Copyright © The Author(s) 2025
Bayt Al Hikmah Vol 1 No 1, Juni 2025

Kejahatan Dunia Maya (Cybercrime) dalam Prespektif Hukum Islam dan Hukum Positif Masyarakat di Indonesia

A. Muh Fauzan [1*], Jusri Mudjrimin [2], Sulfikar [3]

[1] Universitas Islam Ahmad Dahlan Sinjai, Indonesia, email: Ujangfauzan67@gmail.com
[2] Universitas Islam Ahmad Dahlan Sinjai, Indonesia, email: jusri.mudjrimin@gmail.com
[3] Universitas Islam Ahmad Dahlan Sinjai, Indonesia, email: sulfikar@gmail.com

Abstract

Urgensi penelitian ini terletak pada kebutuhan mendesak akan pemahaman yang komprehensif dan integratif mengenai bagaimana kedua sistem hukum tersebut merespons dan mengatur kejahatan dunia maya. Penelitian ini bertujuan untuk menganalisis kejahatan dunia maya (cybercrime) dalam prespektif hukum islam dan hukum positif masyarakat di Indonesia. Penelitian ini menggunakan metode normatif dan kualitatif dengan pendekatan yang berfokus pada pencarian kaidah hukum, asas hukum, serta doktrin hukum guna menjawab berbagai pertanyaan terkait hukum. Analisis data dengan mengkaji Pustaka berupa peraturan perundangundangan terkait, pelacakan buku-buku dan jurnal-jurnal di internet yang berisi konsep substansial yang terakait permasalahan kejahatan dunia maya (cybercrime). Penelitian ini menunjukkan bahwa kejahatan dunia maya merupakan tantangan hukum yang kompleks dan membutuhkan penanganan yang komprehensif dari berbagai perspektif, termasuk hukum positif Indonesia dan hukum Islam. Dalam hukum positif Indonesia, pengaturan mengenai cybercrime telah diatur dalam berbagai peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik namun dalam implementasinya masih menghadapi sejumlah kendala, baik dari aspek penegakan hukum maupun pemahaman masyarakat terhadap norma hukum tersebut. Sementara itu, dalam perspektif hukum Islam, cybercrime dipandang sebagai perbuatan yang merusak tatanan sosial dan melanggar prinsip-prinsip moral serta etika Islam, seperti larangan melakukan penipuan, pencurian, perusakan, dan penyebaran fitnah atau berita palsu. Meskipun tidak secara eksplisit membahas kejahatan berbasis digital, prinsip-prinsip dalam hukum Islam bersifat universal dan dapat diadaptasi untuk merespons perkembangan zaman, termasuk kejahatan siber. Kajian ini menjadi dasar penting untuk pengembangan kebijakan hukum yang tidak hanya legal-formal, tetapi juga berlandaskan pada nilai-nilai keadilan substansial.

Keywords: *Kejahatan Dunia Maya, Cybercrime, Prespektif, Hukum Islam, Hukum Positif, Masyarakat Indonesia*

Pendahuluan

Kemajuan masyarakat saat ini semakin dipacu oleh perkembangan teknologi telekomunikasi, globalisasi hubungan antarbangsa, dan kemunculan tatanan dunia baru. Tidak dapat disangkal, masyarakat Indonesia yang tengah berkembang di era reformasi dihadapkan pada berbagai krisis di bidang politik, ekonomi, dan sosial budaya yang memengaruhi perkembangan bangsa (Ariyaningsih et al 2023). Oleh karena itu, upaya mengatasi berbagai tantangan tersebut menjadi suatu keharusan untuk memastikan eksistensi Indonesia di tengah persaingan global. Pesatnya perkembangan teknologi

https://doi.org/10.30605/BaytAl-Hikmah.414

informasi dan komunikasi telah. Membawa transformasi signifikan, dengan kehadiran teknologi ini dalam perangkat seluler. Aktivitas yang sebelumnya hanya dilakukan di dunia nyata kini banyak beralih ke dunia digital melalui perangkat seperti ponsel pintar, tablet, dan laptop. Contohnya adalah penggunaan aplikasi media sosial seperti Facebook, Twitter, Instagram, serta aplikasi pesan instan seperti WhatsApp, Line, dan WeChat yang menjadi alat komunikasi utama (Djanggih & Qamar, 2018).

Media sosial memungkinkan siapa saja untuk berpartisipasi, memberikan umpan balik secara terbuka, berbagi informasi, dan berkomentar secara cepat tanpa batasan waktu maupun tempat. Dampak media sosial terhadap kehidupan seseorang sangat besar. Seseorang yang sebelumnya memiliki penghasilan kecil dapat memperoleh peluang baru melalui media sosial, meskipun ada juga yang menghadapi tantangan baru karenanya. Media sosial didefinisikan sebagai platform daring yang memungkinkan pengguna untuk berpartisipasi, berbagi, dan menciptakan konten, termasuk blog, jejaring sosial, wiki, forum, serta dunia virtual (Fauziah et al., 2024). Bentuk media sosial yang populer di kalangan masyarakat dunia seperti Facebook, Instagram, X (Twitter), dan YouTube telah merambah ke berbagai kalangan usia. Kaplan dan Haenlein mendefinisikan media sosial sebagai kelompok aplikasi berbasis teknologi Web 2.0 yang memungkinkan penciptaan dan pertukaran konten yang dihasilkan pengguna. Kini, akses informasi dari berbagai penjuru dunia menjadi jauh lebih mudah, didukung oleh teknologi informasi dan komunikasi yang canggih serta keberadaan banyak hotspot gratis di berbagai tempat strategis (Habibi & Liviani, 2020).

Melihat sisi positif dari dunia maya, sedang terbentuk tren perkembangan teknologi di dunia yang memanfaatkan seluruh kreativitas manusia. Meski begitu, kehadiran Internet saat ini semakin memudahkan dalam mengakses dan menerima informasi dan berkomunikasi melalui media sosial serta jejaring sosial tanpa perlu melakukan pertemuan langsung. Pesatnya perkembangan teknologi membawa berbagai permasalahan akibat penyalahgunaan teknologi informasi (Juita et al., 2018). Sementara itu, penggunaan Internet yang hampir tidak terkendali telah mengakibatkan kejahatan berbeda terjadi di dunia maya, dan jumlah kejahatan online, yang juga dikenal sebagai kejahatan dunia maya, kini menjadi tren yang muncul di banyak negara, termasuk Indonesia. Sebagai jaringan global yang kompleks, internet terdiri dari berbagai protokol, aplikasi, router, dan gateway yang bersama-sama membentuk layanan internet itu sendiri (Mokobombang et al., 2023).

Perkembangan pesat teknologi informasi dan komunikasi turut diiringi dengan semakin meluasnya penyalahgunaan teknologi tersebut, yang memunculkan permasalahan kejahatan dunia maya atau "*cybercrime*." Di Indonesia, upaya untuk menanggulangi *cybercrime* diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Secara kriminologis, cybercrime dalam pandangan Islam pada dasarnya merupakan bentuk kejahatan yang muncul dari dinamika masyarakat dan menjadi fenomena umum (Nugraha et al., 2022). Perkembangan pesat teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, mulai dari cara berkomunikasi, bertransaksi, hingga mengakses informasi. Namun, di balik berbagai manfaat yang ditawarkan, kemajuan teknologi ini juga membuka ruang bagi penyalahgunaan yang semakin meluas.

Salah satu dampak negatif yang paling menonjol adalah munculnya berbagai bentuk kejahatan dunia maya atau yang dikenal dengan istilah *cybercrime*. Kejahatan ini mencakup

berbagai tindakan ilegal yang dilakukan melalui jaringan komputer atau internet, seperti pencurian data, penipuan daring, penyebaran konten ilegal, hingga peretasan system (Yurita et al., 2023). Pemerintah merespons fenomena tersebut dengan merumuskan regulasi khusus, yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini menjadi landasan hukum utama dalam upaya penanggulangan cybercrime dan telah mengalami beberapa kali revisi untuk menyesuaikan dengan perkembangan teknologi serta kebutuhan hukum di masyarakat. UU ITE tidak hanya menetapkan ketentuan pidana terhadap pelanggaran-pelanggaran di dunia maya, tetapi juga memberikan kerangka kerja hukum dalam penyelenggaraan transaksi elektronik secara aman, sah, dan bertanggung jawab (Suharyadi et al., 2020).

Cybercrime dipandang sebagai bentuk kejahatan modern yang berakar pada dinamika sosial masyarakat kontemporer. Cybercrime merupakan bentuk kejahatan yang tidak terlepas dari perubahan perilaku sosial sebagai dampak dari globalisasi teknologi (Fitri & Yusi, 2024). Islam memandang kejahatan termasuk kejahatan digital sebagai pelanggaran terhadap norma-norma syariah yang mengganggu kemaslahatan umum dan merusak nilai keadilan. Oleh karena itu, dalam hukum Islam, kejahatan siber dikategorikan sebagai bentuk kejahatan yang harus ditindak secara serius, karena berpotensi besar merugikan individu maupun masyarakat secara luas. Fenomena cybercrime dalam konteks masyarakat modern telah menjadi tantangan besar bagi sistem hukum yang ada, baik hukum positif maupun hukum Islam. Kejahatan ini sering kali sulit dideteksi dan dibuktikan, serta melibatkan pelaku lintas negara yang mempersulit proses penegakan hukum. Oleh karena itu, selain pendekatan hukum positif yang bersifat normatif, diperlukan juga pendekatan moral dan etika keagamaan sebagai fondasi dalam membentuk kesadaran masyarakat terhadap bahaya serta dampak dari penyalahgunaan teknologi (Bego et al., 2025).

Banyak upaya telah dilakukan untuk menyelesaikan masalah kemanusiaan dan sosial tertua ini dengan berbagai cara. Upaya penanggulangan kejahatan sebenarnya merupakan upaya berkelanjutan yang terus menerus terjadi tanpa adanya upaya yang pasti. Implikasinya adalah tidak ada sistem pencegahan kejahatan yang dapat menjamin secara pasti bahwa kejahatan tidak akan terjadilagi atau tidak akan memunculkan bentuk kejahatan baru (Mulasari, 2012). Oleh karena itu, diperlukan upaya berkelanjutan untuk memastikan perlindungan dan kesejahteraan masyarakat secara lebih efektif. Upaya ini menjadi bagian dari sistem sosial yang dianggap lebih efisien dalam menangani permasalahan sosial terkait kejahatan di masyarakat. Perubahan sosial sering kali memengaruhi jenis dan bentuk kejahatan yang muncul, seiring dengan dinamika perkembangan sosial itu sendiri (Gunawan, 2020)). seiring berkembangnya masyarakat, hukum-hukum masyarakat juga harus berubah.

Pembahasan antara pembangunan hukum dan pembangunan sosial yang saling berkaitan dengan Islam sehingga dapat menjadi titik awal pengembangan pencegahan kejahatan dalam pembangunan sosial (Hamzani, 2022). Kejahatan ini memerlukan penyelidikan dan penyidikan khusus yang melibatkan semua pihak dan pihak berwenang (Ramadani et al., 2025). Penelitian ini bertujuan untuk menganalisis fenomena kejahatan dunia maya (cybercrime) dalam perspektif hukum Islam dan hukum positif yang berlaku di Indonesia. Dalam konteks perkembangan teknologi informasi yang begitu pesat, kejahatan digital telah menjadi isu serius yang mengancam keamanan, privasi, dan

ketertiban sosial. Oleh karena itu, perlu adanya kajian yang mendalam untuk memahami bagaimana sistem hukum di Indonesia merespons persoalan ini, baik melalui perangkat perundang-undangan nasional maupun melalui pendekatan nilai-nilai hukum Islam yang hidup di tengah masyarakat.

Kebaruan dalam penelitian ini dengan menyandingkan dua pendekatan hukum yakni hukum positif Indonesia dan hukum Islam dalam memahami dan menganalisis kejahatan dunia maya. Penelitian ini tidak hanya menyoroti aspek yuridis dari cybercrime, tetapi juga menggali dimensi moral dan etika agama sebagai dasar penguatan kesadaran hukum di masyarakat. Melalui integrasi ini diharapkan lahir suatu pendekatan yang lebih komprehensif dan kontekstual dalam menanggulangi kejahatan digital di era modern.

Metode

Penelitian ini termasuk dalam jenis penelitian hukum normatif yang bersifat kualitatif. Pendekatan normatif digunakan untuk menelaah berbagai peraturan perundang-undangan, prinsip-prinsip hukum, serta putusan pengadilan yang berkaitan dengan kejahatan siber (*cybercrime*). Tujuannya adalah untuk memahami dasar hukum dan interpretasi yang digunakan dalam menangani kasus-kasus *cybercrime* di Indonesia. Di sisi lain, pendekatan kualitatif diterapkan untuk menganalisis dampak sosial serta praktik penegakan hukum di lapangan. Kombinasi dua pendekatan ini memungkinkan peneliti mendapatkan gambaran yang utuh, baik dari sisi teoritis maupun empiris.

Metode pengumpulan data dalam penelitian ini dilakukan melalui dua teknik utama, yaitu studi kepustakaan (*library research*) dan studi lapangan (*field research*). Studi kepustakaan mencakup analisis terhadap berbagai peraturan seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008 beserta perubahannya, serta dokumen hukum lainnya. Selain itu, kajian literatur dari buku, jurnal, dan artikel ilmiah yang membahas *cybercrime*, hukum Islam (*fiqh jinayah*), dan hukum pidana Indonesia turut digunakan untuk memperkaya perspektif teoritis. Dokumen resmi dari lembaga penegak hukum di Kabupaten Bone, seperti Kepolisian, Kejaksaan, dan Pengadilan, juga menjadi sumber data penting dalam penelitian ini.

Sementara itu, studi lapangan dilakukan melalui wawancara semi-terstruktur dengan berbagai narasumber. Para informan mencakup aparat penegak hukum dari Polres Bone dan Kejaksaan Negeri Bone, akademisi dari Universitas Islam Ahmad Dahlan Sinjai (UIAD), serta tokoh agama atau ulama yang memahami hukum Islam, khususnya dalam konteks kejahatan digital. Observasi langsung terhadap beberapa kasus cybercrime yang telah ditangani di wilayah Kabupaten Bone juga dilakukan untuk memperoleh pemahaman yang lebih mendalam mengenai dinamika penanganan kasus tersebut di tingkat lokal.

Lokasi penelitian ini dipusatkan di Kabupaten Bone, Sulawesi Selatan. Wilayah ini dipilih karena memiliki tingkat kasus kejahatan digital yang cukup tinggi, serta karakter masyarakat yang religius dan memiliki nilai budaya lokal yang kuat. Hal ini menjadikan Kabupaten Bone sebagai representasi menarik untuk mengkaji penerapan hukum positif dan nilai-nilai keadilan dalam konteks masyarakat yang beragam. Subjek penelitian mencakup pelaku kejahatan siber (jika memungkinkan untuk diwawancarai), korban, aparat penegak hukum seperti Polisi bagian *Cyber Crime* dan hakim di Pengadilan Negeri

Bone, serta akademisi dan praktisi hukum yang memahami aspek hukum baik secara normatif maupun empiris.

Teknik analisis data yang digunakan dalam penelitian ini bersifat kualitatif. Pertama, analisis isi (*content analysis*) digunakan untuk menelaah teks-teks hukum, putusan pengadilan, dan dokumen kebijakan yang relevan dengan kasus *cybercrime*. Kedua, dilakukan analisis komparatif antara konsep-konsep dalam hukum Islam seperti tazir dan maqasid syariah dengan hukum positif Indonesia yang diatur dalam UU ITE. Ketiga, untuk menjaga keabsahan data, dilakukan triangulasi data dengan membandingkan dan memverifikasi informasi dari wawancara, dokumen resmi, serta literatur ilmiah.

Instrumen yang digunakan dalam penelitian ini disusun untuk mendukung akurasi pengumpulan data. Di antaranya adalah pedoman wawancara terstruktur yang ditujukan bagi aparat penegak hukum dan korban cybercrime, kuesioner tertutup yang digunakan untuk mengukur tingkat pemahaman masyarakat terhadap UU ITE, serta daftar peraturan perundang-undangan yang menjadi rujukan utama dalam studi normatif ini. Dengan pendekatan dan metode yang menyeluruh ini, diharapkan hasil penelitian dapat memberikan kontribusi yang bermakna dalam pengembangan sistem hukum *cyber* di Indonesia, khususnya yang selaras dengan nilai-nilai lokal dan agama.

Hasil dan Pembahasan

Kejahatan Dunia Maya (*Cybercrime*)

Kejahatan dalam dunia maya biasa disebut juga sebagai *Cybercrime* yang secara umum diartikan sebagai aktivitas ilegal yang melibatkan penggunaan komputer, perangkat digital lainnya, atau jaringan komputer. Contoh dari kejahatan dalam dunia maya mencakup ancaman terhadap keamanan dunia maya seperti manipulasi sosial, eksploitasi kelemahan perangkat lunak, dan serangan terhadap jaringan. Jenis kejahatan ini sering kali menargetkan individu maupun perusahaan besar . Pelaku serangan biasanya menyasar organisasi untuk memperoleh keuntungan finansial secara langsung atau mengganggu kelancaran operasi bisnis. Mereka juga sering menipu individu dalam jumlah besar atau memanipulasi perangkat untuk dijadikan platform dalam menjalankan aktivitas berbahaya. *cybercrime* merujuk pada aktivitas kriminal yang dilakukan di dunia maya, dengan jaringan komputer sebagai alat dan internet sebagai medianya (Baiq, 2021).

Kejahatan dunia maya dalam arti luas merupakan aktivitas ilegal yang dilakukan melalui jaringan komputer atau internet untuk memperoleh keuntungan dengan merugikan pihak lain. Sementara itu, dalam pengertian yang lebih spesifik, cybercrime mengacu pada tindakan melanggar hukum yang ditujukan untuk menyerang sistem keamanan komputer serta data yang diolah oleh sistem tersebut. Seiring berjalannya waktu dan internet semakin mudah diakses, cara orang melakukan kejahatan dan cara mereka menyelidiki atau menganalisis masalah juga berubah. Perkembangan teknologi dan informasi di Indonesia perkembangan terus menunjukkan peningkatan dari tahun ke tahun. Jaringan internet tidak hanya membawa dampak positif, seperti menjadi sarana komunikasi bagi individu yang berjauhan, tetapi juga memberikan dampak negatif bagi penggunanya.

Dampak negatif antara lain kemungkinan terjadinya kecanduan perjudian di internet dan media sosial serta lupa akan kewajibannya, kemungkinan terjadinya penyebaran ujaran kebencian dan misinformasi kepada pengguna jaringan internet lainnya, serta

kemungkinan terjadinya kejahatan siber seperti carding dan phishing. Seharusnya Teknologi dan informasi bisa mencapai suatu hal positif jika kita sebagai masyarakat dan pengguna mampu menyikapinya serta memanfaatkannya secara bijak demi kebaikan bersama dan dengan tujuan yang positif. Namun, banyak pengguna teknologi, informasi, dan jaringan internet yang memanfaatkan hal ini secara tidak etis untuk memperoleh keuntungan dengan merugikan orang lain dan melanggar hukum.

Cybercrime atau biasa disebut dengan covert cybercrime disebut juga dengan cybercrime, yaitu merujuk pada kejahatan yang melibatkan jaringan komputer untuk melakukan sebuah tindakan jahat atau menjadi target kejahatan tersebut. Cybercrime dapat diartikan sebagai aktivitas yang dilakukan oleh individu, kelompok, atau entitas hukum yang menggunakan komputer sebagai alat untuk melakukan tindak kejahatan atau sebagai target dari kejahatan tersebut. Beberapa jenis kejahatan yang sering terjadi di dunia maya meliputi: akses ilegal atau tidak sah ke sistem dan layanan komputer adalah bentuk kejahatan yang dilakukan dengan meretas atau menyusup ke dalam jaringan komputer tanpa izin dari pemilik sistem tersebut. Konten ilegal mencakup penyebaran informasi atau data yang tidak benar, tidak etis, melanggar hukum, atau mengganggu ketertiban umum melalui internet, menjadi salah satu modus operandi dalam cybercrime ini. Pemalsuan data (*data forgery*) merupakan kejahatan dunia maya yang dilakukan dengan memalsukan dokumen penting yang disimpan secara digital. Modus ini biasanya menargetkan dokumen e-commerce untuk menipu korban agar menyerahkan data pribadi dan informasi kartu kredit mereka (Pansariadi & Soekorini, 2023).

Mata-mata dunia maya (*cyber espionage*) adalah kejahatan yang melibatkan penyusupan ke dalam sistem jaringan komputer target untuk memperoleh informasi rahasia atau sensitif. Sabotase dan pemerasan dunia maya (*cyber sabotage and extortion*) mencakup tindakan merusak, mengganggu, atau menghancurkan data, program komputer, atau sistem jaringan dengan cara seperti memasukkan virus, logic bomb, atau program berbahaya lainnya, sehingga sistem tidak dapat berfungsi normal kecuali dikendalikan oleh pelaku. Pelanggaran terhadap hak kekayaan intelektual melibatkan tindakan ilegal seperti meniru atau menduplikasi tampilan situs web milik orang lain tanpa izin, dengan tujuan merugikan pemilik asli. Pelanggaran privasi (*infringements of privacy*) adalah kejahatan yang menargetkan informasi pribadi yang disimpan dalam sistem komputerisasi. Kebocoran data ini, seperti nomor PIN ATM, dapat menyebabkan kerugian materiil dan immateriil bagi korban (Mustofa et al., 2022).

Sifat kejahatan cybercrime dapat dikategorikan sebagai berikut: Cybercrime sebagai tindakan criminal Cybercrime dalam kategori ini mengacu pada kejahatan yang dilakukan dengan menggunakan internet sebagai alat atau sarana untuk melakukan tindakan melawan hukum. Misalnya, pengiriman email anonim yang berisi iklan (spamming), yang dapat dianggap sebagai pelanggaran privasi dan dituntut secara hukum. Cybercrime sebagai kejahatan "abu-abu" Jenis kejahatan ini berada di wilayah "abu-abu," di mana motif aktivitasnya tidak selalu jelas sebagai kejahatan, sehingga sulit untuk menentukan apakah tindakan tersebut melanggar hukum. Contoh dari kategori ini adalah probing atau port scanning, yang merupakan aktivitas memantau sistem orang lain untuk mengumpulkan informasi sebanyak mungkin, yang sering kali disalahgunakan (Putri et al., 2024).

Kejahatan Dunia Maya dalam Prespektif Hukum Islam

Hukum Islam pemberlakuan pemidanaan atas tindak pidana yang merugikan telah disyariatkan. Hukuman ini bertujuan untuk memperbaiki perilaku manusia sekaligus memberikan solusi agar individu dapat menjauhi berbagai bentuk kemaksiatan. Selain itu, tujuan utama dari pemidanaan ini adalah mendorong umat untuk menjalankan perilaku yang sesuai dengan perintah Allah SWT sehingga dapat mengurangi tingkat kemaksiatan dan penyimpangan dalam masyarakat. *Cybercrime* adalah tindak pidana yang melanggar hukum dengan memanfaatkan peralatan komputer atau jaringan komputer tanpa izin, membobol atau mengubah atau tidak merubah (merusak) peralatan komputer yang digunakan, atau penggunaan media elektronik di Internet. Cybercrime dilihat dari perspektif hukum pidana Islam. Landasan utama dalam hukum Islam adalah teori Maqasid al-Syariah, yang menetapkan asas-asas penting sebagai pertimbangan utama untuk mencapai tujuan hukum. asas ini bertujuan untuk memenuhi kepentingan umat manusia, baik di dunia maupun di akhirat, melalui pemeliharaan lima kebutuhan dasar kehidupan manusia (*al-masalih al-khamsa*). Kebutuhan tersebut meliputi perlindungan terhadap agama (*hifz al-din*), jiwa (*hifz al-nafs*), garis keturunan atau kehormatan (hifz al-nasl), kekayaan (*hifz al-mal*), dan akal (*hifz al-aql*). Aktivitas kejahatan siber dipandang dapat mengancam kelima elemen dasar kehidupan manusia ini (Purba & Kholik, 2023).

Cybercrime merupakan kejahatan yang dilakukan dengan memanfaatkan komputer atau jaringan komputer secara ilegal dan melanggar hukum. Tindakan ini dapat mencakup penggunaan, akses, atau modifikasi fasilitas komputer tanpa izin, bahkan tanpa merusak sistem yang diakses. Selain itu, *cybercrime* juga mencakup aktivitas kejahatan yang menggunakan media elektronik dan internet, sehingga dikenal sebagai kejahatan dunia maya atau kejahatan berbasis komputer. Jenis kejahatan ini sering kali menargetkan sistem atau jaringan komputer, mencakup berbagai bentuk kejahatan baru yang memanfaatkan teknologi elektronik dan internet sebagai media utamanya. Hukuman bagi pelaku cybercrime menurut hukum Islam adalah tazir, melalui persidangan dengan putusan pengadilan yang dapat berupa pidana penjara, pengusiran, cambuk, hingga ancaman hukuman mati, tergantung besarnya kerugian yang ditimbulkan (Tanjung & Adriani, 2022).

Kejahatan Dunia Maya dalam Prespektif Hukum Positif Masyarakat di Indonesia

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur berbagai perbuatan yang dilarang dan dikategorikan sebagai tindak pidana cybercrime. Sebelum keberadaan UU ITE, tindak pidana cybercrime hanya dapat diancam hukuman berdasarkan ketentuan hukum yang bersifat umum, khususnya dalam Kitab Undang-Undang Hukum Pidana (KUHP). Namun, regulasi tersebut belum sepenuhnya mampu mengakomodasi kejahatan yang berkaitan dengan komputer, karena fokusnya masih terbatas pada aspek telekomunikasi secara umum. Dalam KUHP, tindak pidana cybercrime dapat didefinisikan secara luas sebagai setiap tindak pidana yang menggunakan sarana atau bantuan sistem elektronik. Kejahatan konvensional seperti pembunuhan atau perdagangan manusia, jika dilakukan dengan bantuan sistem elektronik, dapat digolongkan sebagai tindak pidana cyber dalam arti luas.

KUHP juga mengatur beberapa pasal yang relevan untuk menindak kejahatan cybercrime, antara lain: Pasal 362 KUHP: Mengatur kasus carding (penipuan kartu kredit). Pasal 378 KUHP: Mengatur tindak pidana penipuan, Pasal 335 KUHP: Digunakan untuk

kasus ancaman atau pemerasan melalui email, di mana pelaku memaksa korban melakukan tindakan tertentu Pasal 311 KUHP: Mengatur kasus pencemaran nama baik menggunakan media internet (Amzah et al., 2024). Peraturan dalam KUHP ini menjadi landasan hukum awal sebelum UU ITE hadir untuk memberikan pengaturan lebih khusus terhadap tindak pidana cybercrime. Meski masih terjadi perdebatan, namun dapat diartikan bahwa Indonesia merupakan suatu negara dengan mrmiliki kesenjangan digital yang signifikan. Kesenjangan digital ini dapat merauk pada perbedaan antara individu atau kelompok yang memiliki akses dan kemampuan menggunakan teknologi komunikasi dengan mereka yang tidak memilikinya. Ketimpangan standar pendidikan dan ekonomi di Indonesia turut berkontribusi pada ketidakmerataan akses terhadap teknologi komunikasi (Soediro, 2018). Kesenjangan ini, yang disebabkan oleh kurangnya akses terhadap informasi dan komunikasi, dapat diklasifikasikan ke dalam beberapa kategori. Salah satu kategori utama melibatkan akses yang lebih mudah bagi mereka yang berada dekat dengan Pusat Informasi Daerah. Meskipun kesenjangan digital masih menjadi tantangan, kejahatan dunia maya tetap marak terjadi di Indonesia. Salah satu kasus yang paling umum adalah peretasan kartu kredit yang dilakukan oleh peretas dengan motif jahat. Selain KUHP, cybercrime diatur dalam peraturan perUndang-undang Transaksi Elektornik Nomor 8 Tahun 2011 Sebagaimana telah di ubah menjadi Undang-undang Nomor 19 tahun 2016 (UU ITE) khususnya pada pasal 27 hingga dengan pasal 30 terkait perbuatan dilarang. Kemudian pada pasal 45 hingga dengan pasal 50 diatur terkait ketentuan Pidana (Hidayah, 2020).

Upaya penanggulangan kejahatan *cyber* di Indonesia dilakukan dengan mengoptimalkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam konteks pencegahan penyalahgunaan internet, keberadaan UU ini seharusnya tidak menjadi perdebatan karena pada dasarnya bertujuan melindungi masyarakat dari kerugian dan kerusakan moral yang dapat berdampak pada keberlangsungan hidup berbangsa dan bernegara. Pasal 5 ayat 1 dan 2 UU ITE menyatakan bahwa Dokumen Elektronik dan Informasi Elektronik dapat digunakan sebagai alat bukti yang sah. Selain itu, Pasal 44 UU ITE menjelaskan bahwa alat bukti yang dapat digunakan dalam penyidikan, penuntutan, dan pemeriksaan di pengadilan meliputi: Alat bukti sebagaimana diatur dalam ketentuan perundang-undangan lainnya dan Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dijelaskan dalam Pasal 1 angka 1 dan 4 serta Pasal 5 ayat (1), (2), dan (3). UU ITE juga memperkenalkan konsep alat bukti digital. Jika kejahatan tradisional meninggalkan bukti fisik yang berwujud, kejahatan di dunia komputer dan internet juga meninggalkan jejak digital. Proses kejahatan dalam dunia siber melibatkan aspek pendukung tertentu, seperti pertukaran atribut, yang dapat digunakan sebagai petunjuk dalam mengungkap tindakan kriminal (Laksana, 2025).

Kesimpulan

Penelitian ini menunjukkan bahwa kejahatan dunia maya (*cybercrime*) merupakan tantangan hukum yang kompleks dan membutuhkan penanganan yang komprehensif dari berbagai perspektif, termasuk hukum positif Indonesia dan hukum Islam. Dalam hukum positif Indonesia, pengaturan mengenai cybercrime telah diatur dalam berbagai peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun dalam implementasinya masih menghadapi sejumlah kendala, baik dari aspek

penegakan hukum maupun pemahaman masyarakat terhadap norma hukum tersebut. Sementara itu, dalam perspektif hukum Islam, *cybercrime* dipandang sebagai perbuatan yang merusak tatanan sosial dan melanggar prinsip-prinsip moral serta etika Islam, seperti larangan melakukan penipuan, pencurian, perusakan, dan penyebaran fitnah atau berita palsu. Meskipun tidak secara eksplisit membahas kejahatan berbasis digital, prinsip-prinsip dalam hukum Islam bersifat universal dan dapat diadaptasi untuk merespons perkembangan zaman, termasuk kejahatan siber. Oleh karena itu, diperlukan harmonisasi antara hukum positif dan hukum Islam dalam menangani *cybercrime* agar penegakan hukum dapat berjalan lebih efektif dan diterima secara sosial maupun spiritual oleh masyarakat Indonesia. Kajian ini menjadi dasar penting untuk pengembangan kebijakan hukum yang tidak hanya legal-formal, tetapi juga berlandaskan pada nilai-nilai keadilan substansial.

Namun demikian penelitian ini memiliki keterbatasan salah satunya adalah keterbatasan akses terhadap pelaku *cybercrime* dan kerahasiaan informasi kasus membuat penggalian data lapangan menjadi kurang optimal. Oleh karena itu, disarankan untuk penelitian selanjutnya agar Penelitian mendatang juga diharapkan dapat menggali lebih jauh pendekatan perbandingan hukum, serta mengintegrasikan perspektif teknologi dan keamanan siber agar solusi yang ditawarkan lebih adaptif terhadap perkembangan zaman.

Acknowledgment

-

Daftar Pustaka

Amzah, R. A., Fitri, L. E., & Lubis, P. (2024). Analisis Pengaruh Kualitas Layanan Dan Presepsi Cybercrime Terhadap Loyalitas Nasabah Pengguna E-Banking Pada Bank Syariah Indonesia Kota Jambi. Bertuah Jurnal Syariah dan Ekonomi Islam, 5(2), 229-238. https://doi.org/10.56633/jsie.v5i2.818

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: Jurnal Ilmu Hukum, 1(1), 1-11. https://doi.org/10.56457/jjih.v1i1.38

Baiq, P. A. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. DIKTUM, 149-165. https://doi.org/10.35905/diktum.v19i2.2463

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya (Desember 2024). Jurnal Kolaboratif Sains, 8(1), 506-511. https://doi.org/10.56338/jks.v8i1.6740

Djanggih, H., & Qamar, N. (2018). Penerapan teori-teori kriminologi dalam penanggulangan kejahatan siber (cyber crime). Pandecta Research Law Journal, 13(1), 10-23. https://doi.org/10.15294/pandecta.v13i1.14020

Fauziah, I. N. N., Saputri, S. A., & Herlambang, Y. T. (2024). Teknologi informasi: Dampak media sosial pada perubahan sosial masyarakat. Indo-MathEdu Intellectuals Journal, 5(1), 757-766. https://doi.org/10.54373/imeij.v5i1.645

Fitri, A., & Yusi, S. (2024). Kejahatan Dunia Maya (Cybercrime) Dalam Presfektif Hukum Islam Dan Hukum Positif Indonesia. Justici, 17(1), 11-19. https://doi.org/10.35449/justici.v17i1.773

Gunawan, H. (2020). Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah. Jurnal El-Qanuniy: Jurnal Ilmu-Ilmu Kesyariahan dan Pranata Sosial, 6(1), 96-110. https://doi.org/10.24952/el-qanuniy.v6i1.2473

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam, 23(2), 400-426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hidayah, I. R. (2020). Representasi Social Engineering Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall). Tibanndaru: Jurnal Ilmu Perpustakaan Dan Informasi, 4(1), 30-47. http://dx.doi.org/10.30742/tb.v4i1.905

Juita, S. R., Sihotang, A. P., & Ariyono, A. (2018). Cyber Bullying Pada Anak Dalam Perspektif Politik Hukum Pidana: Kajian Teoretis Tentang Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Diubah Dengan Undang-Undang No. 19 Tahun 2016. Jurnal Dinamika Sosial Budaya, 20(2), 134-147. https://doi.org/10.26623/jdsb.v20i2.1244

Laksana, T. G. (2025). Urgensi Pengaturan Kejahatan Dunia Maya Berkelanjutan EraSociety 5.0. Jurnal Pesona Indonesia, 2(2), 71-79. https://doi.org/10.71436/jpi.v2i2.45

Mokobombang, W., Syafaruddin, S., Syafaruddin, A. R. A., Khaeriyah, K., & Natsir, N. (2023). Dampak Perubahan Layanan Publik Yang Disebabkan Oleh Teknologi Dan Media Sosial. Journal of Business, Finance, and Economics (JBFE), 4(1), 348-359. https://doi.org/10.32585/jbfe.v4i1.4180

Mulasari, L. (2012). Kebijakan Formulasi Tentang Tindak Pidana Kesusilaan Di Dunia Maya Dalam Perspektif Hukum Islam. Masalah-Masalah Hukum, 41(1), 98-109. https://doi.org/10.14710/mmh.41.1.2012.98-109

Mustofa, M. B., Dwiandrini, E. L., Agustin, I., Esyarito, M. A., Anggraeni, M., & Wuryan, S. (2022). Media Massa Dan Cyber Crime Di Era Society 5.0. At-Tanzir: Jurnal Ilmiah Prodi Komunikasi Penyiaran Islam, 77-98. https://doi.org/10.47498/tanzir.v13i1.996

Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Al Romadhona, R. A. (2022). Cybercrime, Pancasila, and Society: Various Challenges in the Era of the Industrial Revolution 4.0. Indonesian Journal of Pancasila and Global Constitutionalism, 1(2), 307-390. https://doi.org/10.15294/ijpgc.v1i2.59802

Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. Binamulia Hukum, 12(2), 287-298. https://doi.org/10.37893/jbh.v12i2.605

Purba, I. A., & Kholik, J. A. (2023). Penggunaan Mobile Banking Dalam Pandangan Maqashid Syariah Serta Problematika Atas Kejahatan Cyber. Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam, 5(2), 178-188. https://doi.org/10.47435/asy-syarikah.v5i2.2035

Putri, E. H. A. D., Kasim, R., & Nurmala, L. D. (2024). Analisis Yuridis Terhadap Penegakan dan Pengaturan Hukum Kejahatan Dunia Maya (Cyebercrime) di Indonesia. ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 2(3), 102-111. https://doi.org/10.59246/aladalah.v2i3.865

Ramadani, E. W., Harahap, R. D. K. A., & Fibriani, R. (2025). Kejahatan Siber dengan Metode DDOS Attack terhadap Website dalam Perspektif Fiqih Jinayah. Jurnal Hukum Lex Generalis, 6(2). https://doi.org/10.56370/jhlg.v6i2.765

Soediro, S. (2018). Prinsip Keamanan, Privasi, Dan Etika Dalam Undang-Undang Informasi Dan Transaksi Elektronik Dalam Perspektif Hukum Islam. Kosmik Hukum, 18(2). 10.30595/kosmikhukum.v18i2.3439

Suharyadi, S., Sampara, S., & Ahmad, K. (2020). Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam. Journal of Lex Generalis (JLG), 1(5), 761-773. https://doi.org/10.52103/jlg.v1i5.199

Tanjung, I. U., & Adriani, E. N. (2022). Politik Hukum Terhadap Penanggulangan Kejahatan Dunia Maya. Judge: Jurnal Hukum, 3(01), 1-8. https://doi.org/10.54209/judge.v3i01.371

Yurita, I., Ramadhan, M. K., & Candra, M. (2023). Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (studi kasus phising sebagai ancaman keamanan digital). Jurnal Hukum Legalita, 5(2), 143-155. https://doi.org/10.47637/legalita.v5i2.995