, dan perancang strategi keamanan siber sebagai panduan normatif dalam menilai legalitas tindakan siber di tingkat internasional.

Secara prinsipil, Tallinn Manual menegaskan bahwa hukum internasional tetap berlaku dalam ruang siber, termasuk prinsip-prinsip kedaulatan negara, tanggung jawab negara (state responsibility), serta larangan penggunaan kekuatan bersenjata kecuali untuk pembelaan diri sebagaimana diatur dalam Pasal 2(4) dan Pasal 51 Piagam PBB. Dengan demikian, manual ini memainkan peran penting dalam mengisi kekosongan regulatif dalam tata hukum internasional kontemporer terkait cyber warfare.

A. Budapest Convention

Budapest Convention on Cybercrime, atau dikenal juga sebagai Convention on Cybercrime, merupakan perjanjian internasional pertama yang secara komprehensif mengatur mengenai penanggulangan kejahatan siber dan kerja sama internasional dalam ranah penegakan hukum digital. Konvensi ini diadopsi oleh Council of Europe pada 23 November 2001 di Budapest, Hongaria, dan mulai berlaku secara efektif pada 1 Juli 2004.

1. Tujuan Budapest Convention

Tujuan utama dari Budapest Convention adalah untuk membangun kerangka hukum internasional yang harmonis dalam menghadapi kejahatan siber yang bersifat lintas yurisdiksi.

Pertama, konvensi ini bertujuan menyelaraskan unsur-unsur hukum pidana substantif di antara negara-negara peserta, khususnya dalam mendefinisikan dan mengkriminalisasi berbagai bentuk kejahatan siber, seperti akses ilegal, gangguan data, serta penyalahgunaan perangkat.

Kedua, Budapest Convention menetapkan standar prosedur hukum acara pidana yang relevan dan dapat diterapkan dalam konteks digital, termasuk pengumpulan, penyitaan, dan pelestarian bukti elektronik.

Ketiga, konvensi ini mendorong kerja sama internasional yang efektif dan cepat dalam proses penyidikan dan penuntutan tindak pidana siber, melalui mekanisme bantuan hukum timbal balik dan saluran komunikasi langsung antarpenegak hukum. Tujuan-tujuan tersebut menegaskan posisi Budapest Convention sebagai landasan penting dalam pembentukan tatanan hukum global yang adaptif terhadap perkembangan teknologi dan dinamika kejahatan siber modern.

2. Ruang Lingkup Budapest Convention

Budapest Convention mencakup berbagai jenis tindak pidana yang terjadi di ranah digital. Konvensi ini menetapkan kriminalisasi atas akses ilegal ke sistem komputer (illegal access), yaitu tindakan masuk tanpa izin ke sistem informasi milik pihak lain. Selain itu, diatur pula larangan atas gangguan terhadap integritas data dan sistem komputer (data and system interference), termasuk perusakan, pengubahan, atau penghapusan data secara tidak sah.

Penyalahgunaan perangkat (misuse of devices), seperti kepemilikan dan distribusi malware atau alat peretasan, juga termasuk dalam cakupan konvensi ini. Di samping itu, Budapest Convention mencakup kejahatan yang berkaitan dengan konten (content-related offences), terutama pornografi anak, sebagai bentuk perlindungan terhadap kelompok rentan.

Terakhir, konvensi ini juga mengatur penipuan berbasis komputer dan pelanggaran hak kekayaan intelektual, khususnya pelanggaran hak cipta dalam lingkungan digital, yang semakin sering terjadi seiring berkembangnya teknologi distribusi informasi.

Walaupun diinisiasi oleh negara-negara Eropa, konvensi ini bersifat terbuka untuk ditandatangani dan diratifikasi oleh negara di luar kawasan Eropa, sehingga menjadi acuan global dalam membangun kerangka hukum penanggulangan kejahatan siber. Negara-negara seperti Amerika Serikat, Jepang, dan Australia turut serta dalam ratifikasi konvensi ini.

Indonesia hingga kini belum meratifikasi Budapest Convention, namun prinsip-prinsip di dalamnya telah menginspirasi pembentukan dan amandemen sejumlah peraturan perundang-undangan nasional, seperti UU ITE, UU PDP, serta kerja sama internasional dalam penegakan hukum siber.

Sebagai instrumen internasional, Budapest Convention juga menyediakan dasar hukum yang kuat untuk kerja sama lintas batas dalam pengumpulan barang bukti digital, pertukaran informasi intelijen siber, dan penanganan kejahatan siber yang bersifat transnasional—suatu tantangan hukum yang sangat krusial dalam era digital saat ini.

3. Tantangan Budapest Convention

a) Kurangnya Representasi Global

Meskipun bersifat terbuka, konvensi ini diprakarsai dan didominasi oleh negara-negara Eropa di bawah Dewan Eropa. Banyak negara berkembang, termasuk beberapa negara besar seperti Tiongkok, India, dan Brasil, tidak meratifikasi konvensi ini karena menganggapnya tidak mencerminkan kepentingan dan kebutuhan mereka, serta tidak inklusif dalam proses penyusunannya.

b) Kedaulatan Negara dan Masalah Yurisdiksi

Budapest Convention memungkinkan kerja sama lintas batas dalam penyidikan kejahatan siber. Namun, beberapa ketentuan—seperti akses langsung ke data komputer di luar yurisdiksi tanpa pemberitahuan negara terkait—dianggap melanggar prinsip kedaulatan negara dan berpotensi menimbulkan konflik antarnegara.

c) Keterbatasan Pengaturan atas Perkembangan Teknologi Baru

Konvensi ini disusun pada awal 2000-an, sebelum munculnya banyak teknologi modern seperti media sosial, AI generatif, ransomware-as-a-service, dan blockchain. Akibatnya, banyak jenis kejahatan siber terbaru tidak secara eksplisit tercakup dalam teks asli konvensi, meskipun ada protokol tambahan yang mencoba menyesuaikan.

d) Kesenjangan Kapasitas Penegakan Hukum

Tidak semua negara yang meratifikasi konvensi memiliki sumber daya teknis dan kapasitas hukum yang memadai untuk menerapkannya secara efektif. Hal ini membuat kerja sama internasional yang diharapkan oleh konvensi seringkali tidak berjalan optimal.

e) Tidak Mengatur Perlindungan Data Secara Spesifik

Konvensi ini lebih fokus pada pemberantasan kejahatan siber dan belum secara khusus mengatur perlindungan data pribadi atau privasi digital, padahal isu ini menjadi sangat penting dalam ekosistem digital modern. Beberapa pihak menilai hal ini sebagai kekosongan normatif yang perlu dilengkapi melalui instrumen hukum lainnya.

BAB 11

E-Commerce dan Fintech Law

E-commerce Law dan Fintech Law merupakan dua bidang hukum yang mengatur aktivitas ekonomi dan keuangan yang dilakukan melalui teknologi digital, terutama melalui internet dan sistem elektronik. E-commerce Law fokus pada regulasi perdagangan elektronik, termasuk transaksi jual beli online, perlindungan konsumen, dan keamanan data, sedangkan Fintech Law mengatur layanan keuangan berbasis teknologi seperti pembayaran digital, pinjaman online, dan aset kripto. Kedua bidang hukum ini penting untuk menciptakan kerangka hukum yang mendukung pertumbuhan ekonomi digital sekaligus melindungi hak dan kepentingan pelaku usaha serta konsumen di era digital.

A. E-Commerce Law

E-commerce Law merupakan cabang hukum yang mengatur segala aktivitas perdagangan yang dilakukan secara elektronik, baik melalui internet maupun sistem digital lainnya. Tujuan utamanya adalah menciptakan kerangka hukum yang jelas, terukur, dan adaptif terhadap dinamika perdagangan digital. Hukum ini meliputi aspek-aspek penting seperti kontrak elektronik, perlindungan konsumen, tanda tangan digital, keamanan dan privasi data, serta penyelesaian sengketa secara daring.

Beberapa aspek utama dalam E-commerce Law mencakup:

1. Pengakuan Kontrak Elektronik

Hukum mengakui keabsahan kontrak yang dibuat secara elektronik, yang memiliki kekuatan hukum yang setara dengan kontrak konvensional berbasis kertas.

2. Perlindungan Konsumen
   Regulasi menjamin hak-hak konsumen dalam transaksi daring, termasuk kewajiban pelaku usaha untuk menyediakan informasi produk yang transparan, hak konsumen untuk membatalkan transaksi dalam jangka waktu tertentu, serta perlindungan dari praktik penipuan atau manipulasi.
3. Keamanan dan Privasi Data
   Pengaturan mengenai pengumpulan, penyimpanan, dan pemrosesan data pribadi konsumen guna memastikan informasi tersebut tidak disalahgunakan atau mengalami kebocoran.
4. Sertifikat dan Tanda Tangan Digital
   Ketentuan mengenai penggunaan teknologi tanda tangan elektronik dan sertifikat digital guna menjamin keaslian, integritas, dan non-repudiation (tidak dapat disangkal) atas dokumen transaksi.
5. Penyelesaian Sengketa Elektronik
   Penyediaan mekanisme penyelesaian sengketa secara efisien, termasuk melalui mediasi, arbitrase online, atau sistem penyelesaian sengketa elektronik (online dispute resolution/ODR).

Dengan kemajuan teknologi dan semakin meluasnya ruang digital dalam aktivitas ekonomi, E-commerce Law memainkan peran yang sangat krusial dalam membangun ekosistem perdagangan digital yang adil, aman, dan terpercaya. Di Indonesia, pengaturan mengenai transaksi elektronik ini tercermin dalam Undang-Undang Informasi dan Transaksi Elektronik (UU No. 11 Tahun 2008 yang telah diubah dengan UU

No. 19 Tahun 2016 dan UU No. 1 Tahun 2024), yang menjadi dasar hukum bagi kontrak elektronik, tanda tangan digital, serta perlindungan data dan privasi. Selain itu, Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) juga memberikan perlindungan kepada konsumen dalam transaksi daring, seperti hak atas informasi yang benar dan mekanisme penyelesaian sengketa.

Keberadaan regulasi ini menjadi fondasi penting dalam menjembatani fleksibilitas transaksi digital dengan tuntutan akan akuntabilitas dan transparansi. Dengan demikian, E-commerce Law tidak hanya mendukung pertumbuhan ekonomi digital nasional, tetapi juga memperkuat kepercayaan masyarakat terhadap sistem perdagangan elektronik yang semakin berkembang di era globalisasi.

B. Fintech Law

Fintech Law merupakan cabang hukum yang mengatur inovasi keuangan berbasis teknologi, termasuk layanan pembayaran digital, pinjaman peer-to-peer (P2P lending), robo-advisory, aset kripto, hingga teknologi blockchain. Di Indonesia, pengaturan terkait sektor fintech tersebar di berbagai regulasi yang dikeluarkan oleh Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK), seperti POJK No. 77/POJK.01/2016 tentang layanan pinjam meminjam uang berbasis teknologi informasi, serta regulasi BI mengenai sistem pembayaran dan uang elektronik.

Di samping itu, Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) juga menjadi bagian integral dalam Fintech Law karena tingginya volume pemrosesan data pribadi konsumen oleh platform fintech. Tantangan utama dalam pengaturan ini meliputi isu perlindungan konsumen, integritas sistem keuangan, transparansi algoritma, dan pencegahan penyalahgunaan teknologi untuk kejahatan finansial. Oleh karena

itu, Fintech Law tidak hanya berfungsi untuk mendukung perkembangan industri keuangan digital, tetapi juga menjaga stabilitas sistem keuangan nasional dan kepercayaan publik terhadap layanan keuangan berbasis teknologi.

1. Tujuan dan Ruang Lingkup Fintech Law

Fintech Law bertujuan menciptakan kerangka hukum yang mampu:

- Menjamin keamanan transaksi dan perlindungan data konsumen;
- Mendorong inovasi dan inklusi keuangan digital;
- Mencegah penyalahgunaan sistem keuangan digital, seperti pencucian uang dan pendanaan terorisme;
- Menyediakan kepastian hukum bagi pelaku usaha dan investor;
- Menyelaraskan regulasi domestik dengan standar dan praktik internasional.

Ruang lingkup Fintech Law mencakup berbagai sektor, antara lain:

- Sistem pembayaran digital: termasuk e-wallet, e-money, dan QRIS;
- P2P lending dan crowdfunding: yang menghubungkan penyedia dan peminjam modal secara langsung;
- Kripto dan blockchain: termasuk aset digital, smart contract, dan tokenisasi;
- Robo-advisory dan digital wealth management;
- Insurtech: pengembangan layanan asuransi berbasis teknologi.

2. Regulasi Fintech di Indonesia

Di Indonesia, pengaturan fintech melibatkan beberapa lembaga:

- Otoritas Jasa Keuangan (OJK): bertanggung jawab atas pengawasan fintech di sektor non-bank, seperti P2P

lending, crowdfunding, dan robo-advisory. OJK juga menerapkan sistem regulatory sandbox untuk menguji inovasi sebelum diberikan izin penuh.

- Bank Indonesia (BI): mengatur sistem pembayaran, termasuk e-money dan penyelenggara payment gateway.
- BAPPEBTI (Badan Pengawas Perdagangan Berjangka Komoditi): mengawasi perdagangan aset kripto dan derivatif digital.

Beberapa regulasi penting di Indonesia antara lain:

- POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi;
- Peraturan BI tentang Penyelenggaraan Jasa Sistem Pembayaran;
- Peraturan BAPPEBTI tentang Penyelenggaraan Pasar Fisik Aset Kripto.

3. Tantangan Hukum dalam Pengembangan Fintech

Pengembangan fintech menghadirkan sejumlah tantangan hukum, di antaranya:

- Kepastian hukum dan dualisme regulasi: tumpang tindih pengawasan antara OJK dan BI dapat menimbulkan ketidakpastian hukum bagi pelaku usaha.
- Perlindungan konsumen: banyak layanan fintech belum memiliki sistem keamanan yang memadai, menimbulkan risiko penyalahgunaan data atau kebocoran informasi.
- Risiko sistemik: skala pertumbuhan fintech yang pesat dapat menimbulkan risiko keuangan nasional bila tidak diatur secara tepat.
- Akses lintas batas dan yurisdiksi: layanan fintech dapat diakses secara global, sementara kerangka hukum

masih terfragmentasi berdasarkan wilayah hukum masing-masing negara.

4. Pendekatan Internasional terhadap Fintech Law

Di tingkat global, beberapa pendekatan regulasi yang berkembang meliputi:

- Uni Eropa (UE): melalui Payment Services Directive 2 (PSD2) dan Markets in Crypto-Assets Regulation (MiCA), UE mendorong sistem keuangan yang terbuka (open banking), penguatan keamanan data, dan pengawasan terhadap stablecoin serta aset digital lainnya.
- Amerika Serikat: menggunakan pendekatan yang lebih sektoral, dengan pengawasan yang dilakukan oleh lembaga federal (misalnya SEC dan CFTC) dan otoritas negara bagian. Meski mendorong inovasi, AS memiliki kerangka ketat terhadap Anti-Money Laundering (AML) dan perlindungan investor.
- Singapura: mengatur fintech melalui Payment Services Act, yang menjadi contoh regulasi terpadu dan pro-pertumbuhan. Monetary Authority of Singapore (MAS) juga aktif membangun regulatory sandbox yang fleksibel.
- Australia dan Inggris: memberikan insentif inovasi melalui regulatory sandbox dan kemudahan lisensi fintech, disertai pedoman etika berbasis risiko.

5. Solusi dan Rekomendasi

Untuk menghadapi tantangan tersebut, solusi berikut direkomendasikan:

- Penguatan koordinasi antar-lembaga regulator agar regulasi fintech bersifat komplementer dan tidak tumpang tindih;

- Transparansi dan perlindungan konsumen melalui kewajiban disclosure, audit sistem keamanan, dan edukasi pengguna;
- Pengembangan regulatory sandbox yang adaptif, agar inovasi tidak terhambat, namun tetap berada dalam koridor hukum;
- Kerja sama internasional dalam harmonisasi regulasi fintech, terutama terkait transaksi lintas negara dan perlindungan data pribadi;
- Peningkatan literasi keuangan dan digital, baik kepada masyarakat maupun pelaku usaha kecil-menengah agar dapat berpartisipasi dalam ekosistem fintech.

6. Perbandingan Hukum Fintech di Beberapa Negara

Indonesia

- Regulasi terfragmentasi: OJK mengatur sektor pembiayaan digital, sedangkan BI mengatur sistem pembayaran. BAPPEBTI mengawasi aset kripto. Meskipun sudah ada sandbox, kepastian hukum masih berkembang.
- Fokus utama: perlindungan konsumen, mitigasi risiko sistemik, dan pengendalian kegiatan ilegal seperti pinjol ilegal.

Singapura

- Regulasi tunggal dan komprehensif melalui Payment Services Act (PSA) yang mencakup berbagai jenis layanan fintech, termasuk dompet digital, transfer lintas negara, dan kripto.
- Regulator aktif dan adaptif: MAS menyediakan sandbox dan insentif bagi startup fintech untuk menguji solusi keuangan inovatif dalam lingkungan yang terkontrol.

- Fokus utama: inklusi keuangan, perlindungan konsumen, dan pengembangan sektor fintech sebagai pilar ekonomi digital.

Uni Eropa

- Pendekatan harmonisasi: dengan adanya PSD2 yang mewajibkan perbankan terbuka (open banking) dan mendorong inovasi melalui integrasi API.
- MiCA (Markets in Crypto-Assets Regulation): menjadi salah satu kerangka hukum pertama yang mengatur stablecoin dan aset kripto secara komprehensif.
- Fokus utama: keamanan transaksi, perlindungan data (GDPR), interoperabilitas sistem, dan inovasi terukur.

Amerika Serikat

- Regulasi sektoral dan tersebar, dengan pengawasan federal dan negara bagian. SEC dan CFTC berperan penting dalam pengawasan kripto dan derivatif.
- Pendekatan yang hati-hati terhadap kripto, namun terbuka terhadap inovasi di sektor pembayaran dan investasi digital.
- Fokus utama: stabilitas keuangan, pengawasan pasar modal, dan perlindungan investor.

7. Studi Kasus

Sejak tahun 2016, industri pinjaman online berbasis peer-to-peer (P2P) lending di Indonesia mengalami pertumbuhan yang pesat, seiring meningkatnya kebutuhan masyarakat terhadap akses pembiayaan yang mudah dan cepat. Namun, perkembangan ini juga disertai dengan munculnya ratusan platform pinjaman ilegal yang tidak terdaftar di Otoritas Jasa Keuangan (OJK).

Pada periode 2019 hingga 2021, masyarakat mulai melaporkan berbagai kasus penyimpangan yang dilakukan oleh layanan pinjol ilegal tersebut, termasuk intimidasi dalam proses

penagihan, pemberlakuan bunga yang tidak transparan, serta pencurian data pribadi—khususnya data kontak telepon pengguna—yang digunakan untuk menekan atau mempermalukan peminjam.

Kasus-kasus ini menunjukkan lemahnya perlindungan hukum terhadap konsumen yang menggunakan layanan keuangan digital tanpa izin, serta keterbatasan penegakan hukum akibat tidak adanya mekanisme pengawasan terpadu dan kesulitan yurisdiksi atas platform yang server-nya berada di luar negeri.

Sebagai respons, OJK mewajibkan semua penyelenggara P2P lending untuk berizin dan terdaftar secara resmi. Selain itu, Bank Indonesia (BI) dan Kementerian Komunikasi dan Informatika (Kominfo) bekerja sama menutup ribuan aplikasi pinjol ilegal melalui pemblokiran dan pelacakan digital. Pemerintah juga membentuk Satgas Waspada Investasi sebagai forum koordinasi lintas lembaga untuk meningkatkan efektivitas pengawasan.

Dari sisi hukum, kasus ini memberikan sejumlah pelajaran penting. Pertama, regulasi fintech harus bersifat proaktif dan adaptif terhadap perkembangan teknologi yang sangat cepat. Kedua, perlindungan data pribadi menjadi sangat penting, terutama dalam mencegah penyalahgunaan data pengguna untuk tindakan yang merugikan.

Ketiga, diperlukan kerja sama internasional dalam penegakan hukum lintas batas, mengingat banyak pelaku pinjol ilegal berada di luar yurisdiksi Indonesia. Terakhir, edukasi publik menjadi kunci dalam mencegah masyarakat terjebak pada layanan pinjaman ilegal. Regulasi yang kuat saja tidak cukup tanpa kesadaran hukum dan literasi digital yang memadai dari masyarakat.

C. Hukum dalam Transaksi Digital

Hukum dalam transaksi digital merujuk pada seperangkat aturan hukum yang mengatur segala bentuk aktivitas pertukaran barang, jasa, atau informasi yang dilakukan melalui media elektronik, terutama internet. Perkembangan teknologi informasi yang pesat telah mendorong transformasi dalam cara masyarakat melakukan transaksi, dari sistem konvensional menjadi sistem digital yang lebih cepat, efisien, dan lintas batas. Oleh karena itu, keberadaan kerangka hukum yang jelas sangat penting untuk menjamin keabsahan, keamanan, serta perlindungan bagi semua pihak yang terlibat.

Beberapa aspek penting yang diatur dalam hukum transaksi digital antara lain pengakuan terhadap kontrak elektronik, yang memiliki kekuatan hukum sama seperti kontrak tertulis biasa; tanda tangan digital, yang digunakan untuk memastikan keaslian dan integritas dokumen elektronik; serta perlindungan data pribadi, guna mencegah penyalahgunaan informasi pengguna dalam setiap transaksi. Selain itu, hukum ini juga mencakup perlindungan konsumen digital, terutama dalam menjamin transparansi informasi, hak pengembalian, serta tanggung jawab penyedia platform terhadap penyalahgunaan layanan.

Di Indonesia, transaksi digital diatur dalam berbagai peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi, serta sejumlah peraturan turunan dari Otoritas Jasa Keuangan (OJK), Bank Indonesia, dan Kementerian Kominfo. Di tingkat global, transaksi digital juga diatur melalui prinsip-prinsip umum hukum kontrak, konvensi internasional seperti UNCITRAL Model Law on Electronic Commerce, serta standar teknis yang menjamin interoperabilitas antarnegara.

Dengan meningkatnya aktivitas e-commerce, fintech, dan layanan digital lainnya, hukum transaksi digital menjadi fondasi penting dalam menciptakan ekosistem digital yang adil, aman, dan terpercaya. Keberadaan hukum ini tidak hanya melindungi hak dan kewajiban para pihak, tetapi juga memperkuat kepercayaan publik terhadap teknologi digital sebagai sarana transaksi modern.

BAB 12

Etika dan Hak Digital

Etika dan hak digital merupakan dua konsep penting dalam dunia maya yang berkembang seiring dengan pesatnya kemajuan teknologi informasi dan komunikasi. Etika digital mengacu pada prinsip moral dan norma perilaku yang mengatur interaksi individu dalam ruang digital, sementara hak digital merujuk pada hak-hak fundamental yang dimiliki setiap individu dalam menggunakan teknologi, internet, dan informasi digital secara bebas dan aman.

A. Pengertian Etika Digital

Etika digital merujuk pada seperangkat prinsip moral dan nilai-nilai etis yang mengatur perilaku individu maupun kelompok dalam menggunakan teknologi informasi dan komunikasi, termasuk internet, media sosial, perangkat digital, dan platform daring lainnya. Dalam konteks ini, etika digital tidak hanya berkaitan dengan apa yang benar atau salah secara moral, tetapi juga mencerminkan tanggung jawab sosial dan kesadaran terhadap dampak dari setiap tindakan di ruang maya.

Etika digital mencakup sejumlah nilai utama seperti kejujuran, tanggung jawab, rasa hormat terhadap hak orang lain, serta penggunaan teknologi secara bijak dan bertanggung jawab. Meskipun sebagian dari pelanggaran etika digital dapat dikenai sanksi hukum, banyak tindakan tidak etis dalam dunia digital tidak secara eksplisit diatur oleh undang-undang, sehingga penegakan norma sosial dan kesadaran pribadi menjadi sangat penting.

Contoh Pelanggaran Etika Digital:

- Menyebarkan hoaks atau informasi palsu, yang dapat menyesatkan publik atau menimbulkan kepanikan.
- Melakukan cyberbullying atau ujaran kebencian, baik terhadap individu maupun kelompok tertentu berdasarkan ras, agama, gender, atau orientasi seksual.
- Melakukan plagiarisme dalam karya digital, seperti menyalin artikel, desain, atau konten multimedia tanpa menyebutkan sumber atau izin.
- Mengakses sistem, akun, atau data orang lain tanpa izin, yang dapat merusak kepercayaan serta melanggar privasi.
- Melanggar hak cipta digital, misalnya dengan membagikan musik, film, atau perangkat lunak tanpa lisensi resmi.

Etika digital sangat penting karena kehidupan modern kini sangat bergantung pada ekosistem digital. Interaksi sosial, aktivitas ekonomi, pendidikan, hingga layanan publik banyak yang berpindah ke ruang daring. Tanpa etika digital yang kuat, ruang digital akan dipenuhi dengan tindakan merugikan, disinformasi, serta pelanggaran hak-hak orang lain. Oleh karena itu, edukasi mengenai etika digital harus menjadi bagian integral dari literasi digital secara keseluruhan, baik dalam lingkungan pendidikan, keluarga, maupun masyarakat luas.

B. Hak Digital

Seiring dengan berkembangnya teknologi informasi dan komunikasi, muncul pula tuntutan untuk melindungi hak-hak dasar manusia dalam ruang digital. Hak digital adalah perpanjangan dari hak asasi manusia (HAM) yang diterapkan dalam konteks kehidupan maya. Dalam dunia yang semakin

terdigitalisasi, hak digital menjadi sangat penting agar individu tetap terlindungi, dihargai, dan memiliki otonomi terhadap identitas dan aktivitas mereka di internet.

Hak digital tidak menggantikan HAM konvensional, melainkan memperluas cakupan perlindungan terhadap hak-hak tersebut ke dalam ranah teknologi dan jaringan global. Berikut adalah beberapa bentuk utama hak digital yang kini diakui dan diperjuangkan oleh komunitas global:

1. Hak atas Privasi (Right to Privacy)

Hak atas privasi merupakan salah satu hak digital paling fundamental. Di era big data dan ekonomi berbasis algoritma, data pribadi pengguna sangat rentan terhadap pengumpulan, pemrosesan, dan penyebaran tanpa persetujuan. Hak ini menjamin bahwa setiap individu memiliki kontrol atas informasi pribadinya, termasuk data identitas, kebiasaan daring, lokasi, hingga komunikasi pribadi.

Negara, perusahaan, dan institusi wajib menerapkan prinsip informed consent, menyimpan data dengan aman, dan memberikan hak kepada pengguna untuk mengakses atau menghapus informasi mereka.

2. Hak atas Kebebasan Berekspresi

Setiap individu berhak menyampaikan pendapat, ide, dan informasi melalui media digital, termasuk media sosial, blog, dan forum daring. Kebebasan ini meliputi hak untuk menerima dan menyampaikan informasi tanpa campur tangan dari otoritas, selama tidak melanggar hukum yang berlaku seperti ujaran kebencian, fitnah, atau provokasi kekerasan.

Namun, kebebasan berekspresi secara digital harus diimbangi dengan tanggung jawab etis dan penghormatan terhadap hak orang lain, termasuk hak atas reputasi dan keamanan.

3. Hak atas Akses Informasi

Akses ke internet dan informasi digital telah menjadi kebutuhan dasar, baik dalam konteks pendidikan, pekerjaan, layanan publik, maupun partisipasi dalam demokrasi. Hak ini mencakup ketersediaan infrastruktur digital, keterjangkauan layanan internet, serta literasi digital yang memadai agar semua lapisan masyarakat dapat menikmati manfaat teknologi.

Pembatasan akses internet yang tidak proporsional atau pemutusan layanan secara sepihak sering dianggap sebagai pelanggaran terhadap hak asasi manusia di era digital.

4. Hak untuk Dilupakan

Hak untuk dilupakan memungkinkan individu untuk meminta penghapusan data pribadi mereka dari mesin pencari atau platform digital jika data tersebut sudah tidak relevan, menyesatkan, atau bersifat merugikan. Hak ini menjadi penting dalam era di mana jejak digital dapat bertahan selamanya dan berdampak buruk pada kehidupan pribadi maupun profesional seseorang.

Meskipun masih menjadi perdebatan hukum di berbagai negara, konsep ini telah diadopsi secara eksplisit dalam regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa.

Secara keseluruhan, hak digital berfungsi sebagai jembatan antara prinsip-prinsip HAM tradisional dan tantangan baru yang muncul akibat perkembangan teknologi. Negara dan lembaga internasional dituntut untuk terus mengembangkan kebijakan dan regulasi yang menjamin bahwa ruang digital tetap menjadi lingkungan yang adil, inklusif, dan menghormati martabat setiap manusia.

C. Kebebasan Berekspresi dalam Ruang Digital

Kebebasan berekspresi merupakan salah satu hak asasi manusia yang paling fundamental dan telah diakui secara

internasional, terutama dalam Pasal 19 Deklarasi Universal Hak Asasi Manusia yang menyatakan bahwa setiap orang memiliki hak untuk berpendapat tanpa campur tangan serta hak untuk mencari, menerima, dan menyampaikan informasi serta ide melalui media apa pun, tanpa memandang batas negara.

Di era digital, hak ini memperoleh relevansi yang semakin besar karena internet dan berbagai platform digital seperti media sosial, blog, forum diskusi, dan kanal video menjadi ruang utama untuk berbagi opini, ide, serta informasi secara luas dan cepat. Ruang digital memungkinkan individu dari berbagai latar belakang untuk mengekspresikan diri tanpa hambatan geografis dan birokratis, sekaligus membuka peluang bagi partisipasi publik yang lebih inklusif dalam wacana sosial, politik, dan budaya.

Namun, meskipun kebebasan berekspresi di dunia maya sangat penting untuk demokrasi dan pembangunan sosial, hak ini tidak bersifat absolut. Ia harus dilaksanakan secara bertanggung jawab, dengan mempertimbangkan batas-batas hukum dan etika, seperti larangan terhadap ujaran kebencian, fitnah, konten kekerasan, hoaks, serta pelanggaran privasi.

Pemerintah dan penyedia platform digital juga memiliki tanggung jawab untuk menjaga keseimbangan antara melindungi kebebasan berekspresi dan mencegah penyalahgunaan yang dapat merugikan individu atau masyarakat luas. Oleh karena itu, regulasi yang proporsional, transparan, dan berbasis hak asasi manusia sangat penting untuk memastikan bahwa kebebasan berekspresi tetap terlindungi tanpa membuka celah bagi penyebaran kebencian dan disinformasi.

Dengan meningkatnya peran teknologi dalam kehidupan sehari-hari, literasi digital dan kesadaran etis dalam bermedia menjadi hal yang tak kalah penting. Masyarakat perlu dibekali pemahaman tentang bagaimana mengekspresikan diri secara

bebas namun bertanggung jawab di ruang digital, serta bagaimana melindungi diri dari manipulasi informasi dan penyalahgunaan data. Dengan demikian, kebebasan berekspresi di era digital tidak hanya menjadi hak, tetapi juga menjadi tanggung jawab bersama demi terciptanya ruang digital yang sehat, demokratis, dan beradab.

1. Pentingnya Kebebasan Berekspresi di Dunia Maya

Media digital memberikan peluang luar biasa untuk partisipasi publik dan dialog sosial yang lebih luas dan inklusif. Melalui platform daring seperti media sosial, blog, podcast, dan kanal video, masyarakat dari berbagai latar belakang dapat menyuarakan pendapatnya secara langsung dan cepat.

Ini termasuk kelompok-kelompok marginal dan minoritas yang sebelumnya kerap terpinggirkan dalam media arus utama, kini memiliki ruang untuk menyampaikan pandangan, pengalaman, dan aspirasi mereka kepada khalayak yang lebih luas. Dengan demikian, kebebasan berekspresi di ruang digital turut berperan dalam mendorong demokratisasi komunikasi.

Selain itu, ruang digital menjadi medium penting bagi inovasi dan kreativitas. Ide-ide baru dapat dikomunikasikan dan diuji secara terbuka, menghasilkan kolaborasi lintas disiplin dan memperkaya wacana publik. Media digital juga memperkuat kontrol sosial dan mekanisme akuntabilitas. Masyarakat kini lebih mudah menyampaikan kritik terhadap pemerintah, korporasi, atau institusi yang dianggap melakukan penyimpangan atau pelanggaran. Fungsi ini menjadikan media digital sebagai instrumen penting dalam menjaga transparansi dan mendorong perubahan kebijakan.

Tak kalah penting, kebebasan berekspresi di media digital mempercepat proses pendidikan dan penyebaran informasi. Materi edukatif, berita, hasil riset, dan pengetahuan umum dapat disebarkan dalam hitungan detik dan diakses oleh siapa saja yang

terhubung dengan internet. Hal ini memperluas akses terhadap ilmu pengetahuan dan memungkinkan pertukaran informasi secara global, menjadikan media digital sebagai tulang punggung literasi abad ke-21. Namun demikian, peluang ini juga disertai tantangan etis dan hukum, terutama dalam menangani disinformasi dan ujaran kebencian, sehingga kebebasan berekspresi harus senantiasa dibarengi dengan tanggung jawab serta pemahaman kritis.

D. Sensor dalam Etika dan Hak Digital

Sensor dalam konteks digital merujuk pada tindakan pembatasan, penghapusan, atau pengawasan terhadap konten yang disebarluaskan melalui media digital. Sensor dapat dilakukan oleh pemerintah, platform digital (seperti media sosial), atau bahkan oleh pengguna sendiri (self-censorship). Tujuannya bisa bermacam-macam, mulai dari menjaga ketertiban umum, melindungi keamanan nasional, hingga mencegah penyebaran konten ilegal seperti ujaran kebencian, pornografi anak, atau terorisme.

1. Sensor dan Etika Digital

Secara etis, sensor merupakan persoalan yang kompleks dan sering kali menjadi medan tarik-menarik antara kepentingan kolektif dan hak individual. Di satu sisi, pembatasan terhadap konten tertentu dapat dibenarkan secara moral apabila bertujuan untuk menjaga nilai-nilai kemanusiaan, ketertiban umum, dan perlindungan terhadap kelompok rentan. Misalnya, sensor terhadap konten kekerasan ekstrem, pornografi anak, ujaran kebencian, atau ajakan terorisme dapat dianggap sebagai langkah preventif yang sah demi keamanan dan kesejahteraan sosial. Dalam hal ini, sensor menjadi alat etis untuk mencegah kerusakan yang lebih luas.

Namun, di sisi lain, sensor yang dilakukan secara berlebihan, sewenang-wenang, atau tanpa mekanisme akuntabilitas dapat merusak prinsip-prinsip demokrasi digital, seperti kebebasan berekspresi dan hak atas informasi. Penyensoran yang tidak proporsional berisiko menghambat diskusi publik yang sehat, membungkam kritik terhadap kekuasaan, dan mempersempit ruang dialog sosial yang inklusif.

Oleh karena itu, etika digital mengedepankan prinsip keseimbangan antara perlindungan kepentingan umum dan penghormatan terhadap hak individu. Artinya, sensor harus dilakukan secara selektif, proporsional terhadap risiko yang ditimbulkan, dilandasi aturan yang jelas, serta transparan dan dapat dipertanggungjawabkan secara moral maupun hukum. Pendekatan ini menjadi fondasi penting untuk menjaga integritas ruang digital yang terbuka, aman, dan adil bagi semua pihak.

2. Sensor dan Hak Digital

Sensor memiliki hubungan yang erat dan sering kali menimbulkan ketegangan dengan hak-hak digital, khususnya dalam hal kebebasan berekspresi, akses terhadap informasi, dan hak atas privasi. Dalam konteks kebebasan berekspresi, sensor yang dilakukan tanpa dasar hukum yang sah atau bersifat sewenang-wenang dapat secara langsung melanggar hak individu untuk menyampaikan pendapat, ide, atau ekspresi secara bebas di ruang digital.

Padahal, kebebasan berekspresi merupakan elemen esensial dalam sistem demokrasi dan pengembangan masyarakat yang terbuka. Ketika ekspresi dikekang secara tidak proporsional, bukan hanya suara kritis yang dibungkam, tetapi juga kualitas wacana publik yang ikut terdegradasi.

Selain itu, sensor juga dapat membatasi hak atas akses informasi, terutama apabila informasi yang diblokir sebenarnya bersifat legal, bermanfaat, dan relevan untuk kepentingan publik. Akses informasi merupakan prasyarat penting bagi masyarakat untuk memperoleh pendidikan, melakukan partisipasi politik yang bermakna, serta mengembangkan potensi pribadi dan profesional. Sensor yang tidak selektif dapat menutup pintu terhadap berbagai sumber pengetahuan dan wawasan yang dibutuhkan dalam kehidupan modern.

Lebih lanjut, praktik sensor sering kali disertai dengan mekanisme pengawasan atau pelacakan terhadap aktivitas daring individu. Dalam konteks ini, sensor bisa menjadi pintu masuk bagi pelanggaran terhadap hak atas privasi digital. Ketika pemerintah atau platform memantau konten yang dikonsumsi atau dipublikasikan oleh pengguna, bahkan hingga mengumpulkan data tanpa persetujuan, maka terjadi pelanggaran terhadap integritas ruang pribadi digital.

Oleh karena itu, penerapan sensor harus dilakukan dengan prinsip kehati-hatian, transparansi, dan akuntabilitas yang tinggi, agar tidak merusak prinsip-prinsip hak asasi manusia dalam ekosistem digital yang sehat dan adil.

BAB 13

Kasus Cyber Law di Indonesia

Seiring dengan semakin masifnya penggunaan internet dan digitalisasi sistem, tantangan hukum di ruang siber pun semakin kompleks. Indonesia sebagai negara dengan jumlah pengguna internet yang sangat besar dihadapkan pada berbagai persoalan hukum digital, seperti penyebaran informasi palsu, pencemaran nama baik melalui media sosial, kejahatan siber, pelanggaran data pribadi, hingga penyalahgunaan teknologi untuk kepentingan ilegal.

Oleh karena itu, pemahaman terhadap Cyber Law dan penerapannya dalam kasus-kasus nyata menjadi hal yang sangat penting bagi masyarakat, akademisi, maupun penegak hukum. Beberapa kasus cyber law di Indonesia adalah:

A. Kasus UU ITE dan Pidana Pencemaran Nama Baik: Jerinx SID (2020)

Salah satu kasus paling menonjol yang memicu perdebatan publik tentang penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) adalah kasus Jerinx, drummer band Superman Is Dead, pada tahun 2020. Jerinx dipidana karena unggahannya di media sosial yang menyebut "IDI sebagai kacung WHO" sebagai bentuk kritik terhadap kebijakan rapid test COVID-19. Ia kemudian dijerat dengan Pasal 27 ayat (3) jo. Pasal 45 ayat (3) UU ITE tentang pencemaran nama baik, dan divonis bersalah oleh pengadilan.

Kasus ini menimbulkan kontroversi luas, terutama terkait batas antara kebebasan berekspresi dan pencemaran nama baik

di ruang digital. Banyak pihak menilai bahwa pernyataan Jerinx, meskipun kontroversial dan keras, seharusnya ditempatkan dalam konteks kebebasan menyampaikan pendapat. Di sisi lain, ada pula yang berpendapat bahwa kritik yang dilontarkan dengan bahasa yang merendahkan suatu institusi publik dapat berdampak buruk dan mencemarkan reputasi lembaga tersebut.

Implikasi hukum dari kasus ini menunjukkan bagaimana Pasal 27 ayat (3) UU ITE sering disebut sebagai pasal karet, karena dianggap memiliki tafsir yang luas dan rentan disalahgunakan untuk membungkam kritik. Kasus Jerinx pun menjadi contoh nyata bagaimana hukum siber di Indonesia masih memerlukan reformasi agar lebih seimbang dalam melindungi kehormatan individu maupun hak kebebasan berekspresi di era digital.

B. Kasus Peretasan Website Pemerintah: Situs KPU (2019)

Menjelang pelaksanaan Pemilihan Umum (Pemilu) tahun 2019, publik Indonesia dikejutkan dengan dugaan peretasan terhadap situs resmi Komisi Pemilihan Umum (KPU). Dalam kasus ini, beredar informasi bahwa data pemilih Indonesia telah dicuri dan dijual di forum-forum gelap (dark web), termasuk informasi sensitif seperti nama, NIK, dan alamat. Meskipun pihak KPU sempat membantah adanya kebocoran data, kasus ini memicu kekhawatiran luas terkait integritas sistem elektronik negara dan perlindungan terhadap data pribadi warga negara.

Dari perspektif hukum, peretasan terhadap sistem KPU dapat dikategorikan sebagai pelanggaran terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya pasal-pasal yang mengatur tentang akses ilegal (illegal access) dan gangguan terhadap sistem elektronik. Kasus ini juga menjadi pengingat penting akan

kerentanan infrastruktur digital lembaga negara terhadap serangan siber.

Implikasi hukumnya tidak hanya menyangkut aspek pidana bagi pelaku peretasan, tetapi juga menyoroti perlunya peningkatan keamanan siber oleh institusi pemerintahan serta pentingnya reformasi regulasi perlindungan data pribadi. Kejadian ini turut mempercepat diskusi publik mengenai urgensi hadirnya Undang-Undang Perlindungan Data Pribadi (UU PDP) yang pada saat itu masih dalam tahap pembahasan

C. Kasus Pinjol Ilegal dan Kebocoran Data (2019-2021)

Antara tahun 2019 hingga 2021, Indonesia dihadapkan pada ledakan kasus pinjaman online (pinjol) ilegal yang menyebabkan keresahan masyarakat luas. Banyak korban melaporkan telah menjadi sasaran intimidasi, pelecehan verbal, dan bahkan ancaman kekerasan oleh oknum penagih dari platform pinjol yang tidak berizin. Salah satu praktik yang paling meresahkan adalah penyalahgunaan data pribadi—di mana platform pinjol mengakses seluruh kontak ponsel nasabah dan menyebarkan pesan penagihan kepada keluarga, rekan kerja, hingga orang yang tidak terkait sama sekali.

Secara hukum, kasus ini menyoroti lemahnya perlindungan terhadap data pribadi masyarakat Indonesia, terutama sebelum disahkannya Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan sejumlah peraturan Otoritas Jasa Keuangan (OJK) sudah eksis, penegakannya terhadap pelaku lintas yurisdiksi sangat terbatas. Selain itu, banyak platform pinjol ilegal beroperasi dari luar negeri, sehingga menyulitkan proses hukum dan pelacakan.

Sebagai respons, pemerintah melalui OJK, Kementerian Komunikasi dan Informatika (Kominfo), serta Satgas Waspada Investasi bergerak secara kolaboratif dengan menutup ribuan aplikasi pinjol ilegal. Namun, kasus ini menjadi pengingat penting bahwa kecepatan inovasi teknologi finansial (fintech) harus diimbangi dengan regulasi yang adaptif, serta sistem perlindungan hukum yang kuat dan responsif terhadap risiko-risiko digital yang terus berkembang.

D. Kasus Deepfake dan Pornografi Non-Konsensual

Seiring kemajuan teknologi kecerdasan buatan (AI), muncul fenomena deepfake—teknologi manipulasi video yang dapat menampilkan wajah seseorang secara realistis pada tubuh orang lain dalam sebuah rekaman visual. Di Indonesia, beberapa kasus penyebaran video deepfake yang menampilkan wajah artis atau tokoh publik dalam konten pornografi telah mencuat ke publik. Konten semacam ini tidak hanya mencemarkan nama baik korban, tetapi juga melanggar hak privasi dan martabat mereka secara serius.

Secara hukum, Indonesia saat ini belum memiliki regulasi yang secara eksplisit mengatur penggunaan dan penyebaran konten deepfake. Namun, pelaku dapat dijerat dengan pasal-pasal dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya terkait pencemaran nama baik dan pelanggaran privasi, serta Undang-Undang Pornografi untuk konten seksual non-konsensual. Ketiadaan aturan khusus menimbulkan tantangan dalam penegakan hukum, terutama dalam aspek pembuktian dan yurisdiksi digital.

Kasus ini menyoroti kebutuhan mendesak akan kerangka hukum yang responsif terhadap perkembangan teknologi digital. Penggunaan AI dalam manipulasi identitas dan konten digital

harus diatur secara spesifik untuk melindungi individu dari bentuk-bentuk kekerasan berbasis gender online, eksploitasi seksual digital, dan pencemaran reputasi yang dapat berdampak jangka panjang. Selain itu, edukasi publik tentang bahaya dan potensi penyalahgunaan deepfake juga penting sebagai bagian dari literasi digital nasional.

E. Kasus Tokoh Publik dan Ujaran Kebencian

Pada tahun 2018, musisi dan tokoh politik Ahmad Dhani dijerat hukum karena unggahan di media sosial yang dinilai mengandung ujaran kebencian terhadap kelompok tertentu. Ia dijatuhi hukuman berdasarkan Pasal 45A ayat (2) jo. Pasal 28 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur larangan menyebarkan kebencian atau permusuhan individu dan/atau kelompok masyarakat berdasarkan suku, agama, ras, dan antargolongan (SARA). Pengadilan memutuskan bahwa pernyataan Dhani melanggar hukum dan berpotensi memicu konflik sosial.

Kasus ini menegaskan bahwa ujaran kebencian di ruang digital tidak dapat dianggap sebagai kebebasan berekspresi yang tak terbatas. Meskipun hak untuk berpendapat dijamin oleh konstitusi, batasannya menjadi jelas ketika pendapat tersebut berpotensi merugikan martabat kelompok tertentu atau mendorong permusuhan di masyarakat. Dalam konteks hukum siber, penegakan aturan terhadap ujaran kebencian menjadi penting untuk menjaga harmoni sosial dan mencegah penyebaran intoleransi di ruang digital.

Lebih jauh, kasus ini juga menunjukkan urgensi literasi digital dan edukasi publik mengenai perbedaan antara kebebasan berekspresi dengan ujaran yang mengandung diskriminasi dan provokasi. Dengan berkembangnya media sosial

sebagai saluran komunikasi utama, pemahaman masyarakat terhadap etika dan batasan hukum dalam menyampaikan opini secara daring harus ditingkatkan agar tidak berujung pada pelanggaran hukum yang merugikan diri sendiri maupun orang lain.

DAFTAR PUSTAKA

Arief Mansur, D. M. (2020). *Hukum Siber: Perlindungan dan Penegakan Hukum di Era Digital*. Jakarta: Rajawali Pers.

Budhijanto, D. (2019). "Cyber Law sebagai Instrumen Perlindungan Sistem Informasi." *Jurnal Hukum dan Teknologi*, 6(2), 98-112.

Lubis, M. R. (2021). *Perlindungan Data Pribadi dan Hukum Siber di Indonesia*. Bandung: Citra Aditya Bakti.

Nugroho, A. B. (2022). "Urgensi Cyber Law dalam Menangani Kejahatan Digital." *Jurnal Hukum dan Masyarakat*, 8(1), 45-59.

UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific). (2018). *Cyber Law and Policy*. Retrieved from https://www.unescap.org

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (UU ITE).

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi* (UU PDP).

Otoritas Jasa Keuangan (OJK). (2016). *Peraturan OJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi*.

Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). (2023). *Strategi Nasional Keamanan Siber Indonesia*. Jakarta: Kominfo.

Komnas HAM. (2021). *Laporan Perlindungan Hak Privasi di Era Digital*. Jakarta: Komnas HAM.

European Union. (2016). *General Data Protection Regulation (GDPR)*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Retrieved from https://ccdcoe.org/uploads/2018/10/Tallinn-Manual-2.0.pdf

United Nations Human Rights Council. (2011). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Retrieved from https://undocs.org/A/HRC/17/27

Handoko, Y. (2020). *Cyber law di Indonesia: Tantangan dan implementasi*. Rajawali Pers.

Santoso, B. (2021). Perlindungan data pribadi di era digital: Studi kasus pinjaman online di Indonesia. *Jurnal Hukum dan Teknologi*, *5*(2), 115–130.

Wahyudi, A., & Fadilah, R. (2022). Kontroversi UU ITE dan implikasinya terhadap kebebasan berekspresi di Indonesia. *Jurnal Hukum dan HAM*, *13*(1), 45–60.

CNN Indonesia. (2020, Juli 10). *Kasus Jerinx dan UU ITE: Kritik atau pencemaran nama baik?*https://www.cnnindonesia.com/nasional/20200710135133-12-522066/kasus-jerinx-dan-uu-ite-kritik-atau-pencemaran-nama-baik

Detik.com. (2018). *Putusan kasus Ahmad Dhani terkait ujaran kebencian*. https://news.detik.com

Detik.com. (2020). *Penagihan pinjol ilegal dan penyalahgunaan data pribadi*. https://finance.detik.com

Komisi Pemilihan Umum (KPU). (2019). *KPU bantah terjadi kebocoran data pemilih Pemilu 2019*. Liputan6. https://www.liputan6.com/news/read/3931343/kpu-bantah-terjadi-kebocoran-data-pemilih-pemilu-2019

Otoritas Jasa Keuangan. (2021). *Publikasi dan laporan kinerja*. https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi

The Conversation Indonesia. (2021). *Deepfake di Indonesia: Tantangan dan regulasi*. https://theconversation.com/deepfake-di-indonesia-tantangan-dan-regulasi-158452

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). https://peraturan.bpk.go.id/Home/Details/38614/uu-no-11-tahun-2008

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE. (2016). https://peraturan.bpk.go.id/Home/Details/69421/uu-no-19-tahun-2016

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022). https://peraturan.bpk.go.id/Home/Details/215877/uu-no-27-tahun-2022

BIOGRAFI PENULIS

Dr. Dian Eka Kusuma Wardani, S.H., M.H., adalah seorang akademisi dan praktisi hukum yang telah menekuni dunia pendidikan tinggi dan kajian hukum selama lebih dari satu dekade. Lahir di Ujung Pandang pada tanggal 28 November 1984, beliau menyelesaikan pendidikan sarjana hukumnya di Universitas 45 Makassar (2008), kemudian melanjutkan pendidikan magister dan doktoralnya di Universitas Hasanuddin Makassar, dengan gelar doktor yang diraih pada tahun 2021. Fokus kajian akademis beliau terutama pada bidang hukum pidana, hukum siber, serta perlindungan hukum terhadap kelompok rentan.

Saat ini, Dr. Dian aktif sebagai Dekan Fakultas Hukum Universitas Sawerigading Makassar. Sebelumnya, beliau menjabat sebagai Kepala Laboratorium Hukum dan Sekretaris Rektor, serta pernah menjadi Dosen Luar Biasa di berbagai perguruan tinggi di Makassar seperti Universitas Atma Jaya, Politeknik Negeri Ujung Pandang, dan Politeknik Negeri Media Kreatif. Selain itu, beliau juga menjabat sebagai Editor in Chief pada Sawerigading Law Journal serta aktif sebagai verifikator SINTA, asesor rekognisi pembelajaran lampau, asesor beban kerja dosen, dan anggota tim integritas akademik.

Dalam bidang penelitian dan publikasi, Dr. Dian telah menghasilkan berbagai karya ilmiah baik dalam jurnal nasional terakreditasi maupun internasional bereputasi. Beberapa penelitiannya mencakup isu-isu kontemporer seperti kejahatan skimming, perlindungan terhadap whistle blower, serta kekerasan seksual. Beliau juga telah menerbitkan sejumlah buku referensi hukum, di antaranya *Hukum Pidana di Luar Kodifikasi*, *Telaah Tematik Hukum Pidana di Indonesia Pasca Disahkannya KUHP Baru*, *Hukum Kepolisian*, dan *Aspek Hukum dan Pembuktian Kejahatan Skimming: Studi Kasus dalam Sistem Peradilan Pidana Indonesia*. Karyanya mencerminkan perhatian mendalam terhadap dinamika hukum positif di Indonesia yang terus berkembang.

Komitmennya dalam bidang pengabdian masyarakat juga dibuktikan melalui berbagai program penyuluhan hukum, pelatihan pencegahan stunting, serta perlindungan hak atas tanah, yang bahkan telah mendapatkan perlindungan hak cipta (HKI). Sebagai peneliti sekaligus pendidik, beliau percaya bahwa hukum bukan hanya untuk ditafsirkan di ruang akademik, melainkan juga harus hadir secara nyata dalam kehidupan masyarakat sebagai instrumen keadilan dan perlindungan hak-hak sipil.