

Penegakan Hukum Pidana Terhadap Tindak Pidana Siber (*Cyber Crime*) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia

Bagas Intan Sanjaya

Universitas Widya Mataram, Yogyakarta, Indonesia

E-mail: bagasintansanjaya@gmail.com

Article History:

Received: 16 Juli 2026

Revised: 19 Juli 2026

Accepted: 02 Agustus 2026

Keywords: *Cybercrime, UU ITE, Kepastian Hukum.*

Abstrak: Perkembangan teknologi informasi dan komunikasi telah mendorong meningkatnya tindak pidana siber (*cybercrime*) di Indonesia yang menimbulkan berbagai permasalahan hukum, khususnya dalam aspek penegakan hukum pidana. Penelitian ini bertujuan untuk menganalisis penegakan hukum pidana terhadap tindak pidana siber berdasarkan Undang-Undang Informasi dan Transaksi Elektronik serta mengkaji konsistensi dan harmonisasi regulasi dalam menjamin kepastian hukum. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, menggunakan data sekunder berupa bahan hukum primer, sekunder, dan tersier. Hasil penelitian menunjukkan bahwa meskipun penegakan hukum terhadap *cybercrime* telah memiliki dasar hukum yang memadai, dalam praktiknya masih menghadapi berbagai kendala, seperti keterbatasan aparat penegak hukum, kompleksitas pembuktian digital, serta rendahnya kesadaran hukum masyarakat. Selain itu, terdapat disharmoni antara Undang-Undang ITE dengan KUHP dan Undang-Undang Pelindungan Data Pribadi yang berpotensi menimbulkan kapasitas aparat penegak hukum, serta penguatan kesadaran hukum masyarakat guna mewujudkan penegakan hukum yang efektif dan memberikan kepastian hukum di era digital.

PENDAHULUAN

Arus globalisasi saat ini sedang menuju era serba digital (*digital world*) dengan kemajuan teknologi informasi dan komunikasi (Shidarta, 2022). Oleh karena itu, sangat menggembirakan melihat kemajuan dunia yang rumit, beragam, dan pluralistik, karena pertumbuhan teknologi komputer dan internet telah menjadi instrumen baru bagi negara-negara di dunia untuk digunakan sebagai alat pengaruh dan filtrasi ke berbagai negara (Widodo, 2019). Atas kemajuan teknologi informasi dan komunikasi ini telah membawa perubahan signifikan terhadap perilaku masyarakat

serta peradaban manusia di seluruh dunia. Salah satu dampaknya adalah terjadinya transformasi sosial yang berlangsung secara cepat, termasuk hilangnya batas-batas geografis antarnegara sebagai konsekuensi dari perkembangan teknologi informasi.

Saat ini banyak sekali platform-platform yang menawarkan media komunikasi dengan sangat mudah dipakai oleh masyarakat di Indonesia. Dengan kecanggihan yang diberikan oleh media komunikasi tersebut banyak orang-orang yang mendapatkan dampak positif dari menggunakan platform tersebut, akan tetapi dibalik kecanggihan teknologi komunikasi tersebut terdapat beberapa oknum yang menyalahgunakan platform tersebut. Penggunaan teknologi sistem informasi dan teknologi informasi dimulai pada inovasi yang berbasis pada integrasi antara teknologi komunikasi dengan teknologi komputer atau internet. Aktivitas penggunaan teknologi tidak sesederhana lagi karena kegiatannya tidak dibatasi oleh teritorial suatu negara (*borderless*) yang dapat diakses dengan mudah.

Sebagai hasil dari globalisasi, negara-negara dapat berdagang secara bebas satu sama lain, melewati kekuatan hegemonik dalam prosesnya (Widhiyanti, 2020). Perang ekonomi, sosial, dan budaya pecah sebagai hasil dari upaya masing-masing bangsa untuk tumbuh secara ekonomi, sosial, dan budaya. Konflik energi, konflik pangan, dan konflik air semuanya meningkat sebagai akibat dari negara-negara yang bersaing untuk menguasai sumber daya yang langka atas nama globalisasi, perdagangan bebas, dan pasar bebas (Widhiyanti, 2020).

Indonesia sebagai negara hukum memiliki nilai-nilai yang dianut bersama atau berkenaan dengan penghargaan kolektif (*sinngebungen*) atau kepentingan hukum tentang apa yang baik, benar dan karena itu patut diraih. Nilai-nilai dimaksudkan untuk melindungi, baik terhadap pelanggaran maupun ancaman bahaya atau resiko dengan cara merumuskan suatu ketentuan pidana (Remmelink, 2014). Negara seharusnya memberikan keamanan terhadap data pribadi bagi masyarakat yang berpotensi baik dalam bentuk penyalahgunaan atau kejahatan yang berasal dari dalam maupun luar negara. Sehingga negara dianggap perlu untuk memiliki regulasi yang menggambarkan dan memetakan klasifikasi bahwa data pribadi dibatasi dalam keadaan tertentu dan langkah-langkah yang diambil dengan dasar keputusan yang khusus oleh otoritas negara sebagai perlindungan dan jaminan oleh hukum atas pelanggaran yang merugikan.

Sejak tahun 1983, Indonesia telah mengalami kejahatan dunia maya, terutama di industri keuangan (Gorde, 2022). Berbagai bentuk kejahatan dunia maya, seperti pembajakan perangkat lunak, pembonolan enskripsi, penggunaan kartu kredit curian, penipuan bank, penyebaran konten pornografi, dan bentuk kejahatan dunia maya lainnya, semuanya terjadi di Indonesia pada tahun-tahun setelahnya (Dasco, 2022). Selain penyelundupan foto-foto porno di dunia maya, kejahatan terkait komputer lainnya di Indonesia termasuk *pagejacking* (*mousetrapping*), *spam* (*junkmail*), intersepsi, *cybersquatting*, dan *typosquatting*. Sedangkan *hacking*, vandlisme, serangan DoS/DdoS, penyebaran virus/*worm*, dan pemasangan bom logika merupakan contoh kejahatan yang dilakukan terhadap sistem dan jaringan komputer (Widayanti, 2022).

Kejahatan dunia maya bersifat lebih umum, terlepas dari fitur uniknya, seperti fakta bahwa kejahatan tersebut dilakukan oleh mereka yang memiliki akses dan kekuasaan atas internet dan teknologi terkaitnya. Tidak ada profil atau rentang usia yang ditetapkan untuk orang-orang yang melakukan kejahatan ini. Untuk mengklasifikasikan aktivitas dunia maya sebagai tindakan dan perbuatan hukum nyata bahkan ketika itu terjadi di ruang virtual. Terlalu banyak kerumitan dan hal-hal yang dapat lolos dari pelanggaran hukum jika dunia maya diperlakukan sebagai sesuatu dengan kualifikasi hukum tradisional untuk digunakan sebagai objek dan tindakan. Fenomena ini berkembang seiring dengan meningkatnya penetrasi internet di Indonesia, dimana pengguna aktif di internet nasional terus mengalami pertumbuhan signifikan dari tahun ke tahun. Kondisi demikian

menciptakan medan yang subur bagi para pelaku kejahatan untuk memanfaatkan celah-celah teknologi sebagai instrumen perbuatan melawan hukum, mulai dari penipuan daring, penyebaran informasi palsu (*hoax*), ujaran kebencian, pencemaran nama baik melalui media sosial, hingga peretasan sistem elektronik dan pencurian data pribadi.

Regulasi yang mengatur berkaitan perlindungan data pribadi di Indonesia memang secara eksplisit telah diatur di beberapa Undang-Undang, diantaranya Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pada Pasal 26 ayat (1) Undang-Undang ITE mengenai informasi melalui media elektronik yang mengandung data pribadi tidak menjelaskan secara detail dan komprehensif mengenai prinsip-prinsip perlindungan data pribadi, hak dan kewajiban bagi pemilik data dan stakeholder atau pemerintah dalam mengelola dan menggunakan data pribadi.

Penjelasan Undang-Undang pada Pasal tersebut hanya memberikan definisi secara umum mengenai hak pribadi. Pada Ayat (2) dapat dilihat konsekuensi bila terjadi pelanggaran berkaitan dengan data pribadi yang hanya bersifat ganti rugi, potensi lemahnya kedudukan pemilik dari data pribadi terlihat ketika terjadi sesuatu tindakan yang merugikan pemilik data pribadi, bahkan pemilik data pribadi tidak menyadari telah dirugikan dan dalam hal ini peran negara hanyalah bersifat pasif. Konstitusi telah mengatur mengenai hak setiap orang atas perlindungan diri pribadi, walaupun tidak secara detail mencantumkan mengenai perlindungan data pribadi. Regulasi tersebut juga diikuti dengan kebijakan pemerintah yang mereformasi birokrasi secara masif dengan mulai beralih menggunakan media elektronik atau digital.

Respons negara terhadap fenomena tersebut diwujudkan melalui pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah pertama kali melalui Undang-Undang Nomor 19 Tahun 2016, dan yang paling mutakhir diubah kembali melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perubahan kedua ini hadir dengan tujuan untuk menjaga ruang digital Indonesia agar lebih bersih, sehat, beretika, produktif, dan berkeadilan, serta memberikan kejelasan terhadap pasal-pasal yang selama ini menimbulkan multitafsir dan kontroversi di tengah masyarakat. Secara substansial, Undang-Undang Nomor 1 Tahun 2024 ini menambahkan tujuh pasal baru, meliputi Pasal 13A, 16A, 16B, 18A, 27A, 27B, dan 40A, serta mempertegas kewenangan penyidik dalam melakukan intervensi terhadap akun media sosial dan aset digital yang berkaitan dengan proses penyidikan. Namun demikian, berbagai kalangan akademisi, praktisi hukum, dan organisasi masyarakat sipil menilai bahwa revisi tersebut menyisakan sejumlah persoalan yang belum diselesaikan.

Penelitian ini dilakukan karena meningkatnya penggunaan teknologi digital di Indonesia tidak diimbangi dengan perlindungan yang optimal terhadap data pribadi pengguna internet. Maraknya kasus kebocoran dan penyalahgunaan data pribadi menunjukkan bahwa keamanan data masih menjadi persoalan serius di era digital. Data pribadi yang seharusnya dilindungi justru rentan disalahgunakan untuk berbagai tindak pidana, seperti penipuan, pencurian identitas, hingga akses ilegal terhadap akun digital. Kondisi tersebut menimbulkan keresahan masyarakat serta menunjukkan pentingnya kehadiran perlindungan hukum yang efektif dalam menghadapi perkembangan teknologi informasi.

Penelitian ini dipilih karena tindak pidana siber di Indonesia terus mengalami peningkatan seiring dengan tingginya teknologi digital. Meskipun Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik sebagai dasar hukum dalam penanganan cybercrime,

penegakan hukumnya masih menghadapi berbagai kendala, baik dari aspek substansi hukum, aparat penegak hukum, maupun perkembangan modus kejahatan digital yang sangat cepat (Munir, 2024).

Meskipun demikian, terdapat *gap* penelitian yang signifikan dalam kajian tersebut. Sebagian besar penelitian terdahulu memfokuskan pembahasannya pada satu jenis tindak pidana siber tertentu, misalnya pencemaran nama baik, penipuan daring atau peretasan sistem elektronik, tanpa mengkajinya secara holistik dalam kerangka pengaturan yang komprehensif. Selain itu, kajian yang secara spesifik menganalisis implikasi yuridis normatif dari keseluruhan perubahan substansial dalam Undang-Undang No. 1 Tahun 2024 terhadap konstruksi tindak pidana siber termasuk relevansinya dengan KUHPidana baru dan Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 masih sangat terbatas. Disamping itu, belum terdapat penelitian yang secara eksplisit menganalisis keterkaitan antara kelemahan normatif dalam UU ITE dengan konsistensi putusan pengadilan dalam menangani perkara tindak pidana siber. Kesenjangan inilah yang menjadi pijakan *novelty* dari penelitian ini.

Berdasarkan latar belakang tersebut, maka terdapat beberapa permasalahan yang perlu dikaji dalam penelitian ini. Permasalahan tersebut dirumuskan dalam bentuk rumusan masalah sebagai berikut:

1. Bagaimana penegakan hukum pidana terhadap tindak pidana siber (*cybercrime*) berdasarkan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia?
2. Bagaimana konsistensi dan harmonisasi UU ITE dalam menjamin kepastian hukum?

METODE PENELITIAN

Penelitian ini fokus pada studi hukum normatif yang menyelidiki bagaimana hukum pidana di Indonesia mengatur kejahatan dunia maya dan bagaimana kebijakan hukum di masa depan dapat bekerja untuk mencegah, menghukum, dan mengadili kejahatan dunia maya (Muhammad, 2004). Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan dan putusan pengadilan yang berkaitan dengan tindak pidana siber. Bahan hukum sekunder diperoleh dari buku, jurnal ilmiah, serta hasil penelitian yang relevan dengan objek penelitian. Adapun teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan, kemudian analisis secara kualitatif dengan metode deskriptif-analitis untuk memperoleh kesimpulan yang sesuai dengan permasalahan penilitan.

HASIL DAN PEMBAHASAN

1. Formulasi Hukum Tindak Pidana Siber dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia

Tindak pidana dalam beberapa literatur sering disebut sebagai “delik” atau perbuatan pidana, ketika berbicara mengenai perbuatan dan jenis-jenis delik sama halnya kita berbicara mengenai unsur-unsur perbuatan pidana dan jenis-jenis perbuatan pidana (Hiariej, 2016). Perilaku masyarakat dan peradaban manusia di seluruh dunia telah diubah oleh kemajuan teknologi informasi dan komunikasi. Selain itu, perubahan sosial yang cepat dan penghapusan batas-batas negara merupakan hasil dari kemajuan teknologi informasi (Nazran & Siregar, 2022). Terlepas dari efek positifnya pada masyarakat, pertumbuhan, dan peradaban, teknologi informasi saat ini juga dapat digunakan untuk tujuan kriminal (Dermawan et al., 2021). Sejak penemuan internet sebagai salah satu kemampuan produk IPTEK, bidang telekomunikasi, media, dan komputasi telah menyatu. Internet merupakan produk dari konvergensi beberapa

bentuk teknologi komunikasi dan media serta teknologi komputer. Internet telah memberi orang sesuatu yang sepenuhnya baru.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan repons legislatif terhadap dinamika kejahatan digital yang terus berkembang di Indonesia. Secara konstruktif, undang-undang ini memuat sejumlah perbuatan yang dikualifikasikan sebagai tindak pidana siber, di antaranya penyebaran konten asusila melalui Pasal 27 ayat (1), penyebaran informasi *hoax* yang merugikan konsumen dalam transaksi elektronik sebagaimana Pasal 28 Ayat (1), serta penyebaran ujaran kebencian berbasis SARA dalam pasal 28 Ayat (2). Perubahan kedua ini turut menambahkan Pasal 27A yang mengatur serangan terhadap kehormatan atau nama baik secara elektronik, dan Pasal 27B yang mengatur pemerasan berbasis informasi elektronik, dan Pasal 27B yang mengatur pemerasan berbasis informasi elektronik. Konstruksi delik dalam pasal-pasal tersebut menggunakan pendekatan *actus reus* yang mensyaratkan perbuatan yang dilakukan dengan sengaja dan tanpa hak, sejalan dengan prinsip dasar hukum pidana yang mensyaratkan adanya unsur *mens rea* dan *actus reus* sebagai fondasi pertanggungjawaban pidana (Yudustira & Ramadani, 2023).

Dalam konteks penegakan hukum, konstruksi delik dalam UU ITE seringkali bersinggungan dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana Nasional. Hal ini terlihat dari kenyataan bahwa Pasal II Undang-Undang No. 1 Tahun 2024 secara eksplisit menegaskan bahwa sejumlah pasal pidana di dalamnya hanya berlaku sampai dengan diberlakukannya Undang-Undang No. 1 Tahun 2023 tentang KUHP. Artinya, terdapat *sunset clause* yang menciptakan kondisi transisi normatif yang berpotensi menimbulkan keambiguan terhadap penerapan hukum. Aspek penting lainnya adalah kedudukan alat bukti elektronik sebagaimana diatur dalam Pasal 5 Undang-Undang No. 1 Tahun 2024, yang menegaskan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah sebagai perluasan dari alat bukti konvensional. Hal ini menjadi dasar yuridis bagi aparat penegak hukum dalam memproses perkara tindak pidana siber di pengadilan, meskipun dalam tatanan praktis pembuktian digital masih menghadapi berbagai kendala teknis (Zhafira et al., 2023).

Salah satu unsur dari *cyber crime* adalah penggunaan teknologi dalam modus operandinya. Sifat inilah yang membuat *cyber crime* berbeda dengan tindak pidana lainnya. Namun demikian, kejahatan yang terjadi sebenarnya adalah kejahatan biasa dan masih memungkinkan diselesaikan dengan KUHPidana. Sedangkan dalam masalah kejahatan siber ada beberapa rumusan pidana yang dapat digunakan yaitu :

- a. Pencurian;
- b. Penggelapan;
- c. Pembukaan rahasia;
- d. Pemalsuan;
- e. Pengancaman;
- f. Pornografi;
- g. Penghasutan;
- h. Pelecehan seksual;
- i. Penghinaan;
- j. Penyebaran berita *hoax*.

Dalam suatu perbuatan penyebarluasan pornografi yang dilakukan oleh seseorang atau kelompok yang sangat ditentang oleh negara melalui peraturan hukum yang ada. Penggunaan

media sosial internet adalah suatu kejahatan yang memiliki klasifikasi yang berbeda dengan kejahatan yang lainnya. Seperti muatan yang telah diatur dalam UU ITE terkait dengan cyberphornography yaitu mengenai tindakan seperti kejahatan siber. Dalam Pasal 27 sampai 36 UU ITE dan dalam Pasal 42 UU ITE diatur mengenai ketentuan suatu penyidik untuk membuktikan bahwa sistem pembuktian yang diyakini adalah sistem pembuktian dalam UU ITE berdasarkan sistem yang telah diyakini dalam KUHPidana.

Perkembangan teknologi informasi yang semakin pesat telah memberikan dampak besar terhadap aktivitas masyarakat di era digital. Namun, kemajuan tersebut juga diiringi dengan meningkatnya ancaman tindak pidana siber yang menasar individu, perusahaan, hingga lembaga pemerintahan. Kejahatan siber tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan data dan privasi masyarakat. Berbagai bentuk cybercrime seperti peretasan, pencurian data pribadi, phishing, dan serangan ransomware menunjukkan bahwa sistem keamanan digital masih memiliki banyak celah yang dapat dimanfaatkan oleh pelaku kejahatan.

Salah satu kasus cybercrime di Indonesia tahun 2024 terjadi pada Pusat Data Nasional Sementara (PDNS) yang mengalami serangan ransomware. Serangan tersebut menyebabkan terganggunya berbagai layanan publik digital di Indonesia, termasuk layanan administrasi pemerintahan dan imigrasi. Pelaku diduga menggunakan ransomware untuk mengenkripsi data sehingga sistem tidak dapat diakses secara normal. Kasus ini menunjukkan bahwa ancaman tindak pidana siber tidak hanya menasar sektor privat, tetapi juga infrastruktur digital milik negara yang memiliki peran penting dalam pelayanan publik. Peristiwa tersebut menjadi perhatian serius karena menunjukkan pentingnya penguatan sistem keamanan siber serta efektivitas penegakan hukum pelaku kejahatan siber di Indonesia.

Secara konseptual, inti dari penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang dijabarkan dalam kaidah-kaidah yang bertujuan untuk menciptakan, memelihara, dan mempertahankan keadamaian pergaulan hidup. Penegakan hukum memiliki proses atau upaya untuk melakukan tegaknya suatu aturan dengan tujuan untuk menjaga norma-norma yang berlaku secara nyata sebagai pedoman dalam kehidupan masyarakat dan bernegara (Soekanto, 2008). Penegakan hukum memiliki proses atau upaya untuk melakukan tegaknya suatu aturan yang berfungsi untuk norma-norma yang berlaku di masyarakat. Teori penegakan hukum menurut Joseph Goldstein dibedakan menjadi tiga diantaranya (Arif, 2007).

a. *Total Enforcement*

Konsep penegakan hukum secara total (*total enforcement*) merupakan upaya penegakan seluruh ketentuan hukum pidana sebagaimana telah diatur dalam hukum pidana substantif. Namun, pelaksanaan *total enforcement* ini tidak dapat dilakukan secara sepenuhnya karena adanya pembatasan yang diatur dalam hukum acara pidana. Pembatasan tersebut meliputi ketentuan mengenai penangkapan, penahanan, penggeledahan, penyitaan, dan prosedur hukum lainnya yang harus dilaksanakan sesuai aturan yang berlaku. Oleh karena itu, terdapat ruang lingkup tertentu yang tidak dapat dilakukan penegakan hukum secara penuh, yang dikenal sebagai *area of no enforcement*. Dengan demikian, pelaksanaan *total enforcement* dalam praktiknya harus disesuaikan dengan batasan-batasan yang ditentukan dalam hukum acara pidana.

b. *Full Enforcement*

Konsep penegakan hukum secara aktual (*full enforcement*) merupakan upaya aparat penegak hukum dalam menegakkan hukum secara maksimal terhadap setiap pelanggaran yang terjadi. Namun, penerapan konsep tersebut seringkali dianggap kurang

realistis karena adanya berbagai keterbatasan, seperti keterbatasan waktu, sumber daya manusia, fasilitas, serta anggaran dalam proses penyidikan dan penegakan hukum lainnya. Oleh karena itu, pelaksanaan penegakan hukum dalam praktiknya harus disesuaikan dengan kemampuan dan sarana yang dimiliki oleh aparat penegak hukum.

c. *Actual Enforcement*

Konsep penegakan hukum secara aktual (*actual enforcement*) merupakan pelaksanaan penegakan hukum yang dilakukan secara realistis sesuai dengan kondisi dan kemampuan yang ada. Dalam praktiknya, penegakan hukum tidak dapat dilakukan secara ideal sepenuhnya karena adanya berbagai keterbatasan tertentu, seperti keterbatasan sumber daya, sarana, maupun kemampuan aparat penegak hukum. Meskipun demikian, penegakan hukum tetap harus dilaksanakan secara terpadu dan terarah agar dapat memberikan kepastian hukum serta menciptakan dampak positif bagi masyarakat.

Ketika menghadapi kejahatan siber, KUHPidana masih menjadi rujukan utama penegakan hukum pidana. Hal ini disebabkan belum adanya aturan yang secara spesifik mengatur tindak pidana yang dilakukan dengan media teknologi informasi dan internet. Penegakan hukum masih berusaha menggunakan pasal-pasal dalam KUHPidana yang dianggap relevan untuk mengatasi kejahatan yang muncul di ranah dunia maya. Terdapat perbedaan mendasar antara kejahatan konvensional dan cybercrime meskipun secara teoritis tindak pidana yang dilakukan melalui media digital pada dasarnya memiliki kesamaan dengan delik yang telah diatur dalam KUHPidana. Sebagai contoh, seseorang dapat melaporkan tindak pidana kesusilaan terkait penyebaran pornografi secara online maupun tindak penipuan kartu kredit yang dilakukan melalui media elektronik. Namun demikian, perkembangan kejahatan siber yang semakin kompleks menimbulkan pandangan bahwa diperlukan pengaturan khusus mengenai kejahatan siber, atau setidaknya penyesuaian terhadap ketentuan hukum pidana yang telah ada agar mampu mengakomodasi perkembangan teknologi informasi dan komunikasi (Herlindah & Darmawan, 2022).

Hal ini disebabkan oleh kenyataan bahwa meskipun telah diterapkan berbagai instrumen hukum pidana yang ada, penanggulangan kejahatan siber tetap menghadapi tantangan yang signifikan, karena kejahatan tersebut cenderung semakin kompleks, berkembang, dan beroperasi dengan berbagai motif. Oleh karena itu, upaya untuk mengubah atau membentuk regulasi baru yang berkaitan dengan kejahatan dunia maya merupakan bagian dari proses berkelanjutan dalam penyempurnaan formulasi hukum pidana. Dalam praktiknya, pelaku kejahatan siber tetap dapat ditangkap dan diproses oleh aparat penegak hukum berdasarkan ketentuan KUHPidana, khususnya pada pasal-pasal yang relevan. Namun, perkembangan bentuk dan modus kejahatan online yang semakin kompleks menyebabkan ketentuan dalam KUHPidana, seperti undang-undang khusus yang mengatur tindak pidana di bidang teknologi informasi dan transaksi elektronik. Melalui pengaturan tersebut, penanganan kejahatan siber dapat dilakukan secara lebih efektif dengan perkembangan teknologi (Irfani, 2020).

Oleh karena itu, dalam rangka penanggulangan kejahatan, penanggulangan terhadap pelaku kejahatan dimungkinkan dengan menggunakan perpaduan antara sarana hukum pidana dan non-pidana yang dapat dipadukan satu sama lain. Jika sistem peradilan pidana digerakkan, maka politik hukum pidana akan dijalankan, berupa diadakannya pemilihan untuk menghasilkan peraturan perundang-undangan pidana yang sesuai dengan kondisi dan situasi baik sekarang maupun yang akan datang. Upaya peningkatan kesejahteraan masyarakat (*social welfare*) antara lain meliputi upaya penanggulangan kejahatan melalui pembentukan

peraturan perundang-undangan pidana (Atmadja, 2021).

Dalam pengertian tersebut, kebijakan sosial mencakup setiap dan semua tindakan yang sengaja diambil untuk meningkatkan kesejahteraan sekelompok orang dan memastikan keselamatan mereka. Dengan demikian, kebijakan sosial juga mencakup perlindungan sosial dan program kesejahteraan sosial. Dari sudut pandang ini, cukup jelas bahwa pemecah masalah kebijakan hukum pidana tidak dapat ditemukan sendiri dalam penerapan prosedur peradilan yang normatif dan sistematis. Perspektif yuridis faktual, yang bersifat sosiologis, psikologis, historis, atau komparatif, bahkan pendekatan integratif dengan kebijakan sosial dan pembangunan nasional, semuanya diperlukan untuk kebijakan hukum pidana yang efektif.

Apabila kejahatan dunia maya dipandang sebagai bentuk kejahatan yang memiliki karakteristik berbeda dari tindak pidana konvensional, maka diperlukan pengaturan khusus di luar ketentuan KUPidana. Hal tersebut disebabkan oleh perkembangan teknologi informasi yang sangat cepat dan melahirkan berbagai bentuk kejahatan baru yang sulit dijangkau oleh pengaturan hukum pidana konvensional. Dengan demikian, kejahatan siber memerlukan regulasi yang mampu mengakomodasi karakteristik unik dari kejahatan berbasis teknologi digital. Namun demikian, sistem hukum di Indonesia yang dipengaruhi oleh tradisi hukum kontinental masih menempatkan KUHPidana sebagai dasar utama dalam hukum pidana. Oleh karena itu, pembentukan pengaturan mengenai kejahatan siber atau *cybercrime* sebaiknya dilakukan secara terpadu melalui pembaruan dan penyesuaian terhadap ketentuan KUHPidana, sehingga hukum pidana nasional dapat mengikuti perkembangan teknologi dan kebutuhan masyarakat di era digital.

2. Konsistensi dan Harmonisasi Pengaturan Tindak Pidana Siber dalam Undang-Undang ITE dalam Menjamin Kepastian Hukum

Pelaku kejahatan dunia maya pada dasarnya dapat ditangkap dan diproses oleh aparat penegak hukum berdasarkan ketentuan hukum yang berlaku. Dalam praktiknya, penegakan hukum terhadap kejahatan siber kerap menggunakan ketentuan dalam KUHPidana yang dinilai masih dapat mengakomodasi jenis tindak pidana tertentu, seperti penipuan atau pencemaran nama baik. Sebagai contoh, dalam kasus penipuan online, pelaku tetap dapat dijerat dengan pasal penipuan dalam KUHPidana, meskipun perbuatan tersebut dilakukan melalui media elektronik. Namun demikian, penegakan hukum pidana terhadap kejahatan siber di Indonesia merupakan tantangan yang kompleks dan memerlukan pendekatan yang komprehensif. Penanganannya tidak hanya melibatkan aparat penegak hukum, tetapi juga membutuhkan koordinasi antar lembaga serta kerja sama nasional. Dengan adanya pembaruan dalam UU ITE diharapkan penegakan hukum dapat menjadi lebih efektif dalam menghadapi dinamika kejahatan siber yang terus berkembang. Meski demikian, upaya tersebut perlu didukung oleh peningkatan kapasitas aparat penegak hukum, pembaruan regulasi, peningkatan kesadaran masyarakat, serta penguatan kerja sama nasional (Budhiyanto, 2014).

Penegakan hukum terhadap tindak pidana siber secara mutlak memerlukan pemanfaatan sarana atau alat, mengingat karakteristik kejahatan ini dilakukan melalui media teknologi, baik yang berwujud *hardware* maupun tidak berwujud atau *software*. Penentuan waktu dan tempat terjadinya kejahatan siber tidak selalu dapat dilihat secara fisik, melainkan ditentukan berdasarkan kapan dan dimana sistem atau alat tersebut beroperasi secara efektif. Pengaruh perkembangan kejahatan siber terhadap penegakan hukum pidana terdiri dari beberapa faktor, di antaranya :

a. Faktor Pengaturan Hukum

Faktor pertama yang memengaruhi penegakan hukum adalah faktor peraturan

perundang-undangan. Undang-undang menjadi dasar utama dalam menjunjung terlaksananya penegakan hukum yang efektif. Yang dimaksud dengan undang-undang dalam arti materiil adalah peraturan tertulis yang berlaku umum serta dibentuk oleh penguasa pusat maupun daerah yang berwenang. Dengan demikian, undang-undang mencakup peraturan yang berlaku secara nasional maupun yang hanya berlaku pada wilayah atau kelompok tertentu (Soekanto, 2008).

Dengan demikian, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jadi instrumen hukum yang penting. Undang-undang tersebut secara tegas mengatur berbagai larangan terkait tindak pidana di bidang teknologi informasi, termasuk judi lewat media elektronik. Aturannya ada di Pasal 27 ayat (2) *jo* Pasal 45, yang memberikan sanksi pidana bagi pelaku. Secara umum, pengaturan ini diharapkan mampu memberikan efek jera serta mendukung upaya penegakan hukum terhadap kejahatan siber di Indonesia.

b. Faktor Penegak Hukum

Faktor lain yang memengaruhi penegakan hukum adalah aparat penegak hukum itu sendiri. Aparat penegak hukum meliputi hakim, jaksa, kepolisian, advokat, dan petugas pemasyarakatan. Mereka bekerja langsung dalam proses penegakan hukum untuk memastikan hukum dapat diterapkan secara efektif dan adil. Seorang penegak hukum pada dasarnya memiliki berbagai kedudukan dan peranan sebagaimana anggota masyarakat lainnya. Kondisi tersebut memungkinkan terjadinya konflik, baik konflik kedudukan (*status conflict*) maupun konflik peranan (*conflict of roles*). Selain itu, dalam praktik seringkali terjadi kesenjangan antara peranan yang seharusnya dijalankan (*ideal role*) dengan peranan yang benar-benar dilaksanakan (*actual role*). Kesenjangan ini dikenal sebagai *role distance*, yang dapat memengaruhi efektivitas penegakan hukum di masyarakat.

c. Faktor Masyarakat

Partisipasi masyarakat memperkuat penegakan hukum. Penegakan hukum bergantung pada kesadaran hukum masyarakat. Kesadaran hukum masyarakat yang tinggi membuka peluang penegakan hukum yang baik. Kesadaran hukum masyarakat yang rendah menghambat penegakan hukum yang optimal. Penanganan tindak pidana siber juga memerlukan peran aktif masyarakat. Peran aktif masyarakat terlihat dalam pelaporan dan pemberian informasi. Di lapangan, masyarakat menghadapi beberapa masalah. Banyak orang takut menjadi saksi, meskipun ada aturan perlindungan saksi dan korban. Selain itu, masyarakat kurang mengerti hukum, sehingga proses penegakan hukum terhambat. Oleh karena itu, harus ada upaya meningkatkan kesadaran hukum dan memberi edukasi hukum kepada masyarakat. Edukasi hukum penting agar penegakan hukum lebih efektif, terutama dalam melawan kejahatan siber.

Dalam perspektif hukum positif, ketidakharmonisan UU ITE dengan regulasi lain semakin tampak ketika dikonfrontasikan dengan ketentuan dalam Undang-Undang No. 1 Tahun 2023 tentang KUHPidana. KUHPidana baru memuat sejumlah delik yang secara substansial serupa dengan ketentuan dalam UU ITE, namun dengan formulasi dan ancaman pidana yang berbeda, sehingga menciptakan potensi disharmoni regulasi yang membingungkan baik penegak hukum maupun masyarakat. Tentang tindak pidana penipuan online juga mengungkap bahwa dalam praktiknya, aparat penegak hukum kerap mengalami kebingungan dalam memilih landasan hukum yang tepat antara KUHPidana dan UU ITE untuk

menjerat pelaku kejahatan siber. Kondisi ini mempertegas urgensi harmonisasi menyeluruh antara kedua instrumen hukum guna menghindari inkonsistensi penuntutan dan disparitas putusan yang dapat merusak kepercayaan publik terhadap sistem peradilan pidana (Audina, 2026).

Upaya mewujudkan kepastian hukum dalam penegakan tindak pidana siber juga dipengaruhi oleh kapasitas kelembagaan penegak hukum itu sendiri. Menemukan bahwa meskipun UU No. 27 Tahun 2022 atau UU PDP telah mengatur sanksi pidana, efektivitasnya masih sangat rendah akibat ketidakjelasan unsur-unsur delik, disharmoni atarperaturan, serta minimnya kapasitas aparat penegak hukum dalam bidang forensik digital. Temuan ini selaras dengan hasil penelitian yang mengidentifikasi bahwa jaksa sebagai dominus litis dalam penuntutan perkara ITE masih menghadapi hambatan serius berupa keterbatasan SDM yang menguasai cyber law serta tantangan teknis dalam pengumpulan dan pembuktian bukti elektronik. Dengan demikian, pencapaian kepastian hukum tidak semata bergantung pada kualitas norma undang-undang, melainkan juga pada penguatan kapasitas kelembagaan dan harmonisasi regulasi secara menyeluruh.

Ketidakpastian hukum dalam penegakan tindak pidana siber juga tampak dari lemahnya sinergi antara UU ITE dengan regulasi perlindungan data pribadi sebagai instrumen hukum yang saling berkaitan. UU PDP telah mengatur sanksi pidana bagi pelaku pelanggaran data, namun belum terdapat koordinasi normatif yang jelas antara UU PDP dan UU ITE dalam konteks penanganan tindak pidana siber yang berkaitan dengan pencurian atau penyalahgunaan data pribadi secara elektronik. Kebutuhan untuk mengatasi masalah kebocoran data menjadi fokus utama yang harus segera diselesaikan, mengingat kasus-kasus kebocoran data di Indonesia terus meningkat dan menimbulkan kerugian yang sangat signifikan bagi masyarakat.

Aspek pembuktian dalam perkara tindak pidana siber merupakan salah satu dimensi yang paling kritis dalam konteks kepastian hukum. Meskipun Pasal 5 UU ITE telah menegaskan kedudukan informasi elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah, persoalan teknis terkait keabsahan, keutuhan, an chain of custody bukti digital dalam proses peradilan masih menjadi titik lemah yang belum sepenuhnya teratasi menegaskan bahwa jaksa sebagai penuntut umum dalam perkara ITE masih menghadapi tantangan serius dalam pengumpulan dan pembuktian bukti elektronik, yang berpengaruh pada kualitas dakwaan dan keberhasilan penuntutan di persidangan. Kondisi ini diperparah oleh minimnya standar prosedur operasional yang baku dalam penanganan barang bukti digital, sehingga tidak jarang ditemukan putusan pengadilan yang tidak konsisten dalam menilai keabsahan alat bukti elektronik yang diajukan penuntut umum.

KESIMPULAN

Penegakan hukum terhadap kejahatan siber di Indonesia telah memiliki landasan hukum yang cukup memadai melalui Undang-Undang ITE serta didukung oleh ketentuan dalam KUHP. Namun, dalam pelaksanaannya, penegakan hukum masih menghadapi berbagai tantangan, baik dari segi substansi hukum, aparat penegak hukum maupun faktor-faktor masyarakat. Di samping itu, evolusi kejahatan siber yang semakin rumit menuntut adanya pendekatan yang lebih menyeluruh dan responsif terhadap kemajuan teknologi. Di sisi lain, masih ada ketidakharmonisan antara UU ITE dengan peraturan lain, seperti KUHPidana dan Undang-Undang Pelindungan Data Pribadi, yang berpotensi menimbulkan kepastian hukum. Oleh karena itu, diperlukan harmonisasi regulasi peningkatan kapasitas aparat penegak hukum, serta peningkatan kesadaran hukum masyarakat agar

penegakan hukum terhadap tindak pidana siber dapat berjalan efektif dan mampu memberikan kepastian hukum di Indonesia.

DAFTAR REFERENSI

- Arif, B. N. (2007). *Tindak pidana mayantara: Perkembangan kajian cyber crime di Indonesia*. Rajagrafindo Persada.
- Atmadja, I. D. G. (2021). Legal ideology on social justice perspective. *Journal of Equity of Law and Governance*, 1(2), 158–163.
- Audina, W. (2026). Kajian yuridis normatif terhadap pengaturan tindak pidana siber dalam Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(2), 7374–7386.
- Budhiyanto. (2014). *Teori hukum konvergensi*. Refika Aditama.
- Dermawan, A., Saputra, E., & Hutagalung, J. E. (2021). Peran masyarakat dalam menaati hukum dan mendukung perkembangan teknologi komputer dalam bisnis digital. *Community Development Journal: Jurnal Pengabdian Masyarakat*, 2(3), 569–573.
- Herlindah, & Darmawan, Y. (2022). Development legal theory and progressive legal theory: A review in Indonesia's contemporary legal reform. *Peradaban Journal of Law and Society*, 1(1), 20–30.
- Dasco, S. (2022). Cybercrime in the context of criminal defamation in Indonesia. *Webology*, 19(2), 803–813.
- Gorde, F. (2022). Beyond cybercrime: New perspective on crime, harm and digital technologies. *International Journal for Crime, Justice and Social Democracy*, 11(1), 1–8.
- Hiariej, E. O. S. (2016). *Prinsip-prinsip hukum pidana*. Cahaya Atma Pustaka.
- Irfani, N. (2020). Asas *lex superior, lex specialis*, dan *lex posterior*: Pemaknaan, problematika, dan penggunaannya dalam penalaran dan argumentasi hukum. *Jurnal Legislasi Indonesia*, 17(3), 307–316.
- Muhammad, A. (2004). *Hukum dan penelitian hukum*. Citra Aditya Bakti.
- Munir. (2024). Kajian Pasal 27A UU No. 1 Tahun 2024 tentang perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Fundamental: Jurnal Ilmiah Hukum*, 13(2), 1–12.
- Nazran, F., & Siregar, F. Y. D. (2022). Realizing people's welfare in economic globalization: Perspective of the law on information and electronic transactions. *Veteran Law Review*, 5(1), 1–14.
- Rommelink, J. (2014). *Pengantar hukum pidana material: Prolegomena dan uraian tentang teori, ajaran dasar*. Maharsa.
- Shidarta. (2022). *Multisentrisme humaniora digital: Filsafat hukum masa depan dan masa depan filsafat hukum*. Binus University.
- Soekanto, S. (2008). *Faktor-faktor yang mempengaruhi penegakan hukum*. Rajawali Pers.
- Widayanti, P. W. (2022). Tindak pidana pencurian data nasabah dalam bidang perbankan sebagai cyber crime. *Legacy: Jurnal Hukum dan Perundang-Undangan*, 2(2), 1–21.
- Widhiyanti, H. N. (2020). The urgency of harmonizing competition laws in moving towards the ASEAN Free Trade Area. *Fiat Justisia: Jurnal Ilmu Hukum*, 14(1), 45–68.
- Widodo, D. P. (2019). Pancasila di era paska ideologi. *Veritas et Justitia*, 5(1), 1–9.
- Yudustira, M., & Ramadani, R. (2023). Tinjauan yuridis terhadap efektivitas penanganan kejahatan siber terkait pencurian data pribadi menurut Undang-Undang Nomor 27 Tahun 2022 oleh KOMINFO. *UNES Law Review*, 5(4), 3917–3929.

Zhafira, I., Ismansyah, & Yoserwan. (2023). Tinjauan yuridis tindak pidana pencemaran nama baik dalam Kitab Undang-Undang Hukum Pidana dikaitkan dengan Pasal 27 ayat (3) Undang-Undang Informasi dan Transaksi Elektronik (Studi Putusan Nomor 1909 K/Pid.Sus/2021). *UNES Journal of Swara Justicia*, 7(3), 901–912.