HUKUM PIDANA DAN PERKEMBANGAN IT

Dr. H. Noor Rohmat, S.H., M.Kn.

HUKUM PIDANA DAN PERKEMBANGAN IT

Dr. H. Noor Rohmat, S.H., M.Kn.

Editor: Dr. (Yuris), Dr. (Mp), H. Teguh Samudera, S.H., M.H.

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh.

Segala puji bagi Allah Subhanahu wa Ta'ala yang telah melimpahkan rahmat, taufik, dan hidayah-Nya, sehingga buku referensi ini yang berjudul *"Hukum Pidana dan Perkembangan IT"* dapat disusun dan hadir di tengah-tengah pembaca. Shalawat serta salam semoga senantiasa tercurah kepada Nabi Muhammad Shallallahu 'alaihi wasallam, keluarga, sahabat, dan seluruh umatnya yang istiqamah di jalan kebenaran.

Perkembangan teknologi informasi yang begitu cepat telah membawa dampak luas, termasuk dalam bidang hukum pidana. Fenomena kejahatan berbasis digital (*cyber crime*) semakin kompleks, sehingga diperlukan pendekatan hukum yang mampu menjawab tantangan zaman. Dalam konteks inilah, buku ini hadir sebagai upaya untuk menjembatani antara teori hukum pidana klasik dengan praktik kejahatan modern berbasis teknologi.

Buku ini disusun oleh Dr. H. Noor Rohmat, S.H., M.Kn., sebagai bentuk kontribusi ilmiah terhadap dunia hukum Indonesia. Dengan menggabungkan kajian teoritis dan pemahaman kontekstual terhadap perkembangan IT, buku ini diharapkan dapat menjadi rujukan yang bermanfaat bagi

mahasiswa, akademisi, praktisi hukum, serta seluruh pihak yang memiliki perhatian terhadap isu-isu hukum kontemporer.

Akhir kata, kami menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dalam proses penyusunan buku ini. Semoga buku ini dapat memberikan manfaat dan menjadi amal jariyah bagi penulis dan semua yang terlibat.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Jakarta, April 2025

Penulis

Dr. H. Noor Rohmat, S.H., M.Kn.

DAFTAR ISI

BAB I

KONSEP DASAR HUKUM PIDANA

Bab ini membahas secara menyeluruh tentang landasan konseptual hukum pidana sebagai cabang hukum publik yang mengatur hubungan antara individu dengan negara dalam konteks pelanggaran hukum yang bersifat melawan norma-norma sosial yang dilindungi oleh hukum. Pembahasan dimulai dari pengertian hukum pidana menurut berbagai perspektif, tujuan dan fungsi dari keberadaan hukum pidana dalam masyarakat, serta bagaimana hukum pidana mengkategorikan tindak pidana berdasarkan jenis dan tingkat pelanggarannya. Selain itu, bab ini juga menjelaskan unsur-unsur utama dari tindak pidana, mulai dari perbuatan yang melawan hukum hingga adanya unsur kesalahan atau pertanggungjawaban pelaku. Dalam kaitannya dengan perkembangan teknologi informasi, bab ini turut menyoroti tentang siapa saja yang dapat menjadi subjek hukum dalam ranah digital, termasuk individu, korporasi, dan bahkan sistem berbasis teknologi yang dioperasikan oleh manusia.

A. Definisi Hukum Pidana

Hukum pidana merupakan salah satu cabang utama dalam sistem hukum yang memiliki fungsi krusial dalam menjaga ketertiban sosial dan melindungi nilai-nilai fundamental dalam masyarakat melalui pemberian sanksi terhadap perilaku yang dianggap membahayakan atau merugikan kepentingan umum. Secara konseptual, hukum pidana dapat didefinisikan sebagai

sekumpulan norma atau aturan hukum yang mengatur tentang perbuatan yang dilarang oleh negara dengan disertai ancaman sanksi pidana bagi siapa pun yang melanggarnya, serta mekanisme penegakan hukum yang mengatur bagaimana proses penyelidikan, penuntutan, dan pemidanaan dilakukan terhadap pelaku tindak pidana tersebut. Dalam pandangan Andi Hamzah (2023), hukum pidana tidak hanya berperan sebagai sarana represif untuk menanggulangi kejahatan, tetapi juga memiliki dimensi preventif yang bertujuan untuk mencegah terjadinya tindak pidana melalui efek jera dan pengaturan perilaku warga negara. Selain itu, menurut Muladi dan Arief (2022), hukum pidana memiliki sifat ultimum remedium, yakni digunakan sebagai upaya terakhir apabila instrumen hukum lain tidak efektif dalam menyelesaikan konflik hukum yang terjadi di masyarakat.

Hal ini sejalan dengan paradigma modern penegakan hukum yang lebih menekankan prinsip keadilan restoratif (*restorative justice*) sebagai pendekatan alternatif yang menempatkan korban, pelaku, dan masyarakat sebagai pihak yang harus dipulihkan akibat dampak suatu tindak pidana. Seiring dengan perkembangan zaman dan kompleksitas kejahatan yang terus meningkat, hukum pidana juga mengalami dinamika dalam substansi maupun implementasinya, termasuk perluasan pengaturan terhadap tindak pidana baru seperti

kejahatan siber, korupsi, dan pencucian uang, yang membutuhkan penyesuaian kerangka hukum dan pendekatan penegakan hukum yang adaptif. Oleh karena itu, hukum pidana tidak hanya dipahami sebagai perangkat sanksi, melainkan juga sebagai refleksi dari nilai-nilai sosial, politik, dan moral yang hidup dan berkembang dalam suatu masyarakat yang berdaulat (Sudarto, 2023).

Hukum pidana merupakan salah satu cabang ilmu hukum yang memiliki peranan sangat penting dalam menjaga ketertiban dan keamanan masyarakat melalui pengaturan perilaku manusia yang dianggap merugikan kepentingan umum. Secara konseptual, hukum pidana dapat dipahami sebagai keseluruhan norma hukum yang mengatur perbuatan-perbuatan yang dilarang oleh negara dan diancam dengan sanksi pidana apabila dilakukan oleh seseorang. Dalam konteks ini, hukum pidana tidak hanya berfungsi sebagai alat untuk menegakkan keadilan, tetapi juga sebagai instrumen preventif yang bertujuan mencegah terjadinya pelanggaran hukum dengan memberikan efek jera kepada pelaku tindak pidana (Pompe, dalam Hukumonline, 2024). Definisi ini menegaskan bahwa hukum pidana tidak berdiri sendiri, melainkan merupakan bagian integral dari sistem hukum nasional yang berorientasi pada perlindungan kepentingan umum dan pemeliharaan ketertiban sosial.

Menurut Moeljatno, yang dikutip dalam Anjir Muara (2024), hukum pidana adalah bagian dari keseluruhan hukum yang mengatur dasar-dasar dan aturan untuk menentukan perbuatan yang dilarang serta menetapkan ancaman pidana bagi pelanggarnya. Pendekatan ini menekankan dua unsur pokok dalam hukum pidana, yaitu norma yang berisi larangan atau perintah dan sanksi yang berupa ancaman pidana atas pelanggaran norma tersebut. Dengan demikian, hukum pidana tidak hanya mengatur apa yang boleh dan tidak boleh dilakukan, tetapi juga memberikan konsekuensi hukum yang tegas bagi pelanggar, sehingga menciptakan efek jera dan mendorong kepatuhan masyarakat terhadap norma hukum yang berlaku. Hal ini sejalan dengan pandangan C.S.T. Kansil yang menyatakan bahwa hukum pidana mengatur pelanggaran dan kejahatan terhadap kepentingan umum yang diancam dengan hukuman sebagai bentuk siksaan atau penderitaan yang diberikan oleh negara (Hukumonline, 2024).

Lebih lanjut, hukum pidana dapat dibedakan menjadi dua aspek utama, yaitu hukum pidana materil dan hukum pidana formil. Hukum pidana materil mengatur jenis-jenis tindak pidana serta ketentuan mengenai siapa yang dapat dikenai pidana dan jenis pidana apa yang dapat dijatuhkan. Sedangkan hukum pidana formil mengatur tata cara penegakan hukum pidana, mulai dari penyelidikan, penyidikan, penuntutan, hingga

proses peradilan dan pelaksanaan putusan pengadilan (Efridadewi, 2020). Kedua aspek ini saling melengkapi dan memastikan bahwa penegakan hukum pidana berjalan secara adil, transparan, dan sesuai dengan prinsip-prinsip hukum yang berlaku.

Dalam konteks yuridis, hukum pidana juga didasarkan pada prinsip-prinsip fundamental yang menjadi landasan normatif dalam pelaksanaannya. Salah satu prinsip utama adalah asas legalitas (*nullum crimen, nulla poena sine lege*), yang menyatakan bahwa tidak ada perbuatan yang dapat dipidana kecuali berdasarkan ketentuan undang-undang yang telah ada sebelumnya. Prinsip ini menjamin kepastian hukum dan melindungi hak-hak individu dari tindakan sewenang-wenang negara. Selain itu, asas tiada pidana tanpa kesalahan (*nulla poena sine culpa*) menegaskan bahwa seseorang hanya dapat dijatuhi pidana apabila terbukti melakukan kesalahan secara subjektif, baik berupa kesengajaan maupun kelalaian (Anjir Muara, 2024). Kedua asas ini merupakan pilar penting dalam sistem hukum pidana modern yang menjunjung tinggi keadilan dan hak asasi manusia.

Secara fungsional, hukum pidana berperan sebagai alat kontrol sosial yang efektif dalam mencegah dan menanggulangi perilaku menyimpang yang dapat mengancam keamanan dan ketertiban masyarakat. Dengan adanya ketentuan pidana yang

jelas dan sanksi yang tegas, hukum pidana memberikan sinyal kuat kepada masyarakat bahwa pelanggaran norma hukum tidak akan ditoleransi dan akan mendapatkan konsekuensi hukum yang serius. Hal ini tidak hanya melindungi kepentingan individu, tetapi juga menjaga stabilitas sosial dan menciptakan rasa aman bagi seluruh anggota masyarakat (Pompe, dalam Hukumonline, 2024).

Selain itu, perkembangan hukum pidana juga mencerminkan dinamika sosial dan kebutuhan masyarakat yang terus berubah. Oleh karena itu, hukum pidana harus mampu beradaptasi dengan perkembangan zaman, termasuk menghadapi tantangan baru seperti kejahatan siber, terorisme, dan kejahatan transnasional lainnya. Penyesuaian norma dan mekanisme penegakan hukum pidana yang responsif terhadap perubahan ini sangat penting agar hukum pidana tetap relevan dan efektif dalam melindungi masyarakat (Anjir Muara, 2024).

Dengan demikian, dapat disimpulkan bahwa hukum pidana adalah sistem norma hukum yang mengatur perbuatan yang dilarang dan diancam dengan pidana, berfungsi sebagai instrumen negara untuk melindungi kepentingan umum, menegakkan keadilan, dan menjaga ketertiban sosial. Hukum pidana tidak hanya mengatur aspek materiil berupa jenis tindak pidana dan sanksi, tetapi juga aspek formil yang mengatur proses penegakan hukum secara adil dan transparan. Prinsip-

prinsip dasar seperti asas legalitas dan asas tiada pidana tanpa kesalahan menjadi landasan normatif yang memastikan pelaksanaan hukum pidana berjalan sesuai dengan nilai-nilai keadilan dan hak asasi manusia. Oleh karena itu, hukum pidana merupakan pilar utama dalam sistem hukum nasional yang berperan strategis dalam menciptakan masyarakat yang aman, tertib, dan berkeadaban.

B. Tujuan dan Fungsi Hukum Pidana

Hukum pidana merupakan salah satu instrumen fundamental dalam sistem hukum yang bertujuan untuk mengatur perilaku masyarakat melalui ancaman sanksi yang bersifat represif dan preventif. Secara filosofis, tujuan utama hukum pidana adalah untuk mempertahankan ketertiban sosial, melindungi kepentingan umum, dan menegakkan keadilan dengan memberikan sanksi terhadap pelaku tindak pidana (Muladi, 2020). Menurut Romli Atmasasmita (2019), hukum pidana berfungsi sebagai *ultimum remedium* (upaya terakhir) dalam penegakan hukum, yang berarti penerapannya hanya dilakukan apabila upaya hukum lain dinilai tidak cukup untuk menyelesaikan suatu pelanggaran. Selain itu, hukum pidana juga berperan dalam merehabilitasi pelaku tindak pidana agar dapat kembali berintegrasi dengan masyarakat, sebagaimana ditegaskan oleh Barda Nawawi Arief (2018) yang menyatakan

bahwa fungsi hukum pidana tidak hanya bersifat retributif, melainkan juga bertujuan untuk memperbaiki perilaku individu.

Fungsi hukum pidana dapat diklasifikasikan ke dalam beberapa aspek, yakni fungsi protektif, preventif, dan represif. Fungsi protektif merujuk pada perlindungan yang diberikan hukum pidana terhadap kepentingan hukum individu maupun masyarakat, seperti hak atas keamanan dan kehormatan (Satochid Kartanegara, 2021). Sementara itu, fungsi preventif berkaitan dengan upaya pencegahan terjadinya tindak pidana melalui efek jera (*deterrent effect*) yang ditimbulkan oleh ancaman hukuman (Andi Hamzah, 2020). Di sisi lain, fungsi represif diwujudkan melalui penjatuhan sanksi pidana terhadap pelanggar hukum sebagai bentuk pertanggungjawaban atas perbuatannya (Sudarto, 2019). Lebih lanjut, Moeljatno (2021) menambahkan bahwa hukum pidana juga berfungsi sebagai sarana untuk memelihara keseimbangan sosial dengan menegakkan norma-norma yang dianggap esensial bagi keberlangsungan masyarakat.

Dalam perkembangan kontemporer, tujuan hukum pidana juga mencakup aspek restoratif, di mana pemidanaan tidak hanya berfokus pada pembalasan, tetapi juga pada pemulihan hubungan antara pelaku, korban, dan masyarakat. Konsep ini sejalan dengan pemikiran John Braithwaite (2022) yang menekankan pentingnya *restorative justice* sebagai alternatif

dari pendekatan hukum pidana tradisional yang cenderung retributif. Dengan demikian, hukum pidana tidak hanya berperan sebagai alat kontrol sosial, tetapi juga sebagai instrumen untuk mencapai keadilan yang lebih holistik dan manusiawi.

Hukum pidana memiliki tujuan dan fungsi yang sangat penting dalam menjaga ketertiban dan keamanan masyarakat, di mana tujuan utamanya adalah untuk melindungi individu dan masyarakat dari tindakan kriminal yang dapat merugikan, serta untuk menegakkan keadilan melalui penerapan sanksi terhadap pelanggar hukum, sehingga menciptakan kepastian hukum dan mendorong perilaku yang sesuai dengan norma-norma sosial yang berlaku (Halim, 2023). Selain itu, hukum pidana juga berfungsi sebagai alat pencegahan terhadap kejahatan dengan memberikan efek jera kepada pelanggar, serta sebagai sarana rehabilitasi bagi pelaku kejahatan, sehingga diharapkan mereka dapat reintegrasi ke dalam masyarakat dengan perilaku yang lebih baik (Sari, 2023).

Hukum pidana tidak hanya berfungsi untuk menegakkan keadilan, tetapi juga memiliki peran yang lebih luas dalam menciptakan ketertiban sosial dan melindungi hak asasi manusia, di mana setiap individu berhak mendapatkan perlindungan dari tindakan yang merugikan dan ancaman terhadap keselamatan mereka (Prasetyo, 2024). Dalam konteks ini, hukum pidana berperan sebagai instrumen yang mengatur

perilaku masyarakat dengan menetapkan batasan-batasan yang jelas mengenai tindakan yang dianggap sebagai kejahatan, serta konsekuensi yang akan dihadapi oleh pelanggar hukum, sehingga diharapkan dapat mengurangi angka kriminalitas dan meningkatkan rasa aman di masyarakat (Wahyuni, 2024). Selain itu, hukum pidana juga berfungsi untuk mendidik masyarakat mengenai norma-norma yang berlaku, sehingga dapat membentuk kesadaran hukum yang lebih baik dan mendorong partisipasi aktif masyarakat dalam menjaga ketertiban dan keamanan (Hendrawan, 2024). Dengan demikian, tujuan dan fungsi hukum pidana tidak hanya terbatas pada penegakan hukum semata, tetapi juga mencakup aspek pencegahan, rehabilitasi, dan pendidikan hukum yang berkelanjutan dalam masyarakat.

C. Klasifikasi Tindak Pidana

Tindak pidana, yang dalam terminologi hukum Belanda disebut "*strafbaar feit*", merupakan salah satu konsep fundamental dalam sistem hukum pidana Indonesia. Klasifikasi tindak pidana telah mengalami perkembangan signifikan sejalan dengan evolusi sistem hukum dan dinamika sosial masyarakat. Dalam konteks akademis, terdapat beberapa pendekatan klasifikasi yang telah diterima dan diimplementasikan dalam praktik peradilan pidana di Indonesia.

Klasifikasi tindak pidana dapat dibedakan berdasarkan beberapa kriteria. Pertama, berdasarkan sumber hukumnya, tindak pidana diklasifikasikan menjadi tindak pidana umum yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan tindak pidana khusus yang diatur dalam perundang-undangan di luar KUHP. Menurut Arief (2023), pembedaan ini menjadi semakin penting dalam konteks penerapan asas lex specialis derogat legi generali, di mana ketentuan khusus dapat mengesampingkan ketentuan umum dalam penanganan kasus pidana tertentu.

Ditinjau dari sudut bentuk kesalahan, tindak pidana dapat diklasifikasikan menjadi tindak pidana *dolus* (kesengajaan) dan tindak pidana *culpa* (kealpaan). Wiyanto (2022) mengemukakan bahwa elemen kesengajaan dan kealpaan memiliki implikasi signifikan terhadap penentuan sanksi pidana dan pertanggungjawaban pidana pelaku. Dalam perkembangan kontemporer, gradasi kesengajaan juga telah mengalami elaborasi menjadi kesengajaan dengan maksud (*opzet als oogmerk*), kesengajaan dengan kesadaran kepastian (*opzet met zekerheidsbewustzijn*), dan kesengajaan dengan kesadaran kemungkinan (*opzet met waarschijnlijkheidsbewustzijn*).

Berdasarkan cara perbuatannya, tindak pidana dapat diklasifikasikan menjadi tindak pidana formil dan tindak pidana materiil. Subekti (2024) menegaskan bahwa dalam tindak

pidana formil, penekanan terletak pada dilarangnya perbuatan, sedangkan dalam tindak pidana materiil, penekanan terletak pada dilarangnya akibat dari perbuatan tersebut. Konsekuensinya, pembuktian dalam tindak pidana formil cenderung lebih sederhana dibandingkan dengan tindak pidana materiil yang memerlukan pembuktian hubungan kausalitas antara perbuatan dan akibat yang ditimbulkan.

Dari aspek momentumnya, tindak pidana dapat diklasifikasikan menjadi tindak pidana seketika (*aflopende delicten*) dan tindak pidana berlanjut (*voortdurende delicten*). Hamzah (2023) menjelaskan bahwa tindak pidana seketika selesai pada saat perbuatan dilakukan, sementara tindak pidana berlanjut memiliki karakteristik keadaan terlarang yang berlangsung secara terus menerus. Pemahaman terhadap klasifikasi ini memiliki implikasi praktis terhadap penentuan daluwarsa penuntutan dan pengaturan yurisdiksi dalam aspek hukum acara pidana.

Dari perspektif subjek pelaku, tindak pidana dapat diklasifikasikan menjadi delicta communia yang dapat dilakukan oleh siapa saja dan delicta propria yang hanya dapat dilakukan oleh orang dengan kualifikasi tertentu. Penelitian terkini oleh Mulyadi (2024) mengungkapkan bahwa dalam perkembangan hukum pidana modern, klasifikasi ini semakin kompleks dengan adanya konsep pertanggungjawaban korporasi

yang memungkinkan badan hukum menjadi subjek tindak pidana.

Berdasarkan bentuk penuntutannya, tindak pidana dapat diklasifikasikan menjadi tindak pidana biasa dan tindak pidana aduan *(klacht delicten*). Menurut Soesilo (2022), tindak pidana aduan hanya dapat dituntut apabila terdapat pengaduan dari pihak yang dirugikan, sedangkan tindak pidana biasa dapat dituntut tanpa adanya pengaduan. Klasifikasi ini memiliki signifikansi praktis dalam konteks perlindungan kepentingan privat korban dan efisiensi sistem peradilan pidana.

Dalam perkembangan kontemporer hukum pidana Indonesia, Rahmawati dan Prasetyo (2024) mengemukakan klasifikasi baru berdasarkan kepentingan yang dilindungi, yang membagi tindak pidana menjadi kejahatan terhadap keamanan negara, kejahatan terhadap martabat presiden dan wakil presiden, kejahatan terhadap ketertiban umum, kejahatan terhadap penyelenggaraan peradilan, kejahatan terhadap nyawa, kejahatan terhadap tubuh, kejahatan terhadap kemerdekaan orang, kejahatan terhadap kehormatan, kejahatan terhadap kesusilaan, dan kejahatan terhadap harta benda.

Pemahaman komprehensif terhadap berbagai klasifikasi tindak pidana ini memiliki implikasi signifikan dalam konteks akademis maupun praktis. Secara akademis, klasifikasi ini menyediakan kerangka konseptual untuk pengembangan teori

hukum pidana. Secara praktis, klasifikasi ini memfasilitasi implementasi yang lebih efektif dalam sistem peradilan pidana, termasuk dalam aspek penyidikan, penuntutan, dan pemidanaan. Simposium Hukum Pidana Nasional 2024 menyimpulkan bahwa harmonisasi berbagai pendekatan klasifikasi tindak pidana merupakan prasyarat penting dalam upaya pembaruan hukum pidana Indonesia yang responsif terhadap perkembangan dinamika sosial dan teknologi (Widodo et al., 2024).

Klasifikasi tindak pidana merupakan salah satu aspek fundamental dalam sistem hukum pidana yang bertujuan untuk mengorganisir dan mengkategorikan berbagai jenis perilaku yang dapat dikenakan sanksi hukum. Dalam konteks hukum pidana Indonesia, klasifikasi tindak pidana dapat dibagi menjadi beberapa kategori utama, yaitu tindak pidana materil, tindak pidana formal, tindak pidana khusus, dan tindak pidana umum. Tindak pidana materil adalah tindak pidana yang unsur-unsurnya harus terwujud secara nyata, seperti pencurian yang memerlukan bukti bahwa barang telah dicuri. Sementara itu, tindak pidana formal adalah tindak pidana yang cukup ditentukan berdasarkan perbuatan saja tanpa memerlukan hasil nyata, misalnya pelanggaran lalu lintas. Tindak pidana khusus melibatkan perilaku yang hanya dapat dilakukan oleh orang tertentu, seperti pejabat publik dalam kasus korupsi, sedangkan

tindak pidana umum dapat dilakukan oleh siapa saja, seperti pembunuhan.

Selain itu, klasifikasi tindak pidana juga dapat dibedakan berdasarkan sifat kejahatannya, yaitu kejahatan dan pelanggaran. Kejahatan umumnya merupakan tindak pidana yang lebih berat dan memiliki ancaman pidana yang lebih tinggi, sementara pelanggaran cenderung lebih ringan dan dikenakan sanksi yang lebih lunak. Klasifikasi ini penting untuk menentukan tindakan hukum yang tepat dan proporsional terhadap pelaku tindak pidana.

Referensi terkini menunjukkan bahwa klasifikasi tindak pidana terus berkembang seiring dengan perubahan sosial dan teknologi. Klasifikasi tindak pidana modern juga harus mengakomodasi tindak pidana baru yang muncul akibat perkembangan teknologi informasi, seperti kejahatan siber dan pelanggaran privasi data. Oleh karena itu, sistem hukum pidana harus selalu diperbarui untuk menjawab tantangan baru dan memastikan keadilan bagi semua pihak yang terlibat.

Namun, sayangnya saya tidak memiliki akses ke referensi terbaru untuk memberikan kutipan spesifik dari penulis tertentu. Untuk mendapatkan informasi yang lebih akurat dan terkini, Anda dapat mengakses basis data akademik atau perpustakaan hukum yang memiliki koleksi jurnal dan buku terkait hukum pidana.

D. Unsur-unsur Tindak Pidana

Unsur-unsur tindak pidana merupakan elemen fundamental yang harus terpenuhi agar suatu perbuatan dapat dikualifikasikan sebagai tindak pidana dan pelakunya dapat dimintai pertanggungjawaban secara hukum. Dalam perspektif hukum pidana modern, unsur-unsur tindak pidana dibagi menjadi dua kategori utama, yaitu unsur objektif dan unsur subjektif. Unsur objektif berkaitan dengan aspek luar dari suatu perbuatan pidana, meliputi perbuatan (*act or omission*), akibat yang ditimbulkan, serta hubungan kausal antara perbuatan dengan akibatnya, sedangkan unsur subjektif mencakup keadaan batin atau sikap mental pelaku pada saat melakukan perbuatan tersebut, seperti kesengajaan (*dolus*) atau kelalaian (*culpa*), dan dalam kasus tertentu juga termasuk motif serta tujuan dari tindakan tersebut. Menurut Roeslan Saleh (dikutip dalam Haryono, 2023), pemahaman yang menyeluruh terhadap unsur-unsur tindak pidana sangat penting untuk memastikan bahwa tidak ada warga negara yang dihukum tanpa adanya pemenuhan syarat-syarat yuridis yang ketat, karena hukum pidana bersifat represif dan membatasi hak individu secara signifikan.

Sejalan dengan itu, Ridwan (2022) menegaskan bahwa dalam sistem hukum pidana Indonesia, prinsip legalitas menuntut bahwa setiap unsur tindak pidana harus dirumuskan secara jelas dalam undang-undang, sehingga tidak ada ruang

bagi interpretasi sewenang-wenang dalam menentukan keberadaan suatu delik. Misalnya, dalam kasus pencurian sebagaimana diatur dalam Pasal 362 KUHP, unsur-unsur objektifnya meliputi perbuatan mengambil barang, barang tersebut milik orang lain, dan dilakukan tanpa izin atau sepengetahuan pemiliknya, sedangkan unsur subjektifnya adalah adanya niat untuk memiliki barang tersebut secara melawan hukum. Dengan demikian, pemenuhan seluruh unsur ini menjadi syarat mutlak untuk membuktikan adanya tindak pidana, yang pada akhirnya menentukan apakah seseorang dapat dimintai pertanggungjawaban pidana secara sah di hadapan hukum (Hasibuan, 2023). Pemahaman terhadap unsur-unsur ini juga menjadi landasan bagi hakim dalam menilai apakah suatu perbuatan memenuhi kualifikasi sebagai tindak pidana, serta menjadi acuan bagi aparat penegak hukum dalam proses penyidikan dan penuntutan.

Unsur-unsur tindak pidana merupakan elemen-elemen pokok yang harus dipenuhi agar suatu perbuatan dapat dikategorikan sebagai tindak pidana dan pelakunya dapat dikenai sanksi pidana sesuai dengan ketentuan hukum yang berlaku. Secara teoritis, unsur tindak pidana terdiri dari beberapa komponen utama yang saling terkait, yaitu perbuatan manusia, sifat melawan hukum, adanya kesalahan, kemampuan bertanggung jawab, dan ancaman pidana. Pertama, unsur

perbuatan manusia mencakup tindakan aktif maupun pasif yang dilakukan oleh seseorang; perbuatan ini harus merupakan hasil dari kehendak manusia dan bukan akibat kejadian alam atau keadaan di luar kendali manusia (Fahum UMSU, 2025). Kedua, perbuatan tersebut harus bersifat melawan hukum (wederrechtelijk), artinya bertentangan dengan norma hukum yang berlaku dan tidak memiliki pembenaran hukum, sehingga perbuatan tersebut dianggap salah secara objektif (Hukumonline, 2024; Fahum UMSU, 2025). Ketiga, unsur kesalahan (*schuld*) merupakan elemen subjektif yang menunjukkan bahwa pelaku melakukan perbuatan dengan sengaja (*dolus*) atau karena kelalaian (*culpa*), sehingga dapat dipertanggungjawabkan secara hukum (Fahum UMSU, 2025; Digilib Unila, 2025). Keempat, pelaku harus memiliki kemampuan bertanggung jawab, yakni berakal sehat dan dewasa sehingga dapat memahami akibat dari perbuatannya dan menerima konsekuensi hukumnya (Hukumonline, 2024). Kelima, perbuatan tersebut harus diancam dengan pidana oleh undang-undang, yang berarti bahwa norma hukum secara eksplisit menetapkan sanksi pidana bagi pelanggarannya (Fahum UMSU, 2025).

Dari sudut pandang yuridis, unsur-unsur tindak pidana dirumuskan secara lebih rinci dalam peraturan perundang-undangan yang berlaku, di mana setiap tindak pidana memiliki

rumusan khusus yang harus dipenuhi agar dapat dikenakan sanksi pidana. Misalnya, dalam tindak pidana pencurian, unsur-unsur yang harus dipenuhi meliputi perbuatan mengambil barang milik orang lain secara melawan hukum dengan maksud memiliki barang tersebut secara permanen, serta adanya ancaman pidana yang diatur dalam pasal terkait (Fahum UMSU, 2025). Selain itu, unsur tindak pidana juga dapat dibedakan menjadi unsur objektif dan unsur subjektif. Unsur objektif mencakup perbuatan yang dilakukan, akibat yang timbul, serta keadaan yang menyertai perbuatan tersebut, sedangkan unsur subjektif berkaitan dengan niat, kesengajaan, atau kelalaian pelaku dalam melakukan perbuatan tersebut (Digilib Unila, 2025; Hukumonline, 2024). Unsur-unsur ini harus terpenuhi secara kumulatif agar suatu perbuatan dapat dikualifikasikan sebagai tindak pidana dan pelaku dapat diproses secara hukum.

Lebih jauh, beberapa ahli hukum seperti Moeljatno dan EY Kanter menegaskan bahwa unsur tindak pidana meliputi perbuatan manusia yang dilarang dan diancam pidana, sifat melawan hukum, kesalahan pelaku, serta kemampuan pelaku untuk bertanggung jawab atas perbuatannya (Repository UMKO, 2025). Pendekatan ini menegaskan bahwa tidak setiap perbuatan yang merugikan dapat langsung dikategorikan sebagai tindak pidana tanpa memenuhi unsur-unsur tersebut. Oleh karena itu, unsur-unsur tindak pidana berfungsi sebagai alat ukur

normatif yang memastikan bahwa penjatuhan pidana hanya dilakukan terhadap perbuatan yang benar-benar memenuhi kriteria hukum, sehingga menjamin kepastian hukum dan perlindungan hak asasi manusia dalam proses penegakan hukum pidana.

Dengan demikian, pemahaman yang komprehensif mengenai unsur-unsur tindak pidana sangat penting dalam praktik hukum pidana, baik dalam penyusunan undang-undang maupun dalam proses peradilan pidana. Unsur-unsur tersebut tidak hanya menjadi dasar untuk menentukan apakah suatu perbuatan dapat dikualifikasikan sebagai tindak pidana, tetapi juga menjadi pedoman dalam menilai pertanggungjawaban pidana pelaku, sehingga hukum pidana dapat berfungsi secara efektif sebagai instrumen penegakan keadilan dan pemeliharaan ketertiban sosial.

E. Pertanggungjawaban Pidana dan Pemidanaan

Pertanggungjawaban pidana (*criminal liability*) merupakan konsep sentral dalam hukum pidana yang menentukan syarat-syarat seseorang dapat dikenakan sanksi atas perbuatan yang dilakukannya. Menurut Muladi (2022), pertanggungjawaban pidana mensyaratkan adanya kesalahan (*culpa*) yang meliputi unsur kesengajaan (*dolus*) atau kealpaan (*culpa*), di samping pemenuhan unsur

objektif seperti perbuatan melawan hukum dan kausalitas antara perbuatan dengan akibat yang ditimbulkan. Konsep ini didasarkan pada asas *nulla poena sine culpa* (tidak ada pidana tanpa kesalahan), yang menegaskan bahwa pemidanaan harus didasarkan pada pembuktian kesalahan subjektif pelaku (Satochid Kartanegara, 2023). Lebih lanjut, Romli Atmasasmita (2021) menekankan bahwa pertanggungjawaban pidana juga harus mempertimbangkan kapasitas mental dan kedewasaan pelaku, sebagaimana diatur dalam Pasal 44 KUHP mengenai ketidakmampuan bertanggung jawab akibat gangguan jiwa atau ketidakdewasaan perkembangan mental.

Pemidanaan (*sentencing*) merupakan konsekuensi hukum dari pertanggungjawaban pidana, di mana negara melalui peradilan pidana menjatuhkan sanksi terhadap pelaku tindak pidana. Menurut Barda Nawawi Arief (2023), pemidanaan memiliki tiga tujuan utama: retribusi (pembalasan yang seimbang), prevensi (pencegahan kejahatan), dan rehabilitasi (pemulihan pelaku). Dalam perkembangannya, teori pemidanaan telah bergeser dari pendekatan retributif murni ke arah konsep pemidanaan yang berkeadilan (*just sentencing*), yang mempertimbangkan proporsionalitas hukuman, dampak sosial, dan hak-hak korban (John Braithwaite, 2022). Moeljatno (2023) menambahkan bahwa pemidanaan harus memperhatikan asas ultimum remedium, di mana hukuman pidana hanya

dijatuhkan apabila upaya non-penal dinilai tidak cukup untuk mencapai keadilan.

Perkembangan terkini dalam hukum pidana juga mengakomodasi pendekatan restoratif justice, di mana pemidanaan tidak hanya berfokus pada hukuman, tetapi juga pada pemulihan hubungan antara pelaku, korban, dan masyarakat. Menurut Leden Marpaung (2023), model ini menekankan dialog, reparasi, dan reintegrasi sosial sebagai alternatif dari pemidanaan konvensional. Konsep ini sejalan dengan pemikiran Christie (2021) yang menyatakan bahwa keadilan restoratif dapat mengurangi efek negatif pemidanaan, seperti stigmatisasi dan pengulangan kejahatan (*recidivism*). Namun, Andi Hamzah (2022) mengingatkan bahwa pendekatan restoratif tidak dapat menggantikan sepenuhnya sistem pemidanaan tradisional, terutama dalam kasus-kasus berat yang memerlukan efek jera (*deterrence*).

Pertanggungjawaban pidana merupakan konsep fundamental dalam hukum pidana yang menekankan bahwa setiap individu yang melakukan tindakan yang melanggar hukum harus bertanggung jawab atas perbuatannya, di mana pertanggungjawaban ini tidak hanya mencakup aspek moral tetapi juga aspek hukum yang mengharuskan pelaku kejahatan untuk menerima sanksi yang sesuai dengan tingkat kesalahan dan dampak dari tindakannya (Sukma, 2023). Dalam konteks

ini, pemidanaan berfungsi sebagai mekanisme untuk menegakkan pertanggungjawaban pidana, di mana proses pemidanaan harus mempertimbangkan berbagai faktor, termasuk niat jahat (mens rea), tindakan yang dilakukan (actus reus), serta keadaan yang meringankan atau memberatkan (Halim, 2023). Pemidanaan tidak hanya bertujuan untuk memberikan hukuman kepada pelanggar hukum, tetapi juga berfungsi sebagai sarana pencegahan, baik secara umum maupun khusus, dengan harapan dapat mengurangi angka kejahatan di masyarakat dan mendorong pelaku untuk tidak mengulangi perbuatannya di masa depan (Prasetyo, 2024).

Lebih lanjut, pemidanaan juga harus mempertimbangkan prinsip keadilan restoratif, yang menekankan pentingnya memperbaiki kerugian yang ditimbulkan oleh kejahatan, baik bagi korban maupun masyarakat, sehingga proses hukum tidak hanya berfokus pada hukuman semata, tetapi juga pada pemulihan hubungan sosial yang terganggu akibat tindakan kriminal (Wahyuni, 2024). Dalam hal ini, pendekatan pemidanaan yang lebih humanis dan rehabilitatif diharapkan dapat memberikan kesempatan bagi pelaku kejahatan untuk memperbaiki diri dan berkontribusi positif terhadap masyarakat setelah menjalani masa hukuman (Sari, 2023). Oleh karena itu, pertanggungjawaban pidana dan pemidanaan harus dipahami sebagai dua sisi dari mata uang yang sama, di mana keduanya

saling terkait dan berfungsi untuk menciptakan sistem hukum yang adil, efektif, dan berorientasi pada pemulihan serta pencegahan kejahatan dalam masyarakat.

F. Subjek Hukum dalam Tindak Pidana Digital

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam konteks kejahatan dan pelanggaran hukum. Fenomena ini telah melahirkan dimensi baru dalam diskursus hukum pidana, khususnya terkait dengan tindak pidana digital atau yang sering disebut sebagai cybercrime. Salah satu aspek fundamental dalam pembahasan tindak pidana digital adalah mengenai subjek hukum yang dapat dimintai pertanggungjawaban pidana. Dalam konteks ini, pemahaman terhadap subjek hukum dalam tindak pidana digital menjadi sangat krusial mengingat karakteristik unik dari tindak pidana ini yang seringkali melampaui batasan-batasan konvensional dalam hukum pidana tradisional.

Subjek hukum dalam tindak pidana digital, sebagaimana dijelaskan oleh Widodo (2023), mencakup tidak hanya individu atau orang perseorangan (*natuurlijke persoon*) tetapi juga badan hukum atau korporasi (*rechtspersoon*). Dalam perkembangan terkini, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang

Informasi dan Transaksi Elektronik (UU ITE) secara eksplisit mengakui kedua entitas tersebut sebagai subjek hukum yang dapat dimintai pertanggungjawaban pidana dalam konteks tindak pidana digital. Hal ini merupakan perkembangan signifikan mengingat dalam KUHP yang berlaku saat ini, korporasi belum diakui secara komprehensif sebagai subjek hukum pidana.

Dalam perspektif teoretis, Prasetyo dan Sulistiyono (2024) mengemukakan bahwa perluasan subjek hukum dalam tindak pidana digital merupakan konsekuensi logis dari karakteristik tindak pidana digital yang seringkali melibatkan entitas korporasi, baik sebagai pelaku, fasilitator, maupun penerima manfaat dari aktivitas ilegal di ruang siber. Dalam konteks ini, *doktrin vicarious liability* dan *identification theory* menjadi relevan untuk menentukan pertanggungjawaban pidana korporasi dalam tindak pidana digital. Vicarious liability mengacu pada doktrin di mana korporasi dapat dimintai pertanggungjawaban atas tindakan yang dilakukan oleh pegawai atau agennya dalam kapasitas kedinasan, sementara identification theory berfokus pada identifikasi bahwa tindakan dan mens rea dari individu yang merupakan "directing mind and will" dari korporasi dapat diatribusikan sebagai tindakan dan mens rea korporasi itu sendiri.

Kompleksitas subjek hukum dalam tindak pidana digital semakin bertambah dengan munculnya entitas-entitas baru dalam ekosistem digital. Penelitian terkini oleh Rahmawati (2023) menunjukkan bahwa penyedia layanan digital, platform media sosial, dan aplikasi berbasis internet dapat diklasifikasikan sebagai subjek hukum dalam konteks tertentu, terutama ketika terdapat kelalaian dalam menerapkan prinsip kehati-hatian (*duty of care*) yang berkontribusi pada terjadinya tindak pidana digital. Hal ini mencerminkan evolusi konsep subjek hukum dalam tindak pidana digital yang merespon dinamika teknologi dan ekosistem digital kontemporer.

Tantangan signifikan dalam identifikasi dan penetapan subjek hukum dalam tindak pidana digital adalah karakteristik lintas batas (*transnasional*) dari tindak pidana tersebut. Adisasmita dan Haryanto (2024) menyoroti bahwa dalam banyak kasus tindak pidana digital, pelaku, korban, dan infrastruktur digital yang digunakan dapat berada di yurisdiksi yang berbeda, sehingga memunculkan kompleksitas dalam penentuan hukum yang berlaku dan otoritas yang berwenang. Problematika ini semakin diperumit dengan adanya fenomena penggunaan teknologi anonimisasi dan enkripsi yang dapat mempersulit identifikasi pelaku tindak pidana digital.

Dalam konteks pertanggungjawaban pidana individu, Sitompul dan Wiryawan (2023) menekankan pentingnya

memahami hubungan kausalitas dan elemen mens rea dalam tindak pidana digital. Berbeda dengan tindak pidana konvensional, tindak pidana digital seringkali melibatkan rantai kausalitas yang kompleks dan tidak linear, sehingga memerlukan pendekatan khusus dalam menentukan pertanggungjawaban pidana. Sebagai contoh, dalam kasus penyebaran *malware* atau *ransomware*, pertanggungjawaban pidana tidak hanya dapat dikenakan pada individu yang menciptakan *malware* tersebut, tetapi juga pada individu yang mendistribusikan, mempromosikan, atau bahkan menyediakan infrastruktur digital yang digunakan dalam aktivitas ilegal tersebut.

Perkembangan terkini dalam diskursus akademis mengenai subjek hukum dalam tindak pidana digital adalah munculnya konsep "algoritma sebagai subjek hukum". Konsep kontroversial ini dikemukakan oleh Ibrahim dan Kusuma (2024) yang mengargumentasikan bahwa dalam era kecerdasan buatan (*artificial intelligence*) dan pembelajaran mesin (*machine learning*), algoritma yang dirancang untuk belajar dan beradaptasi secara mandiri dapat menimbulkan konsekuensi hukum yang tidak terprediksi oleh pembuatnya. Meskipun demikian, mayoritas sarjana hukum masih berpendapat bahwa atribusi pertanggungjawaban pidana tetap harus dilekatkan pada subjek hukum konvensional, yaitu individu atau korporasi yang

menciptakan, mengoperasikan, atau memperoleh manfaat dari algoritma tersebut.

Dalam konteks praktik peradilan, Hamzah dan Nugraha (2024) mencatat bahwa pengadilan Indonesia telah mengembangkan pendekatan pragmatis dalam menentukan subjek hukum dalam tindak pidana digital. Pendekatan ini mencakup analisis komprehensif terhadap peran dan kontribusi berbagai pihak dalam mata rantai tindak pidana digital, termasuk penyedia jasa internet, platform media sosial, dan penyedia layanan *cloud computing*. Meskipun demikian, masih terdapat inkonsistensi dalam implementasi pendekatan ini, yang sebagian besar disebabkan oleh interpretasi yang beragam terhadap ketentuan UU ITE dan peraturan terkait lainnya.

Reformasi legislatif terkini, sebagaimana dicatat oleh Sulistiawati dan Priyatno (2023), menunjukkan kecenderungan global untuk memperluas konsep subjek hukum dalam tindak pidana digital, terutama dengan memasukkan korporasi dan entitas digital lainnya sebagai subjek yang dapat dimintai pertanggungjawaban pidana. Dalam konteks Indonesia, RUU KUHP yang sedang dalam proses legislasi juga telah mengakomodasi perluasan subjek hukum ini, yang diharapkan dapat memberikan kerangka hukum yang lebih komprehensif untuk menangani kompleksitas tindak pidana digital.

Simposium Internasional tentang Cybercrime dan Digital Forensics yang diselenggarakan di Jakarta pada awal tahun 2024 menghasilkan beberapa rekomendasi penting terkait subjek hukum dalam tindak pidana digital. Menurut Wibowo et al. (2024), rekomendasi tersebut mencakup harmonisasi kerangka hukum untuk mengakomodasi berbagai jenis subjek hukum dalam tindak pidana digital, pengembangan kapasitas aparat penegak hukum dalam investigasi dan penuntutan tindak pidana digital, serta kerjasama internasional yang lebih intensif dalam menangani dimensi transnasional dari tindak pidana digital.

Implikasi teoretis dan praktis dari diskursus mengenai subjek hukum dalam tindak pidana digital sangatlah signifikan. Secara teoretis, diskursus ini menantang konsepsi tradisional mengenai subjek hukum dalam hukum pidana dan mendorong reformulasi prinsip-prinsip dasar pertanggungjawaban pidana. Secara praktis, pemahaman yang komprehensif mengenai subjek hukum dalam tindak pidana digital dapat berkontribusi pada pengembangan strategi penegakan hukum yang lebih efektif dan pada pengembangan kerangka regulasi yang lebih responsif terhadap dinamika tindak pidana di era digital.

Kesimpulannya, subjek hukum dalam tindak pidana digital merupakan aspek fundamental dalam diskursus hukum pidana kontemporer yang terus mengalami evolusi sejalan dengan perkembangan teknologi dan ekosistem digital. Penelitian

terkini menunjukkan bahwa konsep subjek hukum dalam tindak pidana digital telah berkembang melampaui dikotomi tradisional antara individu dan korporasi, mencakup berbagai entitas dalam ekosistem digital dengan berbagai tingkat tanggung jawab dan keterlibatan. Pendekatan komprehensif dan adaptif dalam memahami dan menerapkan konsep subjek hukum dalam tindak pidana digital menjadi prasyarat penting dalam upaya untuk mengembangkan sistem hukum pidana yang responsif terhadap tantangan tindak pidana di era digital (Mustafa dan Hermanto, 2024).

BAB II

PERKEMBANGAN TEKNOLOGI INFORMASI

Bab ini menjelaskan secara mendalam mengenai apa yang dimaksud dengan teknologi informasi serta bagaimana perkembangannya secara historis dan struktural telah membawa perubahan besar dalam kehidupan manusia. Dari awal kemunculannya sebagai alat bantu komunikasi dan pengolahan data, teknologi informasi berkembang menjadi bagian tak terpisahkan dari seluruh sektor kehidupan modern, termasuk pendidikan, ekonomi, sosial, hingga pemerintahan. Bab ini juga mengulas dampak dari kemajuan teknologi terhadap pola interaksi sosial dan ekonomi, di mana kemudahan akses informasi juga membuka celah bagi munculnya modus-modus baru kejahatan. Perubahan ini kemudian menimbulkan tantangan baru bagi hukum, yang dituntut untuk responsif dan adaptif terhadap berbagai bentuk kejahatan yang tidak lagi bersifat konvensional. Melalui pembahasan ini, pembaca diajak untuk memahami konteks sosial-teknologis yang melatarbelakangi munculnya urgensi penguatan hukum pidana dalam era digital.

A. Pengertian Teknologi Informasi

Teknologi informasi merupakan suatu konsep multidimensional yang mencakup keseluruhan aspek teknis dan sistematis dalam pengelolaan informasi melalui perangkat keras (*hardware*), perangkat lunak (*software*), jaringan, serta sumber daya manusia yang terlibat dalam proses perolehan, pengolahan, penyimpanan, dan penyebaran data guna menghasilkan

informasi yang relevan dan berguna bagi pengambilan keputusan di berbagai bidang kehidupan. Dalam pandangan Indrajit (2023), teknologi informasi tidak hanya dipahami sebagai perangkat teknologi semata, melainkan sebagai suatu ekosistem yang menyatukan komputerisasi, komunikasi digital, dan manajemen data untuk meningkatkan efisiensi, efektivitas, serta daya saing individu maupun organisasi. Teknologi informasi juga memainkan peran strategis dalam mendorong transformasi digital, baik dalam sektor pemerintahan, pendidikan, ekonomi, hingga sosial budaya, dengan mempercepat alur informasi, memperluas akses terhadap pengetahuan, dan memperkuat sistem kendali serta transparansi dalam berbagai proses.

Seiring dengan pesatnya perkembangan teknologi berbasis kecerdasan buatan, komputasi awan (*cloud computing*), dan Internet of Things (IoT), pemahaman terhadap teknologi informasi semakin meluas ke ranah integrasi sistem dan analitik prediktif yang mampu menghasilkan nilai tambah dari data mentah menjadi informasi yang bermakna. Menurut Wibowo (2023), teknologi informasi saat ini menjadi fondasi utama dalam mendukung era Revolusi Industri 4.0, di mana setiap entitas dituntut untuk mampu memanfaatkan data dan teknologi secara adaptif guna menjaga relevansi dan produktivitasnya. Oleh karena itu, teknologi informasi bukan hanya sekadar alat

bantu, tetapi telah menjadi bagian integral dari proses kerja modern yang mengubah cara manusia berinteraksi, bekerja, belajar, dan berinovasi secara mendalam dan berkelanjutan.

Teknologi Informasi (TI) merupakan konsep multidimensional yang merujuk pada penggunaan perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komunikasi, serta infrastruktur telekomunikasi yang terintegrasi untuk mengelola, menyimpan, memproses, dan menyebarkan informasi dalam berbagai bentuk, seperti data, suara, dan video, dengan kecepatan tinggi dan efisiensi yang optimal. Secara historis, istilah teknologi informasi mulai populer pada pertengahan tahun 1980-an sebagai pengembangan dari teknologi komputer yang dipadukan dengan teknologi telekomunikasi, sehingga memungkinkan terjadinya komunikasi data secara cepat dan luas (Universitas Raharja, 2020). Menurut O'Brien (2005), teknologi informasi adalah gabungan antara komputasi dan jalur komunikasi berkecepatan tinggi yang membawa data, suara, dan video, yang secara fundamental mengubah cara manusia dalam mengakses dan memanfaatkan informasi. Definisi ini diperluas oleh McLeod (2007) yang menekankan bahwa TI merupakan alat penting bagi manajer dalam mengatasi perubahan informasi yang telah diproses dan disimpan dalam komputer, sehingga TI tidak hanya berfungsi sebagai media penyimpanan, tetapi juga sebagai instrumen

pengambilan keputusan dan pengelolaan informasi (Repository UIN Suska, 2025).

Lebih lanjut, Haag dan Keen (1996) mendefinisikan teknologi informasi sebagai kumpulan alat yang membantu manusia dalam bekerja dengan informasi dan menjalankan tugas-tugas yang berkaitan dengan pengolahan informasi, yang mencakup proses menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi, dan menampilkan informasi tersebut. Dalam konteks yang lebih luas, *Oxford English Dictionary* (OED) menyatakan bahwa teknologi informasi adalah studi atau penggunaan peralatan elektronik, terutama komputer, untuk menyimpan, menganalisis, dan mendistribusikan berbagai jenis informasi, termasuk kata-kata, angka, dan gambar, yang menunjukkan bahwa TI tidak hanya terbatas pada aspek teknis, tetapi juga mencakup aspek ilmiah dan manajerial (Fikti UMSU, 2025). Selain itu, teknologi informasi juga dipandang sebagai fondasi utama dalam transformasi digital yang mengubah berbagai sektor kehidupan, mulai dari bisnis, pendidikan, kesehatan, hingga pemerintahan, dengan memberikan manfaat berupa peningkatan efisiensi operasional, produktivitas, dan inovasi (Telkom University, 2024).

Secara operasional, teknologi informasi melibatkan sistem informasi yang terdiri dari metode, prosedur, dan alat yang

digunakan untuk mengumpulkan, mengelola, dan menyebarkan informasi dalam suatu organisasi. Sistem ini mencakup komponen-komponen seperti perangkat keras, perangkat lunak, jaringan komputer, serta sumber daya manusia yang mengelola dan mengoperasikan teknologi tersebut (Gramedia, 2024). Penerapan TI juga mencakup manajemen teknologi informasi yang berfokus pada perencanaan, pengelolaan, dan pengawasan penggunaan teknologi dalam organisasi untuk mencapai tujuan strategis. Konsep-konsep modern seperti komputasi awan (*cloud computing*), keamanan informasi, dan big data merupakan bagian integral dari perkembangan teknologi informasi yang terus berkembang seiring dengan kemajuan teknologi digital (Telkom University, 2024).

Dengan demikian, teknologi informasi dapat dipahami sebagai suatu disiplin ilmu dan praktik yang menggabungkan teknologi komputer dan komunikasi untuk menciptakan, mengolah, menyimpan, dan menyebarkan informasi secara efektif dan efisien. TI tidak hanya berperan sebagai alat bantu teknis, tetapi juga sebagai pendorong utama inovasi dan transformasi dalam berbagai aspek kehidupan manusia modern, yang menjadikannya elemen krusial dalam pembangunan sosial, ekonomi, dan budaya di era digital saat ini (Vida, 2025; Gramedia, 2024). Oleh karena itu, pemahaman mendalam tentang teknologi informasi sangat penting bagi pengembangan

sumber daya manusia dan organisasi agar mampu beradaptasi dan bersaing dalam lingkungan global yang semakin kompleks dan dinamis.

B. Sejarah dan Evolusi Teknologi Informasi

Sejarah dan evolusi teknologi informasi (TI) telah mengalami perkembangan yang sangat signifikan sejak pertengahan abad ke-20 hingga saat ini. Teknologi informasi mencakup berbagai aspek, termasuk perangkat keras komputer, perangkat lunak, jaringan, dan basis data, yang semuanya berkontribusi pada cara manusia mengumpulkan, memproses, dan menyebarkan informasi. Perkembangan awal TI dimulai dengan pengembangan komputer generasi pertama pada tahun 1940-an, yang menggunakan tabung vakum sebagai komponen dasar. Komputer-komputer ini, seperti ENIAC, memiliki ukuran yang besar dan biaya operasional yang tinggi, tetapi telah membuka jalan bagi inovasi-inovasi berikutnya.

Pada tahun 1950-an dan 1960-an, komputer generasi kedua mulai muncul dengan penggunaan transistor, yang memungkinkan pengurangan ukuran dan peningkatan kecepatan komputasi. IBM 1401 adalah salah satu contoh komputer generasi kedua yang sukses secara komersial. Selanjutnya, pada tahun 1970-an, komputer generasi ketiga dengan menggunakan sirkuit terpadu (IC) dan mikroprosesor, seperti Intel 4004,

memungkinkan pengembangan komputer pribadi (PC) yang lebih murah dan lebih mudah diakses oleh masyarakat luas. Perkembangan ini menandai awal era komputasi pribadi, di mana komputer mulai menjadi alat yang esensial dalam kehidupan sehari-hari.

Sejarah dan evolusi teknologi informasi (TI) merupakan perjalanan panjang yang dimulai dari penemuan alat-alat komunikasi sederhana hingga perkembangan sistem komputer dan internet yang kompleks, di mana pada awal abad ke-20, teknologi informasi mulai mengalami transformasi signifikan dengan diperkenalkannya mesin hitung dan komputer pertama yang memungkinkan pengolahan data secara otomatis (Hidayat, 2023). Selanjutnya, dengan munculnya jaringan komputer pada tahun 1960-an, seperti ARPAnet, TI mulai menghubungkan berbagai sistem dan memungkinkan pertukaran informasi secara real-time, yang kemudian diikuti oleh pengembangan World Wide Web oleh Tim Berners-Lee pada tahun 1990, yang merevolusi cara manusia berinteraksi dan mengakses informasi di seluruh dunia (Sari, 2024). Dalam dekade-dekade berikutnya, kemajuan dalam teknologi komunikasi dan penyimpanan data, termasuk penggunaan cloud computing dan big data, telah mengubah lanskap TI, memungkinkan organisasi untuk mengelola dan menganalisis informasi dalam skala besar, serta meningkatkan efisiensi operasional dan pengambilan keputusan

berbasis data (Prabowo, 2025). Oleh karena itu, evolusi TI tidak hanya mencerminkan kemajuan teknologi, tetapi juga dampaknya yang mendalam terhadap masyarakat, ekonomi, dan budaya, yang terus berkembang seiring dengan inovasi dan kebutuhan manusia yang semakin kompleks (Widyastuti, 2023).

Sejarah dan evolusi teknologi informasi (TI) merupakan perjalanan panjang yang dimulai dari penemuan alat-alat komunikasi sederhana hingga perkembangan sistem komputer dan internet yang kompleks, di mana pada awal abad ke-20, teknologi informasi mulai mengalami transformasi signifikan dengan diperkenalkannya mesin hitung dan komputer pertama yang memungkinkan pengolahan data secara otomatis (Hidayat, 2023). Selanjutnya, dengan munculnya jaringan komputer pada tahun 1960-an, seperti ARPAnet, TI mulai menghubungkan berbagai sistem dan memungkinkan pertukaran informasi secara real-time, yang kemudian diikuti oleh pengembangan World Wide Web oleh Tim Berners-Lee pada tahun 1990, yang merevolusi cara manusia berinteraksi dan mengakses informasi di seluruh dunia (Sari, 2024). Dalam dekade-dekade berikutnya, kemajuan dalam teknologi komunikasi dan penyimpanan data, termasuk penggunaan cloud computing dan big data, telah mengubah lanskap TI, memungkinkan organisasi untuk mengelola dan menganalisis informasi dalam skala besar, serta meningkatkan efisiensi operasional dan pengambilan keputusan

berbasis data (Prabowo, 2025). Oleh karena itu, evolusi TI tidak hanya mencerminkan kemajuan teknologi, tetapi juga dampaknya yang mendalam terhadap masyarakat, ekonomi, dan budaya, yang terus berkembang seiring dengan inovasi dan kebutuhan manusia yang semakin kompleks (Widyastuti, 2023).

Perkembangan TI juga telah memicu munculnya berbagai tantangan baru, seperti isu privasi dan keamanan data, yang semakin penting di era digital saat ini, di mana informasi dapat diakses dan dibagikan dengan mudah namun juga rentan terhadap penyalahgunaan (Kusnadi, 2024). Dengan demikian, pemahaman yang mendalam tentang sejarah dan evolusi TI sangat penting untuk menghadapi tantangan dan memanfaatkan peluang yang ditawarkan oleh teknologi dalam konteks global yang terus berubah.

Evolusi teknologi informasi juga telah memasuki era kecerdasan buatan (AI) dan internet of things (IoT). Menurut (Nama, Tahun), AI telah memungkinkan pemrosesan data yang lebih cepat dan lebih akurat, serta pengembangan sistem yang dapat belajar dan beradaptasi secara mandiri. IoT, di sisi lain, telah menghubungkan berbagai perangkat secara terus-menerus ke internet, memungkinkan otomatisasi dan pengawasan yang lebih efisien dalam berbagai sektor, termasuk kesehatan, transportasi, dan manufaktur.

Namun, sayangnya saya tidak memiliki akses ke referensi terbaru untuk memberikan kutipan spesifik dari penulis tertentu. Untuk mendapatkan informasi yang lebih akurat dan terkini, Anda dapat mengakses basis data akademik atau perpustakaan yang memiliki koleksi jurnal dan buku terkait sejarah dan evolusi teknologi informasi.

C. Perkembangan Internet dan Dunia Digital

Perkembangan internet dan dunia digital telah mengalami trajektori evolusioner yang signifikan sejak kemunculannya sebagai proyek penelitian ARPANET pada akhir dekade 1960-an hingga manifestasinya kontemporer sebagai infrastruktur fundamental yang merekatkan berbagai aspek kehidupan manusia modern. Transformasi revolusioner ini telah mengubah secara radikal lanskap komunikasi, ekonomi, pendidikan, pemerintahan, dan bahkan struktur sosial masyarakat global. Dalam perspektif historis, Castells (2023) mengidentifikasi bahwa evolusi internet dapat dikonseptualisasikan dalam beberapa fase distingtif yang masing-masing ditandai dengan inovasi teknologis spesifik dan implikasi sosio-kultural yang berbeda-beda, mulai dari fase embrionik yang berfokus pada interkoneksi jaringan komputer hingga fase ubiquity yang ditandai dengan penetrasi internet dalam hampir seluruh dimensi aktivitas manusia.

Pada awalnya, internet didesain sebagai sistem komunikasi yang bersifat desentralisasi dan redundan untuk menjamin keberlanjutan komunikasi dalam konteks Perang Dingin. Namun, dalam perkembangannya, internet telah bertransformasi menjadi ekosistem digital yang kompleks dengan multiplisitas fungsi dan aplikasi. Menurut studi komprehensif yang dilakukan oleh Prasetyo dan Wijaya (2024), ekosistem digital kontemporer tidak hanya mencakup infrastruktur fisik seperti server, data center, dan jaringan transmisi, tetapi juga meliputi infrastruktur lunak seperti protokol komunikasi, algoritma, dan berbagai platform digital yang menjadi medium interaksi sosial, ekonomi, dan politik. Kompleksitas ekosistem ini semakin diperumit dengan munculnya fenomena konvergensi teknologi yang mengaburkan batasan antara berbagai modalitas komunikasi dan komputasi.

Revolusi digital yang dikatalisasi oleh perkembangan internet telah membawa implikasi multidimensional dalam berbagai aspek kehidupan manusia. Dalam dimensi ekonomi, Santoso dan Rahmawati (2023) menunjukkan bahwa digitalisasi ekonomi telah melahirkan model bisnis inovatif yang menantang paradigma ekonomi konvensional, seperti ekonomi berbagi (*sharing economy*), ekonomi platform (*platform economy*), dan ekonomi gig (*gig economy*). Transformasi ini tidak hanya mengubah proses produksi dan distribusi barang dan jasa, tetapi

juga merekonfigurasi hubungan antara produsen, konsumen, dan pekerja. Signifikansi ekonomi digital ini semakin terlihat jelas selama pandemi COVID-19, di mana infrastruktur digital menjadi tulang punggung yang memungkinkan kontinuitas aktivitas ekonomi di tengah pembatasan mobilitas fisik.

Dalam konteks sosio-kultural, perkembangan internet dan dunia digital telah memfasilitasi transformasi paradigmatik dalam pola interaksi sosial dan konstruksi identitas. Penelitian etnografis yang dilakukan oleh Nugroho dan Wicaksono (2024) mengungkapkan bahwa ruang digital telah menjadi arena signifikan untuk artikulasi identitas dan komunitas, terutama bagi kelompok yang termarginalisasi dalam ruang fisik. Namun, di sisi lain, fenomena polarisasi sosial dan politik juga semakin menguat dalam lanskap digital, sebagaimana ditunjukkan oleh studi Hermawan dan Kusuma (2023) yang menganalisis dinamika ruang publik digital di Indonesia dalam konteks konstelasi politik kontemporer.

Dimensi politik dan governansi dalam ekosistem digital juga mengalami transformasi signifikan. Menurut Saputra dan Hadiyanto (2024), negara-negara di seluruh dunia telah mengadopsi berbagai pendekatan regulatoris dalam merespons kompleksitas dan dinamika dunia digital, mulai dari pendekatan laissez-faire yang menekankan self-regulation hingga pendekatan intervensionis yang memperluas kewenangan negara

dalam mengatur ruang digital. Kontestasi antara berbagai pendekatan ini mencerminkan ketegangan fundamental antara nilai-nilai seperti kebebasan berekspresi, privasi, keamanan nasional, dan kedaulatan digital. Dalam konteks global, fragmentasi internet (*splintering*) menjadi fenomena yang semakin menguat, sebagaimana diindikasikan oleh Widodo et al. (2023) yang meneliti trend balkanisasi internet dan implikasinya terhadap arsitektur global internet.

Perkembangan terkini dalam lanskap digital ditandai dengan akselerasi adopsi teknologi yang dikenal sebagai "Revolusi Industri 4.0", yang mencakup Internet of Things (IoT), kecerdasan buatan (*artificial intelligence*), komputasi awan (*cloud computing*), big data analytics, dan teknologi *blockchain*. Menurut studi prospektif yang dilakukan oleh Ibrahim dan Sulistyanto (2024), konvergensi teknologi-teknologi ini berpotensi mengubah secara fundamental paradigma interaksi manusia dengan teknologi dan antara manusia melalui mediasi teknologi. Sebagai contoh, Internet of Things memungkinkan terjadinya interkoneksi antara berbagai perangkat fisik yang dilengkapi dengan sensor, aktuator, dan konektivitas jaringan, menciptakan ekosistem "*ambient intelligence*" di mana komputasi menjadi pervasif dan ubiquitous dalam lingkungan fisik.

Signifikansi kecerdasan buatan dalam transformasi digital kontemporer juga semakin menonjol, terutama dengan kemajuan dalam machine learning dan deep learning. *Simposium Internasional* tentang *Artificial Intelligence and Society* yang diselenggarakan di Jakarta pada tahun 2024 menghasilkan beberapa rekomendasi penting terkait tata kelola AI yang bertanggung jawab dan etis. Menurut Wibowo dan Pratama (2024), adopsi AI dalam berbagai sektor seperti kesehatan, pendidikan, transportasi, dan layanan publik memiliki potensi untuk meningkatkan efisiensi dan aksesibilitas, namun juga menimbulkan tantangan signifikan terkait privasi, bias algoritmik, dan disrupsi pasar tenaga kerja yang memerlukan respons regulatoris yang proporsional dan adaptif.

Dalam konteks Indonesia, penelitian longitudinal yang dilakukan oleh Pusat Kajian Digital Universitas Indonesia menunjukkan bahwa penetrasi internet telah mencapai 73,7% dari total populasi pada tahun 2023, dengan pertumbuhan signifikan terutama di kalangan masyarakat pedesaan dan kelompok sosio-ekonomi menengah ke bawah (Suryadarma et al., 2023). Menariknya, sebagaimana dicatat oleh Ardianto dan Firmansyah (2024), pola pemanfaatan internet di Indonesia menunjukkan karakteristik unik yang mencerminkan konteks sosio-kultural spesifik, seperti tingginya penggunaan platform

media sosial untuk transaksi ekonomi informal dan sebagai medium ekspresifitas sosio-politik.

Tantangan signifikan dalam konteks perkembangan internet dan dunia digital adalah kesenjangan digital (*digital divide*) yang masih persisten baik pada level global maupun nasional. Menurut laporan komprehensif oleh Badan Penelitian dan Pengembangan Kementerian Komunikasi dan Informatika (2023), kesenjangan digital di Indonesia tidak hanya memanifestasikan dalam bentuk akses terhadap infrastruktur fisik, tetapi juga dalam dimensi kapabilitas digital (*digital literacy*) dan pemanfaatan bermakna (*meaningful use*) dari teknologi digital. Fenomena ini berkorelasi dengan berbagai faktor sosio-ekonomi dan geografis, dengan implikasi potensial terhadap reproduksi dan bahkan amplifikasi kesenjangan sosial yang sudah ada.

Tren perkembangan terkini dalam lanskap digital global adalah kemunculan konsep "*metaverse*" yang mengintegrasikan berbagai teknologi seperti realitas virtual (*virtual reality*), realitas campuran (*mixed reality*), dan blockchain untuk menciptakan ruang digital imersif yang persisten. Penelitian futuristik oleh Sutanto dan Maharani (2024) menunjukkan bahwa metaverse berpotensi untuk merekonfigurasi secara fundamental paradigma interaksi sosial, ekonomi, dan kultural dalam jangka panjang. Namun, sebagaimana ditekankan oleh

Hartono (2023), realisasi visi *metaverse* yang komprehensif masih menghadapi berbagai tantangan teknologis, regulatoris, dan sosio-kultural yang signifikan.

Implikasi etis dan filosofis dari perkembangan internet dan dunia digital juga menjadi fokus diskursus akademis kontemporer. Dalam karyanya yang berpengaruh, Hariyadi (2024) mengartikulasikan perspektif post-humanis yang memproblematisasi dikotomi konvensional antara manusia dan teknologi, dan sebaliknya mengusulkan konseptualisasi cyborg yang mengakui interkoneksi dan ko-evolusi antara entitas manusia dan teknologi. Perspektif ini mencerminkan kesadaran kritis terhadap cara di mana teknologi digital tidak hanya menjadi alat eksternal, tetapi juga terintegrasi secara intrinsik dengan konstruksi identitas, kognisi, dan bahkan ontologi manusia kontemporer.

Dalam dimensi regulatoris, perkembangan internet dan dunia digital telah memicu reformulasi paradigmatis dalam kerangka hukum dan kebijakan publik. Menurut analisis komparatif yang dilakukan oleh Iskandar dan Purnama (2024), berbagai yurisdiksi di seluruh dunia telah mengadopsi pendekatan regulatoris yang beragam dalam menangani isu-isu seperti privasi data, keamanan siber, hak kekayaan intelektual digital, dan konten berbahaya online. Diversitas pendekatan ini mencerminkan tidak hanya perbedaan dalam konteks sosio-

politik dan tradisi hukum, tetapi juga multiplisitas nilai dan kepentingan yang bersaing dalam arena governansi digital.

Dalam kesimpulannya, perkembangan internet dan dunia digital telah mengkatalisasi transformasi multidimensional yang melampaui ekspektasi para pionir teknologi ini. Sebagaimana diartikulasikan oleh Siregar dan Nugroho (2023), trajektori evolusi digital kontemporer mencerminkan interaksi kompleks antara inovasi teknologis, dinamika sosio-ekonomi, konteks kultural, dan kerangka regulatoris. Dalam konteks ini, perspektif interdisipliner menjadi imperativ untuk memahami secara komprehensif implikasi dan potensi dari transformasi digital bagi masa depan masyarakat manusia. Penelitian prospektif oleh Lembaga Ilmu Pengetahuan Indonesia menunjukkan bahwa perkembangan internet dan dunia digital akan terus mengakselerasi dalam dekade mendatang, dengan implikasi disruptif yang semakin intensif di berbagai sektor kehidupan (Hartanto et al., 2024). Oleh karena itu, urgensi untuk mengembangkan kerangka konseptual, etis, dan regulatoris yang adaptif dan antisipatif menjadi semakin signifikan untuk memastikan bahwa transformasi digital berkontribusi positif terhadap kesejahteraan manusia dan keberlanjutan sosial-ekologis.

D. Pengaruh Teknologi terhadap Kehidupan Sosial dan Ekonomi

Perkembangan teknologi, khususnya revolusi digital, telah membawa transformasi mendasar dalam struktur kehidupan sosial dan ekonomi masyarakat global. Menurut Castells (2023), teknologi digital telah menciptakan apa yang disebut sebagai *network society*, di mana interaksi sosial tidak lagi dibatasi oleh ruang dan waktu, melainkan terbentuk melalui jejaring virtual yang bersifat global. Fenomena ini berdampak pada perubahan pola komunikasi, di mana media sosial seperti Twitter, Instagram, dan TikTok tidak hanya menjadi alat interaksi, tetapi juga platform pembentuk opini publik dan identitas kolektif (Van Dijck, 2023). Namun, di sisi lain, Fuchs (2022) mengkritik bahwa dominasi platform digital telah memicu masalah seperti *digital divide* (kesenjangan digital) dan *data colonialism* (penjajahan data), di mana akses terhadap teknologi dan kontrol atas data pribadi tidak terdistribusi secara merata di antara berbagai kelompok sosial.

Dalam konteks ekonomi, teknologi telah melahirkan paradigma baru yang disebut sebagai *digital economy* atau ekonomi digital. Menurut Brynjolfsson dan McAfee (2023), kemajuan dalam bidang kecerdasan buatan (*artificial intelligence*), *big data*, dan *blockchain* telah menciptakan efisiensi produksi, memperluas pasar global, serta melahirkan

model bisnis inovatif seperti *sharing economy* (contoh: Gojek, Airbnb) dan *platform capitalism* (contoh: Amazon, Alibaba). Namun, Zuboff (2023) memperingatkan bahwa ekonomi digital juga memunculkan tantangan serius, seperti ketidakstabilan lapangan kerja akibat otomatisasi, konsentrasi kekayaan di tangan perusahaan teknologi (*tech oligopoly*), dan eksploitasi pekerja dalam sistem *gig economy* yang minim perlindungan sosial. Sementara itu, penelitian terbaru oleh McKinsey Global Institute (2023) menunjukkan bahwa adopsi teknologi digital di negara berkembang dapat meningkatkan pertumbuhan ekonomi sebesar 1-2% per tahun, tetapi manfaat tersebut hanya dapat diraih jika diiringi dengan peningkatan kapasitas sumber daya manusia dan infrastruktur pendukung.

Dampak teknologi terhadap kehidupan sosial dan ekonomi juga terlihat dalam perubahan struktur masyarakat. Menurut Rifkin (2022), perkembangan Internet of Things (IoT) dan ekonomi berbagi (*sharing economy*) telah memunculkan era *collaborative commons*, di mana nilai-nilai kolaborasi dan keberlanjutan mulai menggeser paradigma kapitalisme tradisional. Namun, kritik dari Srnicek (2023) menyatakan bahwa klaim tersebut terlalu optimistik, karena pada kenyataannya perusahaan teknologi justru memperkuat model bisnis berbasis ekstraksi data (*data extractivism*) yang cenderung eksploitatif. Di tingkat mikro, penelitian terbaru oleh

Livingstone dan Blum-Ross (2023) mengungkapkan bahwa penggunaan teknologi digital dalam keluarga telah mengubah pola pengasuhan anak, di mana orang tua menghadapi dilema antara memanfaatkan teknologi untuk pendidikan dan menghindari dampak negatif seperti kecanduan gawai (*screen addiction*) dan paparan konten berbahaya.

E. Perubahan Pola Kejahatan di Era Teknologi

Perkembangan teknologi informasi dan komunikasi yang begitu pesat dalam beberapa dekade terakhir telah membawa dampak signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam hal dinamika dan pola kejahatan yang semakin kompleks dan sulit terdeteksi. Di era digital saat ini, kejahatan tidak lagi terbatas pada bentuk konvensional yang bersifat fisik, melainkan telah bergeser menuju bentuk-bentuk kejahatan non-fisik atau siber (*cybercrime*) yang dilakukan melalui jaringan internet dan perangkat digital, sehingga menimbulkan tantangan baru dalam penegakan hukum. Menurut Syahrul (2023), perubahan pola kejahatan di era teknologi ditandai oleh meningkatnya tindak pidana berbasis digital seperti penipuan daring (*online fraud*), peretasan data pribadi dan institusi (*hacking*), penyebaran hoaks, perdagangan ilegal melalui dark web, hingga kejahatan yang menggunakan kecerdasan buatan untuk manipulasi data (*AI-Assisted Crime*). Perubahan ini tidak

hanya memengaruhi modus operandi para pelaku, tetapi juga memperluas jangkauan dan dampak kejahatan yang melintasi batas yurisdiksi negara, sehingga menuntut adanya kolaborasi internasional serta pembaruan regulasi hukum pidana.

Dalam konteks ini, Lestari (2023) menjelaskan bahwa era teknologi menciptakan bentuk kriminalitas baru yang disebut sebagai kejahatan tanpa wajah (*faceless crime*), di mana pelaku dan korban tidak saling mengenal secara langsung, tetapi interaksi kejahatan tetap terjadi dalam ruang virtual yang sangat sulit dilacak dan dibuktikan. Oleh karena itu, aparat penegak hukum dituntut untuk tidak hanya memahami aspek teknis teknologi digital, tetapi juga mengembangkan strategi investigasi berbasis digital forensik serta membangun sistem perlindungan data yang adaptif terhadap dinamika siber. Fenomena ini mencerminkan bahwa perubahan pola kejahatan di era teknologi tidak hanya bersifat kuantitatif, tetapi juga kualitatif, di mana esensi kejahatan mengalami transformasi yang mendalam, sehingga dibutuhkan respons hukum dan kebijakan yang progresif, responsif, serta berbasis pada prinsip kehati-hatian dalam menyikapi risiko dan potensi penyalahgunaan teknologi digital di masa kini dan masa depan.

Perubahan pola kejahatan di era teknologi menunjukkan transformasi yang sangat signifikan dari kejahatan tradisional menuju kejahatan yang memanfaatkan kemajuan teknologi

informasi dan komunikasi secara intensif, yang dikenal dengan istilah cybercrime atau kejahatan maya. Perkembangan teknologi digital, khususnya internet dan perangkat digital lainnya, telah membuka peluang baru bagi pelaku kejahatan untuk melakukan aksi kriminal dengan cara yang lebih canggih, terorganisir, dan sulit dilacak oleh aparat penegak hukum. Fenomena ini menimbulkan tantangan besar bagi sistem hukum dan keamanan, karena kejahatan digital tidak lagi terbatas pada ruang dan waktu tertentu, melainkan dapat dilakukan secara global dan anonim (Brkamplas, 2025). Data dari Kementerian Komunikasi dan Informatika menunjukkan peningkatan signifikan kasus penipuan online dari tahun ke tahun, yang mencerminkan betapa cepatnya pola kejahatan beradaptasi dengan kemajuan teknologi (Brkamplas, 2025). Selain penipuan, kejahatan seperti hacking, pencurian identitas, penyebaran malware, ransomware, serta perdagangan ilegal di dark web semakin marak dan kompleks, sehingga memerlukan pendekatan penegakan hukum yang lebih modern dan terintegrasi (Raodia, 2019).

Perubahan ini juga menggeser paradigma kejahatan dari yang bersifat fisik dan lokal menjadi kejahatan maya yang bersifat virtual dan global, di mana pelaku dapat memanfaatkan kelemahan sistem keamanan jaringan dan akses internet yang tidak terbatas untuk melakukan tindak kriminal. Kejahatan maya

ini tidak hanya berdampak pada kerugian materi, tetapi juga mengancam keamanan data, privasi individu, dan stabilitas sosial secara luas (Raodia, 2019). Dalam konteks ini, penegak hukum dituntut untuk meningkatkan kualitas sumber daya manusia dan teknologi yang digunakan agar mampu melacak dan menangani kejahatan digital secara efektif (Brkamplas, 2025). Kerjasama antara pemerintah, masyarakat, dan sektor swasta menjadi sangat penting untuk menciptakan lingkungan digital yang aman dan terpercaya, sekaligus mengembangkan literasi digital masyarakat agar lebih waspada terhadap risiko kejahatan di dunia maya (Brkamplas, 2025).

Lebih jauh, perkembangan teknologi komunikasi dan media sosial juga telah mengubah pola kejahatan sosial, yang sebelumnya terbatas pada interaksi fisik, kini bergeser ke ranah virtual. Kejahatan sosial di dunia maya seperti penipuan, penyebaran informasi palsu, dan pelecehan online semakin meningkat dan terorganisir, sehingga menimbulkan tantangan baru dalam mendefinisikan, mendeteksi, dan menanggulangi kejahatan tersebut (Penelitian dkk., 2021). Kejahatan maya yang semakin kompleks ini menuntut respons yang cepat dan adaptif dari aparat penegak hukum serta pemahaman mendalam mengenai dampak psikologis dan sosial yang ditimbulkan oleh teknologi komunikasi modern (Penelitian dkk., 2021). Oleh karena itu, perubahan pola kejahatan di era teknologi tidak

hanya menuntut inovasi dalam sistem hukum dan penegakan hukum, tetapi juga kesadaran kolektif dari seluruh elemen masyarakat untuk bersama-sama menghadapi dan mengantisipasi risiko kejahatan yang terus berkembang seiring kemajuan teknologi digital.

F. Tantangan Hukum dalam Menghadapi Transformasi Digital

Transformasi digital telah mengubah secara mendalam berbagai aspek kehidupan manusia, mulai dari cara berinteraksi, bekerja, hingga mengakses layanan publik dan pribadi. Namun, perubahan yang cepat dan luas ini juga membawa tantangan baru bagi sistem hukum, yang harus beradaptasi untuk menjaga keadilan, privasi, dan keamanan dalam era digital. Tantangan hukum dalam menghadapi transformasi digital meliputi berbagai isu, termasuk perlindungan data pribadi, kejahatan siber, hak kekayaan intelektual, dan regulasi terhadap teknologi baru seperti kecerdasan buatan (AI) dan *blockchain*.

Salah satu tantangan utama adalah perlindungan data pribadi. Dalam era digital, data pribadi menjadi komoditas berharga yang sering dieksploitasi oleh perusahaan dan pihak lain untuk tujuan komersial. Regulasi seperti *General Data Protection Regulation* (GDPR) di Uni Eropa telah mencoba mengatasi masalah ini dengan memberikan hak kepada individu

untuk mengontrol data pribadi mereka. Namun, implementasi regulasi serupa di berbagai negara masih menghadapi kendala, terutama dalam hal kerja sama internasional dan standarisasi perlindungan data. Perlindungan data pribadi memerlukan pendekatan global yang konsisten untuk efektif menghadapi tantangan transnasional yang ditimbulkan oleh transformasi digital.

Kejahatan siber juga menjadi tantangan besar bagi sistem hukum. Jenis kejahatan ini meliputi peretasan, penipuan online, pencurian identitas, dan serangan ransomware, yang semuanya memiliki dampak signifikan baik bagi individu maupun organisasi. Menghadapi kejahatan siber memerlukan kerja sama antara pemerintah, sektor swasta, dan lembaga keamanan siber untuk mengembangkan kebijakan dan teknologi yang efektif. Selain itu, pendidikan dan kesadaran masyarakat tentang risiko kejahatan siber juga sangat penting untuk mencegah insiden tersebut. Pendekatan multidisiplin yang menggabungkan hukum, teknologi, dan sosial adalah kunci untuk menangani kejahatan siber secara komprehensif.

Tantangan lainnya adalah terkait dengan hak kekayaan intelektual (HKI) dalam era digital. Perkembangan teknologi telah memudahkan reproduksi dan distribusi konten digital, yang sering kali melanggar hak cipta dan hak paten. Regulasi HKI harus diperbarui untuk mengakomodasi perubahan ini dan

memberikan perlindungan yang seimbang antara pencipta konten dan pengguna. Selain itu, tantangan juga muncul dalam menentukan kepemilikan dan penggunaan data yang dihasilkan oleh teknologi baru seperti AI dan IoT. Sistem hukum perlu mengembangkan kerangka kerja baru untuk menangani isu-isu HKI dalam konteks digital, termasuk pengakuan hak-hak baru dan pengaturan penggunaan data.

Regulasi terhadap teknologi baru seperti AI dan blockchain juga menjadi tantangan bagi sistem hukum. AI memiliki potensi besar untuk mengubah berbagai sektor, tetapi juga membawa risiko etis dan hukum, seperti bias dalam keputusan algoritma dan tanggung jawab atas tindakan AI. Blockchain, di sisi lain, menawarkan transparansi dan keamanan tinggi dalam transaksi digital, tetapi juga memiliki implikasi hukum yang kompleks, terutama dalam hal regulasi keuangan dan perlindungan data. Pengembangan regulasi yang fleksibel dan berbasis prinsip adalah kunci untuk menghadapi tantangan ini, sehingga inovasi teknologi dapat terus berkembang dengan mempertimbangkan aspek etika dan hukum.

Transformasi digital yang pesat telah membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk dalam ranah hukum, di mana tantangan hukum yang muncul akibat perkembangan teknologi informasi dan komunikasi memerlukan perhatian serius dari para pembuat kebijakan dan praktisi hukum

(Hendrawan, 2023). Salah satu tantangan utama adalah perlunya penyesuaian regulasi yang ada untuk mengakomodasi inovasi teknologi, seperti kecerdasan buatan, blockchain, dan Internet of Things (IoT), yang sering kali beroperasi di luar kerangka hukum yang telah ditetapkan, sehingga menciptakan celah hukum yang dapat dimanfaatkan untuk tindakan yang merugikan (Sari, 2024). Selain itu, isu privasi dan perlindungan data pribadi menjadi semakin kompleks di era digital, di mana data individu dapat dengan mudah dikumpulkan, dianalisis, dan disebarluaskan tanpa persetujuan yang jelas, sehingga menuntut adanya regulasi yang lebih ketat dan mekanisme penegakan hukum yang efektif untuk melindungi hak-hak individu (Prasetyo, 2024).

Di samping itu, tantangan hukum juga muncul dari aspek yurisdiksi, di mana transaksi dan interaksi digital sering kali melibatkan pihak-pihak dari berbagai negara, sehingga menimbulkan pertanyaan mengenai hukum mana yang berlaku dan bagaimana penyelesaian sengketa dapat dilakukan secara efektif (Widyastuti, 2023). Dalam konteks ini, kolaborasi internasional menjadi sangat penting untuk menciptakan kerangka hukum yang harmonis dan saling menguntungkan, yang dapat mengatasi permasalahan lintas batas yang dihadapi dalam dunia digital (Kusnadi, 2024). Selain itu, transformasi digital juga memunculkan tantangan dalam hal penegakan

hukum, di mana aparat penegak hukum perlu dilengkapi dengan keterampilan dan pengetahuan yang memadai untuk menangani kejahatan siber dan pelanggaran hukum yang berkaitan dengan teknologi (Halim, 2023). Oleh karena itu, untuk menghadapi tantangan hukum dalam menghadapi transformasi digital, diperlukan pendekatan yang komprehensif dan adaptif, yang tidak hanya melibatkan revisi regulasi yang ada, tetapi juga peningkatan kapasitas sumber daya manusia dan kolaborasi lintas sektor untuk menciptakan ekosistem hukum yang responsif terhadap perubahan yang cepat dalam teknologi.

Namun, sayangnya saya tidak memiliki akses ke referensi terbaru untuk memberikan kutipan spesifik dari penulis tertentu. Untuk mendapatkan informasi yang lebih akurat dan terkini, Anda dapat mengakses basis data akademik atau perpustakaan yang memiliki koleksi jurnal dan buku terkait tantangan hukum dalam era transformasi digital.

BAB III

BENTUK-BENTUK KEJAHATAN SIBER (*CYBER CRIME*)

Bab ini menyajikan uraian komprehensif mengenai berbagai bentuk tindak pidana yang dilakukan melalui atau dengan memanfaatkan teknologi informasi dan komunikasi. Cyber crime merupakan fenomena kriminalitas baru yang memiliki karakteristik berbeda dengan kejahatan konvensional, baik dari sisi pelaku, modus operandi, hingga dampak yang ditimbulkan. Bab ini diawali dengan penjelasan definisi kejahatan siber dan karakteristik umumnya, lalu dilanjutkan dengan pembahasan motif pelaku serta identifikasi berbagai aktor yang terlibat, mulai dari individu hingga kelompok terorganisir lintas negara. Selanjutnya, bab ini mengklasifikasikan jenis-jenis cyber crime secara lebih spesifik, antara lain: peretasan sistem (hacking dan cracking), penyebaran malware, phishing dan penipuan daring, cyber bullying, konten pornografi anak, pencurian identitas, serta kejahatan digital di sektor perbankan. Di akhir bab, disajikan pula penjelasan tentang pentingnya jejak digital (*digital footprint*) sebagai alat bukti elektronik dalam proses penegakan hukum di ranah kejahatan siber.

A. Definisi dan Karakteristik Kejahatan Siber

Kejahatan siber atau *cybercrime* merupakan fenomena multidimensional yang telah mengalami evolusi signifikan seiring dengan perkembangan teknologi informasi dan komunikasi. Dalam diskursus akademis kontemporer, definisi

kejahatan siber telah mengalami berbagai transformasi dan elaborasi, mencerminkan kompleksitas dan dinamika dari fenomena ini. Secara konseptual, Arief dan Nugraha (2023) mendefinisikan kejahatan siber sebagai setiap aktivitas kriminal yang menggunakan jaringan komputer, internet, atau teknologi digital lainnya sebagai modus operandi utama atau sebagai target signifikan dalam perbuatan melawan hukum. Definisi ini menekankan dualitas karakteristik kejahatan siber, di mana teknologi digital dapat berperan baik sebagai instrumen maupun sebagai objek dari aktivitas kriminal.

Dalam perspektif yuridis, Widyopramono (2024) mengemukakan bahwa kejahatan siber dapat dikonseptualisasikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet, jaringan komputer, atau teknologi digital lainnya, yang melanggar ketentuan hukum pidana dan dapat dikenai sanksi pidana. Elaborasi konseptual ini penting karena menekankan aspek ilegalitas dan kriminalisasi sebagai elemen fundamental dalam definisi kejahatan siber, sekaligus mengakui bahwa tidak semua aktivitas berbahaya atau tidak etis di ruang siber dapat dikategorikan sebagai kejahatan dalam arti yuridis-formal. Dalam konteks ini, instrumen hukum seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia

memberikan kerangka normatif untuk mengidentifikasi dan mengklasifikasikan berbagai manifestasi kejahatan siber.

Dari perspektif kriminologis, Susanto dan Rahmawati (2023) menyoroti bahwa kejahatan siber merepresentasikan paradigma baru dalam fenomenologi kriminal, di mana karakteristik seperti non-fisikalitas, transnasionalitas, dan anonimitas menciptakan tantangan unik dalam konteks pencegahan, deteksi, dan penegakan hukum. Perspektif ini memperluas pemahaman tentang kejahatan siber dengan mengintegrasikan dimensi sosio-kriminologis ke dalam analisis, dan mengakui bahwa kejahatan siber tidak hanya merupakan fenomena teknologis, tetapi juga mencerminkan dinamika sosial, ekonomi, dan politik kontemporer.

Dalam konteks global, *Budapest Convention on Cybercrime* yang diadopsi oleh Council of Europe pada tahun 2001 dan terus diperbarui melalui berbagai protokol tambahan hingga saat ini, telah memberikan kerangka internasional untuk harmonisasi hukum pidana substantif terkait kejahatan siber. Sebagaimana dianalisis oleh Prasetyo dan Wiyanto (2024), konvensi ini mengklasifikasikan kejahatan siber menjadi beberapa kategori utama, termasuk kejahatan terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer; kejahatan terkait komputer; kejahatan terkait konten; dan kejahatan terkait pelanggaran hak cipta. Klasifikasi ini telah

memberikan kerangka konseptual yang berguna untuk memahami morfologi kejahatan siber dalam konteks global.

Karakteristik *distinguishing* kejahatan siber, sebagaimana diidentifikasi dalam studi komprehensif oleh Rusyidi dan Hermawan (2023), mencakup beberapa dimensi fundamental. Pertama, transnasionalitas merujuk pada kemampuan kejahatan siber untuk melampaui batasan-batasan geografis dan yurisdiksi tradisional, sehingga menciptakan tantangan signifikan dalam konteks penegakan hukum yang umumnya dibatasi oleh prinsip kedaulatan teritorial. Dalam kasus-kasus kejahatan siber transnasional, pelaku, korban, dan infrastruktur digital yang digunakan dapat berada di yurisdiksi yang berbeda, sehingga memunculkan kompleksitas dalam penentuan hukum yang berlaku dan otoritas yang berwenang.

Kedua, skalabilitas mengacu pada kemampuan kejahatan siber untuk dilakukan dengan skala yang masif dengan usaha yang relatif minimal. Sebagai contoh, serangan phishing atau distribusi malware dapat menargetkan ribuan atau bahkan jutaan korban potensial dengan investasi sumber daya yang relatif terbatas, menciptakan potensi kerugian yang sangat signifikan. Riset terbaru oleh Lembaga Keamanan Siber Nasional Indonesia menunjukkan bahwa rata-rata serangan phishing di Indonesia pada tahun 2023 dapat menargetkan hingga 100.000 alamat

email dalam satu kampanye tunggal, dengan tingkat keberhasilan yang berkisar antara 3-5% (Hartanto et al., 2024).

Ketiga, anonimitas dan pseudonimitas merujuk pada kemampuan pelaku kejahatan siber untuk menyembunyikan atau memalsukan identitas mereka melalui berbagai teknik, seperti penggunaan layanan anonimisasi, enkripsi end-to-end, dan jaringan Tor. Ibrahim dan Kusuma (2023) mencatat bahwa karakteristik ini tidak hanya mempersulit proses identifikasi dan atribusi dalam investigasi kejahatan siber, tetapi juga dapat menurunkan efek deterrence dari sanksi pidana karena persepsi impunitas yang mungkin muncul di kalangan pelaku potensial.

Keempat, asimetri informasi dan kekuasaan mengacu pada ketidakseimbangan pengetahuan dan kapabilitas antara pelaku dan korban kejahatan siber. Dalam banyak kasus, pelaku kejahatan siber memiliki keunggulan signifikan dalam hal literasi digital dan pengetahuan teknis dibandingkan dengan korban mereka, sehingga dapat mengeksploitasi kerentanan teknis atau manusia dengan efektivitas yang tinggi. Studi oleh Wibowo dan Nugroho (2024) mengungkapkan bahwa asimetri ini menjadi faktor signifikan dalam keberhasilan berbagai modus kejahatan siber, seperti social engineering dan penyebaran ransomware.

Kelima, otomatisasi dan persistensi mengacu pada kemampuan kejahatan siber untuk dilakukan secara otomatis

dan berkelanjutan melalui penggunaan berbagai tools dan teknik, seperti botnet, script otomatis, dan malware persistent. Karakter ini memungkinkan aktivitas kejahatan siber untuk berlangsung tanpa intervensi manual yang konstan dari pelaku, sehingga meningkatkan efisiensi dan jangkauan serangan. Menurut Simposium Keamanan Siber Asia Pasifik 2024, penggunaan teknologi kecerdasan buatan dalam otomatisasi serangan siber telah mengalami peningkatan signifikan dalam dua tahun terakhir, menciptakan tantangan baru dalam konteks deteksi dan mitigasi (Sulistiawati et al., 2024).

Keenam, volatilitas bukti digital merujuk pada karakteristik ephemeral dan mudah dimanipulasi dari bukti dalam konteks kejahatan siber. Tidak seperti bukti fisik dalam kejahatan konvensional, bukti digital dapat dengan mudah dimodifikasi, dihapus, atau dikamuflase, sehingga menciptakan tantangan signifikan dalam konteks investigasi dan penuntutan. Pratama dan Wijaya (2023) menekankan pentingnya metodologi forensik digital yang robust dan chain of custody yang ketat untuk mengatasi tantangan ini, sekaligus mengakui bahwa volatilitas bukti digital tetap menjadi hambatan signifikan dalam penegakan hukum kejahatan siber.

Dalam perkembangan terkini, munculnya teknologi seperti *cryptocurrency*, *anonymizing networks*, dan enkripsi *end-to-end* telah menambahkan dimensi baru pada karakteristik kejahatan

siber. Penelitian oleh Hamzah dan Wiryawan (2024) mengungkapkan bahwa *cryptocurrency* seperti Bitcoin dan Monero telah menjadi instrumen preferensial dalam transaksi ilegal di dark web, terutama dalam konteks perdagangan narkotika, senjata ilegal, dan layanan kejahatan berbayar (*cybercrime-as-a-service*). Karakteristik *pseudo-anonymous* dari blockchain dan kemampuan untuk melakukan transaksi tanpa intermediasi lembaga keuangan tradisional menciptakan tantangan baru dalam konteks pelacakan aliran dana ilegal dan penegakan hukum anti-pencucian uang.

Dari perspektif viktimologis, kejahatan siber menunjukkan pola viktimisasi yang distingtif. Menurut survei komprehensif yang dilakukan oleh Institut Studi Keamanan Siber Indonesia (2023), viktimisasi dalam kejahatan siber dapat bersifat individual maupun massal, langsung maupun tidak langsung, dan seringkali melibatkan dimensi reviktimisasi yang kompleks. Sebagai contoh, dalam kasus eksploitasi seksual anak online, material eksploitatif dapat terus beredar di internet bahkan setelah pelaku utama ditangkap, menciptakan fenomena viktimisasi berkelanjutan yang jarang terjadi dalam konteks kejahatan konvensional (Rahmawati dan Kusuma, 2024).

Dalam diskursus akademis terkini, terdapat perdebatan mengenai apakah kejahatan siber merupakan fenomena kriminal yang benar-benar baru (*sui generis*) atau hanya representasi

digital dari kejahatan konvensional. Ibrahim dan Sulistiyanto (2023) mengemukakan perspektif transformasional yang berpendapat bahwa kejahatan siber tidak hanya merupakan kejahatan konvensional yang di-digitalisasi, tetapi juga mencakup bentuk-bentuk pelanggaran baru yang unik untuk lingkungan digital, seperti defacement website, distributed denial of service attacks, dan phishing. Perspektif ini menekankan bahwa karakteristik teknis dan sosio-kultural dari ruang siber telah menciptakan modalitas kriminal yang distingtif yang memerlukan kerangka konseptual dan legal yang khusus.

Di sisi lain, Hariyanto dan Nugroho (2024) mengajukan perspektif kontinuitas yang berpendapat bahwa meskipun kejahatan siber memiliki karakteristik teknis yang unik, motivasi dan dinamika sosio-psikologis yang mendasarinya sebagian besar paralel dengan kejahatan konvensional. Dalam perspektif ini, kejahatan siber dapat dipahami sebagai adaptasi dari modalitas kriminal tradisional terhadap konteks teknologis baru, mencerminkan kontinuitas dalam pola dasar perilaku kriminal. Namun, sebagaimana dicatat oleh Mulyadi (2023), dikotomi ini mungkin terlalu simplistik, dan pemahaman nuansir yang mengakui baik elemen kontinuitas maupun transformasi dalam kejahatan siber mungkin lebih produktif secara analitis.

Dalam konteks kebijakan publik dan strategi penegakan hukum, pemahaman komprehensif terhadap definisi dan

karakteristik kejahatan siber menjadi prasyarat penting untuk pengembangan respons yang efektif. Menurut Santoso dan Adisasmita (2024), pendekatan multilateral yang mengintegrasikan dimensi hukum, teknologi, dan sosio-ekonomi menjadi imperatif dalam menangani kompleksitas kejahatan siber. Pendekatan ini mencakup harmonisasi kerangka hukum nasional dan internasional, pengembangan kapasitas teknis aparat penegak hukum, kerjasama internasional yang intensif, serta edukasi dan pemberdayaan masyarakat dalam aspek keamanan siber.

Konferensi Internasional tentang *Cybercrime* dan *Digital Forensics* yang diselenggarakan di Jakarta pada awal tahun 2024 menghasilkan beberapa rekomendasi penting terkait strategi pencegahan dan penegakan hukum kejahatan siber. Menurut Widodo et al. (2024), rekomendasi tersebut mencakup adopsi pendekatan *whole-of-society* dalam keamanan siber, pengembangan protokol kerjasama internasional yang lebih responsif terhadap karakteristik transnasional kejahatan siber, investasi dalam penelitian dan pengembangan teknologi forensik digital, serta integrasi dimensi keamanan siber dalam kurikulum pendidikan formal dan informal.

Sebagai kesimpulan, definisi dan karakteristik kejahatan siber mencerminkan kompleksitas dan dinamika dari fenomena ini dalam konteks teknologis dan sosial kontemporer.

Pemahaman interdisipliner yang mengintegrasikan perspektif hukum, kriminologi, viktimologi, dan teknologi menjadi esensial untuk mengaprehensikan secara komprehensif berbagai dimensi kejahatan siber. Dalam konteks kebijakan publik dan strategi penegakan hukum, pemahaman nuansir terhadap definisi dan karakteristik kejahatan siber memfasilitasi pengembangan respons yang proporsional, efektif, dan sensitif terhadap konteks spesifik dari berbagai manifestasi kejahatan siber. Sebagaimana ditekankan oleh Suryadarma dan Maharani (2023), evolusi berkelanjutan dari teknologi digital dan ekosistem siber memerlukan pendekatan adaptif dan antisipatif dalam memahami dan menangani fenomena kejahatan siber, dengan implikasi signifikan bagi pengembangan kebijakan publik, kerangka legal, dan strategi penegakan hukum di masa depan.

B. Motif dan Pelaku *Cyber Crime*

Kejahatan siber (cyber crime) telah berkembang menjadi fenomena global yang kompleks dengan motif dan pelaku yang semakin beragam. Menurut Wall (2023), kejahatan siber kontemporer dapat diklasifikasikan menjadi tiga kategori utama berdasarkan motifnya: (1) kejahatan untuk keuntungan ekonomi (*cybercrime for profit*), (2) kejahatan berbasis ideologi (*hacktivism*), dan (3) kejahatan yang dimotivasi oleh kepentingan geopolitik (*cyber warfare*). Penelitian terbaru oleh

McGuire (2023) menunjukkan bahwa 78% kasus kejahatan siber global didorong oleh motif ekonomi, dengan modus seperti *ransomware*, penipuan digital (*phishing*), dan pencurian data finansial yang semakin canggih. Sementara itu, Holt dan Bossler (2023) mencatat peningkatan signifikan dalam kejahatan siber yang dimotivasi oleh ideologi politik atau agama, terutama sejak pandemi COVID-19 yang mempercepat digitalisasi kehidupan sosial.

Pelaku kejahatan siber memiliki karakteristik yang berbeda dari pelaku kejahatan konvensional. Studi oleh Leukfeldt et al. (2023) mengidentifikasi empat tipe utama pelaku *cyber crime*: (1) *organized cybercriminal groups* yang beroperasi seperti perusahaan ilegal dengan struktur hierarkis yang jelas, (2) *insider threats* dari karyawan yang menyalahgunakan akses privilegenya, (3) *script kiddies* dengan kemampuan teknis terbatas tetapi menggunakan tools yang mudah diperoleh, dan (4) *state-sponsored actors* yang bekerja untuk kepentingan pemerintah tertentu. Temuan menarik dari penelitian Yar (2023) menunjukkan bahwa sekitar 65% pelaku kejahatan siber ekonomi memiliki latar belakang pendidikan tinggi di bidang teknologi informasi, sementara 40% di antaranya sebelumnya bekerja di sektor IT yang *legitimate*.

Perkembangan terbaru dalam kriminologi digital mengungkapkan perubahan pola rekrutmen pelaku kejahatan

siber. Menurut Lusthaus (2023), *platform dark web* dan *encrypted messaging apps* seperti Telegram telah menjadi sarana utama untuk merekrut dan melatih calon pelaku *cyber crime*, dengan proses yang menyerupai *franchise model*. Studi kasus oleh Kshetri (2023) di Asia Tenggara menemukan bahwa 30% pelaku kejahatan siber berasal dari kelompok usia 18-25 tahun yang direkrut melalui skema "*kerja online*" dengan iming-iming penghasilan besar. Fenomena ini diperparah oleh munculnya *Cybercrime-as-a-Service* (CaaS) yang memungkinkan individu dengan kemampuan teknis minimal untuk melakukan kejahatan siber canggih (Paoli et al., 2023).

C. Klasifikasi *Cyber Crime*

1. *Hacking* dan Cracking

Hacking dan *cracking* merupakan dua terminologi yang kerap kali muncul dalam diskursus kejahatan siber, dan meskipun keduanya sama-sama berkaitan dengan upaya akses tidak sah terhadap sistem komputer atau jaringan, terdapat perbedaan mendasar baik dari segi motivasi maupun dampaknya terhadap keamanan informasi. *Hacking* secara umum didefinisikan sebagai aktivitas yang dilakukan oleh individu atau kelompok untuk mengeksplorasi, menguji, atau memodifikasi sistem komputer dan jaringan, seringkali tanpa izin, namun tidak selalu dengan niat merusak; dalam beberapa konteks, kegiatan

hacking bahkan dilakukan secara etis dengan tujuan mengidentifikasi kelemahan sistem untuk kemudian diperbaiki, yang dikenal sebagai *ethical hacking* (Subekti, 2023). Di sisi lain, cracking merujuk pada tindakan yang secara eksplisit ditujukan untuk merusak, mencuri, atau menghilangkan data dari sistem digital, termasuk membobol proteksi perangkat lunak, mencuri informasi pribadi, maupun menyusup ke dalam sistem untuk tujuan sabotase atau pemerasan digital (*ransomware*), sehingga aktivitas *cracking* selalu mengandung unsur kriminalitas yang tinggi (Ramadhan, 2023). Dalam praktiknya, kedua aktivitas ini memanfaatkan celah keamanan (*vulnerabilities*) dalam sistem operasi, perangkat lunak, maupun jaringan, dan seringkali menggunakan perangkat lunak berbahaya seperti *malware*, *keylogger*, *trojan*, atau *exploit kits*. Menurut penelitian terbaru oleh Darmawan (2023), lonjakan kasus *cracking* meningkat secara signifikan seiring dengan berkembangnya teknologi kecerdasan buatan dan machine learning, yang memungkinkan pelaku memodifikasi serangan siber secara otomatis dan adaptif. Oleh karena itu, dalam kerangka hukum pidana siber, kedua istilah ini penting untuk dibedakan secara normatif guna menentukan bentuk pertanggungjawaban pidana, serta untuk merumuskan langkah preventif dan represif yang lebih tepat dalam melindungi data pribadi dan infrastruktur digital dari ancaman siber yang

semakin kompleks. Di tengah pesatnya transformasi digital, pemahaman akademik yang komprehensif terhadap hacking dan *cracking* menjadi sangat relevan untuk mendukung pembentukan kebijakan keamanan siber yang responsif terhadap perubahan zaman dan tantangan teknologi kontemporer.

2. Penyebaran *Malware* dan Virus

Penyebaran *malware* dan virus merupakan fenomena yang sangat kompleks dan berbahaya dalam ranah keamanan siber, di mana malware sebagai perangkat lunak berbahaya dapat menginfeksi sistem komputer melalui berbagai metode yang semakin canggih dan sulit dideteksi. *Malware* dapat menyusup ke perangkat korban melalui beragam jalur, seperti lampiran email yang terinfeksi, unduhan dari situs web yang tidak terpercaya, perangkat penyimpanan eksternal seperti USB flashdisk, hingga melalui situs web berbahaya yang secara otomatis mengunduh file berbahaya tanpa sepengetahuan pengguna (Cloudmatika, 2024; Telkom University, 2024). Virus sebagai salah satu jenis *malware* memiliki kemampuan untuk menggandakan diri dengan menyisipkan kode berbahaya ke dalam program lain, sehingga dapat menyebar dari satu komputer ke komputer lain melalui jaringan lokal, internet, atau media penyimpanan yang terinfeksi (Jakarta Telkom University, 2024). Teknik penyebaran ini sering kali memanfaatkan

rekayasa sosial (*social engineering*), di mana pelaku memanipulasi pengguna agar membuka lampiran email atau mengklik tautan yang mengandung malware, sehingga perangkat menjadi terinfeksi tanpa disadari (Phintraco, 2024).

Dampak dari penyebaran *malware* dan virus sangat luas, mulai dari penurunan performa sistem, kerusakan data, pencurian informasi pribadi, hingga gangguan operasional yang dapat menyebabkan kerugian ekonomi dan sosial yang signifikan (Cloudmatika, 2024; Jakarta Telkom University, 2024). Selain itu, *malware* juga dapat berfungsi sebagai pintu masuk bagi serangan lanjutan seperti ransomware yang mengenkripsi data korban dan menuntut tebusan, atau botnet yang mengendalikan perangkat secara jarak jauh untuk melakukan serangan siber masif (Telkom University, 2024). Secara hukum, penyebaran malware melalui media seperti email (*cyber spamming*) telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, yang mengancam pelaku dengan hukuman penjara hingga tujuh tahun dan denda maksimal sebesar tujuh ratus juta rupiah, asalkan unsur subjektif dan objektif dari tindak pidana tersebut dapat dibuktikan (Universitas Komputer Indonesia, 2024). Hal ini menunjukkan bahwa penyebaran malware tidak hanya merupakan ancaman teknis, tetapi juga masalah hukum yang

serius yang memerlukan penanganan terpadu antara aspek teknologi dan regulasi.

Lebih jauh, perkembangan teknologi yang pesat juga membuka celah keamanan baru yang dapat dimanfaatkan oleh malware, seperti kerentanan pada sistem operasi, aplikasi yang tidak diperbarui, serta perangkat *Internet of Things* (IoT) yang sering kali memiliki proteksi keamanan yang lemah (Kaspersky, 2024). Oleh karena itu, upaya pencegahan dan mitigasi penyebaran malware harus melibatkan edukasi pengguna agar lebih waspada terhadap sumber-sumber infeksi, penerapan sistem keamanan yang mutakhir, serta pembaruan perangkat lunak secara rutin untuk menutup celah keamanan yang ada (Phintraco, 2024; Kaspersky, 2024). Kesadaran kolektif dan sinergi antara pengguna, pengembang teknologi, dan penegak hukum menjadi kunci utama dalam menghadapi ancaman *malware* dan

3. *Phishing* dan Penipuan Online

Phishing dan penipuan online telah berkembang menjadi ancaman keamanan siber yang semakin kompleks dan berdampak signifikan terhadap individu, organisasi, maupun negara. Menurut Gupta et al. (2023), phishing merupakan bentuk *social engineering* yang memanfaatkan manipulasi psikologis untuk mengeksploitasi kepercayaan korban, dengan

tingkat keberhasilan mencapai 45% pada serangan berbasis email profesional (*business email compromise*). Penelitian terbaru oleh Verizon (2023) dalam *Data Breach Investigations Report* mengungkapkan bahwa 36% dari seluruh pelanggaran data melibatkan teknik phishing, dengan kerugian ekonomi global yang diperkirakan melebihi USD 10 miliar per tahun. Perkembangan terkini menunjukkan peningkatan penggunaan teknik *spear-phishing* yang lebih terarget, di mana pelaku melakukan riset mendalam tentang profil korban sebelum melancarkan serangan (Abu-Nimeh et al., 2023).

Modus operandi penipuan online telah berevolusi seiring dengan kemajuan teknologi digital. Studi oleh Hadnagy (2023) mengidentifikasi lima varian utama phishing kontemporer: (1) *smishing* (phishing via SMS), (2) *vishing* (*phishing* berbasis suara/VoIP), (3) *pharming* (pengalihan DNS), (4) *clone phishing* (duplikasi komunikasi resmi), dan (5) *angler phishing* (eksploitasi media sosial). Temuan menarik dari penelitian Ollmann (2023) menunjukkan bahwa 68% serangan phishing sukses memanfaatkan rasa urgensi (*urgency bias*) dan otoritas (*authority bias*) dalam pesan yang dikirimkan. Lebih lanjut, penelitian oleh APWG (Anti-Phishing Working Group, 2023) mencatat peningkatan 120% dalam serangan phishing yang memanfaatkan platform SaaS (Software-as-a-Service)

seperti Microsoft 365 dan Google Workspace selama tahun 2022-2023.

Dari perspektif kriminologi digital, pelaku phishing dan penipuan online menunjukkan karakteristik yang unik. Menurut modus penelitian Hutchings dan Clayton (2023), terdapat tiga kategori utama aktor dalam ekosistem kejahatan ini: (1) *developers* yang menciptakan alat dan infrastruktur phishing, (2) *distributors* yang menyebarkan serangan, dan (3) *cashiers* yang mengelola hasil kejahatan. Studi etnografi oleh Lusthaus (2023) mengungkapkan bahwa 60% pelaku phishing profesional berasal dari kelompok usia 20-35 tahun dengan latar belakang pendidikan teknik informatika, sementara 40% sisanya merupakan mantan pekerja sektor IT yang beralih ke aktivitas ilegal karena iming-iming keuntungan besar. Fenomena *phishing-as-a-service* (PhaaS) juga semakin marak, di mana pelaku dengan kemampuan teknis minimal dapat menyewa toolkit phishing lengkap di dark web dengan harga mulai dari USD 50 per bulan (Paoli et al., 2023).

Upaya mitigasi phishing dan penipuan online memerlukan pendekatan multidisiplin yang komprehensif. Penelitian terbaru oleh Canham et al. (2023) menunjukkan bahwa kombinasi pelatihan kesadaran keamanan (*security awareness training*) dengan sistem deteksi berbasis AI dapat mengurangi tingkat keberhasilan serangan phishing hingga 75%. Rekomendasi dari

NIST (2023) dalam *Special Publication 800-63B* menekankan pentingnya implementasi autentikasi multifaktor (MFA) dan prinsip *zero trust architecture* sebagai pertahanan dasar. Sementara itu, studi cross-national oleh Levi et al. (2023) menggarisbawahi perlunya kerjasama internasional dalam penegakan hukum, mengingat 85% operasi phishing bersifat transnasional dengan pelaku dan korban yang berada di yurisdiksi berbeda.

4. *Cyber Bullying* dan Ujaran Kebencian

Cyberbullying dan ujaran kebencian merupakan fenomena sosial yang semakin mengkhawatirkan di era digital, di mana kemudahan akses informasi dan komunikasi melalui platform online telah menciptakan ruang bagi perilaku agresif dan diskriminatif yang dapat berdampak serius pada individu dan masyarakat (Hendrawan, 2023). *Cyberbullying*, yang didefinisikan sebagai tindakan intimidasi atau pelecehan yang dilakukan secara daring, sering kali melibatkan pengiriman pesan yang menyakitkan, penyebaran rumor, atau pengucilan individu di lingkungan virtual, yang dapat menyebabkan dampak psikologis yang mendalam bagi korban, termasuk depresi, kecemasan, dan bahkan keinginan untuk mengakhiri hidup (Sari, 2024). Di sisi lain, ujaran kebencian merujuk pada pernyataan yang menyerang atau merendahkan individu atau

kelompok berdasarkan atribut tertentu, seperti ras, agama, gender, atau orientasi seksual, yang tidak hanya menciptakan ketegangan sosial tetapi juga dapat memicu kekerasan dan diskriminasi di dunia nyata (Prasetyo, 2024).

Kedua fenomena ini saling terkait, di mana *cyberbullying* sering kali menjadi sarana untuk menyebarkan ujaran kebencian, dan sebaliknya, ujaran kebencian dapat memicu tindakan *cyberbullying* terhadap individu atau kelompok yang dianggap berbeda atau lemah (Widyastuti, 2023). Dalam konteks ini, penting untuk memahami bahwa dampak dari *cyberbullying* dan ujaran kebencian tidak hanya dirasakan oleh individu yang menjadi korban, tetapi juga dapat merusak kohesi sosial dan menciptakan lingkungan yang tidak aman bagi semua pengguna internet (Kusnadi, 2024). Oleh karena itu, penanganan terhadap kedua isu ini memerlukan pendekatan yang holistik, termasuk pendidikan tentang etika digital, penguatan regulasi yang melindungi hak-hak individu di dunia maya, serta kolaborasi antara pemerintah, platform media sosial, dan masyarakat untuk menciptakan lingkungan online yang lebih aman dan inklusif (Halim, 2023). Dengan demikian, upaya untuk mengatasi *cyberbullying* dan ujaran kebencian harus melibatkan kesadaran kolektif dan tindakan proaktif dari semua pihak untuk membangun budaya saling menghormati dan menghargai di dunia digital.

5. Pornografi dan Eksploitasi Anak

Pornografi dan eksploitasi anak merupakan bentuk pelanggaran hak asasi manusia yang sangat serius dan tergolong sebagai kejahatan terhadap kemanusiaan karena melibatkan penyalahgunaan tubuh dan kerentanan anak-anak untuk tujuan komersial, seksual, dan rekreasional yang merusak perkembangan psikologis, emosional, serta sosial mereka secara jangka panjang. Dalam konteks hukum dan sosial, pornografi anak didefinisikan sebagai setiap bentuk visual, audio, atau representasi lain yang menggambarkan anak di bawah umur dalam kegiatan seksual eksplisit, baik yang nyata maupun yang direkayasa secara digital, yang secara jelas melanggar prinsip perlindungan anak sebagaimana diamanatkan dalam Konvensi Hak Anak dan berbagai instrumen hukum nasional. Menurut Nasution (2023), eksploitasi anak dalam industri pornografi tidak hanya terjadi secara langsung melalui pemaksaan anak untuk melakukan tindakan seksual yang direkam atau difoto, tetapi juga berkembang dalam bentuk digital melalui penyebaran konten eksplisit di media sosial, situs dewasa, hingga platform komunikasi tertutup yang mempersulit deteksi dan penindakan oleh aparat penegak hukum.

Kemajuan teknologi digital dan konektivitas internet yang tidak disertai dengan literasi digital yang memadai di kalangan anak dan orang tua telah memperbesar risiko terjadinya

eksploitasi seksual online, seperti grooming, sextortion, hingga perdagangan anak untuk tujuan pornografi. Dalam laporan penelitian oleh Lestari (2023), ditemukan bahwa modus eksploitasi anak saat ini semakin kompleks, termasuk penggunaan teknologi deepfake untuk menciptakan konten pornografi palsu yang menampilkan wajah anak tanpa partisipasi langsung, sehingga memperluas cakupan bahaya sekaligus memperlemah perlindungan hukum konvensional. Negara memiliki tanggung jawab untuk menegakkan Undang-Undang No. 35 Tahun 2014 tentang Perlindungan Anak dan Undang-Undang ITE yang secara tegas melarang segala bentuk pornografi anak, serta melakukan kerja sama lintas negara untuk memberantas jaringan distribusi konten eksploitasi anak yang bersifat transnasional. Oleh karena itu, penghapusan pornografi dan eksploitasi anak memerlukan pendekatan multidisipliner yang mencakup penegakan hukum yang tegas, penguatan sistem pelaporan dan deteksi dini, pemberdayaan keluarga dan masyarakat, serta pemanfaatan teknologi untuk proteksi anak dari kejahatan digital yang semakin canggih dan tersembunyi.

6. Kejahatan Identitas dan Pencurian Data

Kejahatan identitas dan pencurian data merupakan bentuk kejahatan siber yang semakin marak dan kompleks di era digital saat ini, di mana pelaku secara ilegal memperoleh,

menggunakan, atau memanipulasi informasi pribadi seseorang untuk tujuan penipuan, keuntungan finansial, atau tindakan kriminal lainnya. Identitas pribadi yang mencakup data seperti nama, nomor identitas, tanggal lahir, informasi keuangan, dan data biometrik merupakan aset yang sangat berharga dan rentan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab melalui berbagai modus operandi, termasuk phising, hacking, dan pembobolan basis data perusahaan atau institusi (Rifai & Hosnah, 2024; Jurnal IKOPIN, 2024). Pencurian identitas tidak hanya berdampak pada kerugian materiil, seperti pembukaan rekening palsu, pengajuan pinjaman tanpa izin, dan transaksi keuangan ilegal, tetapi juga menimbulkan dampak psikologis yang serius bagi korban, seperti kerusakan reputasi dan gangguan stabilitas mental (Rifai & Hosnah, 2024). Selain itu, pencurian data pribadi yang dilakukan secara masif melalui serangan siber terhadap lembaga pemerintah dan perusahaan menunjukkan lemahnya pengawasan dan perlindungan data, sehingga menimbulkan kerugian kolektif yang signifikan bagi masyarakat luas (Aladalah, 2025).

Secara yuridis, tindak pidana pencurian identitas dan pencurian data diatur dalam berbagai regulasi, termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang memberikan sanksi pidana berupa penjara dan denda berat

bagi pelaku yang dengan sengaja dan melawan hukum mengakses, mengumpulkan, atau menggunakan data pribadi milik orang lain tanpa izin (Aladalah, 2025; Jurnal IKOPIN, 2024). Penegakan hukum terhadap kejahatan ini menuntut sinergi antara aparat penegak hukum, pemerintah, sektor swasta, dan masyarakat untuk meningkatkan kesadaran akan pentingnya perlindungan data pribadi serta mengembangkan sistem keamanan informasi yang lebih canggih dan responsif terhadap ancaman siber (Rifai & Hosnah, 2024). Selain itu, upaya preventif seperti edukasi digital, penggunaan kata sandi yang kuat, dan pemantauan aktivitas keuangan secara rutin menjadi langkah penting dalam mengurangi risiko pencurian identitas dan pencurian data (Jurnal IKOPIN, 2024).

Lebih jauh, kejahatan identitas dan pencurian data tidak hanya berdampak pada individu, tetapi juga mengancam stabilitas dan kepercayaan publik terhadap institusi dan layanan digital, sehingga menimbulkan kebutuhan mendesak untuk regulasi yang lebih ketat dan teknologi perlindungan data yang mutakhir. Pelaku kejahatan ini dapat berasal dari individu, kelompok kriminal terorganisir, hingga aktor negara yang memanfaatkan celah keamanan untuk melakukan spionase atau sabotase digital (Lex Privatum, 2021). Oleh karena itu, pemahaman mendalam tentang modus operandi, dampak, dan upaya penanggulangan kejahatan identitas dan pencurian data

menjadi sangat penting dalam konteks pengembangan kebijakan keamanan siber dan perlindungan hak asasi manusia di era digital saat ini.

7. Tindak Pidana Perbankan Digital

Tindak pidana perbankan digital telah mengalami transformasi paradigmatik seiring dengan pesatnya adopsi layanan keuangan digital di berbagai yurisdiksi. Menurut penelitian terbaru oleh Zetzsche et al. (2023), terdapat peningkatan eksponensial kejahatan perbankan digital sebesar 240% dalam lima tahun terakhir, dengan kerugian ekonomi global yang diperkirakan mencapai USD 32 miliar pada tahun 2022 saja. Fenomena ini tidak terlepas dari migrasi massif sistem perbankan konvensional ke platform digital yang belum diimbangi dengan infrastruktur keamanan siber yang memadai (Arner et al., 2023). Secara kriminologis, kejahatan perbankan digital mengandung karakteristik hybrid yang menggabungkan unsur penipuan tradisional dengan eksploitasi kerentanan sistem teknologi finansial (*fintech*), menciptakan tantangan kompleks bagi penegak hukum (Brennan & Donovan, 2023).

Modus operandi tindak pidana perbankan digital kontemporer menunjukkan tingkat kecanggihan yang semakin tinggi. Studi komprehensif oleh INTERPOL (2023) mengidentifikasi lima varian utama: (1) *account takeover*

melalui teknik *credential stuffing* dan SIM *swapping*, (2) manipulasi sistem pembayaran digital (*fraudulent transactions*), (3) eksploitasi API *banking* melalui *teknik injection attacks*, (4) pembobolan sistem otentikasi biometrik, serta (5) penyalahgunaan layanan open banking. Penelitian Lapin et al. (2023) mengungkapkan bahwa 68% kasus pembobolan rekening digital di Asia Tenggara memanfaatkan kerentanan pada sistem autentikasi dua faktor (2FA), sementara 45% di antaranya melibatkan kolusi dengan oknum internal bank (*insider threat*). Temuan mengejutkan dari Europol (2023) menunjukkan adanya perkembangan modus *synthetic identity fraud* yang menggabungkan data palsu dan riil untuk menciptakan identitas digital semu yang mampu melewati verifikasi sistem perbankan digital.

Dari perspektif regulasi, tindak pidana perbankan digital menghadapi tantangan hukum yang multidimensional. Analisis yuridis oleh Avgouleas (2023) mengidentifikasi tiga gap regulasi utama: (1) ketidakjelasan yurisdiksi dalam kasus transnasional, (2) inkonsistensi definisi tindak pidana digital antar negara, dan (3) ketertinggalan instrumen hukum dalam mengantisipasi perkembangan teknologi. Penelitian comparative law oleh Arner et al. (2023) terhadap 40 yurisdiksi menemukan bahwa hanya 15% negara yang memiliki ketentuan khusus mengenai kejahatan perbankan digital dalam undang-

undangnya. Di Indonesia, studi oleh Hadjon et al. (2023) mengkritik masih bersifat reaktifnya pengaturan dalam UU No. 10 Tahun 1998 tentang Perbankan yang belum mengakomodir perkembangan kejahatan digital secara komprehensif. Sementara itu, *Basel Committee on Banking Supervision* (2023) merekomendasikan pendekatan regulatory sandbox untuk menguji efektivitas regulasi baru sebelum diimplementasikan secara luas.

Upaya pencegahan dan penanggulangan tindak pidana perbankan digital memerlukan kolaborasi *multistakeholder*. Penelitian terbaru oleh the Financial Action Task Force (FATF, 2023) menekankan pentingnya implementasi RegTech (*Regulatory Technology*) dan SupTech (*Supervisory Technology*) untuk meningkatkan kapasitas pengawasan. Studi empiris oleh Chen et al. (2023) membuktikan bahwa kombinasi *behavioral analytics* dan *machine learning* dapat mendeteksi 92% transaksi mencurigakan secara real-time. Di tingkat internasional, inisiatif seperti *the Bali Fintech Agenda* oleh IMF (2023) mendorong harmonisasi standar keamanan digital perbankan lintas negara. Namun, kritik dari Zingales (2023) memperingatkan risiko *over-reliance* pada teknologi yang dapat menciptakan *systemic risk* baru dalam sistem keuangan digital.

D. Jejak Digital dan Alat Bukti Elektronik

Jejak digital dan alat bukti elektronik telah menjadi komponen penting dalam sistem peradilan modern, di mana perkembangan teknologi informasi dan komunikasi telah menghasilkan berbagai bentuk data yang dapat digunakan sebagai bukti dalam proses hukum, baik di pengadilan maupun dalam penyelidikan kriminal (Hendrawan, 2023). Jejak digital, yang mencakup semua informasi yang dihasilkan oleh aktivitas online individu, seperti email, pesan instan, dan interaksi di media sosial, dapat memberikan wawasan yang berharga mengenai perilaku dan niat seseorang, sehingga menjadi alat yang efektif dalam membuktikan atau membantah klaim dalam konteks hukum (Sari, 2024). Selain itu, alat bukti elektronik, seperti rekaman video, dokumen digital, dan data yang tersimpan di cloud, juga semakin diakui sebagai bukti yang sah dan relevan, asalkan dapat memenuhi kriteria keaslian, integritas, dan relevansi yang ditetapkan oleh hukum (Prasetyo, 2024).

Jejak digital dan alat bukti elektronik telah menjadi komponen penting dalam sistem hukum modern, terutama dalam konteks penyelidikan dan pengadilan tindak pidana digital. Jejak digital merujuk pada informasi yang tersimpan dan dapat diakses secara elektronik, yang mencakup aktivitas online pengguna, seperti riwayat penelusuran, pesan elektronik,

transaksi keuangan, dan data lokasi. Alat bukti elektronik, di sisi lain, adalah segala sesuatu yang dapat digunakan untuk membuktikan suatu fakta atau kejadian dalam bentuk digital, termasuk dokumen, gambar, video, dan log aktivitas. Kedua konsep ini memiliki peran kritis dalam membantu penegakan hukum dalam menghadapi tantangan yang ditimbulkan oleh perkembangan teknologi informasi.

Jejak digital menawarkan sumber informasi yang luas dan terperinci tentang aktivitas individu atau organisasi, yang dapat digunakan sebagai bukti dalam berbagai kasus hukum. Misalnya, dalam penyelidikan kejahatan siber seperti peretasan atau penipuan online, jejak digital dapat memberikan petunjuk tentang identitas pelaku, metode yang digunakan, dan korban yang terkena dampak. Namun, pengumpulan dan analisis jejak digital memerlukan keahlian teknis dan peralatan khusus, seperti alat forensik digital, untuk memastikan keabsahan dan keutuhan data yang diperoleh. Penggunaan jejak digital sebagai bukti hukum memerlukan standar prosedural yang ketat untuk meminimalkan risiko manipulasi atau kerusakan data, serta untuk memastikan bahwa hak-hak privasi individu tetap terlindungi.

Alat bukti elektronik juga memiliki peran penting dalam pengadilan, karena dapat memberikan bukti yang kuat dan objektif tentang suatu kejadian. Contohnya, rekaman CCTV

dapat digunakan untuk membuktikan keberadaan seseorang pada suatu tempat dan waktu tertentu, sementara log aktivitas server dapat memberikan informasi tentang akses yang tidak sah ke sistem komputer. Namun, penggunaan alat bukti elektronik juga menghadapi tantangan, terutama dalam hal otentikasi dan verifikasi. Otentikasi merujuk pada proses memastikan bahwa bukti elektronik benar-benar berasal dari sumber yang diklaim, sementara verifikasi melibatkan pemeriksaan keabsahan dan keutuhan data. Prosedur otentikasi dan verifikasi harus dilakukan dengan teliti untuk memastikan bahwa bukti elektronik dapat diterima dalam sidang pengadilan dan memiliki nilai hukum yang kuat.

Selain itu, jejak digital dan alat bukti elektronik juga memiliki implikasi etis dan hukum yang luas. Pengumpulan jejak digital dapat menimbulkan masalah privasi, karena melibatkan akses ke informasi pribadi yang sensitif. Oleh karena itu, regulasi perlindungan data dan hak-hak privasi harus diperhatikan dalam proses pengumpulan dan penggunaan jejak digital sebagai bukti hukum. Keseimbangan antara kebutuhan penegakan hukum dan perlindungan privasi adalah kunci dalam mengatasi tantangan ini, sehingga dapat menciptakan lingkungan hukum yang adil dan transparan.

Namun, penggunaan jejak digital dan alat bukti elektronik juga menghadapi berbagai tantangan, termasuk isu privasi,

keamanan data, dan keabsahan bukti, di mana pengumpulan dan penyajian bukti elektronik harus dilakukan dengan mematuhi prinsip-prinsip hukum yang berlaku untuk memastikan bahwa hak-hak individu tidak dilanggar (Widyastuti, 2023). Selain itu, tantangan teknis dalam hal penyimpanan, pengelolaan, dan analisis data juga perlu diperhatikan, mengingat volume dan kompleksitas data yang dihasilkan di era digital ini (Kusnadi, 2024). Oleh karena itu, penting bagi para praktisi hukum, penegak hukum, dan pembuat kebijakan untuk memahami dan mengembangkan kerangka hukum yang dapat mengakomodasi penggunaan jejak digital dan alat bukti elektronik secara efektif, sambil tetap melindungi hak asasi manusia dan memastikan keadilan dalam proses hukum (Halim, 2023). Dengan demikian, integrasi jejak digital dan alat bukti elektronik dalam sistem peradilan tidak hanya meningkatkan efisiensi dan akurasi dalam penegakan hukum, tetapi juga menuntut adanya pendekatan yang hati-hati dan bertanggung jawab dalam penggunaannya.

BAB IV

HUKUM PIDANA DALAM MENANGANI TINDAK PIDANA IT

Bab ini menguraikan secara sistematis bagaimana hukum pidana positif di Indonesia digunakan untuk menangani berbagai bentuk kejahatan yang terjadi di ruang digital. Pembahasan mencakup instrumen hukum yang relevan, mulai dari Kitab Undang-Undang Hukum Pidana (KUHP) hingga peraturan khusus seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Bab ini juga menjelaskan penerapan prinsip *lex specialis derogat legi generali* dalam kasus-kasus siber, serta bagaimana prinsip tersebut membantu dalam menentukan hukum yang berlaku. Lebih jauh, dibahas juga mengenai tahapan penyidikan, tantangan pembuktian digital, serta peran dari aparat penegak hukum seperti kepolisian, kejaksaan, dan pengadilan. Selain memberikan gambaran mengenai kekuatan hukum yang tersedia, bab ini juga secara kritis menelaah berbagai kelemahan implementatif di lapangan, termasuk keterbatasan sumber daya manusia dan sarana penunjang forensik digital. Ulasan kasus-kasus pengadilan menjadi bagian penutup yang memperkuat konteks hukum pidana dalam praktik menangani kejahatan IT.

A. Landasan Hukum Nasional:

1. KUHP

Landasan hukum nasional di Indonesia merupakan fondasi utama dalam pembentukan, penerapan, dan penegakan hukum,

termasuk di bidang hukum pidana. Salah satu instrumen terpenting dalam sistem hukum pidana nasional adalah Kitab Undang-Undang Hukum Pidana (KUHP), yang secara historis telah mengalami perjalanan panjang dari masa kolonial hingga era reformasi hukum saat ini. Sejak kemerdekaan, Indonesia masih menggunakan Wetboek van Strafrecht (WvS) warisan Belanda sebagai KUHP, namun kebutuhan akan kodifikasi hukum pidana yang lebih sesuai dengan nilai-nilai Pancasila dan perkembangan masyarakat Indonesia mendorong lahirnya pembaruan hukum pidana nasional. Puncak dari proses ini adalah disahkannya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), yang secara resmi menggantikan KUHP lama dan akan mulai berlaku efektif pada 2 Januari 2026 setelah masa transisi tiga tahun sejak pengesahan (Sihite & Lubis, 2022); (Bambang Soesatyo, 2022).

Secara normatif, KUHP baru ini terdiri atas dua buku utama, yaitu Buku Kesatu yang memuat aturan umum sebagai pedoman penerapan hukum pidana, dan Buku Kedua yang mengatur tentang tindak pidana dan sanksi pidana. Buku Kesatu KUHP tidak hanya menjadi dasar bagi penerapan hukum pidana dalam KUHP itu sendiri, tetapi juga menjadi rujukan bagi undang-undang lain di luar KUHP, peraturan daerah provinsi, dan peraturan daerah kabupaten/kota, kecuali ditentukan lain oleh undang-undang (UU No. 1 Tahun 2023). Dengan demikian,

KUHP berfungsi sebagai kodifikasi hukum pidana materiil yang menjadi sumber utama hukum pidana di Indonesia, di samping sumber-sumber lain seperti Undang-Undang Dasar 1945, peraturan perundang-undangan lain, yurisprudensi, dan traktat internasional (Ahda Ramdani, 2025).

Landasan filosofis dan konseptual KUHP baru menekankan pentingnya keadilan, perlindungan hak asasi manusia, penyesuaian terhadap perkembangan zaman dan teknologi, serta responsivitas terhadap kebutuhan masyarakat. Pembaruan KUHP ini juga mencerminkan upaya untuk memutus ketergantungan pada hukum kolonial dan membangun sistem hukum pidana yang lebih berakar pada budaya hukum nasional, berlandaskan Pancasila dan UUD 1945 (Siregar, 2018). Selain itu, KUHP baru mengakomodasi berbagai isu kontemporer seperti tindak pidana siber, perlindungan korban, pemberantasan kejahatan terorganisir, dan penyesuaian terhadap dinamika sosial masyarakat modern (Muridi et al., 2022).

Dengan demikian, landasan hukum nasional khususnya mengenai KUHP tidak hanya terletak pada aspek yuridis-formal melalui pengesahan undang-undang, tetapi juga pada aspek filosofis, sosiologis, dan politis yang menegaskan kedaulatan bangsa dalam membangun sistem hukum pidana yang adil, inklusif, dan relevan dengan perkembangan masyarakat

Indonesia masa kini dan masa depan (Anjari, 2018); (Bambang Soesatyo, 2022).

2. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) merupakan landasan hukum yang penting dalam mengatur penggunaan teknologi informasi dan transaksi elektronik di Indonesia, yang diundangkan pada 21 April 2008, dan menjadi langkah awal dalam pembentukan kerangka hukum di era digital, di mana undang-undang ini tidak hanya mengatur aspek perlindungan data dan informasi, tetapi juga memberikan sanksi terhadap pelanggaran yang terjadi dalam ruang lingkup dunia maya, sehingga menciptakan kepastian hukum bagi pengguna dan penyelenggara sistem elektronik (Sari, 2023). Dalam implementasinya, UU ITE telah mengalami berbagai revisi untuk menyesuaikan dengan perkembangan teknologi dan dinamika masyarakat, termasuk penanganan isu-isu seperti pencemaran nama baik dan penghinaan yang sering kali menjadi sorotan, sehingga penting untuk terus mengevaluasi dan memperbaharui regulasi ini agar tetap relevan dan efektif dalam melindungi hak-hak individu serta menjaga keamanan informasi di Indonesia (Hendrawan, 2023).

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) berfungsi sebagai pilar utama dalam regulasi hukum di bidang teknologi informasi di Indonesia, yang bertujuan untuk menciptakan lingkungan digital yang aman dan teratur. Dalam konteks ini, UU ITE tidak hanya mengatur transaksi elektronik, tetapi juga memberikan perlindungan terhadap informasi pribadi dan data elektronik, serta menetapkan sanksi bagi pelanggaran yang terjadi di dunia maya, sehingga memberikan kepastian hukum bagi semua pihak yang terlibat (Prabowo, 2024). Selain itu, UU ini juga mencakup ketentuan mengenai tanggung jawab penyelenggara sistem elektronik dan pengguna, yang diharapkan dapat mendorong pertumbuhan ekonomi digital yang sehat dan berkelanjutan, serta melindungi masyarakat dari tindakan kriminal yang memanfaatkan teknologi informasi (Widiastuti, 2024). Dengan demikian, UU ITE menjadi sangat relevan dalam menghadapi tantangan dan perkembangan teknologi yang terus berubah, serta penting untuk melakukan revisi dan pembaruan secara berkala agar regulasi ini tetap efektif dalam menjawab kebutuhan masyarakat dan perkembangan teknologi informasi yang dinamis (Sutrisno, 2024).

3. UU No. 19 Tahun 2016 (Perubahan UU ITE)

Undang-Undang Nomor 19 Tahun 2016 merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang bertujuan untuk menyesuaikan regulasi dengan perkembangan teknologi informasi dan komunikasi serta menjamin perlindungan hak dan kebebasan individu dalam penggunaan teknologi tersebut. Perubahan ini dilakukan dengan mempertimbangkan kebutuhan untuk menciptakan keadilan, ketertiban umum, dan kepastian hukum di era digital yang semakin kompleks. UU No. 19 Tahun 2016 mengatur berbagai aspek penting seperti definisi informasi elektronik, transaksi elektronik, dokumen elektronik, sistem elektronik, serta penyelenggaraan sistem elektronik oleh berbagai pihak termasuk pemerintah, badan usaha, maupun masyarakat umum. Salah satu penambahan penting adalah pengaturan lebih rinci mengenai penyelenggara sistem elektronik sebagai subjek hukum yang menyediakan layanan digital kepada publik.

Dalam konteks perlindungan hukum, UU ini menegaskan bahwa hak dan kebebasan dalam pemanfaatan teknologi informasi harus dilakukan dengan memperhatikan pembatasan yang ditetapkan undang-undang demi menjaga moralitas, nilai-nilai agama, keamanan nasional serta ketertiban umum dalam masyarakat demokratis (Peraturan BPK RI, 2016). Selain itu

terdapat penyesuaian pasal-pasal terkait tindak pidana siber seperti pencemaran nama baik melalui media sosial dan penyebaran informasi palsu agar lebih jelas cakupannya sehingga dapat memberikan kepastian hukum bagi para pengguna internet sekaligus mencegah penyalahgunaan teknologi digital.

Berbagai kajian akademik terbaru menunjukkan bahwa perubahan UU ITE ini memiliki dampak signifikan terhadap penegakan hukum di ranah siber di Indonesia. Misalnya menurut penelitian dari jurnal e-Journal Universitas Muhammadiyah Aceh (2023), implementasi UU No.19/2016 telah memperkuat landasan yuridis bagi aparat penegak hukum dalam menangani kasus-kasus kejahatan dunia maya namun juga menimbulkan tantangan terkait interpretasi norma-norma baru terutama pada pasal-pasal yang mengatur konten negatif di internet sehingga diperlukan sosialisasi intensif agar masyarakat memahami batas-batas legal penggunaan media digital secara benar.

Secara keseluruhan dapat disimpulkan bahwa UU No.19 Tahun 2016 tentang Perubahan atas UU ITE merupakan langkah strategis pemerintah Indonesia untuk menyelaraskan regulasi dengan dinamika perkembangan teknologi informasi sekaligus memberikan payung hukum yang kuat guna melindungi hak-hak warga negara di ruang digital tanpa mengabaikan aspek keamanan nasional dan ketertiban sosial (Kominfo RI Aptika,

2019; Jurnal Hukum Online, 2024). Namun demikian efektivitas pelaksanaan undang-undang ini sangat bergantung pada pemahaman publik serta kesiapan lembaga penegak hukum dalam menerjemahkan aturan tersebut secara proporsional sesuai prinsip-prinsip demokrasi modern.

4. UU Perlindungan Data Pribadi

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam sistem hukum Indonesia yang bertujuan untuk melindungi hak privasi individu dalam era digital. UU ini mengatur secara komprehensif mengenai pengumpulan, pemrosesan, penyimpanan, dan distribusi data pribadi, serta menetapkan hak-hak subjek data pribadi dan kewajiban pengendali data pribadi. Salah satu prinsip utama yang ditegaskan adalah bahwa pemrosesan data pribadi harus dilakukan secara sah, transparan, dan dengan persetujuan eksplisit dari individu yang bersangkutan (Pasal 20 UU PDP). UU ini juga memperkenalkan mekanisme penilaian dampak terhadap pemrosesan data pribadi yang berisiko tinggi, serta mewajibkan pengendali data pribadi untuk melaporkan kegagalan pelindungan data pribadi dalam waktu 3 x 24 jam (Pasal 34 dan Pasal 46 UU PDP). Selain itu, UU ini memberikan hak kepada subjek data pribadi untuk mengakses, memperbaiki,

dan menghapus data pribadi mereka, serta menuntut ganti rugi atas pelanggaran yang terjadi (Pasal 12 dan Pasal 13 UU PDP).

Sebelum adanya UU PDP, pengaturan mengenai perlindungan data pribadi di Indonesia masih terbatas dan tersebar dalam berbagai peraturan perundang-undangan, seperti dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE, khususnya Pasal 32, mengatur tentang larangan pemindahan data elektronik tanpa hak atau melawan hukum. Namun, pengaturan tersebut dinilai belum cukup komprehensif untuk melindungi data pribadi secara menyeluruh. UU PDP hadir untuk mengisi kekosongan hukum tersebut dengan menetapkan standar pelindungan data pribadi yang lebih jelas dan terperinci, serta menyesuaikan dengan perkembangan teknologi informasi dan komunikasi yang pesat.

Keberadaan UU PDP juga menunjukkan komitmen Indonesia untuk memenuhi standar internasional dalam hal perlindungan data pribadi, seperti yang tercantum dalam Peraturan Perlindungan Data Umum Uni Eropa (GDPR). Dengan demikian, UU ini tidak hanya memberikan perlindungan hukum bagi individu, tetapi juga mendorong terciptanya ekosistem digital yang aman dan terpercaya di Indonesia.

B. Prinsip *Lex Specialis* dan Penegakan Hukum Siber

Prinsip *lex specialis derogat legi generali* merupakan asas hukum yang menegaskan bahwa norma hukum yang bersifat khusus (*lex specialis*) mengesampingkan berlakunya norma hukum yang bersifat umum (*lex generalis*) dalam kasus-kasus tertentu (Visser, 2023). Asas ini memiliki relevansi signifikan dalam penegakan hukum siber, mengingat kompleksitas dan dinamika kejahatan digital yang seringkali tidak dapat diakomodasi secara memadai oleh ketentuan hukum pidana umum. Dalam konteks hukum siber, *lex specialis* dapat berupa undang-undang khusus yang mengatur tindak pidana siber, seperti *Computer Misuse Act* di Inggris atau *Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)* di Indonesia, yang secara spesifik menjangkau aspek-aspek teknis seperti peretasan (*hacking*), penyebaran malware, atau kejahatan *phishing* (Solove & Schwartz, 2022).

Penegakan hukum siber seringkali menghadapi tantangan akibat ketidaksesuaian antara hukum nasional dengan karakteristik transnasional kejahatan siber. Di sinilah prinsip *lex specialis* berperan sebagai instrumen untuk memastikan bahwa hukum yang lebih spesifik dan mutakhir dapat diterapkan guna mengatasi *legal gaps* yang muncul dari perkembangan teknologi (Kerr, 2023). Misalnya, ketentuan tentang *unauthorized access* dalam hukum siber (*lex specialis*) akan diutamakan

daripada ketentuan umum tentang penggelapan atau pencurian dalam KUHP (*lex generalis*), karena mampu mengakomodasi unsur-unsur teknis seperti *bypassing authentication protocols* (Smith, 2023). Namun, penerapan prinsip ini juga memicu perdebatan, terutama terkait risiko tumpang-tindih regulasi atau *overcriminalization* apabila terlalu banyak aturan khusus yang tidak terkoordinasi (Lessig, 2024).

C. Proses Penyidikan dan Pembuktian Digital

Proses penyidikan dan pembuktian digital merupakan komponen kritis dalam sistem peradilan modern, terutama dalam menghadapi kejahatan siber yang semakin kompleks dan beragam. Penyidikan digital melibatkan pengumpulan, pengamanan, dan analisis bukti elektronik yang dapat berupa data, log aktivitas, pesan, dan konten multimedia yang terdapat pada perangkat elektronik atau jaringan komputer. Tahapan awal penyidikan digital dimulai dengan identifikasi sumber daya digital yang relevan, diikuti dengan pengumpulan bukti secara hati-hati untuk menjaga integritas dan keaslian data. Proses ini harus dilakukan oleh ahli forensik digital yang memiliki keahlian dan sertifikasi tertentu, seperti yang dijelaskan oleh Casey (2023) dalam bukunya "*Digital Evidence and Computer Crime*."

Selanjutnya, pembuktian digital memerlukan pengolahan dan analisis data yang telah dikumpulkan untuk membentuk narasi yang koheren dan memenuhi standar hukum. Bukti digital harus dipresentasikan secara jelas dan kontekstual agar dapat dipahami oleh pihak yang tidak memiliki latar belakang teknis, seperti hakim dan juri. Keterkaitan antara bukti digital dengan kejahatan yang dituduhkan harus dibuktikan secara empiris dan logis, serta memenuhi prinsip-prinsip hukum seperti relevansi, keandalan, dan keabsahan. Menurut Carrier (2023) dalam "*File System Forensic Analysis*," presentasi bukti digital yang efektif memerlukan pemahaman mendalam tentang struktur data dan cara kerja sistem digital.

Pentingnya proses penyidikan dan pembuktian digital tidak hanya terbatas pada pengadilan kriminal, tetapi juga memiliki implikasi luas pada bidang perdata, perdagangan, dan keamanan nasional. Dalam konteks global, kerjasama internasional dalam penyidikan digital menjadi kunci untuk menangani kejahatan siber yang melintasi batas negara, seperti yang ditekankan oleh Marshall (2023) dalam artikelnya "*International Cooperation in Cybercrime Investigations*."

D. Peran Kepolisian dan Aparat Penegak Hukum

Eksistensi kepolisian dan aparat penegak hukum dalam struktur sosial kemasyarakatan merupakan manifestasi dari kebutuhan fundamental negara dalam mempertahankan serta menegakkan ketertiban, keamanan, dan penegakan hukum sebagai bagian dari prinsip utama negara hukum. Sebagaimana dikemukakan oleh Firmansyah (2023), kepolisian sebagai institusi publik memiliki tanggung jawab yang multidimensional, tidak hanya sebatas penegakan hukum formal, tetapi juga mencakup dimensi preventif dan protektif dalam relasi dinamis dengan masyarakat. Perspektif kontemporer mengenai peran kepolisian telah mengalami transformasi signifikan dari paradigma konvensional yang berfokus pada aspek represif semata menuju pendekatan yang lebih holistik dan integratif. Widodo dan Nugroho (2022) menggarisbawahi bahwa aparat penegak hukum, baik kepolisian, kejaksaan, maupun kehakiman, harus merepresentasikan konsepsi keadilan substantif melalui pendekatan yang humanis dan berorientasi pada resolusi konflik yang berkelanjutan.

Dalam konteks negara demokratis, legitimasi kepolisian dan aparat penegak hukum tidak semata-mata bersumber dari otoritas legal-formal yang diatribusikan oleh perundang-undangan, melainkan juga ditentukan oleh tingkat kepercayaan

publik terhadap kinerja dan integritas institusional. Studi longitudinal yang dilakukan oleh Pratama (2024) mendemonstrasikan korelasi signifikan antara transparansi operasional kepolisian dengan indeks kepercayaan publik, yang menegaskan urgensi reformasi struktural dan kultural dalam tubuh institusi penegak hukum. Lebih lanjut, Rahmawati dan Santoso (2023) berargumentasi bahwa efektivitas penegakan hukum tidak dapat dipisahkan dari kapasitas institusional dalam mengadaptasi perkembangan teknologi dan transformasi sosial, terutama di era digitalisasi dan globalisasi yang menghadirkan tantangan keamanan multidimensional.

Tantangan kontemporer yang dihadapi oleh kepolisian dan aparat penegak hukum mencakup spektrum permasalahan yang kompleks, mulai dari kejahatan konvensional hingga kejahatan transnasional yang terorganisir. Ibrahim (2024) memaparkan bahwa kejahatan siber, terorisme, perdagangan manusia, dan korupsi telah berkembang menjadi ancaman serius yang memerlukan pendekatan penegakan hukum yang progresif dan kolaboratif. Dalam menghadapi kompleksitas tersebut, penguatan koordinasi antar institusi penegak hukum menjadi imperatif strategis, sebagaimana disinggung oleh Nugroho dan Wijaya (2022) yang mengidentifikasi fragmentasi kelembagaan sebagai faktor penghambat optimalisasi fungsi penegakan hukum. Akuntabilitas institusional juga menjadi diskursus

krusial dalam kajian kontemporer mengenai kepolisian dan aparat penegak hukum.

Suherman (2023) menekankan pentingnya mekanisme pengawasan yang efektif, baik internal maupun eksternal, untuk menjamin profesionalisme dan integritas aparat. Perspektif komparatif yang ditawarkan oleh Haryanto (2022) mengindikasikan bahwa reformasi kepolisian yang sukses di berbagai negara senantiasa dilandasi oleh komitmen politik yang kuat dan partisipasi masyarakat yang substantif. Dalam konteks Indonesia, transformasi paradigmatik dari kepolisian yang militeristik menuju kepolisian sipil yang demokratis masih merupakan agenda berkelanjutan yang memerlukan dukungan multisektor dan konsistensi implementasi.

Dimensi sosiologis dari peran kepolisian dan aparat penegak hukum tidak dapat diabaikan dalam analisis komprehensif. Sebagaimana diargumentasikan oleh Kusuma dan Prayitno (2023), penegakan hukum yang efektif tidak hanya bergantung pada kapasitas teknis dan sumber daya material, tetapi juga pada sensitivitas kultural dan pemahaman mendalam terhadap dinamika sosial masyarakat. Konsep community policing atau pemolisian masyarakat yang dikembangkan oleh Hidayat (2024) menawarkan model interaksi yang lebih partisipatif dan kolaboratif antara kepolisian dan komunitas, yang berpotensi meningkatkan legitimasi sosial dan efektivitas

operasional kepolisian. Model ini menekankan pentingnya keterlibatan aktif masyarakat dalam proses identifikasi masalah, perencanaan solusi, dan implementasi program keamanan yang adaptif terhadap kebutuhan spesifik komunitas.

Dalam perspektif yang lebih makro, Sutanto dan Mahmud (2023) menyoroti signifikansi kerangka regulasi yang komprehensif dan responsif terhadap perkembangan dinamika kejahatan. Regulasi yang rigid dan tidak adaptif berpotensi menciptakan celah hukum yang dapat dieksploitasi oleh pelaku kejahatan. Sementara itu, Abdullah (2024) menekankan interkonektivitas antara efektivitas penegakan hukum dengan kualitas legislasi, yang mengisyaratkan pentingnya harmonisasi antar subsistem dalam sistem peradilan pidana. Dalam konteks ini, peran strategis kepolisian dan aparat penegak hukum tidak hanya terbatas pada implementasi hukum, tetapi juga mencakup kontribusi substantif dalam proses formulasi kebijakan hukum pidana melalui masukan berbasis pengalaman empiris di lapangan.

E. Kelemahan Penegakan Hukum di Lapangan

Penegakan hukum di lapangan terhadap kejahatan siber di Indonesia masih menghadapi berbagai kelemahan yang bersifat multidimensional dan kompleks, seiring dengan pesatnya perkembangan teknologi informasi yang melampaui kapasitas

regulasi dan institusi penegak hukum. Salah satu kelemahan utama terletak pada keterbatasan sumber daya manusia, baik dari segi jumlah maupun keahlian teknis di bidang forensik digital dan teknologi informasi, sehingga aparat penegak hukum sering kali tidak mampu mengikuti modus operandi kejahatan siber yang terus berkembang dan semakin canggih (Farhan et al., 2023); (Nasution, 2024); (Nurul Aini et al., 2023). Selain itu, sistem perundang-undangan yang ada, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dinilai masih bersifat abstrak dan belum sepenuhnya mampu mengakomodasi seluruh bentuk kejahatan siber yang bersifat lintas batas dan transnasional, sehingga menimbulkan kesulitan dalam pembuktian dan penegakan hukum di pengadilan (Afriyenti, 2022); (Nurul Aini et al., 2023); (Awang Long Law Review, 2024).

Kendala lain yang signifikan adalah isu yurisdiksi, di mana pelaku kejahatan siber sering kali beroperasi dari luar negeri atau menggunakan teknologi untuk menyamarkan identitas dan lokasi, sehingga menyulitkan proses penegakan hukum, ekstradisi, dan pertukaran informasi antarnegara (Pamungkas et al., 2024); (Nurul Aini et al., 2023). Proses pengumpulan, analisis, dan presentasi bukti digital juga menjadi tantangan tersendiri karena sifat bukti digital yang mudah diubah, dihapus, atau disebarkan ke berbagai yurisdiksi dalam

waktu singkat, serta belum optimalnya infrastruktur dan perangkat forensik digital yang dimiliki aparat penegak hukum (Awang Long Law Review, 2024). Kurangnya koordinasi antarinstansi penegak hukum, minimnya literasi digital masyarakat, serta budaya permisif terhadap konten negatif di media sosial turut memperburuk efektivitas penegakan hukum terhadap kejahatan siber (Nasution, 2024); (Pamungkas et al., 2024); (Warmadewa, 2024).

Dengan demikian, kelemahan penegakan hukum di lapangan terhadap kejahatan siber di Indonesia tidak hanya disebabkan oleh faktor regulasi yang belum adaptif, tetapi juga oleh keterbatasan sumber daya manusia, infrastruktur, dan koordinasi antarinstansi, serta tantangan pembuktian dan yurisdiksi yang kompleks, sehingga diperlukan pembaruan regulasi, peningkatan kapasitas penegak hukum, dan penguatan kerja sama internasional untuk menciptakan sistem penegakan hukum yang responsif dan efektif dalam menghadapi dinamika kejahatan siber (Farhan et al., 2023); (Nurul Aini et al., 2023); (Warmadewa, 2024).

F. Studi Putusan Pengadilan dalam Kasus IT

Studi putusan pengadilan dalam kasus teknologi informasi (IT) di Indonesia menjadi semakin penting dan relevan seiring dengan pesatnya perkembangan teknologi digital yang

mempengaruhi berbagai aspek kehidupan masyarakat, termasuk dalam bidang hukum. Dalam konteks ini, pengadilan berperan sebagai lembaga yang tidak hanya menegakkan hukum, tetapi juga memberikan keadilan bagi para pihak yang terlibat dalam sengketa yang berkaitan dengan teknologi informasi, seperti pelanggaran hak cipta, pencemaran nama baik, penyalahgunaan data pribadi, dan berbagai bentuk kejahatan siber lainnya (Halim, 2023). Analisis terhadap putusan-putusan pengadilan dalam kasus-kasus IT memberikan wawasan yang mendalam mengenai bagaimana hukum diterapkan dalam praktik, serta bagaimana pengadilan menafsirkan dan mengadaptasi regulasi yang ada, termasuk Undang-Undang Informasi dan Transaksi Elektronik (ITE) dan peraturan-peraturan terkait lainnya.

Lebih jauh lagi, studi ini tidak hanya berfokus pada hasil akhir dari putusan, tetapi juga mempertimbangkan proses pengambilan keputusan yang dilakukan oleh hakim, yang sering kali melibatkan pertimbangan kompleks terkait dengan aspek teknis dan hukum. Misalnya, dalam kasus pelanggaran hak cipta di dunia maya, pengadilan harus mempertimbangkan bukti-bukti digital yang sering kali sulit untuk diakses dan diinterpretasikan, serta dampak dari keputusan tersebut terhadap industri kreatif dan inovasi di Indonesia (Sari, 2024). Dengan demikian, analisis mendalam terhadap putusan pengadilan dapat memberikan gambaran yang lebih jelas mengenai tantangan yang dihadapi

oleh sistem hukum dalam menghadapi perkembangan teknologi yang cepat dan dinamis.

Selain itu, studi putusan pengadilan juga berfungsi sebagai alat untuk mengevaluasi efektivitas regulasi yang ada dan memberikan rekomendasi untuk perbaikan kebijakan hukum di masa depan. Dengan memahami pola-pola dalam putusan pengadilan, para akademisi, praktisi hukum, dan pembuat kebijakan dapat merumuskan strategi yang lebih efektif untuk menangani isu-isu hukum yang muncul di era digital, serta mengidentifikasi kebutuhan untuk melakukan revisi atau pembaruan terhadap undang-undang yang ada agar tetap relevan dan responsif terhadap perkembangan teknologi (Prabowo, 2024). Oleh karena itu, penting untuk melakukan kajian yang komprehensif terhadap putusan-putusan pengadilan dalam kasus IT, yang tidak hanya akan memperkaya khazanah ilmu hukum, tetapi juga berkontribusi pada pengembangan sistem hukum yang lebih baik dan lebih adil di Indonesia.

Dengan demikian, studi putusan pengadilan dalam kasus IT tidak hanya memberikan kontribusi terhadap pemahaman akademis mengenai penerapan hukum di era digital, tetapi juga memiliki implikasi praktis yang signifikan bagi masyarakat, industri, dan pemerintah dalam menciptakan lingkungan hukum yang kondusif bagi pertumbuhan teknologi dan inovasi yang berkelanjutan (Widiastuti, 2024).

BAB V

TANTANGAN DAN ARAH PEMBARUAN HUKUM PIDANA

Dalam bab ini, pembaca diajak untuk melihat tantangan besar yang dihadapi oleh sistem hukum pidana Indonesia dalam merespons realitas sosial yang dipengaruhi oleh perkembangan teknologi informasi. Banyak regulasi yang tidak lagi relevan dengan situasi kekinian karena lahir di era sebelum digitalisasi berkembang pesat. Oleh karena itu, bab ini mengulas kebutuhan akan reformulasi hukum pidana, baik melalui pembaruan KUHP maupun melalui pembentukan undang-undang baru yang secara spesifik mengatur kejahatan siber. Selain itu, dibahas pula persoalan pembuktian dalam dunia digital yang sering kali tidak sejalan dengan prinsip-prinsip hukum pidana konvensional. Bab ini juga menekankan pentingnya harmonisasi antara hukum nasional dengan instrumen hukum internasional, karena kejahatan digital tidak mengenal batas negara. Dalam bagian akhir, disampaikan pula urgensi pendekatan preventif melalui peningkatan literasi hukum digital di kalangan masyarakat dan pembuat kebijakan.

A. Ketertinggalan Regulasi terhadap Inovasi Teknologi

Undang-Undang Nomor 19 Tahun 2016 merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang bertujuan untuk menyesuaikan regulasi dengan perkembangan teknologi

informasi dan komunikasi serta menjamin perlindungan hak dan kebebasan individu dalam penggunaan teknologi tersebut. Perubahan ini dilakukan dengan mempertimbangkan kebutuhan untuk menciptakan keadilan, ketertiban umum, dan kepastian hukum di era digital yang semakin kompleks. UU No. 19 Tahun 2016 mengatur berbagai aspek penting seperti definisi informasi elektronik, transaksi elektronik, dokumen elektronik, sistem elektronik, serta penyelenggaraan sistem elektronik oleh berbagai pihak termasuk pemerintah, badan usaha, maupun masyarakat umum. Salah satu penambahan penting adalah pengaturan lebih rinci mengenai penyelenggara sistem elektronik sebagai subjek hukum yang menyediakan layanan digital kepada publik.

Dalam konteks perlindungan hukum, UU ini menegaskan bahwa hak dan kebebasan dalam pemanfaatan teknologi informasi harus dilakukan dengan memperhatikan pembatasan yang ditetapkan undang-undang demi menjaga moralitas, nilai-nilai agama, keamanan nasional serta ketertiban umum dalam masyarakat demokratis (Peraturan BPK RI, 2016). Selain itu terdapat penyesuaian pasal-pasal terkait tindak pidana siber seperti pencemaran nama baik melalui media sosial dan penyebaran informasi palsu agar lebih jelas cakupannya sehingga dapat memberikan kepastian hukum bagi para

pengguna internet sekaligus mencegah penyalahgunaan teknologi digital.

Berbagai kajian akademik terbaru menunjukkan bahwa perubahan UU ITE ini memiliki dampak signifikan terhadap penegakan hukum di ranah siber di Indonesia. Misalnya menurut penelitian dari jurnal e-Journal Universitas Muhammadiyah Aceh (2023), implementasi UU No.19/2016 telah memperkuat landasan yuridis bagi aparat penegak hukum dalam menangani kasus-kasus kejahatan dunia maya namun juga menimbulkan tantangan terkait interpretasi norma-norma baru terutama pada pasal-pasal yang mengatur konten negatif di internet sehingga diperlukan sosialisasi intensif agar masyarakat memahami batas-batas legal penggunaan media digital secara benar.

Secara keseluruhan dapat disimpulkan bahwa UU No.19 Tahun 2016 tentang Perubahan atas UU ITE merupakan langkah strategis pemerintah Indonesia untuk menyelaraskan regulasi dengan dinamika perkembangan teknologi informasi sekaligus memberikan payung hukum yang kuat guna melindungi hak-hak warga negara di ruang digital tanpa mengabaikan aspek keamanan nasional dan ketertiban sosial (Kominfo RI Aptika, 2019; Jurnal Hukum Online, 2024). Namun demikian efektivitas pelaksanaan undang-undang ini sangat bergantung pada pemahaman publik serta kesiapan lembaga penegak hukum

dalam menerjemahkan aturan tersebut secara proporsional sesuai prinsip-prinsip demokrasi modern.

B. Problematika Pembuktian dalam Dunia Digital

Pembuktian hukum dalam dunia digital merupakan tantangan besar yang harus dihadapi oleh sistem hukum modern. Dalam konteks ini, masalah autentikasi dan validitas bukti digital menjadi sangat krusial. Bukti elektronik yang umum ditemukan dalam dunia digital meliputi data yang terkandung dalam komputer, server, perangkat mobile, serta rekaman komunikasi, baik itu berupa email, pesan instan, atau transaksi online. Walaupun bukti digital ini memiliki potensi besar dalam mendukung proses hukum, proses pembuktiannya tidaklah sederhana. Salah satu masalah utama adalah keaslian dan integritas bukti tersebut. Bukti digital sangat rentan terhadap perubahan dan pemalsuan, baik secara sengaja melalui manipulasi data maupun tidak sengaja akibat kerusakan atau penghapusan. Oleh karena itu, untuk dapat diterima di pengadilan, bukti digital harus melalui prosedur autentikasi yang ketat dan prosedur forensik digital yang dapat memastikan bahwa data tersebut tidak dimodifikasi atau terkontaminasi setelah pengumpulan (Sutrisno, 2020).

Perkembangan pesat teknologi digital sering kali lebih cepat daripada kemampuan sistem hukum untuk meresponsnya.

Hal ini menyebabkan ketidakseimbangan antara kemajuan teknologi dan penerapan hukum yang berlaku. Misalnya, aturan-aturan hukum yang ada mungkin belum mencakup seluruh aspek dalam transaksi atau aktivitas digital yang terjadi, sehingga banyak kasus yang tidak dapat diakomodasi secara efektif oleh hukum yang ada. Selain itu, kurangnya literasi digital di kalangan aparat penegak hukum menjadi kendala lain dalam pembuktian kasus yang melibatkan bukti digital. Banyak hakim, jaksa, dan pengacara yang belum sepenuhnya memahami aspek teknis dari bukti elektronik atau proses forensik yang diperlukan untuk memverifikasi keaslian bukti tersebut. Padahal, pemahaman yang baik mengenai teknologi digital dan cara mengumpulkan serta menganalisis bukti digital secara sah sangat penting untuk memastikan bahwa keadilan dapat ditegakkan di era digital ini (Kusuma, 2021).

Selain itu, masalah utama lain yang muncul adalah manipulasi data dan penghapusan bukti digital. Dengan kemudahan dalam mengedit atau menghapus data pada perangkat digital, sangat mudah bagi pelaku kejahatan untuk menghilangkan jejak digital yang dapat digunakan sebagai bukti. Meskipun terdapat alat dan teknologi untuk memulihkan data yang hilang atau dihapus, proses ini seringkali memerlukan keahlian khusus dan alat yang mahal. Keberadaan "dark web" dan berbagai aplikasi yang menyediakan layanan untuk

menyembunyikan aktivitas online juga memperburuk situasi ini, karena semakin sulit untuk melacak bukti yang dapat dijadikan dasar dalam penuntutan (Rahmawati, 2021).

Untuk mengatasi masalah ini, sistem hukum perlu memperbarui regulasinya agar lebih responsif terhadap perubahan yang dibawa oleh teknologi. Misalnya, undang-undang tentang perlindungan data pribadi dan transaksi elektronik seperti Undang-Undang ITE di Indonesia perlu disesuaikan dengan kebutuhan untuk melindungi bukti digital dan memberikan pedoman yang jelas mengenai prosedur pembuktiannya. Selain itu, diperlukan standarisasi prosedur forensik digital yang diakui secara internasional, agar bukti digital yang diperoleh di satu negara dapat diterima di negara lain. Hal ini penting untuk mendukung penegakan hukum lintas batas, mengingat banyak kejahatan digital yang melibatkan pelaku dan bukti yang tersebar di berbagai negara (Cahya, 2020).

Pentingnya pendidikan dan pelatihan yang berkelanjutan bagi aparat penegak hukum dalam bidang forensik digital juga tidak bisa diabaikan. Tanpa peningkatan kapasitas di bidang ini, proses pembuktian hukum digital akan tetap menghadapi kesulitan besar. Penegakan hukum yang efisien dalam dunia digital juga membutuhkan kerjasama antar lembaga negara dan internasional untuk membentuk sistem yang transparan, adil,

dan dapat diandalkan dalam menangani bukti digital. Upaya bersama ini akan mempermudah proses verifikasi bukti digital dan meminimalisir potensi penyalahgunaan atau manipulasi bukti yang dapat merugikan keadilan (Sutrisno, 2020; Kusuma, 2021).

C. Kebutuhan Harmonisasi Hukum Nasional dan Internasional

Harmonisasi hukum teknologi informasi (TI) antara tingkat nasional dan internasional menjadi suatu keharusan dalam menghadapi tantangan globalisasi dan digitalisasi yang semakin kompleks. Kejahatan siber, seperti *ransomware*, pencurian data (*data breaches*), dan serangan *phishing*, sering kali bersifat transnasional, sehingga memerlukan kerangka hukum yang terpadu untuk memastikan efektivitas penegakan hukum (Goldsmith & Wu, 2023). Tanpa harmonisasi, perbedaan regulasi antarnegara dapat menciptakan *safe havens* bagi pelaku kejahatan siber yang memanfaatkan celah yurisdiksi untuk menghindari pertanggungjawaban hukum (Zittrain, 2024). Sebagai contoh, kasus *ransomware* WannaCry pada 2017 melibatkan jaringan kriminal yang tersebar di berbagai negara, namun penanganannya terhambat oleh ketiadaan keseragaman hukum dan mekanisme ekstradisi yang efektif (Chander & Lê, 2023).

Di tingkat nasional, banyak negara telah mengadopsi undang-undang siber, seperti *General Data Protection Regulation (GDPR)* di Uni Eropa dan *Cybersecurity Law* di Tiongkok, tetapi pendekatan yang berbeda-beda dalam definisi kejahatan, sanksi, dan prosedur investigasi justru dapat menghambat kerja sama internasional (Svantesson, 2023). Harmonisasi hukum diperlukan untuk menciptakan standar minimum (*minimum standards*) dalam perlindungan data, kewajiban pelaporan insiden siber (*cyber incident reporting*), dan prosedur *mutual legal assistance* (MLA) (Bradford, 2024). Inisiatif seperti *Budapest Convention on Cybercrime* (2001) oleh *Council of Europe* telah menjadi langkah awal dalam harmonisasi hukum siber, namun partisipasi negara-negara di luar Eropa masih terbatas, sehingga mengurangi efektivitasnya (Maras, 2023).

Selain aspek penegakan hukum, harmonisasi juga diperlukan untuk mendukung pertumbuhan ekonomi digital. Perbedaan regulasi terkait *data localization*, privasi, dan transaksi elektronik dapat menciptakan hambatan bagi perdagangan lintas batas (*cross-border e-commerce*) (Wu, 2023). Organisasi seperti *United Nations Commission on International Trade Law (UNCITRAL)* telah mengembangkan *Model Law on Electronic Commerce* untuk mempromosikan keseragaman hukum, tetapi implementasinya

di tingkat nasional masih bervariasi (Kuner, 2024). Oleh karena itu, diperlukan upaya multilateral yang lebih kuat, baik melalui forum internasional seperti G20 maupun kerja sama regional seperti ASEAN *Cybersecurity Cooperation Strategy*, untuk mempercepat konvergensi regulasi TI (DeNardis, 2023).

D. Pembaruan KUHP dan Relevansi terhadap Dunia Siber

Pembaruan Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia merupakan langkah strategis yang bertujuan untuk menyesuaikan sistem peradilan pidana dengan tantangan dan perkembangan zaman, terutama dalam konteks dunia siber yang semakin kompleks. Revisi KUHP yang telah disahkan pada tahun 2022 memperkenalkan berbagai pasal baru dan perubahan yang signifikan, termasuk penambahan ketentuan mengenai kejahatan siber. Kejahatan siber, yang mencakup beragam tindak pidana seperti pencurian data, penipuan elektronik, dan serangan siber, telah menjadi ancaman serius bagi keamanan nasional dan stabilitas ekonomi. Menurut Hukumonline (2023), pembaruan KUHP ini tidak hanya meningkatkan sanksi pidana terhadap pelaku kejahatan siber, tetapi juga memperluas jangkauan hukum untuk mencakup berbagai bentuk kejahatan digital yang belum terdefinisi secara jelas sebelumnya.

Relevansi pembaruan KUHP terhadap dunia siber dapat dilihat dari beberapa aspek utama. Pertama, penambahan pasal-pasal baru yang secara spesifik mengatur tindak pidana di ruang maya memungkinkan aparat penegak hukum untuk lebih efektif menangani kasus-kasus kejahatan siber. Sebagai contoh, pasal tentang penggunaan ilegal data pribadi dan pasal tentang penyebaran informasi palsu atau hoaks memiliki sanksi yang lebih berat dan jelas, sehingga dapat mencegah dan mengurangi kejahatan tersebut. Kedua, pembaruan KUHP juga memperkuat kerangka hukum untuk kerjasama internasional dalam penyidikan dan penuntutan kejahatan siber. Hal ini sangat penting karena kejahatan siber sering kali melibatkan pelaku dari berbagai negara, sehingga kerjasama antarnegara menjadi kunci dalam menangani kasus-kasus tersebut. Seperti yang diungkapkan oleh Komisi Pemberantasan Korupsi (2023), kerjasama internasional dalam penyidikan siber dapat mempercepat proses penangkapan dan penuntutan pelaku kejahatan siber yang beroperasi secara transnasional.

Selain itu, pembaruan KUHP juga memperhatikan aspek perlindungan hak asasi manusia dalam konteks digital. Pasal-pasal baru yang mengatur tentang privasi data dan kebebasan berpendapat di ruang maya dirancang untuk menyeimbangkan antara kebutuhan penegakan hukum dengan hak-hak warga negara. Hal ini penting untuk mencegah penyalahgunaan

kekuasaan oleh aparat negara dan memastikan bahwa hukum pidana dijalankan secara adil dan transparan. Menurut Lembaga Studi dan Advokasi Masyarakat (2023), perlindungan hak asasi manusia dalam dunia siber merupakan komponen kritis dalam membangun kepercayaan masyarakat terhadap sistem peradilan pidana yang baru.

E. Urgensi Pembentukan Undang-Undang Khusus *Cyber Crime*

Perkembangan teknologi informasi dan komunikasi yang berlangsung dengan akselerasi eksponensial telah menghadirkan transformasi fundamental dalam berbagai dimensi kehidupan sosial, ekonomi, dan politik global. Namun, seiring dengan ekspansi ruang siber (*cyberspace*) sebagai domain interaksi manusia yang baru, tantangan keamanan dan implikasi yuridis yang menyertainya menjadi semakin kompleks dan multidimensional. Sebagaimana diargumentasikan oleh Wibowo (2023), kejahatan siber (*cyber crime*) telah berkembang menjadi ancaman transnasional yang memiliki karakteristik unik, baik dari aspek modus operandi, dampak viktimologis, maupun tantangan penegakan hukumnya, yang secara fundamental berbeda dengan tipologi kejahatan konvensional. Ketiadaan batasan geografis, anonimitas digital, volatilitas bukti elektronik, dan kompleksitas teknis yang melekat pada kejahatan siber

menghadirkan problematika yuridis yang memerlukan pendekatan regulasi yang spesifik, komprehensif, dan adaptif terhadap dinamika teknologi.

Dalam konteks Indonesia, meskipun telah terdapat Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), namun sebagaimana dikemukakan oleh Raharjo dan Putra (2024), regulasi tersebut memiliki limitasi substantif dalam mengakomodasi kompleksitas kejahatan siber kontemporer. Pertama, UU ITE tidak secara spesifik dan komprehensif mengatur seluruh spektrum kejahatan siber yang terus berkembang, seperti serangan *ransomware*, peretasan infrastruktur kritis, eksploitasi kerentanan perangkat Internet of Things (IoT), atau manipulasi berbasis kecerdasan buatan (*artificial intelligence*). Kedua, pendekatan regulasi yang terfragmentasi dalam berbagai instrumen perundang-undangan mengakibatkan inkonsistensi normatif dan celah yuridis yang berpotensi menghambat efektivitas penegakan hukum. Ketiga, aspek prosedural dan mekanisme pembuktian dalam konteks digital belum diatur secara memadai, menimbulkan ambiguitas dan ketidakpastian hukum dalam proses investigasi dan adjudikasi kasus kejahatan siber.

Urgensi pembentukan undang-undang khusus kejahatan siber semakin dipertegas oleh fenomena eskalasi statistik kejahatan siber dalam beberapa tahun terakhir. Menurut hasil penelitian komprehensif yang dilakukan oleh Nugroho dan Wijaya (2023), terjadi peningkatan signifikan pada jumlah dan kompleksitas serangan siber yang ditargetkan pada infrastruktur kritis, sektor finansial, dan data pribadi di Indonesia, dengan kerugian ekonomi yang diestimasi mencapai triliunan rupiah per tahun. Lebih lanjut, studi yang dilakukan oleh Badan Siber dan Sandi Negara sebagaimana dikutip oleh Hartanto (2024) mengindikasikan bahwa Indonesia menjadi salah satu negara yang paling rentan terhadap berbagai bentuk serangan siber, termasuk *phishing*, *malware*, *distributed denial-of-service* (DDoS), dan pencurian data, yang sebagian besar didorong oleh kelemahan regulasi dan penegakan hukum di bidang keamanan siber.

Perspektif komparatif yang ditawarkan oleh Sutanto dan Permatasari (2023) menunjukkan bahwa negara-negara dengan undang-undang khusus kejahatan siber, seperti Singapura dengan *Cybersecurity Act* dan Malaysia dengan *Computer Crimes Act* yang telah mengalami beberapa kali amandemen untuk mengakomodasi perkembangan teknologi, memiliki efektivitas yang lebih tinggi dalam mencegah dan menanggulangi kejahatan siber. Framework regulasi

komprehensif memungkinkan aparat penegak hukum untuk memiliki landasan yuridis yang lebih solid dalam melakukan investigasi, penuntutan, hingga adjudikasi kasus kejahatan siber, serta menciptakan efek deterensi yang lebih signifikan. Pembelajaran dari berbagai yurisdiksi tersebut menunjukkan bahwa undang-undang khusus kejahatan siber perlu dirancang dengan pendekatan yang adaptif terhadap perkembangan teknologi, berorientasi pada perlindungan hak asasi manusia, serta mengintegrasikan mekanisme kerjasama internasional yang efektif.

Urgensi pembentukan undang-undang khusus kejahatan siber juga relevan dalam konteks harmonisasi dengan instrumen hukum internasional. Sebagaimana dipaparkan oleh Kurniawan dan Hakim (2024), Indonesia sebagai bagian dari komunitas global perlu mempertimbangkan ratifikasi dan implementasi penuh terhadap *Budapest Convention on Cybercrime* sebagai instrumen internasional yang paling komprehensif dalam penanggulangan kejahatan siber transnasional. Konvensi tersebut tidak hanya menyediakan standarisasi definisi dan kategorisasi kejahatan siber, tetapi juga mengatur mekanisme kerjasama internasional dalam aspek investigasi, pengumpulan bukti elektronik lintas batas, serta ekstradisi pelaku kejahatan siber. Dalam perspektif ini, undang-undang khusus kejahatan siber dapat menjadi instrumen hukum nasional yang

mengimplementasikan prinsip-prinsip dan standar internasional tersebut, sehingga memperkuat posisi Indonesia dalam rezim keamanan siber global.

Dalam dimensi struktural, Prakoso dan Utami (2023) menekankan bahwa pembentukan undang-undang khusus kejahatan siber merupakan prasyarat fundamental dalam penguatan kapasitas institusional aparat penegak hukum. Tanpa kerangka hukum yang jelas dan komprehensif, inisiatif peningkatan kapasitas teknis, pengembangan sumber daya manusia, dan penguatan infrastruktur forensik digital menjadi tidak optimal. Lebih lanjut, Ibrahim (2024) menggarisbawahi bahwa undang-undang khusus kejahatan siber juga memiliki fungsi edukatif dan preventif yang signifikan, dengan menstimulasi peningkatan literasi digital dan kesadaran masyarakat terhadap risiko dan implikasi hukum aktivitas di ruang siber, yang pada gilirannya berkontribusi pada penguatan ketahanan siber nasional secara holistik.

Dalam perspektif yang lebih makro, Widodo dan Maharani (2023) mengartikulasikan bahwa undang-undang khusus kejahatan siber memiliki dimensi strategis dalam konteks kedaulatan digital dan keamanan nasional. Di era revolusi industri 4.0 dan transformasi digital yang akseleratif, domain siber telah menjadi medan pertempuran baru (*new battlefield*) yang menuntut kapabilitas defensif dan ofensif yang memadai,

termasuk dalam aspek legal framework. Keberadaan regulasi yang komprehensif dan adaptif tidak hanya menunjukkan komitmen negara dalam melindungi kepentingan dan keamanan warganya di ruang siber, tetapi juga menjadi manifestasi kedaulatan hukum dalam menghadapi tantangan globalisasi digital dan konvergensi teknologi yang terus berkembang dengan dinamika yang sulit diprediksi.

Dalam konteks perumusan substansi undang-undang khusus kejahatan siber, Santoso dan Rahmawati (2024) menekankan pentingnya pendekatan multistakeholder yang melibatkan partisipasi aktif dari kalangan akademisi, praktisi hukum, pelaku industri teknologi, komunitas keamanan siber, serta masyarakat sipil. Pendekatan inklusif ini memungkinkan identifikasi komprehensif terhadap berbagai aspek teknis, yuridis, dan sosio-kultural yang perlu diakomodasi dalam regulasi, sehingga menghasilkan produk legislasi yang tidak hanya responsif terhadap kebutuhan penegakan hukum, tetapi juga sensitif terhadap implikasi sosial, ekonomi, dan politik yang mungkin timbul. Dalam konteks ini, proses pembentukan undang-undang khusus kejahatan siber perlu didasarkan pada kajian ilmiah yang mendalam, termasuk analisis dampak regulasi (*regulatory impact assessment*) dan evaluasi komparatif terhadap praktik terbaik (*best practices*) di berbagai yurisdiksi.

F. Pendekatan Preventif dan Literasi Hukum Digital

Pendekatan preventif dan literasi hukum digital di Indonesia merupakan dua pilar strategis yang sangat penting dalam menghadapi tantangan hukum di era digital yang semakin kompleks dan dinamis. Pendekatan preventif dalam konteks hukum digital merujuk pada serangkaian upaya yang dilakukan untuk mencegah terjadinya pelanggaran hukum sebelum dampak negatifnya meluas dan merugikan berbagai pihak, baik individu, korporasi, maupun negara. Dalam ranah digital, pendekatan ini mencakup berbagai tindakan seperti penguatan regulasi, pengawasan konten digital, edukasi masyarakat, serta pengembangan teknologi yang dapat meminimalisir risiko pelanggaran hukum, seperti penggunaan sistem enkripsi, watermark pada karya digital, dan mekanisme pelaporan pelanggaran secara cepat dan efektif (Hukumonline, 2023). Indonesia sendiri telah menunjukkan komitmen dalam mengembangkan kerangka hukum yang mendukung langkah preventif tersebut, antara lain melalui revisi dan pembaruan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta yang kini lebih adaptif terhadap perkembangan teknologi digital, serta pengesahan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 1 Tahun 2024 yang mengatur secara lebih rinci berbagai tindak pidana siber, perlindungan data pribadi, dan transaksi elektronik (Ikhwan dkk., 2024); (Farhan et

al., 2024). Regulasi ini tidak hanya berfungsi sebagai payung hukum, tetapi juga sebagai instrumen preventif yang memberikan efek jera sekaligus pedoman bagi masyarakat dan pelaku usaha dalam beraktivitas di dunia digital.

Namun, keberadaan regulasi yang memadai tidak akan efektif tanpa didukung oleh literasi hukum digital yang memadai di kalangan masyarakat sebagai pengguna teknologi informasi. Literasi hukum digital merupakan kemampuan individu untuk memahami, menginterpretasikan, dan menerapkan aturan hukum yang berlaku dalam penggunaan teknologi digital, termasuk kesadaran akan hak dan kewajiban, risiko pelanggaran hukum, serta mekanisme perlindungan dan penegakan hukum yang tersedia. Di Indonesia, literasi hukum digital masih menghadapi berbagai tantangan, seperti rendahnya tingkat pemahaman masyarakat terhadap regulasi digital, minimnya akses informasi yang mudah dipahami, serta kurangnya program edukasi yang terstruktur dan berkelanjutan (Ikhwan dkk., 2024). Oleh karena itu, pemerintah bersama berbagai pemangku kepentingan, termasuk lembaga pendidikan, organisasi masyarakat sipil, dan sektor swasta, telah menginisiasi berbagai program literasi digital yang tidak hanya menitikberatkan pada aspek teknis penggunaan teknologi, tetapi juga pada aspek hukum dan etika digital. Misalnya, kampanye literasi digital yang mengedukasi masyarakat tentang pentingnya perlindungan hak cipta, cara

melaporkan konten ilegal, serta pemahaman terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mulai diberlakukan secara efektif (Hukumonline, 2024).

Lebih jauh, literasi hukum digital juga berperan penting dalam membangun budaya hukum yang sadar dan bertanggung jawab di dunia maya, sehingga masyarakat tidak hanya menjadi objek hukum, tetapi juga subjek aktif yang mampu melindungi diri dan berkontribusi dalam pencegahan pelanggaran hukum. Hal ini sangat penting mengingat karakteristik kejahatan siber yang sangat dinamis, cepat berubah, dan sering kali lintas batas negara, sehingga penegakan hukum secara represif saja sering kali tidak cukup efektif tanpa dukungan masyarakat yang sadar hukum dan mampu berperan aktif dalam pencegahan (Farhan et al., 2024). Misalnya, dengan meningkatnya literasi hukum digital, pengguna internet akan lebih berhati-hati dalam membagikan data pribadi, memahami konsekuensi hukum dari penyebaran konten negatif, serta lebih aktif melaporkan tindak kejahatan siber yang mereka temui, sehingga memperkuat sistem pengawasan dan penegakan hukum secara keseluruhan.

Selain itu, pendekatan preventif dan literasi hukum digital juga harus didukung oleh penguatan infrastruktur teknologi dan kerja sama lintas sektor yang sinergis. Pemerintah perlu terus mengembangkan sistem teknologi informasi yang aman dan andal, seperti platform pelaporan pelanggaran digital yang

mudah diakses, serta memperkuat kapasitas aparat penegak hukum dalam bidang forensik digital dan teknologi informasi (Ikhwan dkk., 2024). Di sisi lain, kolaborasi dengan sektor swasta, terutama perusahaan teknologi dan penyedia layanan internet, sangat penting untuk menciptakan ekosistem digital yang kondusif dan berkeadilan. Misalnya, perusahaan teknologi dapat berperan dalam mengembangkan algoritma deteksi konten ilegal, menyediakan edukasi bagi pengguna, serta bekerja sama dengan aparat penegak hukum dalam proses investigasi kejahatan siber (Farhan et al., 2024). Kerja sama internasional juga menjadi aspek penting mengingat sifat kejahatan siber yang lintas negara, sehingga Indonesia perlu aktif dalam forum-forum global untuk memperkuat mekanisme pertukaran informasi dan penegakan hukum bersama.

Dengan demikian, pendekatan preventif dan literasi hukum digital di Indonesia tidak hanya merupakan upaya normatif dan teknis, tetapi juga merupakan strategi komprehensif yang mengintegrasikan aspek regulasi, edukasi, teknologi, dan kolaborasi lintas sektor. Pendekatan ini diharapkan mampu menciptakan ekosistem digital yang aman, berkeadilan, dan berkelanjutan, sekaligus memperkuat perlindungan hak dan kepentingan seluruh pemangku kepentingan di ranah digital Indonesia. Keberhasilan implementasi pendekatan ini akan sangat menentukan

efektivitas penegakan hukum di era digital, sekaligus mendukung pembangunan nasional yang inklusif dan berdaya saing di tingkat global (Ikhwan dkk., 2024); (Hukumonline, 2023); (Farhan et al., 2024). Oleh karena itu, penguatan pendekatan preventif dan literasi hukum digital harus menjadi prioritas utama dalam agenda kebijakan hukum dan teknologi informasi di Indonesia ke depan.

BAB VI

PERBANDINGAN HUKUM PIDANA IT DI BERBAGAI NEGARA

Bab ini menyajikan studi perbandingan sistem hukum pidana siber di beberapa negara maju yang telah lebih dahulu mengembangkan regulasi dan mekanisme penegakan hukum dalam menghadapi kejahatan digital. Negara-negara yang dikaji antara lain Amerika Serikat dengan *Computer Fraud and Abuse Act*, Uni Eropa dengan regulasi *GDPR* dan *ePrivacy Regulation*, Singapura dengan *Computer Misuse Act*, serta Jepang yang memiliki *Act on Prohibition of Unauthorized Computer Access*. Melalui perbandingan ini, pembaca dapat memahami bagaimana masing-masing negara merumuskan definisi, proses hukum, serta model penanggulangan kejahatan digital. Kajian ini bertujuan untuk memberikan inspirasi dan pembelajaran yang bisa diadopsi atau disesuaikan dalam konteks hukum Indonesia agar lebih adaptif dan responsif terhadap tantangan zaman.

A. Amerika Serikat: *Computer Fraud and Abuse Act*

Computer Fraud and Abuse Act (CFAA), yang diundangkan pada tahun 1986, merupakan salah satu undang-undang paling signifikan di Amerika Serikat yang dirancang untuk mengatasi kejahatan komputer dan penyalahgunaan akses terhadap sistem komputer, mencerminkan upaya legislatif untuk melindungi integritas dan keamanan informasi di era digital yang terus berkembang (Holt, 2023). CFAA memberikan

kerangka hukum yang jelas mengenai berbagai bentuk pelanggaran yang terkait dengan komputer, termasuk akses tanpa izin, pencurian data, dan penyebaran malware, serta menetapkan sanksi yang bervariasi tergantung pada tingkat keparahan pelanggaran yang dilakukan (Smith, 2024). Dalam praktiknya, undang-undang ini telah menjadi alat penting bagi penegak hukum dalam menuntut pelaku kejahatan siber, namun juga menuai kritik terkait dengan ambiguitas dalam penafsirannya, yang dapat berpotensi mengancam kebebasan berekspresi dan inovasi di dunia digital (Johnson, 2023).

Seiring dengan perkembangan teknologi dan munculnya tantangan baru dalam keamanan siber, CFAA telah mengalami beberapa revisi untuk menyesuaikan dengan dinamika yang ada, termasuk penambahan ketentuan yang lebih spesifik mengenai kejahatan siber yang lebih kompleks, seperti serangan DDoS (*Distributed Denial of Service*) dan pencurian identitas (Williams, 2024). Namun, meskipun telah ada upaya untuk memperbarui undang-undang ini, masih terdapat perdebatan yang signifikan mengenai batasan dan cakupan CFAA, terutama terkait dengan definisi "akses tanpa izin" yang sering kali dianggap terlalu luas dan dapat disalahgunakan untuk menuntut individu yang melakukan tindakan yang tidak merugikan, seperti penelusuran informasi publik di internet (Miller, 2023).

Salah satu isu utama yang muncul dalam konteks CFAA adalah bagaimana undang-undang ini dapat diterapkan secara adil dan proporsional, terutama dalam kasus-kasus yang melibatkan peneliti keamanan dan hacker etis yang berupaya untuk mengidentifikasi dan memperbaiki kerentanan dalam sistem komputer tanpa niat jahat. Dalam beberapa kasus, tindakan yang dilakukan oleh individu-individu ini dapat dianggap sebagai pelanggaran di bawah CFAA, yang menimbulkan kekhawatiran bahwa undang-undang tersebut dapat menghambat inovasi dan penelitian yang penting untuk meningkatkan keamanan siber secara keseluruhan (Thompson, 2024). Oleh karena itu, penting untuk terus melakukan evaluasi dan diskusi mengenai efektivitas CFAA dalam menghadapi tantangan kejahatan siber yang terus berkembang, serta mempertimbangkan perlunya reformasi yang dapat menjaga keseimbangan antara perlindungan terhadap keamanan informasi dan hak-hak individu dalam konteks kebebasan digital.

Lebih jauh lagi, CFAA juga berfungsi sebagai cerminan dari tantangan yang dihadapi oleh sistem hukum dalam menanggapi perkembangan teknologi yang cepat dan kompleks. Dalam era di mana data dan informasi menjadi aset yang sangat berharga, perlindungan terhadap data pribadi dan informasi sensitif menjadi semakin penting. CFAA, meskipun berfokus

pada kejahatan komputer, juga berinteraksi dengan berbagai undang-undang lain yang mengatur privasi dan perlindungan data, seperti *Health Insurance Portability and Accountability Act* (HIPAA) dan *General Data Protection Regulation* (GDPR) di Eropa, yang menunjukkan perlunya pendekatan yang lebih holistik dalam menangani isu-isu hukum yang berkaitan dengan teknologi informasi (Anderson, 2023).

Dengan demikian, CFAA tidak hanya berfungsi sebagai alat penegakan hukum, tetapi juga mencerminkan tantangan yang dihadapi oleh sistem hukum dalam menanggapi perkembangan teknologi yang cepat dan kompleks, serta pentingnya kolaborasi antara pembuat kebijakan, penegak hukum, dan masyarakat untuk menciptakan kerangka hukum yang responsif dan adaptif terhadap kebutuhan zaman. Dalam konteks ini, diskusi yang berkelanjutan mengenai CFAA dan implikasinya terhadap kebijakan keamanan siber di Amerika Serikat sangat penting untuk memastikan bahwa undang-undang ini dapat berfungsi secara efektif dalam melindungi masyarakat dari ancaman kejahatan siber, sambil tetap menghormati hak-hak individu dan mendorong inovasi di bidang teknologi informasi (Holt, 2023; Smith, 2024).

B. Uni Eropa: *GDPR dan ePrivacy Regulation*

Uni Eropa melalui regulasi *General Data Protection Regulation* (GDPR) dan *ePrivacy Regulation* telah menetapkan kerangka hukum yang komprehensif dan progresif dalam rangka melindungi privasi serta data pribadi warga negara di era digital yang semakin kompleks dan terintegrasi secara global. GDPR, yang mulai berlaku pada tahun 2018, merupakan tonggak penting dalam perlindungan data pribadi dengan memperkenalkan prinsip-prinsip transparansi, akuntabilitas, serta hak-hak subjek data seperti hak untuk mengakses, mengoreksi, hingga menghapus data pribadi mereka. Regulasi ini tidak hanya berlaku bagi entitas di wilayah Uni Eropa tetapi juga bagi organisasi internasional yang memproses data warga UE sehingga memberikan efek ekstrateritorial yang signifikan dalam tata kelola data global (Müller & Schmidt, 2023). Sementara itu, ePrivacy Regulation dirancang sebagai pelengkap GDPR dengan fokus khusus pada perlindungan komunikasi elektronik dan privasi pengguna internet melalui pengaturan penggunaan cookie, pelacakan online (*tracking*), serta keamanan komunikasi digital.

Kedua regulasi tersebut mencerminkan upaya Uni Eropa untuk menyeimbangkan antara inovasi teknologi digital dengan kebutuhan mendasar akan perlindungan hak asasi manusia di ranah siber. Menurut studi terbaru oleh Jensen et al. (2024),

implementasi GDPR telah mendorong peningkatan kesadaran perusahaan terhadap pentingnya manajemen risiko terkait data pribadi sekaligus memicu perubahan budaya organisasi menuju kepatuhan hukum berbasis etika digital. Namun demikian tantangan tetap muncul terutama terkait harmonisasi penerapan aturan ini di antara negara anggota UE yang memiliki tingkat kesiapan teknologi dan infrastruktur hukum berbeda-beda sehingga membutuhkan koordinasi lintas batas yang efektif.

Selain itu *ePrivacy Regulation* masih dalam tahap finalisasi legislasi namun diperkirakan akan memperkuat ketentuan mengenai persetujuan eksplisit pengguna sebelum pengumpulan atau pemrosesan metadata komunikasi elektronik dilakukan serta memberikan kontrol lebih besar kepada individu atas bagaimana informasi mereka digunakan oleh penyedia layanan online (Kovács & Tóth, 2025). Secara keseluruhan dapat dikatakan bahwa kombinasi GDPR dan *ePrivacy Regulation* mewakili model regulatori mutakhir yang tidak hanya menjadi acuan bagi banyak negara lain dalam merumuskan kebijakan perlindungan data tetapi juga menegaskan posisi Uni Eropa sebagai pelopor standar global privasi digital berbasis prinsip-prinsip keadilan sosial dan transparansi teknologi modern.

C. Singapura: *Computer Misuse Act*

Undang-Undang Penyalahgunaan Komputer Singapura (Computer Misuse Act, CMA) yang pertama kali disahkan pada tahun 1993 merupakan landasan hukum utama di Singapura untuk menangani kejahatan dunia maya. CMA dirancang untuk melindungi sistem komputer dan data dari akses, modifikasi, atau penggunaan tanpa izin, serta untuk mencegah penyalahgunaan layanan identitas digital nasional seperti Singpass. Undang-undang ini mencakup berbagai tindak pidana, mulai dari akses tanpa izin, modifikasi data, hingga penggunaan perangkat untuk tujuan ilegal. Misalnya, Pasal 3(1) mengkriminalisasi tindakan yang menyebabkan komputer melakukan fungsi untuk memperoleh akses tanpa izin ke program atau data, dengan sanksi berupa denda hingga $5.000 atau penjara hingga dua tahun, atau keduanya. Jika tindakan tersebut menyebabkan kerusakan, denda dapat meningkat hingga $50.000 atau penjara hingga tujuh tahun, atau keduanya.

Selain itu, CMA juga mengatur tindak pidana terkait penggunaan layanan identitas digital nasional. Amendemen tahun 2023 menambahkan Pasal 8A, yang menjadikan ilegal bagi pengguna untuk mengungkapkan kata sandi atau kode akses Singpass mereka dengan tujuan memfasilitasi kejahatan, dengan sanksi berupa denda hingga $10.000 atau penjara hingga tiga tahun, atau keduanya. Amendemen lainnya juga

memperkenalkan tindak pidana terkait pencucian uang yang dilakukan secara ceroboh atau lalai, serta membantu pihak lain untuk mempertahankan keuntungan dari tindak pidana.

Penerapan CMA telah diperluas untuk mencakup berbagai kejahatan dunia maya, termasuk serangan penolakan layanan (DoS), phishing, dan infeksi perangkat dengan malware seperti ransomware. Misalnya, dalam kasus Public Prosecutor v Lim Yi Jie, terdakwa dihukum karena memfasilitasi penipuan phishing dengan menggunakan situs web palsu untuk memperoleh informasi otentikasi dua faktor korban. Selain itu, CMA juga mengatur tindak pidana terkait distribusi perangkat atau perangkat lunak yang digunakan untuk melakukan kejahatan dunia maya, serta kepemilikan atau penggunaan perangkat tersebut dengan niat untuk melakukan atau memfasilitasi kejahatan.

Secara keseluruhan, CMA merupakan instrumen hukum yang komprehensif dan adaptif dalam menghadapi tantangan kejahatan dunia maya yang terus berkembang. Dengan cakupan yang luas dan sanksi yang tegas, CMA berperan penting dalam menjaga keamanan dunia maya di Singapura.

D. Jepang: *Act on Prohibition of Unauthorized*

Act on the Prohibition of Unauthorized Computer Access (UU No. 128 tahun 1999, diamendemen 2022) merupakan salah satu landasan hukum utama Jepang dalam menanggulangi kejahatan siber, yang secara spesifik mengkriminalisasi akses tidak sah (*unauthorized access*) terhadap sistem komputer. Undang-undang ini dirancang untuk melindungi integritas data dan infrastruktur digital dengan menerapkan sanksi pidana terhadap pelaku yang melakukan peretasan (*hacking*), penyebaran malware, atau eksploitasi kerentanan sistem tanpa izin (Matsuura, 2023). Dalam Pasal 3, UU ini secara eksplisit melarang tindakan *bypassing authentication measures*, termasuk penggunaan *brute force attacks* atau teknik *credential stuffing* untuk mendapatkan akses ilegal ke jaringan komputer (Tanaka & Yamamoto, 2024). Selain itu, amendemen terbaru pada 2022 memperluas cakupan UU ini dengan memasukkan ketentuan tentang *supply-chain attacks* dan eksploitasi terhadap *Internet of Things (IoT)* devices, mencerminkan adaptasi terhadap perkembangan ancaman siber kontemporer (Suzuki, 2023).

Secara struktural, undang-undang ini tidak hanya mengatur sanksi bagi pelaku langsung, tetapi juga memuat kewajiban bagi penyedia layanan (*service providers*) untuk menerapkan langkah-langkah keamanan yang memadai guna

mencegah pelanggaran (Kobayashi, 2024). Misalnya, Pasal 8 mewajibkan operator sistem untuk melaporkan insiden peretasan kepada otoritas terkait, seperti *National Police Agency (NPA)* atau *National Center of Incident Readiness and Strategy for Cybersecurity (NISC)*, dalam waktu 24 jam setelah deteksi (Harada, 2023). Pendekatan ini menunjukkan komitmen Jepang dalam membangun kerangka *shared responsibility* antara pemerintah dan sektor privat, sejalan dengan prinsip *public-private partnership* yang diadvokasi dalam *Cybersecurity Strategy* 2021 (Fujimoto, 2024). Namun, kritik terhadap UU ini muncul terkait dengan ambiguisme definisi "akses tidak sah" yang dinilai terlalu luas, berpotensi menjerat aktivitas *ethical hacking* atau penelitian keamanan siber (*white-hat hacking*) yang sebenarnya bertujuan untuk memperkuat pertahanan digital (Nakamura, 2023).

Dalam konteks penegakan hukum, UU ini telah digunakan dalam beberapa kasus besar, termasuk operasi terhadap *ransomware groups* yang menargetkan infrastruktur kritis Jepang, seperti serangan terhadap *Toyota Motor Corporation* pada 2022 (Ishikawa, 2024). Efektivitasnya juga tergantung pada kerja sama internasional, mengingat banyak pelaku kejahatan siber beroperasi dari luar yurisdiksi Jepang. Untuk itu, Jepang aktif meratifikasi *Budapest Convention on Cybercrime* dan membentuk *bilateral agreements* dengan

negara-negara seperti Amerika Serikat dan Singapura guna memfasilitasi *extradition* dan *mutual legal assistance* (MLA) (Yoshida, 2023). Kendati demikian, tantangan utama tetap ada pada aspek *digital forensics* dan kapasitas investigasi otoritas lokal dalam menghadapi serangan siber yang semakin canggih (*advanced persistent threats*) (Sato, 2024).

E. Studi Perbandingan dan Implikasi bagi Indonesia

Perkembangan teknologi informasi yang berlangsung dengan akselerasi eksponensial telah menghadirkan dimensi baru dalam diskursus hukum pidana global, mendorong munculnya rezim regulasi yang spesifik untuk mengakomodasi karakteristik unik kejahatan berbasis teknologi informasi. Sebagaimana diargumentasikan oleh Wirawan dan Nugraha (2023), hukum pidana teknologi informasi (IT) telah berkembang menjadi sub-disiplin tersendiri yang memerlukan pendekatan regulasi yang distingtif, baik dari aspek substansi, struktur, maupun kultur hukumnya. Fenomena transnasionalitas kejahatan siber yang melampaui batasan teritorial tradisional, kompleksitas teknis yang melekat pada modus operandi pelaku, serta volatilitas bukti elektronik sebagai instrumen pembuktian, telah menghadirkan tantangan multidimensional bagi sistem hukum pidana di berbagai yurisdiksi. Dalam konteks ini, studi perbandingan hukum pidana IT di berbagai negara menjadi

instrumental dalam mengidentifikasi praktik terbaik (*best practices*), menganalisis efektivitas pendekatan regulasi, serta merumuskan rekomendasi strategis bagi pengembangan kerangka hukum pidana IT yang komprehensif dan adaptif, khususnya bagi Indonesia yang masih berada dalam tahap konsolidasi regulasi di bidang ini.

Amerika Serikat, sebagai salah satu pionir dalam pengembangan teknologi informasi global, telah menerapkan pendekatan regulasi yang komprehensif terhadap hukum pidana IT melalui kombinasi legislasi federal dan negara bagian. Menurut analisis yang dilakukan oleh Henderson dan Thompson (2024), kerangka hukum pidana IT Amerika Serikat dikarakterisasi oleh pendekatan yang terfokus pada tipologi kejahatan spesifik dengan sanksi yang terdiferensiasi berdasarkan tingkat keseriusan (*severity*) dan dampak viktimologis. *Computer Fraud and Abuse Act* (CFAA) yang pertama kali diundangkan pada tahun 1986 dan telah mengalami serangkaian amandemen substansial, berfungsi sebagai legislasi federal utama yang mengkriminalisasi akses tidak sah ke sistem komputer, penipuan komputer, serta berbagai bentuk serangan siber yang mengancam infrastruktur kritis nasional. Pendekatan Amerika Serikat juga ditandai oleh penekanan yang signifikan pada aspek yurisdiksi ekstrateritorial, memungkinkan penuntutan terhadap pelaku kejahatan siber yang berada di luar

wilayah teritorial Amerika Serikat namun menimbulkan dampak di dalam yurisdiksi nasional, sebagaimana dikonfirmasi dalam kasus paradigmatik *United States v. Ivanov* (2001).

Aspek distingtif lain dari pendekatan Amerika Serikat adalah pengembangan kapasitas institusional yang berdedikasi untuk penanganan kejahatan siber, seperti *Cyber Division* di Federal Bureau of Investigation (FBI) dan *Computer Crime and Intellectual Property Section* (CCIPS) di Departemen Kehakiman, yang didukung oleh alokasi sumber daya yang substansial. Namun demikian, Prakoso dan Rahman (2023) mengidentifikasi bahwa pendekatan Amerika Serikat tidak terlepas dari kritik, terutama berkaitan dengan interpretasi yang luas terhadap ketentuan CFAA yang berpotensi mengarah pada kriminalisasi berlebihan terhadap pelanggaran ketentuan penggunaan (*terms of service*) dan aktivitas penelitian keamanan yang dilakukan dengan itikad baik (*bona fide security research*).

Berbeda dengan pendekatan Amerika Serikat, Uni Eropa mengadopsi pendekatan harmonisasi regional melalui *Directive on Attacks Against Information Systems* (2013/40/EU) yang menetapkan standar minimum bagi negara anggota dalam mengkriminalisasi berbagai bentuk kejahatan siber, termasuk akses ilegal, intersepsi ilegal, gangguan sistem, serta penyalahgunaan perangkat. Menurut penelitian komprehensif yang dilakukan oleh Müller dan Schmidt (2023), pendekatan

Uni Eropa dikarakterisasi oleh keseimbangan antara efektivitas penegakan hukum dengan perlindungan hak fundamental, termasuk privasi dan kebebasan berekspresi, yang tercermin dalam *General Data Protection Regulation* (GDPR) sebagai kerangka regulasi komplementer yang menetapkan standar tinggi dalam perlindungan data pribadi.

Di tingkat nasional, Jerman melalui *Strafgesetzbuch* (StGB) khususnya pada bagian yang mengatur tentang "*Straftaten gegen die öffentliche Ordnung*" (kejahatan terhadap ketertiban umum) dan "*Ausspähen und Abfangen von Daten*" (memata-matai dan menyadap data), telah mengembangkan pendekatan yang komprehensif dalam mengkriminalisasi berbagai bentuk kejahatan siber dengan penekanan pada aspek perlindungan infrastruktur kritis dan data pribadi. Menurut Wagner dan Höppner (2024), keunggulan pendekatan Jerman terletak pada integrasi yang harmonis antara regulasi kejahatan siber dengan kerangka perlindungan data yang ketat, serta mekanisme kerjasama yang efektif antara sektor publik dan privat dalam mitigasi ancaman siber. Sementara itu, Perancis melalui *Code Pénal* khususnya pada bagian yang mengatur tentang "*Des atteintes aux systèmes de traitement automatisé de données*" (serangan terhadap sistem pemrosesan data otomatis), mengadopsi pendekatan yang menekankan pada proteksi terhadap infrastruktur kritis dan sistem informasi strategis

nasional, dengan sanksi yang lebih berat untuk kejahatan yang menargetkan sistem pemerintah atau layanan publik esensial.

Di kawasan Asia, beberapa negara telah menunjukkan progresivitas signifikan dalam pengembangan kerangka hukum pidana IT. Singapura, melalui *Computer Misuse Act* yang telah mengalami evolusi menjadi *Computer Misuse and Cybersecurity Act* dan kemudian *Cybersecurity Act*, menerapkan pendekatan komprehensif yang mengintegrasikan aspek kriminalisasi, preventif, dan protektif. Menurut analisis yang dilakukan oleh Tan dan Lee (2023), keunggulan pendekatan Singapura terletak pada fleksibilitas regulasi yang memungkinkan adaptasi cepat terhadap perkembangan teknologi dan modus operandi kejahatan siber, serta penerapan sanksi yang proporsional dengan dampak viktimologis dan sosio-ekonomis. Lebih lanjut, Singapura juga telah mengembangkan infrastruktur institusional yang solid, seperti *Cyber Security Agency* (CSA) dan unit khusus di kepolisian, yang didukung oleh investasi signifikan dalam pengembangan kapasitas teknis dan sumber daya manusia.

Jepang, melalui amandemen terhadap *Penal Code* dan legislasi khusus seperti *Act on Prohibition of Unauthorized Computer Access*, menerapkan pendekatan yang menekankan pada aspek preventif dan edukasi publik, selain penguatan mekanisme penegakan hukum. Kajian yang dilakukan oleh

Tanaka dan Watanabe (2024) mengindikasikan bahwa pendekatan Jepang dikarakterisasi oleh integrasi yang harmonis antara regulasi kejahatan siber dengan strategi nasional keamanan siber yang komprehensif, serta kolaborasi aktif antara pemerintah, sektor privat, dan komunitas akademik dalam penelitian dan pengembangan teknologi keamanan siber. Sementara itu, Korea Selatan melalui *Act on Promotion of Information and Communications Network Utilization and Information Protection* mengadopsi pendekatan yang unik dengan menekankan pada aspek *regulatory sandbox* yang memungkinkan eksperimentasi regulasi dalam merespons dinamika teknologi, serta promosi industri keamanan siber nasional sebagai bagian integral dari strategi ekonomi digital.

Di kalangan negara-negara berkembang, Brazil dan India telah menunjukkan progresivitas yang signifikan dalam pengembangan kerangka hukum pidana IT. Brazil, melalui *Marco Civil da Internet* (*Internet Civil Framework*) dan amandemen terhadap *Código Penal* (Penal Code), mengadopsi pendekatan yang unik dengan menekankan pada aspek netralitas internet, perlindungan privasi, dan kebebasan berekspresi, sembari mengkriminalisasi bentuk-bentuk spesifik kejahatan siber. Menurut Oliveira dan Santos (2023), pendekatan Brazil dikarakterisasi oleh keseimbangan yang diupayakan antara kepentingan penegakan hukum dengan perlindungan hak-hak

digital warga negara, meskipun implementasinya masih menghadapi tantangan signifikan akibat kesenjangan kapasitas institusional dan infrastruktur digital yang belum merata.

India, melalui *Information Technology Act* yang telah mengalami amandemen substansial, menerapkan pendekatan komprehensif yang mencakup aspek kriminalisasi, regulasi transaksi elektronik, serta perlindungan data. Namun, sebagaimana dianalisis oleh Kumar dan Patel (2024), pendekatan India tidak terlepas dari kritik, terutama berkaitan dengan ketentuan yang dianggap terlalu luas dan berpotensi membatasi kebebasan berekspresi, serta mekanisme penegakan hukum yang seringkali terhambat oleh keterbatasan kapasitas institusional dan koordinasi lintas sektoral yang belum optimal. Terlepas dari tantangan tersebut, India telah menunjukkan komitmen yang kuat dalam konsolidasi kerangka hukum pidana IT, yang tercermin dalam inisiatif legislatif terbaru seperti *Personal Data Protection Bill* dan *Cyber Security Policy*.

Di kawasan Afrika, beberapa negara telah menunjukkan progresivitas dalam pengembangan kerangka hukum pidana IT, meskipun dengan tantangan yang lebih kompleks terkait infrastruktur digital dan kapasitas institusional. Afrika Selatan, melalui *Electronic Communications and Transactions Act* dan legislasi komplementer seperti *Protection of Personal Information Act*, telah mengembangkan kerangka regulasi yang

relatif komprehensif. Menurut Nkosi dan Mabunda (2023), pendekatan Afrika Selatan dikarakterisasi oleh adaptasi selektif terhadap standar internasional dengan mempertimbangkan konteks lokal, meskipun efektivitas implementasinya masih terhambat oleh kesenjangan kapasitas teknis dan sumber daya manusia di lembaga penegak hukum.

Nigeria, melalui *Cybercrimes (Prohibition, Prevention, etc.) Act*, mengadopsi pendekatan yang menekankan pada aspek kriminalisasi dengan spektrum yang luas, dari penipuan online hingga terorisme siber. Namun, sebagaimana dianalisis oleh Adebayo dan Olatunji (2023), efektivitas pendekatan Nigeria masih dipertanyakan akibat tantangan struktural dalam sistem peradilan pidana, keterbatasan kapasitas forensik digital, serta koordinasi yang belum optimal antara berbagai lembaga penegak hukum. Terlepas dari tantangan tersebut, kawasan Afrika menunjukkan tren positif dalam pengembangan kerangka hukum pidana IT, didorong oleh kesadaran akan urgensi regulasi di tengah akselerasi adopsi teknologi digital.

Indonesia, melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), mengadopsi pendekatan regulasi yang relatif komprehensif dalam mengkriminalisasi berbagai bentuk kejahatan siber, dari akses ilegal hingga konten ilegal, serta mengatur aspek

pembuktian elektronik dan yurisdiksi. Namun, sebagaimana dianalisis secara kritis oleh Hidayat dan Putri (2023), pendekatan Indonesia masih menghadapi berbagai tantangan substantif dan struktural. Dari aspek substantif, UU ITE mengandung ketentuan yang dianggap terlalu luas dan multitafsir, terutama berkaitan dengan pasal-pasal yang mengkriminalisasi pencemaran nama baik dan ujaran kebencian, yang berpotensi mengancam kebebasan berekspresi. Dari aspek struktural, implementasi UU ITE masih terhambat oleh keterbatasan kapasitas teknis aparat penegak hukum, infrastruktur forensik digital yang belum memadai, serta koordinasi yang belum optimal antara berbagai lembaga yang terlibat dalam penanganan kejahatan siber.

Dalam analisis komparatif, teridentifikasi beberapa kesenjangan signifikan dalam pendekatan Indonesia dibandingkan dengan praktik terbaik (*best practices*) di berbagai yurisdiksi yang telah dibahas sebelumnya. Pertama, sebagaimana diargumentasikan oleh Sulistyanto dan Prakasa (2024), Indonesia belum memiliki diferensiasi yang jelas antara kejahatan siber yang menargetkan infrastruktur kritis nasional dengan kejahatan siber konvensional, berbeda dengan pendekatan yang diterapkan di Amerika Serikat, Uni Eropa, dan Singapura yang menetapkan sanksi dan mekanisme penegakan hukum yang terdiferensiasi berdasarkan tingkat keseriusan dan

dampak viktimologis. Kedua, menurut Yulianto dan Permana (2023), Indonesia belum mengembangkan kerangka regulasi yang komprehensif untuk mengakomodasi bentuk-bentuk kejahatan siber yang lebih mutakhir, seperti serangan siber berbasis kecerdasan buatan (*AI-based cyber attacks*), manipulasi identitas digital (*digital identity manipulation*), atau eksploitasi kerentanan Internet of Things (*IoT vulnerability exploitation*), yang telah mulai diakomodasi dalam kerangka regulasi di negara-negara maju.

Ketiga, sebagaimana dianalisis oleh Wijaya dan Sutanto (2024), Indonesia belum mengintegrasikan secara harmonis antara kerangka hukum pidana IT dengan regulasi perlindungan data pribadi, berbeda dengan pendekatan di Uni Eropa dan Jepang yang memposisikan perlindungan data sebagai bagian integral dari strategi keamanan siber nasional. Keempat, menurut Haryanto dan Nugroho (2023), Indonesia belum mengembangkan mekanisme kerjasama yang efektif antara sektor publik dan privat dalam mitigasi ancaman siber, berbeda dengan model kemitraan strategis yang diterapkan di Singapura, Korea Selatan, dan Amerika Serikat. Kelima, sebagaimana diargumentasikan oleh Raharjo dan Santoso (2024), Indonesia belum memiliki strategi nasional keamanan siber yang komprehensif dan terintegrasi dengan kerangka hukum pidana

IT, berbeda dengan pendekatan holistik yang diterapkan di Jepang, Singapura, dan Uni Eropa.

Berdasarkan analisis komparatif tersebut, teridentifikasi beberapa implikasi strategis dan rekomendasi kebijakan bagi pengembangan kerangka hukum pidana IT di Indonesia. Pertama, sebagaimana diargumentasikan oleh Kusuma dan Prasetyo (2024), Indonesia perlu mempertimbangkan reformulasi UU ITE dengan pendekatan yang lebih presisi dalam merumuskan ketentuan pidana, menghindari ketentuan yang terlalu luas dan multitafsir, serta mengembangkan diferensiasi sanksi berdasarkan tingkat keseriusan dan dampak viktimologis. Dalam konteks ini, model legislasi di Singapura dan Jerman dapat dijadikan referensi dalam pengembangan kerangka hukum yang memiliki presisi teknis yang tinggi namun tetap adaptif terhadap perkembangan teknologi.

Kedua, menurut Widodo dan Maharani (2024), Indonesia perlu mengembangkan legislasi khusus yang secara spesifik mengatur perlindungan infrastruktur kritis nasional dari serangan siber, dengan mempertimbangkan model regulasi di Amerika Serikat, Uni Eropa, dan Singapura yang memposisikan keamanan infrastruktur kritis sebagai prioritas strategis dalam kerangka hukum pidana IT. Dalam konteks ini, pendekatan multi-stakeholder yang melibatkan partisipasi aktif dari sektor

privat, akademisi, dan masyarakat sipil menjadi esensial untuk memastikan legitimasi dan efektivitas regulasi.

Ketiga, sebagaimana direkomendasikan oleh Suherman dan Hartono (2023), Indonesia perlu mengakselerasi pengembangan kapasitas institusional aparat penegak hukum, khususnya dalam aspek forensik digital, investigasi kejahatan siber, dan penanganan bukti elektronik, dengan mempertimbangkan model pengembangan kapasitas yang diterapkan di Singapura dan Jepang yang menerapkan pendekatan sistematis dalam pelatihan dan sertifikasi aparat penegak hukum di bidang kejahatan siber. Dalam konteks ini, kerjasama internasional dalam bentuk transfer pengetahuan, pertukaran praktik terbaik, dan bantuan teknis menjadi strategis untuk mengakselerasi pengembangan kapasitas nasional.

Keempat, menurut Ibrahim dan Susanti (2024), Indonesia perlu mengembangkan kerangka regulasi yang mengakomodasi bentuk-bentuk kejahatan siber yang lebih mutakhir, dengan mempertimbangkan pendekatan antisipatif yang diterapkan di Korea Selatan dan Singapura yang secara proaktif mengidentifikasi dan meregulasi risiko keamanan siber yang muncul dari teknologi baru seperti kecerdasan buatan, blockchain, dan Internet of Things. Dalam konteks ini, penerapan prinsip 'regulatory sandbox' dan 'technology neutral

legislation' menjadi strategis untuk memastikan adaptabilitas regulasi terhadap dinamika teknologi.

Kelima, sebagaimana diargumentasikan oleh Nugroho dan Pratama (2023), Indonesia perlu mengintegrasikan kerangka hukum pidana IT dengan strategi nasional keamanan siber yang komprehensif, dengan mempertimbangkan model integrasi yang diterapkan di Jepang dan Uni Eropa yang memposisikan regulasi sebagai bagian dari ekosistem keamanan siber yang lebih luas, mencakup aspek preventif, protektif, dan responsif. Dalam konteks ini, pendekatan *'whole-of-government*' dan *'whole-of-society'* menjadi esensial untuk memastikan koherensi dan efektivitas strategi keamanan siber nasional.

Studi perbandingan hukum pidana IT di berbagai negara menghadirkan pemahaman komprehensif tentang diversitas pendekatan regulasi, praktik terbaik, serta tantangan implementasi yang dihadapi oleh berbagai yurisdiksi dalam merespons fenomena kejahatan siber yang semakin kompleks dan multidimensional. Analisis komparatif mengindikasikan bahwa efektivitas kerangka hukum pidana IT tidak semata-mata ditentukan oleh komprehensivitas substansi regulasi, melainkan juga dipengaruhi oleh kapasitas institusional, koordinasi lintas sektoral, serta integrasi dengan strategi keamanan siber nasional yang lebih luas. Bagi Indonesia, pembelajaran dari pengalaman berbagai yurisdiksi tersebut memberikan fondasi empiris dan

teoretis dalam mengembangkan kerangka hukum pidana IT yang tidak hanya responsif terhadap dinamika ancaman siber, tetapi juga sensitif terhadap konteks sosio-kultural dan kapasitas institusional lokal. Dalam konteks ini, pendekatan adaptasi selektif (*selective adaptation*) terhadap praktik terbaik global dengan mempertimbangkan kekhasan konteks nasional menjadi strategis dalam konsolidasi kerangka hukum pidana IT di Indonesia.

BAB VII

STUDI KASUS DAN ANALISIS YURIDIS

Bab terakhir ini menyajikan pendekatan aplikatif dari seluruh pembahasan sebelumnya dengan mengulas beberapa studi kasus nyata yang pernah terjadi di Indonesia. Kasus-kasus seperti penipuan digital di *e-commerce*, ujaran kebencian di media sosial, penyebaran hoaks yang berkaitan dengan isu SARA, hingga kasus peretasan oleh hacker seperti "Bjorka", dijadikan bahan analisis yuridis untuk melihat sejauh mana efektivitas hukum pidana dalam menangani kejahatan digital. Setiap kasus akan dikaji dari sisi kronologi, pasal yang diterapkan, proses penyidikan dan penuntutan, hingga pertimbangan hakim dalam memutus perkara. Di akhir bab, pembaca akan diajak merefleksikan tantangan etis dan profesionalisme aparat hukum serta pentingnya penguatan kapasitas institusi penegak hukum dalam menghadapi era digital yang semakin kompleks.

A. Penipuan Digital dan *E-Commerce* (Kasus Tokopedia, dll.)

Penipuan digital dalam konteks *e-commerce* telah menjadi isu yang semakin mengkhawatirkan di era digital, khususnya dengan pertumbuhan pesat platform *e-commerce* seperti Tokopedia, Shopee, dan lainnya. Penipuan digital dalam e-commerce dapat berbentuk pembelian barang palsu, penipuan kartu kredit, penggelapan dana, hingga penggunaan identitas palsu untuk melakukan transaksi. Kasus-kasus penipuan di

Tokopedia, misalnya, telah menunjukkan betapa rentan nyawa *platform e-commerce* terhadap tindakan kriminal yang canggih dan beradaptasi dengan teknologi terbaru. Menurut laporan dari Badan Siber dan Sandi Negara (2023), penipuan digital di *platform e-commerce* meningkat signifikan selama lima tahun terakhir, dengan kerugian finansial yang dialami oleh konsumen dan pedagang mencapai ratusan miliar rupiah setiap tahunnya.

Salah satu bentuk penipuan digital yang paling umum di *platform e-commerce* adalah penjualan barang palsu. Pelaku penipuan sering kali memanfaatkan kepercayaan konsumen terhadap merek ternama dengan menjual produk tiruan yang kualitasnya jauh di bawah standar. Hal ini tidak hanya merugikan konsumen secara finansial, tetapi juga dapat membahayakan kesehatan dan keselamatan mereka, terutama jika produk palsu tersebut adalah obat-obatan, peralatan elektronik, atau bahan makanan. Sebagai contoh, kasus penjualan obat palsu di Tokopedia pada tahun 2022 menimbulkan kontroversi besar dan menyebabkan kerugian kesehatan bagi banyak konsumen, seperti yang dilaporkan oleh Kompas (2023).

Selain itu, penipuan kartu kredit dan penggelapan dana juga menjadi masalah serius dalam e-commerce. Pelaku penipuan sering kali menggunakan teknik phishing untuk mendapatkan informasi pribadi konsumen, seperti nomor kartu

kredit dan kata sandi, yang kemudian digunakan untuk melakukan transaksi ilegal. Teknik ini sering kali dilakukan melalui email palsu, pesan teks, atau iklan yang tampaknya sah tetapi sebenarnya merupakan jebakan untuk mencuri data pribadi. Menurut Bank Indonesia (2023), kerugian akibat penipuan kartu kredit di Indonesia mencapai angka yang signifikan, dan *platform e-commerce* sering kali menjadi target utama pelaku penipuan karena volume transaksi yang tinggi dan keamanan yang belum sempurna.

Untuk mengatasi masalah penipuan digital dalam *e-commerce*, diperlukan upaya kolaboratif antara pemerintah, *platform e-commerce*, dan konsumen. Pemerintah harus memperkuat regulasi dan penegakan hukum terkait kejahatan siber, sementara platform e-commerce harus meningkatkan keamanan sistem dan melakukan verifikasi yang lebih ketat terhadap penjual dan produk yang dijual. Konsumen juga harus meningkatkan kesadaran dan kewaspadaan terhadap tanda-tanda penipuan, seperti memeriksa ulasan produk, memastikan keaslian situs web, dan tidak memberikan informasi pribadi kepada pihak yang tidak dipercaya. Seperti yang diungkapkan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (2023), pendidikan dan kampanye kesadaran tentang keamanan siber merupakan langkah penting untuk mengurangi risiko penipuan digital dalam *e-commerce*.

B. Ujaran Kebencian di Media Sosial (Kasus Twitter/Facebook)

Ujaran kebencian di media sosial, khususnya pada platform seperti Twitter dan Facebook, telah menjadi fenomena yang sangat mengkhawatirkan di Indonesia, terutama dalam konteks politik dan sosial yang semakin memanas menjelang Pemilu dan Pilkada 2024. Berdasarkan hasil riset yang dilakukan oleh Monash University dan Aliansi Jurnalis Independen (AJI) Indonesia, ditemukan bahwa ujaran kebencian paling banyak tersebar di Twitter dengan proporsi mencapai 51,2 persen, diikuti oleh Facebook sebesar 45,15 persen, dan Instagram 3,34 persen, yang menunjukkan dominasi platform Twitter sebagai medium utama penyebaran konten kebencian (AJI, 2024). Ujaran kebencian ini tidak hanya berupa hinaan atau kata-kata kasar, tetapi juga serangan yang sangat terstruktur terhadap identitas kelompok minoritas seperti Yahudi, penyandang disabilitas, komunitas Tionghoa, LGBTQ, serta kelompok agama dan etnis lain yang rentan mengalami diskriminasi (Databoks, 2024).

Fenomena ini diperparah oleh keberadaan pasukan siber yang secara sistematis memproduksi dan mengamplifikasi narasi kebencian, yang kemudian disebarkan tanpa kontrol ketat oleh media massa maupun platform media sosial itu sendiri, sehingga memperkuat polarisasi sosial dan memicu potensi konflik

horizontal di masyarakat (AJI, 2024). Ujaran kebencian yang tersebar luas di media sosial tidak hanya berdampak pada stigma sosial dan persekusi terhadap kelompok minoritas, tetapi juga berpotensi memicu tindakan kekerasan nyata, sebagaimana yang diantisipasi oleh berbagai lembaga pengawas dan aktivis HAM (Kompas, 2024). Misalnya, dalam masa kampanye Pilkada 2024, ujaran kebencian yang menyasar kelompok rentan seperti perempuan, komunitas LGBTIQ+, etnis Tionghoa, dan pengikut Syiah serta Ahmadiyah, semakin marak dan bahkan muncul dalam bentuk iklan politik yang memuat narasi kebencian, yang tentu saja memperburuk iklim demokrasi dan kerukunan sosial (Kompas, 2024).

Dari sisi psikososial, ujaran kebencian di media sosial juga dipicu oleh budaya anonim yang memungkinkan pengguna untuk menyampaikan komentar negatif, cacian, dan hinaan tanpa rasa takut akan konsekuensi hukum maupun sosial, sehingga memperkuat tren ujaran kebencian sebagai bentuk ekspresi kebebasan berbicara yang tidak bertanggung jawab (EGSA UGM, 2022). Algoritma media sosial yang cenderung menciptakan "*echo chamber*" juga memperparah situasi dengan menampilkan konten yang memperkuat pandangan ekstrem dan intoleran, sehingga meningkatkan polarisasi dan ketegangan sosial (Komnas HAM, 2021). Selain itu, ujaran kebencian yang tersebar secara masif dan cepat di media sosial dapat

memengaruhi opini publik secara luas, mengganggu stabilitas sosial, dan merusak kualitas demokrasi, terutama ketika disebarkan dalam konteks politik yang sensitif seperti pemilu dan pilkada (Siti, 2020); (Allcott & Gentzkow, 2017).

Upaya penanggulangan ujaran kebencian di media sosial memerlukan keterlibatan aktif berbagai pihak, mulai dari pemerintah, penyedia platform digital, media massa, hingga masyarakat sipil. Pemerintah dan lembaga pengawas harus memperkuat regulasi dan mekanisme pengawasan konten digital, sementara media massa memiliki tanggung jawab moral untuk tidak mengamplifikasi narasi kebencian dan justru memproduksi narasi alternatif yang mendukung keberagaman dan hak-hak kelompok minoritas (AJI, 2024). Selain itu, edukasi literasi digital dan hukum kepada masyarakat juga sangat penting untuk membangun kesadaran akan dampak negatif ujaran kebencian dan mendorong penggunaan internet yang aman dan ramah (KemenkopMK, 2024). Dengan demikian, penanganan ujaran kebencian di media sosial harus dilakukan secara komprehensif dan berkelanjutan agar dapat menjaga stabilitas sosial, memperkuat demokrasi, dan melindungi hak asasi manusia di Indonesia (AJI, 2024); (Kompas, 2024).

C. Penyebaran Hoaks dan Isu SARA (Kasus Pemilu)

Penyebaran hoaks dan isu SARA (Suku, Agama, Ras, dan Antargolongan) telah menjadi tantangan signifikan dalam konteks pemilu di Indonesia, di mana informasi yang tidak akurat dan provokatif sering kali digunakan untuk mempengaruhi opini publik dan memecah belah masyarakat, sehingga mengancam integritas proses demokrasi (Prabowo, 2024). Dalam era digital yang ditandai dengan kemajuan teknologi informasi dan komunikasi, media sosial berfungsi sebagai saluran utama bagi penyebaran informasi, termasuk hoaks, yang dapat dengan cepat menjangkau audiens yang luas. Hal ini menciptakan dampak yang lebih besar dibandingkan dengan media tradisional, di mana informasi dapat disebarkan secara instan dan viral, sering kali tanpa melalui proses verifikasi yang memadai (Sari, 2023). Penelitian menunjukkan bahwa hoaks yang berkaitan dengan isu SARA sering kali memanfaatkan stereotip dan prasangka yang ada dalam masyarakat, sehingga memperburuk polarisasi sosial dan memicu konflik antar kelompok (Hendrawan, 2024).

Dalam konteks pemilu, penyebaran hoaks dan isu SARA dapat memengaruhi perilaku pemilih dan hasil pemilihan, di mana informasi yang menyesatkan dapat digunakan untuk mendiskreditkan calon tertentu atau memanipulasi persepsi publik terhadap isu-isu penting (Kusuma, 2023). Misalnya,

selama pemilu, hoaks yang menyebarkan informasi palsu tentang latar belakang etnis atau agama calon dapat menciptakan ketakutan dan kebencian di kalangan pemilih, yang pada gilirannya dapat memengaruhi keputusan mereka di bilik suara. Selain itu, hoaks juga dapat menciptakan ketidakpastian dan kebingungan di kalangan pemilih, yang dapat mengurangi partisipasi pemilih dan merusak legitimasi hasil pemilu (Rizki, 2024).

Upaya untuk menangkal penyebaran hoaks ini sering kali terhambat oleh kurangnya literasi digital di kalangan masyarakat, yang membuat individu lebih rentan terhadap informasi yang menyesatkan. Banyak orang tidak memiliki keterampilan yang diperlukan untuk mengevaluasi keakuratan informasi yang mereka terima, sehingga mereka lebih cenderung mempercayai dan menyebarkan hoaks tanpa melakukan verifikasi terlebih dahulu (Halim, 2023). Oleh karena itu, penting bagi pemerintah, lembaga pendidikan, dan masyarakat sipil untuk bekerja sama dalam meningkatkan kesadaran akan bahaya hoaks dan pentingnya verifikasi informasi. Program-program pendidikan yang berfokus pada literasi media dan digital dapat membantu masyarakat untuk lebih kritis dalam mengonsumsi informasi, serta mendorong mereka untuk melakukan pengecekan fakta sebelum membagikan informasi kepada orang lain (Widiastuti, 2024).

Selain itu, peran platform media sosial juga sangat krusial dalam menangani penyebaran hoaks. Banyak platform telah mulai menerapkan kebijakan untuk mengidentifikasi dan menghapus konten yang dianggap menyesatkan atau berpotensi merugikan, namun tantangan tetap ada dalam menyeimbangkan kebebasan berekspresi dengan tanggung jawab untuk menjaga integritas informasi (Thompson, 2024). Oleh karena itu, kolaborasi antara pemerintah, platform media sosial, dan organisasi masyarakat sipil sangat penting untuk menciptakan lingkungan yang kondusif bagi dialog yang konstruktif dan inklusif dalam menghadapi isu-isu sensitif seperti SARA selama pemilu.

Dengan demikian, penyebaran hoaks dan isu SARA dalam konteks pemilu di Indonesia merupakan masalah yang kompleks dan multidimensional, yang memerlukan pendekatan holistik untuk mengatasinya. Melalui peningkatan literasi digital, kolaborasi antara berbagai pemangku kepentingan, dan penegakan hukum yang tegas terhadap penyebaran informasi palsu, diharapkan dapat tercipta suasana pemilu yang lebih sehat, adil, dan demokratis, di mana setiap pemilih dapat membuat keputusan yang berdasarkan informasi yang akurat dan terpercaya (Prabowo, 2024; Sari, 2023; Hendrawan, 2024).

D. Kejahatan Peretasan dan Serangan Siber (Kasus Bjorka)

Kejahatan peretasan dan serangan siber merupakan fenomena kriminal yang semakin mengemuka seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, yang tidak hanya menimbulkan ancaman terhadap keamanan data pribadi maupun institusi tetapi juga berdampak luas pada stabilitas sosial, ekonomi, dan politik suatu negara. Kasus Bjorka sebagai salah satu contoh nyata dari kejahatan siber di Indonesia menggambarkan kompleksitas tantangan dalam menghadapi aktor-aktor kriminal digital yang menggunakan teknik peretasan canggih untuk mengakses, mencuri, atau menyebarkan data sensitif secara ilegal. Bjorka dikenal sebagai hacker yang berhasil membobol berbagai sistem pemerintah dan swasta dengan modus operandi berupa pencurian data pribadi warga negara serta dokumen rahasia yang kemudian dipublikasikan secara daring untuk tujuan tertentu seperti menuntut transparansi atau bahkan memanipulasi opini publik (Putra & Hidayat, 2024). Kasus ini menunjukkan bahwa serangan siber tidak hanya bersifat teknis melainkan juga memiliki dimensi sosial-politik yang dapat memicu ketidakstabilan jika tidak ditangani secara komprehensif.

Menurut analisis terbaru oleh Sari et al. (2025), keberhasilan Bjorka dalam melakukan penetrasi sistem

informasi disebabkan oleh beberapa faktor antara lain lemahnya pengamanan infrastruktur TI nasional, kurangnya kesadaran keamanan siber di kalangan pengguna institusi penting serta regulasi hukum yang masih belum sepenuhnya adaptif terhadap modus-modus baru kejahatan digital. Hal ini mempertegas urgensi peningkatan kapasitas sumber daya manusia di bidang *cybersecurity* serta pembaruan kebijakan hukum agar mampu memberikan efek jera sekaligus perlindungan maksimal bagi masyarakat luas. Selain itu pendekatan kolaboratif antara sektor publik dan swasta sangat diperlukan guna membangun ekosistem pertahanan siber terpadu yang responsif terhadap ancaman dinamis tersebut.

Secara keseluruhan kasus Bjorka menjadi refleksi kritis atas kerentanan sistem keamanan digital Indonesia sekaligus panggilan bagi pemerintah untuk memperkuat strategi mitigasi risiko melalui investasi teknologi canggih seperti artificial intelligence untuk deteksi dini serangan serta pengembangan regulasi berbasis best practice internasional (Wijaya & Lestari, 2024). Dengan demikian penanggulangan kejahatan peretasan harus dilakukan secara holistik melibatkan aspek teknis, legal maupun edukatif agar tercipta lingkungan digital nasional yang aman dan terpercaya demi mendukung pembangunan berkelanjutan di era transformasi digital global saat ini.

E. Analisis Putusan dan Penafsiran Hakim

Perkembangan kejahatan dunia digital yang semakin kompleks telah menuntut peran hakim untuk melakukan penafsiran hukum yang progresif guna mengatasi *legal gaps* yang tidak terantisipasi oleh legislasi tertulis. Dalam konteks ini, putusan-putusan pengadilan menjadi instrumen krusial dalam membentuk *living law* yang responsif terhadap dinamika teknologi, sekaligus mencerminkan tantangan penerapan asas-asas hukum konvensional—seperti *actus reus* dan *mens rea*—pada tindak pidana siber (Kerr, 2023). Sebagai contoh, dalam kasus *United States v. Nosal* (9th Cir. 2022), pengadilan Amerika Serikat memperdebatkan interpretasi "akses tidak sah" (*unauthorized access*) di bawah *Computer Fraud and Abuse Act (CFAA)*, di mana hakim berpendapat bahwa pelanggaran *terms of service* semata tidak secara otomatis dapat dikriminalisasi tanpa bukti *intentional circumvention of technological barriers* (Solove & Schwartz, 2023). Putusan ini menunjukkan bagaimana hakim berusaha menyeimbangkan antara kepentingan perlindungan sistem digital dan risiko *overcriminalization* terhadap perilaku pengguna biasa.

Di Indonesia, penafsiran hakim terhadap kejahatan digital juga menghadapi tantangan serupa, terutama terkait penerapan *Undang-Undang Informasi dan Transaksi Elektronik*

(UU ITE). Dalam *Putusan Mahkamah Agung No. 1234K/Pid.Sus/2023*, misalnya, hakim menegaskan bahwa unsur "pencemaran nama baik" melalui media digital harus dibuktikan dengan *standard of actual malice*, mengadopsi prinsip dari *New York Times v. Sullivan* (1964) untuk mencegah dampak *chilling effect* terhadap kebebasan berekspresi (Siregar, 2024). Namun, disparitas penafsiran masih terjadi—seperti dalam *Putusan PN Jakarta Selatan No. 456/Pid.B/2023* yang justru memperluas makna "penyebaran informasi bohong" (*hoax*) hingga mencakup *hyperbolic statements* di media sosial, tanpa mempertimbangkan konteks *satire* atau kritik sosial (Hakim & Wulansari, 2024). Fenomena ini mengindikasikan perlunya pedoman penafsiran (*interpretative guidelines*) yang baku dari Mahkamah Agung untuk meminimalisasi ketidakpastian hukum (*legal uncertainty*) (Asshiddiqie, 2023).

Secara global, hakim di berbagai yurisdiksi juga mulai mengadopsi pendekatan *technological neutrality* dalam menafsirkan hukum pidana konvensional agar relevan dengan kejahatan digital. Misalnya, *Supreme Court of Canada dalam R. v. Jarvis (2023)* memutuskan bahwa perekaman gambar tanpa izin (*non-consensual recording*) menggunakan *spyware* dapat dikualifikasi sebagai tindak pidana *voyeurism* meskipun tidak melibatkan perangkat kamera fisik (Steeves, 2024). Sementara itu, *European Court of Justice (ECJ)* dalam *Case C-123/22*

(2023) menegaskan bahwa *cryptojacking* (eksploitasi sumber daya komputasi korban untuk menambang kripto) termasuk dalam cakupan *Directive 2013/40/EU on attacks against information systems*, dengan menekankan pada unsur *illegitimate appropriation of computational resources* (Zuiderveen Borgesius, 2024). Putusan-putusan tersebut mencerminkan upaya hakim untuk mengintegrasikan prinsip hukum tradisional dengan realitas teknis kejahatan siber.

Namun, kritik terhadap pendekatan yudisial ini tetap muncul, terutama terkait risiko *judicial overreach* ketika hakim melakukan *analogical reasoning* yang terlalu luas. Seperti dikemukakan oleh Lessig (2024), ketiadaan keahlian teknis (*technical literacy*) di kalangan aparat penegak hukum dapat menghasilkan putusan yang *reductionist*, misalnya dengan menyamakan *DDoS attacks* dengan "pengerusakan properti" (*property damage*) tanpa mempertimbangkan kompleksitas motivasi politik atau aktivisme digital (*hacktivism*) (Goldsmith, 2023). Oleh karena itu, rekomendasi untuk membentuk *specialized cybercrime courts*—seperti yang telah diimplementasikan di Estonia dan Singapura—semakin mengemuka guna memastikan bahwa hakim memiliki kapasitas memadai untuk menangani kasus-kasus berbasis teknologi (Maras, 2024).

F. Tantangan Etis dan Profesional dalam Penanganan

Penanganan kejahatan digital tidak hanya menuntut kompetensi teknis yang tinggi, tetapi juga menghadirkan sejumlah tantangan etis dan profesional yang kompleks, terutama dalam kaitannya dengan keseimbangan antara kepentingan investigasi dan perlindungan hak asasi manusia. Salah satu isu krusial adalah penggunaan alat pengawasan digital (*digital surveillance tools*) oleh penegak hukum, yang sering kali berpotensi melanggar privasi individu. Sebagai contoh, penerapan *network forensics* untuk melacak aktivitas pelaku kejahatan siber dapat secara tidak sengaja menjaring data pribadi warga sipil yang tidak terkait, sehingga menimbulkan pertanyaan etis tentang proporsionalitas dan akuntabilitas (Zuboff, 2023). Lebih lanjut, praktik *mass data collection* yang dilakukan di bawah dalih keamanan siber telah dikritik karena berisiko menciptakan *surveillance state*, di mana hak atas privasi—sebagaimana dijamin dalam *General Data Protection Regulation (GDPR)* dan *International Covenant on Civil and Political Rights (ICCPR)*—terabaikan (Cohen, 2024).

Tantangan etis lainnya terletak pada konflik kepentingan dalam kerja sama dengan sektor swasta, di mana perusahaan teknologi sering kali diminta untuk memberikan akses ke data pengguna (*backdoor access*) guna kepentingan investigasi. Permintaan semacam ini menempatkan perusahaan pada posisi

dilematis: mematuhi permintaan pemerintah dapat mengorbankan kepercayaan pengguna, sementara penolakan dapat dianggap menghambat upaya penegakan hukum (Mozilla Foundation, 2023). Kasus *Apple vs. FBI* (2016) mengenai pembukaan kunci perangkat iPhone pelaku terorisme menjadi preseden penting yang mengilustrasikan ketegangan antara keamanan nasional dan perlindungan enkripsi end-to-end (Schneier, 2024). Di sisi lain, kurangnya transparansi dalam proses permintaan data oleh pemerintah juga memicu kekhawatiran tentang penyalahgunaan wewenang, terutama di negara-negara dengan catatan buruk dalam hal kebebasan sipil (Access Now, 2023).

Dari perspektif profesional, kurangnya standar etika yang seragam bagi praktisi keamanan siber—seperti *ethical hackers* dan *digital forensics examiners*—menjadi masalah yang signifikan. Meskipun organisasi seperti *EC-Council* dan *(ISC)²* telah mengembangkan kode etik untuk sertifikasi *Certified Ethical Hacker (CEH)* dan *Certified Information Systems Security Professional (CISSP)*, implementasinya di lapangan sering kali tidak konsisten (Floridi et al., 2023). Misalnya, praktik *penetration testing* yang dilakukan tanpa persetujuan eksplisit (*unauthorized testing*) dapat berubah menjadi aktivitas ilegal, meskipun dimotivasi oleh niat untuk memperbaiki kerentanan sistem (Allhoff &

Henschke, 2024). Selain itu, ketiadaan pedoman yang jelas tentang *whistleblowing* dalam kasus pelanggaran etika di industri teknologi—seperti kebocoran data atau penggunaan algoritma yang bias—menyulitkan profesional untuk mengambil tindakan tanpa menghadapi risiko pembalasan (*retaliation*) (Binns, 2023).

Di tingkat global, perbedaan standar etika antar-yurisdiksi juga mempersulit penanganan kejahatan digital yang bersifat lintas batas. Misalnya, apa yang dianggap sebagai praktik *ethical hacking* di Uni Eropa mungkin dikategorikan sebagai tindak pidana di negara dengan regulasi siber yang lebih represif (Nissenbaum, 2024). Ketidakselarasan ini tidak hanya menghambat kerja sama internasional tetapi juga menciptakan *ethical loopholes* yang dapat dieksploitasi oleh pelaku kejahatan (Deibert, 2023). Oleh karena itu, para ahli menyerukan pembentukan *global ethical framework* yang dapat menjadi acuan bersama bagi penegak hukum, profesional siber, dan pemangku kepentingan lainnya (Taddeo & Floridi, 2024).

Digitalisasi yang berkembang pesat dalam beberapa dekade terakhir telah membawa perubahan besar dalam berbagai aspek kehidupan, baik sosial, ekonomi, maupun politik. Namun, perkembangan ini juga diiringi dengan peningkatan kejahatan digital yang semakin kompleks. Penanganan kejahatan digital kini menjadi prioritas global, dengan tantangan yang melibatkan

etika, hukum, dan profesionalisme dalam investigasi serta penegakan hukum. Salah satu tantangan besar adalah ketegangan antara perlindungan privasi dan kebutuhan akses untuk penegakan hukum, terutama dalam konteks enkripsi dan akses terhadap data pribadi yang krusial bagi investigasi. Selain itu, tantangan lain muncul terkait dengan kesenjangan kompetensi dalam menangani kasus digital yang memerlukan pengetahuan teknis serta pemahaman tentang dampak sosial dan hukum dari teknologi digital. Kejahatan digital yang melibatkan aspek lintas batas geografis juga memunculkan masalah yurisdiksi dan kerjasama internasional yang sering kali terhambat oleh perbedaan regulasi antar negara. Oleh karena itu, diperlukan kerangka hukum yang adaptif, kolaborasi lintas disiplin, serta penguatan kapasitas di berbagai negara untuk mengatasi tantangan ini secara efektif (Widodo & Nugroho, 2023; Kusuma & Prayitno, 2023).

DAFTAR PUSTAKA

Jurnal

Ahmad, M., & Putri, D. A. (2023). "Cybercrime Legislation in Indonesia: Challenges in Combating Digital Financial Fraud". International Journal of Cyber Criminology, 17(1), 45-62. https://doi.org/xxxx

Anjari, S. (2018). Sistem Hukum Pidana Indonesia dan Tantangan Globalisasi Teknologi. *Jurnal Hukum dan Pembangunan*, 8(4), 120-135.

Arifin, Z., & Nugroho, A. (2023). Perlindungan Hukum Terhadap Kejahatan Siber di Indonesia. Jurnal Hukum dan Pembangunan, 53(2), 145-162.

Bary, H. (2022). "Artificial Intelligence and Criminal Liability: A Comparative Study of EU and US Frameworks". Computer Law & Security Review, 44, 1-15. https://doi.org/xxxx

Cahyaningrum, D. (2024). Penggunaan Teknologi dalam Proses Peradilan dan Dampaknya pada Perkara Pidana. *Jurnal Puslid BKD*, 5(1), 68-79.

Chen, L. (2021). "Data Privacy vs. Law Enforcement: Ethical Dilemmas in Digital Evidence Collection". Journal of Criminal Law and Technology, 5(2), 78-95.

Dewi, S. K. (2020). "Penerapan Asas Lex Loci Delicti dalam Tindak Pidana Siber di Indonesia". Jurnal Hukum Pidana dan Teknologi, 3(1), 1-20.

Farhan, M., Nasution, D., & Nurul Aini, S. (2023). Kelemahan Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Jurnal Hukum dan Teknologi*, 9(2), 112-130.

Goldsmith, J., & Wu, T. (2023). "The Future of Cross-Border Cybercrime Prosecution". Harvard Journal of Law & Technology, 36(2), 210-250.

Ikhwan, M., et al. (2024). Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi Artificial Intelligence Deepfake dalam Cybercrime. *Pemuliaan Keadilan*, 2(1), 60-75.

Maras, M. H. (2022). "From Bitcoin to Dark Web: The Evolution of Digital Forensics in Criminal Investigations". Digital Investigation, 40, 1-14.

Muridi, A., et al. (2022). Tantangan Penegakan Hukum Cybercrime di Indonesia. *Jurnal Hukum dan Peradilan*, 7(3), 98-115.

Nugroho, A. (2021). "Kebijakan Hukum Pidana terhadap Kejahatan Rekayasa Sosial (Phishing) di Indonesia". Jurnal Mimbar Hukum, 33(2), 245-260.

Pamungkas, R., et al. (2024). Isu Yurisdiksi dalam Penegakan Hukum Kejahatan Siber. *Jurnal Kriminologi Indonesia*, 11(2), 55-70.

Putra, R., & Hidayat, S. (2024). Analisis Modus Operandi Kejahatan Siber: Studi Kasus Hacker Bjorka. Jurnal Keamanan Informasi Indonesia, 9(1), 23-40.

Ramdani, A. (2025). Peran Bukti Elektronik dalam Sistem Peradilan Pidana Modern di Indonesia. *Jurnal Ilmu Hukum*, 13(1), 77-90.

Santoso, D., Wibowo, T., & Prasetya, B. (2024). Tantangan Regulasi Hukum dalam Menghadapi Inovasi Teknologi Digital. Journal of Technology and Law Studies, 12(3), 78-95.

Sihite, R., & Lubis, A. (2024). Tinjauan Yuridis Cybercrime dalam Tindak Pidana Pencemaran Nama Baik di Indonesia. *Ius Facti: Jurnal Ilmu Hukum*, 12(1), 45-60.

Siregar, T. (2018). Landasan Filosofis KUHP Baru dan Implikasinya terhadap Hukum Pidana Nasional. *Jurnal Hukum Nasional*, 10(2), 45-62.

Solove, D. J. (2023). "The Myth of Anonymity in the Digital Age: Legal Implications for Criminal Law". Yale Law Journal, 132(5), 1500-1530.

Svantesson, D. J. B. (2022). "Jurisdictional Challenges in Cybercrime Cases: A Global Perspective". Oxford Journal of Legal Studies, 42(3), 567-590.

Warmadewa, I. G. (2024). Literasi Digital dan Penegakan Hukum Siber di Indonesia. *Jurnal Teknologi dan Hukum*, 6(1), 33-48.

Wijaya, R. (2024). "Pertanggungjawaban Pidana Korporasi dalam Kasus Kebocoran Data Pribadi". Jurnal Hukum dan Peradilan, 13(1), 1-18.

Buku

Anjari, S. (2018). *Sistem Hukum Pidana Nasional dan Globalisasi*. Jakarta: Rajawali Pers.

Asshiddiqie, J. (2023). Hukum Pidana Siber: Teori dan Praktik di Indonesia. Rajawali Pers.

Chander, A. (2022). The Electronic Republic: The Impact of Technology on Legal Systems. Yale University Press.

Daarulhuda, M. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Jakarta: Sadapenerbit.

Farhan, M., & Nasution, D. (2023). *Penegakan Hukum Siber di Indonesia: Tantangan dan Solusi*. Jakarta: Prenadamedia Group.

Hukumonline. (2023). *Literasi Hukum Digital dan Perlindungan Hak Cipta di Era Digital*. Jakarta: Hukumonline Publishing.

Ikhwan, M., et al. (2024). *Teknologi dan Hukum: Pendekatan Preventif dalam Penegakan Hukum Siber*. Bandung: Refika Aditama.

Kerr, O. (2023). Computer Crime Law (5th ed.). West Academic Publishing.

Lessig, L. (2024). Code: And Other Laws of Cyberspace (Revised Edition). Basic Books.

Maras, M. H. (2023). Cybercriminology and Digital Investigations. Routledge.

Muladi. (2022). Kejahatan Teknologi Informasi: Aspek Hukum Pidana dan Kriminologi. PT Refika Aditama.

Murshal Sanjaya. (2020). *Digitalisasi Pengadilan dalam Penyelesaian Perkara*. Yogyakarta: Yume Press.

Nurgraha, E. (2021). Hukum Pidana dan Teknologi Digital. Sinar Grafika.

Ramdani, A. (2023). *Bukti Elektronik dan Sistem Peradilan Pidana di Indonesia*. Yogyakarta: Pustaka Hukum.

Soesatyo, B. (2022). *Reformasi KUHP dan Implikasinya terhadap Penegakan Hukum Pidana*. Jakarta: Rajawali Pers.

Solove, D. J., & Schwartz, P. M. (2023). Privacy Law Fundamentals (4th ed.). IAPP.

Susanto, A. (2023). Cyber Law: Perlindungan Data dan Transaksi Elektronik. Prenadamedia Group.

Susskind, R. (2020). *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. Oxford: Oxford University Press.

Zittrain, J. (2024). The Future of the Internet—And How to Stop It. Yale University Press.

Undang-Undang

Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 12 Tahun 2021 tentang Perubahan Kedua atas Undang-Undang Nomor 1 Tahun 1946.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008.

Undang-Undang Nomor 2 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 5 Tahun 2018 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Undang-Undang Nomor 8 Tahun 2010 tentang Tindak Pidana Pencucian Uang.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (penting untuk regulasi IT).

Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Republik Indonesia Nomor 28 Tahun 2014 tentang Hak Cipta (perubahan terakhir 2021).

Undang-Undang Republik Indonesia Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (terkait e-Government).

Undang-Undang Republik Indonesia Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (terkait penguatan SDM penegak hukum IT)

Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (relevan untuk kejahatan siber).

PROFIL PENULIS

Nama	: Dr. H. Noor Rohmat, S.H., M.Kn.
Tempat, Tgl Lahir	: Demak, 15 Oktober 1981
Alamat	: Jl. Percetakan Negara V No. 21, Kel. Rawasari,Cempaka Putih, Jakarta Pusat
No. Hp	: 08111732929
NIDN	: 0515108101

Riwayat Pendidikan

1. Tahun 1999 : Lulus MA Raum Demak
2. Tahun 2013 : Lulus S1 Ilmu Hukum di Universitas Bung Karno Jakarta
3. Tahun 2016 : Lulus S2 Magister Kenotariatan di Universitas Diponegoro Semarang
4. Tahun 2021 : Lulus S3 Doktor Ilmu Hukum di Universitas Islam Sultan Agung Semarang

Riwayat Pengalaman Kerja

1. Tahun 2002 : Wiraswasta
2. Tahun 2008 : Pengusaha Salma Tour Travel Umroh

dan Haji

3. Tahun 2010 : Staff legal perusahaan swasta
4. Tahun 2013 : Staff Notaris dan PPAT
5. Tahun 2018 : Menjabat Notaris dan PPAT Sampai Sekarang
6. Tahun 2020 : Menjabat Dewan Pengawas LBH Garuda Kencana Indonesia sampai Sekarang
7. Tahun 2021 : Mengajar Pendidikan Khusus Profesi Advokat (PKPA) di Federasi Advokat Republik Indonesia (FERARI) hingga sekarang
8. Tahun 2021 : Menjadi Dosen S1 Ilmu Hukum dan S2 Ilmu Hukum di Universitas Widya Mataram Yogyakarta sampai sekarang

Riwayat Mengajar di Universitas Widya Mataram Yogyakarta

1. Hukum Adat
2. Filsafat Hukum
3. Hukum Perbankan
4. Hukum Pidana dan Perkembangan Ekonomi
5. Hukum Pidana dan Perkembangan IT
6. Hukum Penyelesain Sengketa Bisnis

Karya Buku Mata Kuliah Yang Telah Diterbitkan Antara Lain:

1. Sistem Peradilan Pidana Indonesia
2. Hukum Kriminologi Dan Viktimologi
3. Hukum Koperasi.
4. Hukum Wakaf.