Published By : Fakultas Hukum, Universitas Sawerigading Makassar E ISSN : 2828 - 4054
SAWERIGADING LAW JOURNAL

Vol.4 No.2, September 2025, Hal. 106-127

Harmonisasi Lex Specialis UU ITE dan KUHP dalam Penegakan Cybercrime serta Validitas Transaksi Elektronik di Indonesia

Bahtiar[1], Wildanah H.[2], Andi Rivai[3], Ruslan[4]
Institut Cokroaminoto Pinrang[1234]
Email : bahtiar.stihcokro@gmail.com

Abstrak

Transformasi digital telah memperluas aktivitas ekonomi dan komunikasi lintas batas, sekaligus meningkatkan kompleksitas kejahatan siber serta sengketa transaksi elektronik di Indonesia. Dalam konteks ini, pengaturan hukum menghadapi persoalan utama berupa potensi tumpang tindih antara ketentuan umum dalam KUHP dan ketentuan khusus dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), di samping kebutuhan kepastian hukum atas keabsahan perbuatan hukum berbasis sistem elektronik. Artikel ini bertujuan menganalisis konstruksi normatif penanggulangan *cybercrime*, menilai validitas yuridis transaksi elektronik, dan merumuskan arah harmonisasi regulasi yang lebih adaptif terhadap perkembangan teknologi. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual, berbasis bahan hukum primer, sekunder, dan tersier yang dianalisis secara kualitatif-preskriptif. Hasil penelitian menunjukkan: (1) rezim penegakan *cybercrime* di Indonesia menempatkan UU ITE sebagai *lex specialis* yang melengkapi KUHP; (2) transaksi elektronik memiliki kekuatan mengikat setara dengan perjanjian konvensional sepanjang memenuhi syarat formil-materiil, termasuk dukungan sistem keamanan dan tanda tangan elektronik tersertifikasi; dan (3) efektivitas penegakan hukum masih terhambat oleh sifat kejahatan siber yang *borderless*, volatilitas alat bukti digital, serta ketimpangan kapasitas forensik aparat. Penelitian ini menegaskan urgensi harmonisasi norma KUHP–UU ITE secara lebih sistematis, disertai penguatan kelembagaan forensik digital, agar kepastian hukum, perlindungan masyarakat, dan tata kelola ekonomi digital dapat terjamin secara berkelanjutan.

Kata Kunci: *Cybercrime*, UU ITE, Transaksi Elektronik, Yurisdiksi, Bukti Digital.

Abstract

Digital transformation has expanded cross-border economic and communication activities, while increasing the complexity of cybercrime

and electronic transaction disputes in Indonesia. In this context, legal regulations face a major problem in the form of potential overlap between general provisions in the Criminal Code and specific provisions in the Electronic Information and Transaction Law (EIT Law), in addition to the need for legal certainty regarding the validity of legal actions based on electronic systems. This article aims to analyze the normative construction of cybercrime prevention, assess the legal validity of electronic transactions, and formulate the direction of regulatory harmonization that is more adaptive to technological developments. The research uses a normative juridical method with a legislative and conceptual approach, based on primary, secondary, and tertiary legal materials that are analyzed qualitatively and prescriptively. The results of the study show that: (1) the cybercrime enforcement regime in Indonesia places the ITE Law as lex specialis that complements the Criminal Code; (2) electronic transactions have binding force equivalent to conventional agreements as long as they meet formal and material requirements, including the support of security systems and certified electronic signatures; and (3) the effectiveness of law enforcement is still hampered by the borderless nature of cybercrime, the volatility of digital evidence, and the imbalance in the forensic capacity of the authorities. This study emphasizes the urgency of harmonizing the norms of the Criminal Code and the ITE Law in a more systematic manner, accompanied by the strengthening of digital forensic institutions, so that legal certainty, public protection, and digital economic governance can be guaranteed in a sustainable manner.

Keywords: *Cybercrime, UU ITE, Electronic Transactions, Jurisdiction, Digital Evidence.*

PENDAHULUAN

Revolusi teknologi informasi telah menghadirkan ruang baru yang dikenal sebagai cyberspace atau dunia maya. Ruang ini bersifat virtual namun memiliki dampak yang sangat nyata terhadap tatanan kehidupan manusia, baik dalam aspek sosial, ekonomi, maupun hukum. Fenomena ini menjadikan dunia seolah tanpa batas (borderless), di mana interaksi dan transaksi dapat terjadi lintas negara dalam hitungan detik. Kehadiran internet sebagai "the network of networks" telah mengubah paradigma ekonomi dari basis manufaktur menuju ekonomi berbasis jasa dan digital, melahirkan model bisnis baru seperti e-commerce. Demikian pula kehadiran

Di Indonesia, kehadiran internet telah mengubah paradigma ekonomi dari basis manufaktur menuju ekonomi berbasis data dan digital. Fenomena *borderless world* ini memungkinkan transaksi terjadi lintas yurisdiksi dalam hitungan detik. Namun, ketiadaan batas fisik ini pula yang menjadi tantangan

bagi hukum konvensional yang selama ini bersandar pada asas teritorialitas yang kaku.

Pergeseran Paradigma dari *Physical Space* ke *Digital Space* Secara filosofis, hukum dikonstruksi atas dasar batasan fisik yang manifes. Kehadiran ruang siber (*cyberspace*) tidak hanya sekadar penemuan teknologi, melainkan sebuah ledakan ontologis yang mendisrupsi batas-batas kedaulatan negara. Dalam pandangan hukum tradisional, wilayah (*territory*) adalah unsur mutlak kedaulatan. Namun, di dunia maya, data tidak mengenal paspor atau pos lintas batas. Hal ini memicu ketegangan antara hukum positif yang bersifat lokal-nasional dengan aktivitas siber yang bersifat global-universal. Ketertinggalan hukum (*the lag of the law*) dalam merespons kecepatan teknologi informasi sering kali menciptakan "zona abu-abu" yang dimanfaatkan oleh pelaku kejahatan siber untuk berlindung di balik anonimitas teknis.

Dilema *Rechtshandeling* dalam Sistem Elektronik Dalam ranah hukum perdata, perbuatan hukum (*rechtshandeling*) secara klasik mensyaratkan adanya manifestasi kehendak yang jelas dan dapat dibuktikan secara fisik. Transaksi elektronik menghadirkan tantangan terhadap teori kehendak tersebut. Ketika sebuah algoritma atau *smart contract* melakukan transaksi secara otomatis, muncul pertanyaan yuridis mengenai siapa yang bertanggung jawab atas kegagalan sistem atau kerugian yang timbul. Validitas transaksi tidak lagi cukup bersandar pada dokumen fisik di atas kertas, melainkan pada integritas sistem yang mengelolanya. Oleh karena itu, hukum positif Indonesia harus mampu mengonversi nilai-nilai autentisitas, integritas, dan non-repudiasi (nir-sangkal) dari bentuk fisik ke dalam bentuk digital tanpa mengurangi derajat kepastian hukumnya.

Namun, kemajuan ini bagaikan pedang bermata dua. Di satu sisi, ia memberikan efisiensi dan kecepatan; di sisi lain, ia membuka celah bagi kejahatan baru yang dikenal sebagai cybercrime. Kejahatan ini memiliki karakteristik khusus, seperti non-kekerasan fisik, sulit dideteksi, dan pelakunya yang seringkali anonim atau berada di yurisdiksi hukum yang berbeda.

Lebih jauh lagi, tantangan terbesar dalam penegakan hukum siber tidak hanya terletak pada substansi aturan pidana (substantive criminal law), melainkan juga pada aspek yurisdiksi dan pembuktian. Dalam paradigma hukum konvensional, kedaulatan hukum suatu negara umumnya dibatasi oleh teritorial fisik. Namun, sifat ubiquitous dari internet meruntuhkan batas-batas tersebut, menciptakan kompleksitas ketika pelaku (hacker), korban, dan lokasi server berada di negara yang berbeda. Oleh karena itu, penerapan asas yurisdiksi

ekstrateritorial dalam UU ITE menjadi instrumen krusial untuk menjangkau perbuatan hukum yang dilakukan di luar wilayah Indonesia namun memiliki akibat hukum yang merugikan kepentingan nasional.

Urgensi Harmonisasi Hukum Nasional dan Standar Internasional masalah utama dalam *cybercrime* bukan hanya terletak pada perbuatan pidananya, melainkan pada aspek penegakan hukum yang bersifat lintas yurisdiksi. Kejahatan siber sering kali melibatkan aktor di negara A, menggunakan server di negara B, dan menimbulkan kerugian di negara C. Kondisi ini menuntut Indonesia tidak hanya memiliki regulasi internal yang kuat melalui UU ITE, tetapi juga harus menyelaraskan diri dengan standar internasional seperti *Budapest Convention on Cybercrime*. Sinkronisasi ini penting agar Indonesia tidak menjadi *safe haven* bagi para pelaku kejahatan siber global dan sekaligus menjamin bahwa pelaku usaha digital di Indonesia memiliki perlindungan hukum yang setara dengan standar global.

Perkembangan teknologi informasi yang pesat telah membawa perubahan signifikan dalam pola kehidupan masyarakat modern. Ketergantungan manusia terhadap perangkat elektronik yang terhubung dengan internet semakin tinggi, tidak hanya untuk komunikasi sosial tetapi juga untuk transaksi ekonomi dan perbankan. Namun, kemajuan ini ibarat dua sisi mata uang; di satu sisi memberikan kemudahan, namun di sisi lain membuka celah bagi munculnya bentuk kejahatan baru yang dikenal sebagai kejahatan siber atau *cyber crime*.

Kejahatan siber merupakan ancaman global yang tidak hanya menyasar sektor bisnis dan keamanan negara, tetapi juga individu secara personal. Fenomena ini unik karena memungkinkan pelaku melakukan tindak pidana tanpa harus hadir secara fisik di tempat kejadian (Iskandar, 2021). Modus operandi yang berkembang pun semakin variatif, mulai dari peretasan sistem (*hacking*), pencurian data pribadi, hingga penipuan daring.

Penyusunan regulasi siber di Indonesia juga menghadapi tantangan dalam menjaga keseimbangan antara perlindungan hak asasi manusia (seperti kebebasan berekspresi dan hak atas privasi) dengan kebutuhan akan ketertiban umum dan keamanan negara. Analisis yuridis-normatif ini menjadi krusial untuk memastikan bahwa upaya kriminalisasi terhadap perbuatan siber tidak bersifat represif secara berlebihan, namun tetap efektif dalam memitigasi risiko keamanan digital yang kian kompleks seperti *ransomware*, *phishing*, hingga manipulasi data pada skala masif.

Di sisi lain, dalam ranah hukum privat, transformasi digital telah mendisrupsi konsep konvensional tentang perjanjian. Transaksi elektronik (e-

commerce) yang berlangsung secara paperless dan non-face-to-face menuntut redefinisi mengenai keabsahan kontrak. Keraguan mengenai kapan kesepakatan terjadi (moment of agreement), identitas para pihak, hingga kekuatan pembuktian dokumen elektronik seringkali menjadi hambatan bagi terciptanya iklim bisnis digital yang terpercaya. Hukum harus hadir untuk memberikan stempel validitas bahwa data elektronik adalah alat bukti yang sah dan setara dengan bukti tertulis di mata hukum, sebagaimana diamanatkan dalam prinsip functional equivalent approach.

Di Indonesia, respons hukum terhadap fenomena ini diwujudkan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta perubahannya. Meskipun instrumen hukum telah tersedia, penegakan hukum terhadap *cyber crime* masih menghadapi berbagai problematika. Tantangan tersebut meliputi pembuktian yang rumit, kemampuan penyidik, hingga fasilitas forensik yang belum merata (Habibi & Liviani, 2021). Oleh karena itu, penelitian ini bertujuan untuk menganalisis lebih dalam mengenai jenis-jenis kejahatan siber yang menyasar individu, perspektif hukum pidana dalam menjerat pelaku, serta hambatan penegakan hukumnya di Indonesia.

Meskipun Indonesia telah memiliki rezim hukum siber melalui UU ITE, dinamika teknologi yang berkembang secara eksponensial seringkali meninggalkan hukum yang berjalan linear (law lags behind technology). Munculnya modus kejahatan baru seperti ransomware, phishing, hingga pencurian aset kripto, serta sengketa smart contract, terus menguji ketangguhan regulasi yang ada. Kondisi ini menuntut adanya kajian yuridis yang berkelanjutan untuk memastikan bahwa hukum positif tidak hanya bersifat reaktif, tetapi juga prospektif dalam mengantisipasi perkembangan zaman.

Berangkat dari latar belakang tersebut, artikel ini memiliki urgensi untuk menganalisis secara komprehensif konstruksi hukum siber di Indonesia. Fokus pembahasan akan diarahkan pada harmonisasi antara kebutuhan penanggulangan kejahatan (cybercrime) dengan perlindungan aktivitas ekonomi digital, serta mengevaluasi efektivitas instrumen hukum saat ini dalam memberikan keadilan dan kepastian hukum bagi masyarakat di era digital.

Sawerigading Law Journal merupakan jurnal berkala ilmiah yang diterbitkan oleh Fakultas Hukum, Universitas Sawerigading. Jurnal ini menjadi sarana publikasi artikel penelitian orisinal atau artikel analisis yang belum pernah dipublikasikan sebelumnya.

Kevakuman hukum di masa lalu seringkali membuat para pelaku kejahatan siber lolos dari jeratan hukum konvensional (KUHP) yang sangat bergantung pada bukti fisik dan batas territorial. Oleh karena itu, kehadiran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi tonggak sejarah hukum siber di Indonesia, yang berfungsi tidak hanya sebagai instrumen penindak kejahatan (criminal policy), tetapi juga sebagai landasan kepastian hukum bagi transaksi elektronik. Artikel ini akan membedah bagaimana hukum positif Indonesia mengatur dua aspek vital tersebut: kriminalisasi perbuatan siber dan validitas hukum transaksi digital. Tujuan yang ingin di capai yakni untuk mengentahui tentang krimininlisasi perbuatan siber dan validitas hukum transaksi digital.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara meneliti studi kepustakaan atau data sekunder. Pendekatan yang digunakan adalah pendekatan perundang-undangan (statute approach) dengan menelaah UU ITE dan KUHP, serta pendekatan konseptual (conceptual approach) dengan merujuk pada pandangan ahli hukum dalam literatur terkait hukum siber dan teknologi. Analisis dilakukan secara kualitatif untuk menginterpretasikan norma hukum yang berlaku.

Penelitian ini menggunakan jenis penelitian hukum normatif (*normative legal research*). Penelitian hukum normatif adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka. Fokus utama penelitian ini adalah mengkaji penerapan kaidah atau norma-norma dalam hukum positif yang berkaitan dengan pengaturan tindak pidana siber (*cybercrime*) dan keabsahan transaksi elektronik di Indonesia. Untuk menjawab isu hukum yang diangkat, penulis menggunakan dua pendekatan utama: 1. Pendekatan Perundang-undangan (*Statute Approach*) dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Dalam hal ini, fokus telaah adalah Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Pendekatan Konseptual (*Conceptual Approach*) dengan memperoleh data dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum.

Pendekatan ini digunakan untuk memahami konsep-konsep tentang yurisdiksi di ruang siber, konsep "melawan hukum" dalam ranah digital, serta konsep validitas kontrak tanpa tatap muka. Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari bahan hukum primer yang merupakan bahan hukum yang bersifat mengikat, yaitu Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008.

Sedangkan bahan hukum sekunder merupakan Bahan yang memberikan penjelasan mengenai bahan hukum primer, meliputi buku-buku teks hukum, jurnal-jurnal ilmiah (termasuk referensi dari *Jurnal Kolaboratif Sains*, *Jurnal Konstruksi Hukum*, dan *Jurnal Kewarganegaraan*), serta pendapat para sarjana hukum yang relevan dengan *cyberlaw* dan bahan hukum tersier merupakan bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti Kamus Besar Bahasa Indonesia (KBBI) dan Kamus Hukum (*Black's Law Dictionary*). Teknik pengumpulan data yang digunakan adalah studi kepustakaan (*library research*), yaitu dengan cara mencari, menginventarisasi, dan mempelajari bahan-bahan hukum yang relevan.

Seluruh data yang terkumpul kemudian dianalisis secara **kualitatif**. Metode ini tidak menggunakan angka atau statistik, melainkan menguraikan data secara deskriptif-analitis. Penulis melakukan interpretasi hukum (seperti interpretasi gramatikal dan sistematis) untuk menarik kesimpulan deduktif, yaitu menarik kesimpulan dari hal yang bersifat umum (regulasi UU ITE dan KUHP) ke hal yang bersifat khusus (permasalahan validitas transaksi dan penegakan hukum siber).

HASIL PENELITIAN DAN PEMBAHASAN

A. Konstruksi Hukum Regulasi Cybercrime di Indonesia

1. Definisi dan Karakteristik Cybercrime

Secara yuridis, hingga saat ini belum terdapat definisi baku atau kesepahaman tunggal di kalangan ahli maupun instrumen hukum internasional mengenai definisi pasti *cybercrime*. Istilah ini sering disandingkan dengan istilah

lain seperti kejahatan dunia maya, kejahatan virtual, atau *computer crime*, meskipun istilah *computer crime* terkadang dianggap tidak lagi relevan sepenuhnya karena pelaku dapat menggunakan media atau alat lain selain komputer dalam melakukan aksinya.

Cybercrime atau kejahatan siber didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet atau jaringan komputer sebagai alat atau sasaran. Dalam literatur hukum, kejahatan ini sering dibedakan menjadi dua kategori:

- Computer Crime (arti sempit): Kejahatan yang menargetkan keamanan sistem komputer itu sendiri, seperti hacking atau perusakan data.
- Computer-Related Crime (arti luas): Kejahatan konvensional yang menggunakan komputer sebagai alat bantu, seperti penipuan online atau pornografi daring.

Mengacu pada definisi luas tersebut, *cybercrime* merujuk pada segala bentuk aktivitas kriminal yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi (TIK), khususnya internet, sebagai sarana utama. Hal ini berarti semua tindak pidana konvensional dalam KUHP, sepanjang dilakukan dengan bantuan atau sarana Sistem Elektronik, dapat dikategorikan sebagai tindak pidana siber dalam arti luas.

Karakteristik unik dari cybercrime adalah sifatnya yang transnational (melintasi batas negara), non-violence (tidak menimbulkan kekacauan fisik langsung), serta kerugian yang ditimbulkan bisa bersifat materiil maupun non-materiil (seperti pencurian data privasi). Karakteristik *Cybercrime dalam pandangan lain* yang merupakan dimensi baru kejahatan yang berbeda dengan kejahatan konvensional. Beberapa karakteristik utamanya meliputi:

- Tanpa Batas Teritorial (*Borderless*): Kejahatan ini bersifat transnasional dan tidak mengenal batas wilayah suatu negara. Pelaku kejahatan siber seringkali beroperasi dari luar negeri, namun dampaknya dirasakan oleh korban yang berada di dalam negeri, atau sebaliknya. Sifat lintas negara ini menyebabkan penegakan hukum menjadi sangat kompleks karena melibatkan masalah yurisdiksi dan perbedaan regulasi antarnegara.
- Bersifat Virtual dengan Dampak Nyata: Meskipun *cybercrime* dilakukan dalam ruang virtual (*cyberspace*), tindakan tersebut dikategorikan sebagai perbuatan hukum yang nyata karena menimbulkan akibat kerugian materiil maupun non-materiil yang nyata bagi korban.
- Bukti Digital yang Mudah Berubah (*Volatile*): Berbeda dengan kejahatan fisik, alat bukti dalam *cybercrime* bersifat digital atau elektronik. Data yang

tersimpan di komputer, server, atau *cloud* ini sangat mudah diubah, dihapus, atau disembunyikan, sehingga menyulitkan proses penyidikan dan memerlukan kemampuan forensik digital yang tinggi untuk mengamankannya.

- Dinamis dan Terus Berkembang adalah Modus operandi kejahatan ini terus berkembang seiring dengan kemajuan teknologi itu sendiri. Pelaku kejahatan selalu mencari dan memanfaatkan celah keamanan baru dalam sistem digital untuk tujuan ilegal.
- Pelaku yang Sulit Teridentifikasi: Teknologi memungkinkan pelaku untuk menyembunyikan identitas mereka (anonimitas) menggunakan berbagai alat seperti VPN atau jaringan anonim, sehingga kejahatan ini seringkali sulit dilacak (*traceable*) oleh aparat penegak hukum.

2. Pengaturan Tindak Pidana dalam UU ITE

Secara yuridis normatif, UU ITE mengadopsi pendekatan hukum yang komprehensif dengan mengatur perbuatan yang dilarang dalam Bab VII (Pasal 27–37). Beberapa delik utama yang diatur meliputi:

- Konten Ilegal (Illegal Content): Pasal 27 melarang distribusi informasi elektronik yang bermuatan melanggar kesusilaan, perjudian, penghinaan/pencemaran nama baik, serta pemerasan/pengancaman.
- Akses Ilegal (Illegal Access): Pasal 30 mengkriminalisasi tindakan mengakses komputer atau sistem elektronik orang lain dengan cara apa pun, baik menerobos sistem pengamanan (hacking) maupun tidak.
- Intersepsi Ilegal (Illegal Interception): Pasal 31 melarang penyadapan atas informasi elektronik yang tidak bersifat publik.
- Gangguan Data (Data Interference) dan Sistem: Pasal 32 dan 33 mengatur larangan mengubah, merusak, memindahkan, atau menyembunyikan informasi elektronik, serta tindakan yang mengakibatkan terganggunya sistem elektronik.

Selain itu, UU ITE juga mengatur yurisdiksi secara ekstrateritorial (Pasal 2). Artinya, undang-undang ini berlaku bagi setiap orang yang melakukan perbuatan hukum, baik di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di Indonesia dan/atau merugikan kepentingan Indonesia. Asas ini krusial mengingat sifat kejahatan siber yang borderless.

Kehadiran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan respons hukum terhadap perkembangan teknologi yang tidak sepenuhnya dapat diakomodasi oleh KUHP. UU ITE berfungsi sebagai *lex specialis* yang mengatur berbagai aspek, mulai dari regulasi transaksi elektronik hingga penanggulangan penyalahgunaan teknologi informasi seperti peretasan, penyebaran konten ilegal, dan pencurian identitas.

Secara spesifik, pengaturan tindak pidana dalam UU ITE dapat diklasifikasikan berdasarkan jenis perbuatan yang dilarang dan sanksi yang menyertainya, sebagaimana diuraikan berikut ini:

1. Tindak Pidana Akses Ilegal (*Illegal Access*) Salah satu fokus utama dalam UU ITE adalah perlindungan terhadap keamanan sistem elektronik. Tindak pidana peretasan atau akses ilegal diatur secara rinci dalam Pasal 30, yang terdiri dari beberapa unsur:

- **Pasal 30 ayat (1):** Melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun. Unsur "dengan cara apa pun" menegaskan bahwa baik akses melalui perangkat korban maupun melalui jaringan internet tetap merupakan pelanggaran hukum.
- **Pasal 30 ayat (2):** Mengatur larangan akses ilegal dengan tujuan spesifik untuk memperoleh informasi elektronik dan/atau dokumen elektronik. Unsur pembedanya terletak pada niat pelaku untuk mencuri data atau informasi dari sistem korban.
- **Pasal 30 ayat (3):** Melarang tindakan akses ilegal yang dilakukan dengan cara melanggar, menerobos, melampaui, atau menjebol sistem keamanan (*security system*).

2. Ketentuan Sanksi Pidana Sebagai upaya represif untuk memberikan efek jera, UU ITE menetapkan sanksi pidana yang berat bagi pelaku kejahatan siber, khususnya terkait akses ilegal yang diatur dalam Pasal 46 (berkorelasi dengan Pasal 30):

- Pelanggaran terhadap Pasal 30 ayat (1) diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00.
- Pelanggaran terhadap Pasal 30 ayat (2) diancam dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00.

- Pelanggaran terhadap Pasal 30 ayat (3) memiliki sanksi terberat dalam klaster ini, yaitu pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00.

3. Pemberatan Pidana (*Aggravating Circumstances*) UU ITE juga mengatur pemberatan hukuman berdasarkan objek yang diserang dan subjek pelakunya, sebagaimana diatur dalam Pasal 52:

- **Objek Pelayanan Publik:** Sanksi pidana dapat diperberat jika tindak pidana ditujukan terhadap sistem elektronik milik pemerintah atau sistem yang digunakan untuk pelayanan publik (Pasal 52 ayat 2).
- **Objek Keamanan Negara:** Pemberatan juga berlaku jika serangan ditujukan pada situs web atau sistem pemerintah yang berkaitan langsung dengan pertahanan dan keamanan nasional atau stabilitas negara (Pasal 52 ayat 3).
- **Korporasi:** Jika tindak pidana dilakukan oleh korporasi, maka dapat dikenakan pemberatan pidana sesuai Pasal 52 ayat (4).

4. Klasifikasi Tindak Pidana Lainnya Selain peretasan, literatur hukum mengklasifikasikan beberapa jenis tindak pidana siber lainnya yang diakomodasi dalam kerangka hukum siber Indonesia, antara lain:

- **Gangguan Data dan Sistem:** Mencakup *data interference* (mengganggu data) dan *system interference* (mengganggu fungsi sistem komputer).
- **Penyalahgunaan Perangkat:** *Misuse of devices* atau menyalahgunakan peralatan komputer untuk tujuan kejahatan.
- **Konten Ilegal:** Termasuk penyebaran konten yang melanggar kesusilaan, perjudian, penghinaan, pemerasan, serta penyebaran berita bohong (hoaks) yang menyesatkan konsumen.

Pengaturan yang komprehensif ini menunjukkan bahwa Indonesia telah memiliki instrumen hukum yang kuat. Namun, efektivitasnya sangat bergantung pada kemampuan aparat penegak hukum dalam membuktikan unsur-unsur pidana tersebut, mengingat bukti digital yang bersifat *volatile* (mudah berubah).

Pengaturan tindak pidana dalam Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan respons legislatif terhadap keterbatasan KUHP dalam menjangkau karakteristik kejahatan siber yang bersifat virtual. Berdasarkan analisis terhadap substansi undang-undang tersebut, pengaturan tindak pidana dapat diklasifikasikan ke dalam beberapa dimensi yuridis sebagai berikut:

a. Klasifikasi Delik Berbasis Modus Operandi

Secara yuridis, UU ITE tidak hanya memindahkan delik konvensional ke ranah digital, tetapi juga menciptakan jenis delik baru yang spesifik. Pengaturan ini membagi tindak pidana siber ke dalam klaster utama:

1. **Kejahatan terhadap Sistem (Cyber-dependent crimes):** Fokus utama pengaturan ini adalah melindungi integritas sistem komputer itu sendiri. Hal ini tercermin dalam **Pasal 30 UU ITE** yang mengatur tentang Akses Ilegal (*Illegal Access*). Pasal ini secara tegas melarang setiap orang yang dengan sengaja dan tanpa hak mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun. Analisis terhadap frasa "dengan cara apa pun" menunjukkan bahwa undang-undang ini menutup celah bagi pelaku untuk berdalih mengenai metode teknis yang digunakan, baik melalui jaringan maupun akses fisik langsung.
2. **Kejahatan Menggunakan Sarana Teknologi (Cyber-enabled crimes):** Kategori ini mencakup penyalahgunaan teknologi untuk tujuan ilegal lainnya, seperti penyebaran konten ilegal. Ini termasuk penyebaran berita bohong (hoaks), ujaran kebencian, pornografi, hingga penipuan daring (*online fraud*) yang memanfaatkan e-commerce atau manipulasi data.

b. Konstruksi Unsur Pasal 30 dan Korelasinya dengan Sanksi Pidana

Inti dari penanggulangan kejahatan peretasan (*hacking*) terletak pada konstruksi Pasal 30 yang memiliki gradasi perbuatan melawan hukum. Analisis penulis menemukan bahwa gradasi ini berbanding lurus dengan beratnya sanksi yang diatur dalam **Pasal 46**:

- **Akses Ilegal Dasar (Ayat 1):** Delik ini terpenuhi cukup dengan adanya intrusi ilegal ke dalam sistem orang lain. Sanksi pidananya adalah penjara maksimal 6 tahun dan/atau denda Rp600 juta.
- **Pencurian Data (Ayat 2):** Jika akses ilegal tersebut disertai dengan tujuan memperoleh informasi atau dokumen elektronik (pencurian data), maka kualifikasi deliknya meningkat dengan ancaman pidana 7 tahun dan/atau denda Rp700 juta. (Jurnal Konstruksi Hukum, 337 : 2020).
- **Penerobosan Sistem Keamanan (Ayat 3):** Ini adalah kualifikasi terberat, di mana pelaku melakukan *hacking* dengan cara menjebol sistem pengamanan (*security system*). Ancaman pidananya mencapai 8 tahun penjara dan/atau denda Rp800 juta. (Jurnal Konstruksi Hukum, 337 : 2020).

Konstruksi bertingkat ini menunjukkan bahwa UU ITE menerapkan prinsip proporsionalitas dalam pemidanaan, di mana sanksi diperberat seiring dengan tingginya tingkat kerugian dan kecanggihan modus operandi pelaku.

Analisis terhadap **Pasal 52 UU ITE** menunjukkan adanya kebijakan hukum pidana (*criminal policy*) yang memberikan perlindungan khusus terhadap aset strategis negara. UU ITE menetapkan pemberatan pidana dalam kondisi tertentu:

- Jika tindak pidana ditujukan terhadap sistem elektronik milik pemerintah atau yang digunakan untuk pelayanan publik, maka ancaman pidananya dapat diperberat.
    - Pemberatan juga berlaku jika serangan siber mengancam sistem pertahanan dan keamanan negara serta kedaulatan nasional.
    - Selain itu, UU ITE mengakui konsep kejahatan korporasi, di mana pidana dapat diperberat jika tindak pidana dilakukan oleh korporasi.

Meskipun pengaturan dalam UU ITE telah cukup komprehensif dibandingkan KUHP, analisis menunjukkan bahwa undang-undang ini masih menghadapi tantangan relevansi. Pesatnya perkembangan teknologi seperti kecerdasan buatan (*Artificial Intelligence*), *blockchain*, dan *cryptocurrency* memunculkan modus kejahatan baru yang mungkin belum sepenuhnya terakomodasi dalam rumusan pasal yang ada saat ini. Oleh karena itu, pengaturan tindak pidana dalam UU ITE harus bersifat dinamis dan terbuka terhadap penafsiran futuristik atau amandemen berkala.

3. Analisis Unsur Melawan Hukum dan Pertanggungjawaban Pidana

Dalam penegakan hukum cybercrime, pembuktian unsur "tanpa hak" atau "melawan hukum" (wederrechtelijk) memegang peranan vital. Situmeang (2020) menjelaskan bahwa dalam konteks siber, unsur ini harus ditafsirkan secara luas, tidak hanya melanggar peraturan tertulis tetapi juga kepatutan dalam sistem elektronik. Tantangan terbesar muncul dalam pembuktian niat jahat (mens rea). Mengingat cybercrime adalah kejahatan berbasis keahlian, penyidik harus mampu membuktikan bahwa pelaku memiliki kesengajaan (dolus) untuk mengganggu sistem atau mencuri data, bukan sekadar kelalaian teknis.

Selain itu, UU ITE juga memperkenalkan konsep pertanggungjawaban pidana korporasi. Pasal 52 ayat (4) UU ITE memungkinkan pemidanaan terhadap korporasi jika tindak pidana dilakukan atas nama atau untuk kepentingan badan usaha tersebut. Hal ini merupakan langkah maju mengingat

banyak kejahatan siber (seperti pencurian data nasabah atau penipuan investasi bodong) yang berlindung di balik entitas perusahaan. Sanksi yang ditekankan bagi korporasi lebih bersifat denda, yang sejalan dengan prinsip follow the money dalam pemberantasan kejahatan ekonomi.

Pertanggungjawaban pidana bertujuan menentukan apakah terdakwa dapat dimintai pertanggungjawaban atas tindak pidana yang dilakukannya. Dalam hukum pidana, berlaku asas "tiada pidana tanpa kesalahan", yang berarti seseorang hanya dapat dipidana jika perbuatannya didukung oleh bukti sah dan dapat dipertanggungjawabkan kepadanya.

Dalam UU ITE, frasa "Setiap Orang" merujuk pada subjek hukum yang dapat bertanggung jawab dan cakap hukum berdasarkan peraturan perundang-undangan. Hal ini menegaskan bahwa pelaku *cybercrime* haruslah individu yang memiliki kemampuan bertanggung jawab. Mayoritas tindak pidana siber mensyaratkan adanya unsur "dengan sengaja" (*dolus*). Dalam Pasal 30 UU ITE, unsur ini diartikan sebagai niat penuh kesadaran dari pelaku untuk melakukan akses ilegal. Unsur kesengajaan ini juga terlihat dalam Pasal 30 ayat (2), di mana akses ilegal dilakukan dengan tujuan spesifik untuk mencuri data atau memperoleh informasi elektronik.

Karakteristik unik UU ITE adalah pengakuan terhadap pertanggungjawaban korporasi. Berdasarkan Pasal 52 ayat (4) UU ITE, pemberatan pidana dapat dijatuhkan apabila terbukti bahwa tindak pidana siber (seperti peretasan) dilakukan oleh atau atas nama korporasi. Hal ini memperluas jangkauan pertanggungjawaban pidana tidak hanya pada individu (natuurlijke persoon) tetapi juga badan hukum.

Meskipun UU ITE berlaku sebagai *lex specialis*, analisis unsur melawan hukum juga sering dikaitkan dengan KUHP untuk delik-delik tertentu:

- **Pencurian (Pasal 362 KUHP):** Unsur "mengambil barang milik orang lain" dikonstruksikan secara luas untuk mencakup pencurian nomor kartu kredit (*carding*).
- **Penipuan (Pasal 378 KUHP):** Unsur "tipu muslihat" atau "rangkaian kebohongan" relevan untuk penipuan *e-commerce*.
- **Perusakan (Pasal 406 KUHP):** Digunakan untuk kasus *defacing* atau *hacking* yang menyebabkan sistem tidak berfungsi.

Namun, penerapan KUHP seringkali terkendala sanksi yang terlalu ringan dan tidak sepadan dengan kerugian besar akibat *cybercrime*. Oleh karena itu, UU ITE memberikan ancaman pidana yang lebih berat, misalnya pidana

penjara hingga 8 tahun untuk peretasan sistem keamanan (Pasal 46 ayat 3 jo Pasal 30 ayat 3).

Dalam penegakan hukum pidana terhadap *cybercrime*, pembuktian tidak hanya berhenti pada terjadinya suatu peristiwa digital, melainkan harus memenuhi konstruksi yuridis mengenai perbuatan pidana (*strafbaarfeit*) dan kesalahan pelaku. Berdasarkan literatur hukum dan regulasi yang berlaku, berikut adalah analisis unsur-unsur tersebut:

a. Konstruksi Unsur Melawan Hukum (*Wederrechtelijk*) dalam Cybercrime

Secara teoritis, agar suatu perbuatan dapat dipidana, perbuatan tersebut harus memenuhi rumusan delik dalam undang-undang dan memiliki sifat melawan hukum.

Menurut Simons, *strafbaarfeit* adalah tindakan melanggar hukum yang dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan dinyatakan oleh undang-undang sebagai tindakan yang dapat dihukum. Syarat mutlaknya adalah adanya tindakan yang dilarang oleh undang-undang, di mana pelanggaran tersebut pada hakikatnya merupakan tindakan melawan hukum (*onrechtmatige handeling*). (Jurnal Kewarganegaraan Sinta S5, hal : 2171: 2022).

Dalam konteks UU ITE, khususnya pada tindak pidana peretasan (Pasal 30), unsur melawan hukum dirumuskan secara eksplisit dengan frasa "dengan sengaja dan tanpa hak atau melawan hukum".

- **Unsur "Tanpa Hak":** Mengacu pada ketiadaan izin atau otoritas yang sah dari pemilik sistem. Ini menegaskan bahwa akses terhadap sistem elektronik yang bersifat privat (milik orang lain) adalah wilayah yang dilindungi hukum.
- **Unsur "Melawan Hukum":** Merujuk pada niat jahat (*mens rea*) dan kesadaran penuh dari pelaku bahwa tindakannya bertentangan dengan norma hukum yang berlaku.
- **Unsur "Dengan Cara Apapun":** Frasa ini memperluas cakupan delik, menegaskan bahwa metode teknis apa pun yang digunakan—baik melalui perangkat korban langsung maupun jaringan jarak jauh—tetap memenuhi unsur pidana selama akses tersebut ilegal.

Sebelum adanya UU ITE, unsur melawan hukum dalam *cybercrime* sering dipaksakan masuk ke dalam pasal-pasal KUHP. Misalnya, Pasal 406 KUHP tentang perusakan barang digunakan untuk menjerat *hacker* yang melakukan *defacing* situs web. Namun, penerapan ini seringkali tidak memadai karena sanksi dalam KUHP relatif ringan dan tidak sebanding dengan kerugian

masif yang ditimbulkan kejahatan siber. UU ITE hadir mempertegas unsur melawan hukum ini dengan sanksi yang jauh lebih berat, seperti penjara maksimal 8 tahun untuk penerobosan sistem keamanan (Pasal 46 ayat 3).

Pertanggungjawaban pidana berkaitan dengan penilaian apakah pelaku dapat dipersalahkan atas perbuatannya. Asas *geen straf zonder schuld* (tiada pidana tanpa kesalahan) menjadi landasan utama. Dalam UU ITE, frasa "Setiap Orang" merujuk pada subjek hukum pendukung hak dan kewajiban yang cakap hukum. Ini berarti pelaku *cybercrime* haruslah individu yang mampu bertanggung jawab secara hukum. Namun, UU ITE memperluas konsep ini dengan mengakui korporasi sebagai subjek hukum yang dapat dimintai pertanggungjawaban. Pasal 52 ayat (4) UU ITE mengatur pemberatan pidana jika tindak pidana dilakukan oleh korporasi, yang merupakan kemajuan signifikan dibandingkan KUHP konvensional.

Mayoritas tindak pidana siber dalam UU ITE mensyaratkan adanya unsur kesengajaan. Dalam analisis Pasal 30 ayat (2) UU ITE, unsur kesengajaan ini dikaitkan dengan tujuan spesifik (*doel*), yaitu mengakses sistem dengan tujuan memperoleh informasi atau dokumen elektronik. Artinya, pelaku tidak hanya sekadar "masuk" (akses ilegal), tetapi memiliki niat jahat spesifik untuk mencuri data atau informasi (pencurian data/identitas).

Pertanggungjawaban pidana dalam kasus siber memiliki gradasi berat-ringannya hukuman tergantung pada objek yang diserang. Analisis terhadap Pasal 52 UU ITE menunjukkan bahwa negara memberikan perlindungan lebih tinggi pada aset vital:

- Jika peretasan dilakukan terhadap sistem pelayanan publik atau milik pemerintah, sanksi pidana diperberat.
- Jika serangan ditujukan pada sistem pertahanan dan keamanan negara (hankam), pemberatan pidana juga berlaku. (Jurnal Konstruksi Hukum, Hal 337:2020).

Dari uraian di atas, dapat disimpulkan bahwa pembuktian dalam *cybercrime* jauh lebih kompleks dibandingkan kejahatan konvensional. Penegak hukum tidak hanya harus membuktikan *actus reus* (perbuatan akses ilegal atau manipulasi data) melalui bukti digital yang sah, tetapi juga harus membuktikan *mens rea* (niat jahat/kesengajaan) dalam kerangka "tanpa hak" yang seringkali kabur batasannya dalam dunia digital. Keberadaan UU ITE sebagai *lex specialis* sangat krusial karena ia mendefinisikan ulang "unsur melawan hukum" agar relevan dengan karakteristik teknologi yang *borderless* dan virtual, sekaligus memperluas pertanggungjawaban pidana hingga ke entitas korporasi.

4. Tantangan Implementasi Yurisdiksi Ekstrateritorial

Meskipun Pasal 2 UU ITE telah mengadopsi asas ekstrateritorial, Wibowo dkk. (2022) mencatat bahwa eksekusinya menghadapi kendala diplomasi dan kedaulatan negara lain. Penegakan hukum terhadap pelaku yang berada di luar negeri (misalnya hacker dari Eropa Timur yang menyerang bank di Indonesia) sangat bergantung pada Mutual Legal Assistance (MLA) dan perjanjian ekstradisi. Tanpa kerja sama internasional yang kuat, yurisdiksi ekstrateritorial berisiko hanya menjadi "macan kertas" yang memiliki legitimasi hukum namun lemah dalam eksekusi (law in books vs. law in action).

Salah satu karakteristik paling mendasar dari *cybercrime* adalah sifatnya yang transnasional atau melintasi batas negara (*borderless*), di mana pelaku dapat beroperasi dari satu negara sementara korban atau dampak kerugiannya berada di negara lain. Kondisi ini menuntut penerapan yurisdiksi ekstrateritorial, namun implementasinya di lapangan menghadapi berbagai hambatan yuridis dan praktis yang signifikan.

Secara tradisional, hukum pidana Indonesia menganut prinsip yurisdiksi teritorial yang kuat, di mana negara memiliki wewenang penuh atas peristiwa hukum yang terjadi di dalam wilayahnya. Namun, dalam konteks siber, prinsip ini sering kali tidak memadai karena *locus delicti* (tempat kejadian perkara) terjadi di ruang virtual yang tidak mengenal batas geografis. Hal ini menciptakan kekosongan atau kesulitan hukum ketika pelaku berada di luar yurisdiksi Indonesia (ekstrateritorial), sehingga aparat penegak hukum tidak dapat melakukan penangkapan atau penyidikan secara langsung tanpa melanggar kedaulatan negara lain.

Untuk menjangkau pelaku di luar negeri, instrumen hukum internasional seperti ekstradisi dan *Mutual Legal Assistance* (Bantuan Hukum Timbal Balik) menjadi mutlak diperlukan. Namun, terdapat beberapa tantangan utama:

1. Proses ekstradisi sering mensyaratkan bahwa perbuatan tersebut harus dianggap sebagai tindak pidana oleh kedua negara (negara peminta dan negara tempat pelaku berada). Perbedaan regulasi hukum antarnegara sering menjadi penghambat. Sebagai contoh, dalam kasus pornografi, situs yang dianggap ilegal di Indonesia mungkin legal di negara tempat *server* atau domain tersebut terdaftar, sehingga pelaku sulit diekstradisi atau ditindak.
2. Jika Indonesia tidak memiliki perjanjian ekstradisi atau bantuan hukum timbal balik dengan negara tempat pelaku bersembunyi, proses penegakan

hukum menjadi hampir mustahil dilakukan. (*Jurnal Kolaboratif Sains: hal 509*).

Dalam hukum internasional, dikenal beberapa prinsip untuk memperluas jangkauan hukum nasional ke wilayah ekstrateritorial, yaitu:

- Negara berhak mengadili warganegaranya di mana pun mereka melakukan kejahatan.
- Negara berhak bertindak jika kejahatan tersebut mengancam kepentingan vital atau keamanan nasionalnya, meskipun dilakukan oleh orang asing di luar negeri.
- Negara mana pun berhak mengadili kejahatan tertentu yang dianggap musuh seluruh umat manusia.

Meskipun prinsip-prinsip ini diakui, tantangan muncul dalam eksekusinya. Aparat penegak hukum sering kali terkendala prosedur birokrasi internasional yang rumit dan memakan waktu lama, sementara bukti digital yang menjadi kunci pembuktian bersifat mudah hilang atau berubah (*volatile*). Tanpa mekanisme kerjasama global yang cepat dan responsif, penerapan yurisdiksi ekstrateritorial sering kali hanya efektif di atas kertas namun tumpul dalam penindakan nyata.

Dalam praktik penegakan hukum siber di Indonesia, terdapat dualisme instrumen hukum yang digunakan, yaitu KUHP dan UU ITE. Meskipun KUHP merupakan produk hukum lama, instrumen ini masih digunakan melalui metode penafsiran ekstensif untuk menjangkau delik siber. Sebagai contoh, Pasal 362 KUHP tentang pencurian dikonstruksikan untuk menjerat kasus *carding* (pencurian data kartu kredit) , dan Pasal 378 KUHP tentang penipuan digunakan untuk kasus penipuan jual-beli daring (*e-commerce*).

Namun, ketergantungan pada KUHP memiliki kelemahan fundamental. Delik-delik dalam KUHP membutuhkan penafsiran yang sangat luas agar relevan dengan konteks teknologi, yang berpotensi membingungkan hakim dan aparat penegak hukum karena berbenturan dengan asas legalitas (*lex certa*) yang mensyaratkan aturan pidana harus jelas dan tertulis. Selain itu, sanksi dalam KUHP seringkali dinilai terlalu ringan dan tidak sepadan dengan kerugian masif yang ditimbulkan oleh kejahatan siber.

Kehadiran UU ITE sebagai *lex specialis* mengisi kekosongan tersebut dengan memberikan kepastian hukum yang lebih spesifik. Misalnya, tindak pidana peretasan (*hacking*) yang sulit didefinisikan secara pas dalam KUHP ("merusak barang"), diatur secara tegas dalam Pasal 30 UU ITE sebagai tindakan akses ilegal terhadap Sistem Elektronik. UU ITE juga menetapkan sanksi pidana

yang jauh lebih berat, dengan ancaman penjara hingga 8 tahun dan denda hingga Rp800 juta untuk penerobosan sistem keamanan, yang diharapkan memberikan efek jera (*deterrent effect*) yang lebih kuat dibandingkan KUHP.

Analisis terhadap efektivitas penegakan hukum tidak dapat dilepaskan dari aspek pembuktian. Berbeda dengan kejahatan konvensional yang meninggalkan jejak fisik, *cybercrime* meninggalkan jejak digital yang bersifat *volatile* (mudah berubah, hilang, atau dihapus).

Hal ini menuntut transformasi metode penyidikan dari konvensional menjadi berbasis *scientific crime investigation* dengan dukungan forensik digital. Tantangan terbesarnya adalah:

1. Data yang tersimpan di *cloud* atau server luar negeri seringkali menjadi kunci penyidikan, namun sulit diakses karena kendala yurisdiksi.
2. Masih terdapat kesenjangan kompetensi di kalangan aparat penegak hukum (polisi, jaksa, hakim) dalam memahami teknis teknologi digital dan prosedur penanganan bukti elektronik yang sah. Keterbatasan infrastruktur laboratorium forensik digital juga menyebabkan proses penanganan kasus menjadi lambat dan tidak efisien. (*Jurnal Kolaboratif Sains: hal 509*).

Meskipun UU ITE telah mengalami revisi, analisis menunjukkan bahwa regulasi yang ada masih tertinggal dibandingkan laju perkembangan teknologi. Modus operandi kejahatan siber terus berevolusi, memanfaatkan teknologi baru seperti *blockchain*, *cryptocurrency*, dan kecerdasan buatan (*Artificial Intelligence/AI*).

Saat ini, UU ITE belum sepenuhnya mengantisipasi kejahatan yang memanfaatkan teknologi desentralisasi seperti kripto untuk pencucian uang atau penipuan investasi, maupun penggunaan AI untuk *deepfake* atau otomatisasi serangan siber. Oleh karena itu, diperlukan pembaruan regulasi yang adaptif dan proaktif, tidak hanya reaktif terhadap kejahatan yang sudah terjadi. Tanpa pembaruan ini, celah hukum akan terus dimanfaatkan oleh pelaku kejahatan (*cybercriminals*) yang selangkah lebih maju daripada hukum positif yang berlaku.

KESIMPULAN

Berdasarkan analisis yuridis normatif, dapat disimpulkan bahwa: Berdasarkan analisis normatif, penelitian ini menegaskan empat temuan utama. Pertama, konstruksi hukum positif Indonesia terhadap cybercrime telah

terbentuk melalui model **dualisme komplementer**, yakni UU ITE sebagai lex specialis yang mengatur delik siber secara spesifik, sedangkan KUHP berfungsi residual untuk delik konvensional yang menggunakan sarana digital. Kedua, dari perspektif hukum perdata, transaksi elektronik memiliki kekuatan mengikat yang setara dengan transaksi konvensional sepanjang memenuhi syarat formil-materiil dan didukung tanda tangan elektronik tersertifikasi, sehingga prinsip kepastian hukum dalam ekonomi digital tetap dapat dijaga. Ketiga, efektivitas penegakan hukum masih menghadapi hambatan struktural dan teknis, terutama karena sifat kejahatan siber yang lintas yurisdiksi (borderless), karakter bukti digital yang volatile, serta kesenjangan kompetensi aparatur dan keterbatasan infrastruktur forensik digital. Keempat, kerangka regulasi yang ada belum sepenuhnya adaptif terhadap evolusi modus berbasis AI, blockchain, dan aset kripto; karena itu, reformasi hukum harus bergerak dari pola reaktif menuju pola antisipatif-progresif agar tidak terjadi legal lag yang berulang.

SARAN

1. Pemerintah melalui lembaga legislatif perlu segera melakukan harmonisasi antara KUHP (sebagai *lex generalis*) dan UU ITE (sebagai *lex specialis*) untuk menghilangkan tumpang tindih penafsiran pasal. Selain itu, mendesak adanya regulasi turunan atau revisi yang secara spesifik mengatur implikasi hukum dari teknologi baru seperti **Kecerdasan Buatan (AI)**, **Blockchain**, dan **Aset Kripto**. Regulasi harus bersifat futuristik agar tidak selalu tertinggal dari modus operandi kejahatan yang terus berkembang.
2. Polri, Kejaksaan, dan Hakim harus diberikan pelatihan berkelanjutan mengenai *Scientific Crime Investigation* berbasis teknologi. Pemerintah perlu berinvestasi lebih besar pada infrastruktur laboratorium **Forensik Digital** di berbagai daerah, tidak hanya terpusat di kota besar, untuk mempercepat proses pembuktian alat bukti elektronik yang sifatnya mudah berubah (*volatile*).
3. Mengingat sifat *cybercrime* yang tanpa batas (*borderless*), Pemerintah perlu lebih agresif dalam memperluas perjanjian ekstradisi dan Bantuan Hukum Timbal Balik (*Mutual Legal Assistance*) dengan negara-negara lain. Hal ini krusial untuk mempermudah penangkapan pelaku dan pemulihan aset korban yang berada di yurisdiksi asing.

DAFTAR PUSTAKA

Aldriano, M. A., & Priyambodo, M. A. 2022. Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan, 6*(1), 2169-2175.

Barkatullah, A. H. 2017. Hukum Transaksi Elektronik di Indonesia: Sebagai Pedoman dalam Menghadapi Era Digital Bisnis E-Commerce. Bandung: Nusa Media.

Bego, K. C., Aziz, F. R., Rahmad, R. A., Sunarto, & Budiantos, H. 2025. Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya. *Jurnal Kolaboratif Sains, 8*(1), 506-511.

Butarbutar, R. 2023. Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal, 2*(2), Article 3. https://scholarhub.ui.ac.id/telj/vol2/iss2/3/

Habibi, M. R., & Liviani, I. 2021. Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Jurnal Qanun: Jurnal Hukum Islam dan Perundang-undangan, 11*, 1132. https://jurnalfsh.uinsa.ac.id/index.php/qanun/article/download/1132/825/5285

Hanafi. 2022. Dasar Cyber Security dan Forensic. Yogyakarta: Deepublish.

Iskandar, B. 2021. Problematika dalam Penanganan Cyber Crime di Indonesia. *Jurnal Hukum Ius Publicum, 1*(2), 98-106. https://journal.umelmandiri.ac.id/ojs/index.php/jiu/article/view/11

Maskun. 2013. Kejahatan Siber (Cyber Crime): Suatu Pengantar. Jakarta: Kencana.

Nasution, A. R., & Fikri, R. A. 2023. Buku Ajar Hukum Tekhnologi dan Informasi. Surakarta: Tahta Media Group.

Nugroho, A. Y., & Nusanto, T. S. 2025. Buku Ajar Hukum Kebijakan TI. Gemilang Press Indonesia.

Redaksi Jurnal PKN. (n.d.). Cyber Crime dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan, Universitas PGRI Yogyakarta*, Article 2947. https://journal.upy.ac.id/index.php/pkn/article/download/2947/pdf/7209

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. 2020. Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum, 1*(2), 334-339.

Situmeang, S. M. T. 2020. Bahan Ajar Cyber Law. Bandung: Cakra.

Titahelu, J. A. S., et al. 2023. Hukum Cyber. Bandung: Widina Media Utama.

Wibowo, S. H., et al.(2022. Cyber Crime di Era Digital. Padang: PT Global Eksekutif Teknologi.

Yitawati, K., Haryani, A. T., & Nugroho, S. S. 2017. Hukum dan Teknologi: Perlindungan Hukum Jual Beli Melalui Transaksi Elektronik (E-Commerce). Solo: Pustaka Iltizam.