DELICTUM: JURNAL HUKUM PIDANA DAN HUKUM PIDANA ISLAM

https://ejurnal.iainpare.ac.id/index.php/delictum/index

The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions

Alief Tanding Pamungkas[1], Andi Muliyono[2], Nurjana Lahangatubun[3]

[1] STIH Manokwari, Indonesia

[2] STIH Manokwari, Indonesia

[3] STIH Manokwari, Indonesia

eloksae@gmail.com

Article

Keywords:

Legal regulation; Cybercrime; Challenges

Pengaturan hukum; Tindak pidana cybercrime; Tantangan

Abstract

This research aims to explore the regulation of cybercrime in Indonesia, analyze the problems that arise, and offer solutions that can be implemented to improve law enforcement in this field. Using a qualitative descriptive method, this research collects, analyzes, and explains data related to cybercrime regulation in Indonesia. The results show that current legal arrangements still have some weaknesses, such as limited human resources, lack of supporting facilities, and limited budget. In addition, cybercrime is increasing and poses a serious threat to social stability and state sovereignty. This research suggests the need to increase the capacity of law enforcement through training and the provision of more sophisticated technology, greater budget allocations, and strengthening international cooperation to tackle cross-border crime. It is hoped that the results of this research can contribute to increasing the effectiveness of cybercrime law enforcement in Indonesia and strengthening efforts to prevent and tackle cybercrime.

Penelitian ini bertujuan untuk mengeksplorasi pengaturan tindak pidana cybercrime di Indonesia, menganalisis permasalahan yang muncul, serta menawarkan solusi yang dapat diimplementasikan untuk memperbaiki penegakan hukum di bidang ini. Dengan menggunakan metode deskriptif kualitatif, penelitian ini mengumpulkan, menganalisis, dan menjelaskan data terkait regulasi cybercrime di Indonesia. Hasil penelitian menunjukkan bahwa pengaturan hukum saat ini masih memiliki beberapa kelemahan, seperti keterbatasan sumber daya manusia, kurangnya fasilitas pendukung, dan keterbatasan anggaran. Selain itu, kejahatan cybercrime semakin meningkat dan menjadi ancaman serius bagi stabilitas sosial dan kedaulatan negara. Penelitian ini menyarankan perlunya peningkatan kapasitas penegak hukum melalui pelatihan dan penyediaan teknologi yang lebih canggih, alokasi anggaran yang lebih besar, serta penguatan kerjasama internasional untuk menanggulangi kejahatan lintas batas. Diharapkan, hasil penelitian ini dapat berkontribusi pada peningkatan efektivitas penegakan hukum cybercrime di Indonesia serta memperkuat upaya pencegahan dan

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

penanggulangan kejahatan dunia maya.

PENDAHULUAN

Hukum dan perkembangan teknologi informasi merupakan dua aspek yang tidak terpisahkan dalam kehidupan modern. Kemajuan dalam peradaban, dalam berbagai aspek kehidupan manusia dipengaruhi oleh teknologi dan ilmu pengetahuan, termasuk bagaimana hukum harus menyesuaikan diri dengan perkembangan zaman. Kemunculan dunia digital adalah salah satu manifestasi dari Karena kemajuan dalam ilmu pengetahuan dan teknologi banyak bidang.(Andika, 2022)

Indonesia saat ini secara aktif menggunakan dan memanfaatkan teknologi informasi, yang ditunjukkan oleh tingginya adopsi internet. Penggunaan teknologi informasi sangat populer dalam gaya hidup dan hiburan, seperti mengakses media sosial, mengunduh musik, menonton film, mencari informasi tentang hobi, membaca cerita, serta mengakses berita olahraga. Selain itu, pemanfaatan teknologi informasi juga meliputi penggunaan mesin pencari, jejaring sosial, konektivitas smartphone dan internet mobile, serta perkembangan industri komputasi awan sebagai media penyimpanan data. Pertumbuhan Penyebaran cepat dari teknologi informasi dan komunikasi telah mengubah cara masyarakat berperilaku di seluruh dunia, serta menghasilkan perubahan sosial yang signifikan. Namun, meskipun memiliki banyak manfaat positif, pemanfaatan teknologi ini juga memiliki potensi dampak negatif yang perlu diwaspadai.(AYUNDA, 2023)

Penggunaan teknologi tanpa pengawasan yang memadai dapat dimanfaatkan untuk kegiatan yang merugikan pihak lain, yang menyebabkan munculnya hukum siber atau hukum telematika sebagai respons terhadap perkembangan ini. Hukum siber mencakup semua aspek hukum komunikasi dan teknologi informasi, sementara telematika adalah perpaduan dari hukum telekomunikasi, media, dan informatika. Berbagai masalah hukum umum terkait dengan komunikasi, pengiriman informasi dan transaksi digital. Penggunaan komputer dalam berbagai aktivitas manusia juga menimbulkan kemungkinan dampak negatif akibat kelalaian, ketidakmampuan, atau niat jahat. Oleh karena itu, perkembangan teknologi informasi memerlukan penyesuaian hukum lebih lanjut untuk memastikan penggunaan teknologi dalam batas hukum.(Handoyo et al., 2024)

Munculnya berbagai tindak pidana baru, termasuk cybercrime, merupakan tantangan bagi hukum dalam menghadapi perubahan sosial. Penggunaan teknologi sebagai sarana komunikasi global menawarkan peluang positif bagi kemajuan ilmu pengetahuan, namun juga menimbulkan tantangan ketika tidak diimbangi dengan kemampuan mengoperasikan teknologi dan pengaturan hukum yang memadai. Meskipun perkembangan teknologi telekomunikasi semakin maju, perkembangan ini

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

juga membawa dampak terhadap Masyarakat Indonesia yang sedang berkembang di era reformasi menghadapi banyak tantangan dalam bidang politik, ekonomi, dan sosial budaya.(Lestyaningrum et al., 2022)

Saat penyalahgunaan internet menjadi tidak terbatas, sehingga merupakan tindakan kriminal, dunia maya atau cybercrime dewasa ini muncul. Kejahatan komputer atau kejahatan maya biasanya dilakukan dengan pengetahuan teknologi komputer. Karena perkembangan teknologi komputer yang sangat cepat, hukum seringkali datang terlalu lambat untuk menangani kejahatan dunia maya. Jenis kejahatan internet ini mencakup skala internasional dan mencakup Indonesia.(Rizkita, 2023)

Jumlah kasus cybercrime yang meningkat di Indonesia telah mendorong pemerintah untuk membuat undang-undang yang kuat untuk menjerat pelaku cybercrime. Pemerintah Indonesia memasukkan UU Cybercrime (UU Siber) ke dalam Undang-Undang Nomor 19 Tahun 2016 dan Kode Hukum Pidana sebagai revisi dari UU ITE Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, penanggulangan tindak pidana cybercrime masih menghadapi kendala-kendala yang signifikan, seperti keterbatasan sumber daya manusia, fasilitas yang belum memadai, serta anggaran yang terbatas. Hal ini memerlukan perhatian lebih lanjut dari pemerintah demi kemajuan kinerja aparat penegak hukum.(Habibi & Liviani, 2020)

Penelitian ini penting untuk mengatasi keterbatasan dalam penegakan hukum terkait cybercrime. Diharapkan penelitian ini akan memberikan pemahaman baru dan solusi baru untuk menangani kejahatan dunia maya, serta memperkuat kerjasama internasional dalam penanggulangan cybercrime. Dengan demikian, penelitian ini tidak hanya berkontribusi pada pengembangan ilmu hukum, tetapi juga pada keamanan dan stabilitas masyarakat dalam era digital.

Adapun penelitian relevan tentang analisis pengaturan hukum tindak pidana cybercrime di Indonesia: tinjauan masalah dan solusi yaitu dari penelitian Arthur Simada dkk (2024) *Tindak Pidana Cybercrime (Mengganggu dan Mengrusak Sistem Elektronik dan Komunikasi Orang Lain)*, dan penelitian Muhammad Aulia Nasution dkk (2024) *Pengaturan Hukum Concursus terhadap Pelaku Tindak Pidana Cybercrime*.

Persamaan dari penelitian tersebut, yaitu Kedua artikel membahas tentang cybercrime, yaitu kejahatan yang dilakukan melalui teknologi informasi dan komunikasi. Perbedaan antara kedua penelitian tersebut adalah bahwa penelitian yang dilakukan oleh Arthur Simada lebih menyoroti dalam penentuan locus delicti (lokasi terjadinya kejahatan) dalam kasus cybercrime, dan penelitian selanjutnya Muhammad Aulia Nasution lebih mengarah kepada pengaturan pemidanaan terhadap cybercrime, khususnya dalam hal concursus (perbarengan tindak pidana), serta kebijakan hukum pidana terkait cybercrime di masa mendatang.

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

Tujuan dari artikel ini adalah untuk membahas tentang pengaturan hukum Indonesia untuk tindak pidana cybercrime, meninjau tantangan yang dihadapi, serta menawarkan penyelesaiannya. Berbeda dengan penelitian sebelumnya yang bersifat lebih teoretis, artikel ini menawarkan solusi yang lebih praktis dan konkret, antara lain melalui pengadaan teknologi forensik digital, pelatihan intensif bagi aparat penegak hukum, serta pentingnya kerjasama internasional dalam menangani kejahatan siber yang bersifat lintas batas. Artikel ini juga memberikan dimensi baru dalam pemahaman terhadap regulasi cybercrime di Indonesia, dengan melakukan analisis mendalam terkait hambatan internal di kalangan aparat penegak hukum, seperti kurangnya pelatihan, keterbatasan infrastruktur teknologi, serta tantangan operasional yang dihadapi.

Oleh sebab itu, artikel ini merumuskan beberapa rumusan permasalahan sebagai berikut; pertama, Bagaimana efektifitas pengaturan hukum yang ada saat menangani tindak pidana cybercrime di Indonesia? dan jenis kendala utama apa yang dihadapi dalam penegakan hukum tindak pidana cybercrime?

METODE

Studi ini menggunakan metode deskriptif kualitatif untuk mengumpulkan, menganalisis, dan menjelaskan data terkait pengaturan hukum cybercrime di Indonesia. Langkah-langkah penelitian meliputi pengumpulan data hukum dan teknologi informasi, analisis data untuk mengevaluasi efektivitas pengaturan hukum dan mengidentifikasi tantangan serta solusi dalam penegakan hukum cybercrime, serta penyusunan hasil analisis yang dijadikan dasar untuk menyimpulkan dan memberikan saran. Dengan metode ini, studi Ini diharapkan akan meningkatkan pemahaman tentang permasalahan cybercrime di Indonesia dan menghasilkan rekomendasi yang bermanfaat untuk meningkatkan penegakan hukum dalam menghadapi tantangan tersebut.

HASIL DAN PEMBAHASAN

Efektifitas Pengaturan Hukum yang Ada saat ini dalam Menanggulangi Tindak Pidana Cybercrime di Indonesia

Dalam hukum pidana Indonesia, istilah "tindak pidana" digunakan secara umum untuk merujuk pada perbuatan ilegal yang diancam dengan hukuman. Moeljatno juga menyatakan bahwa "tindak pidana" bisa disamakan dengan "perbuatan pidanaMoeljatno menyatakan bahwa tindak pidana adalah tindakan yang dilarang oleh hukum dan disertai dengan ancaman hukuman, sehingga ada hubungan yang erat antara larangan tersebut dan ancaman hukuman yang menyertainya.(Hamid, 2024)

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

Istilah "cyber" berasal dari "cybernetics", sebuah disiplin yang menggabungkan robotika, matematika, teknik listrik, dan psikologi, yang diperkenalkan oleh Norbert Wiener pada tahun 1948. Dalam konteks teknologi informasi, telekomunikasi, dan multimedia, "cybercrime" mengacu pada kejahatan yang terjadi di ruang maya (cyberspace). Cyberspace adalah lingkungan komunikasi berbasis komputer yang dikenal luas sebagai internet dalam rutinitas sehari-hari.(Prabowo et al., 2023)

Kemajuan teknologi komputer dan internet telah memberikan manfaat besar dalam berbagai aspek kehidupan manusia, termasuk keperluan rumah tangga. Kemajuan ini telah membuka cakrawala baru dalam komunikasi dan pertukaran informasi. Namun, di balik kemajuan ini, terdapat konsekuensi negatif, salah satunya adalah meningkatnya kejahatan cybercrime.(Sawitri, 2023)

Kejahatan cybercrime dianggap sebagai ancaman serius yang dapat mengganggu kehidupan masyarakat, kedaulatan bangsa, dan stabilitas negara. Seiring dengan kemajuan teknologi informasi yang tanpa batas, kejahatan ini telah menimbulkan dampak buruk yang dapat merugikan individu, lembaga, dan negara lainnya. Untuk mengatasi masalah ini, diperlukan kerja sama internasional melalui kesepakatan bantuan dan perjanjian ekstradisi. Upaya ini sejalan dengan prinsip-prinsip yang tercantum dalam Konvensi Palermo dan Deklarasi ASEAN.(Azzani et al., 2023)

Menurut Pasal 1 ayat (1) dari Informasi Elektronik, menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, adalah semua data elektronik tunggal atau kelompok, termasuk, tetapi tidak terbatas pada, teks, suara, gambar, peta, dan sebagainya, desain, foto, EDI, surel (email), telegram, teks telepon, faksimili, atau format sejenis lainnya.. Selain itu, informasi elektronik juga dapat terdiri dari karakter, tanda-tanda, angka, kode akses, simbol, atau perforasi dimasukkan ke dalam data elektronik.(Parulian & Putranto, 2022)

Manusia menggunakan media komputer dan internet sebagai alat atau sarana untuk memanfaatkan Informasi Elektronik dan Teknologi Informasi. Menurut Maskun, Jaringan yang menghubungkan komputer satu sama lain disebut internet. melalui serangkaian perangkat atau komputer yang dikenal sebagai router, yang mengintegrasikan berbagai jaringan menjadi satu entitas besar. Bagian-bagian dari internet ini mencakup berbagai jenis jaringan lokal (LAN), komputer mini, mainframe, superkomputer, bahkan hanya sebuah komputer personal (PC). Saat ini, berbagai aplikasi dapat dijalankan melalui internet, seperti Telnet atau akses remote, protokol transfer file FTP, email, berita, Gopher, Wais, dan WWW (World Wide Web).(Syafrizal, 2020)

Meskipun kemajuan Teknologi Informasi dan Elektronik melalui internet memberikan dampak yang menguntungkan bagi kesejahteraan manusia, namun juga menimbulkan konsekuensi negatif yang signifikan dengan munculnya berbagai jenis

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

kejahatan yang memanfaatkan teknologi canggih. Selanjutnya, kejahatan yang terkait jaringan telekomunikasi dapat dikategorikan sesuai dengan teknologi berbasis computer dengan cara operasinya.

Hukum bertujuan untuk mengakomodasi berbagai aktivitas masyarakat yang berkembang seiring dengan zaman. Menurut Sudarto, tujuan umum hukum adalah mencapai kesejahteraan masyarakat secara materiil dan spiritual, sehingga tindakan yang merugikan masyarakat dihindari. Kejahatan cybercrime termasuk dalam kategori kejahatan yang dapat menyebabkan kerugian bagi masyarakat, baik secara materiil maupun spiritual. Karena keterbatasan yurisdiksi hukum dan pengadilan di Indonesia, pelaku kejahatan cybersering sulit ditangkap. Kejahatan ini biasanya melibatkan pelaku dari negara lain, tetapi memiliki konsekuensi hukum di Indonesia. Tiga jenis yurisdiksi yang penting dalam hukum internasional adalah yurisdiksi pembuatan undang-undang, penegakan hukum, dan pengadilan.(Saputra et al., 2023)

Sejumlah negara di Asia telah lebih maju daripada Indonesia dalam pembentukan undang-undang terkait teknologi informasi. Contohnya, Malaysia memiliki The Computer Crime Act of 1997, Singapura dengan The Computer Misuse Act of 1998, dan India dengan The Information Technology Act of 1999. Negara-negara tersebut memiliki kebijakan pidana yang jelas dan tegas dalam menangani kejahatan cybercrime sebagai bagian dari politik kriminal.(Sommaliagustina et al., 2022)

Politik kriminal merupakan upaya untuk membuat peraturan yang sesuai dengan keadaan negara dan kebijakan saat ini dalam menetapkan regulasi yang mencerminkan nilai-nilai masyarakat dan mencapai tujuan yang diinginkan. Di samping itu, politik hukum pidana bertujuan untuk merancang undang-undang pidana yang bertindak baik untuk kepentingan saat ini maupun untuk kepentingan masa depan. Undang-undang yang dimaksudkan harus dapat beradaptasi dengan kemajuan teknologi dan mengantisipasi masalah, termasuk efek negatif dari penyalahgunaan Internet yang berpotensi merugikan korban baik secara materiil maupun non-materiil.

Peraturan hukum Indonesia telah mengatur beberapa ketentuan tentang tindak pidana yang terkait dengan kejahatan cybercrime dalam berbagai pasal hukum yang terpisah. Dalam KUHP belum sepenuhnya efektif dalam menangani kejahatan cyber crime karena belum secara menyeluruh mencakup unsur-unsur materiil kejahatan dunia maya. Dalam konteks pembuktian, KUHP mengikuti prinsip legalitas, yang menyatakan bahwa suatu perbuatan tidak dianggap pidana jika tidak diatur oleh undang-undang. Namun, Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman menyatakan bahwa, pengadilan harus memeriksa dan mengadili suatu perkara tanpa menolaknya karena ketidakjelasan hukum.(Sunaryo, n.d.)

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

Dalam menghadapi kejahatan cyber crime, dunia hukum telah mengadopsi praktik memperluas penafsiran asas dan norma hukum. Kejahatan tersebut pada dasarnya dapat dijerat berdasarkan KUHP dengan menggunakan analogi atau contoh dari beberapa pasal dalam KUHP, seperti Pasal 362 yang berkaitan dengan kasus carding, Pasal 378 yang berkaitan dengan penipuan, dan Pasal 311 yang berkaitan dengan pencemaran nama baik, dan lain-lain, dapat diterapkan dalam menangani berbagai jenis kejahatan cyber crime.(Setiawan et al., 2022)

Dengan demikian, Pasal-Pasal dalam KUHP masih dapat digunakan tanpa perlu adanya regulasi baru untuk menangani kejahatan melalui internet. Dalam hal ini, hakim dapat menggunakan interpretasi yang luas dari pasal-pasal KUHP yang relevan dengan kejahatan cyber crime tanpa menyebutkannya secara spesifik. Selain itu, penting bagi hakim untuk mengingat prinsip-prinsip hukum yang berlaku di masyarakat dan rasa keadilan.(Farah, 2021)

Dalam menangani tindak pidana cybercrime, Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menunjukkan beberapa masalah yang perlu diperhatikan. Meskipun Kitab Undang-Undang Hukum Pidana (KUHP) secara historis dianggap sebagai sumber hukum utama, namun seringkali tidak cukup untuk menindak kejahatan di dunia maya karena unsur-unsur kejahatan tersebut belum sepenuhnya tercakup. Dalam proses pembuktian, KUHP menerapkan prinsip legalitas, yang mengharuskan tindakan diatur dalam undang-undang sebelumnya untuk dianggap sebagai tindak pidana. Namun, Sesuai dengan Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman, setiap perkara yang diajukan harus diperiksa oleh pengadilan, bahkan jika hukumnya tidak jelas.(Jaelani, 2020)

Selain KUHP, serta beberapa undang-undang di luar dari KUHP juga mengatur tentang kejahatan teknologi informasi, namun belum memberikan jaminan kepastian hukum yang memadai dalam menangani tindak pidana siber. Dengan ruang siber yang tidak terbatas oleh batas negara, pelaku transaksi dan pihak lain yang tidak terlibat dalam transaksi dapat mengalami kerugian.

UU No. 19 Tahun 2016 bertujuan untuk untuk memastikan pengakuan terhadap hak dan kebebasan individu serta untuk memastikan keadilan dalam masyarakat demokratis. Meskipun merupakan langkah awal dalam pengaturan teknologi informasi dan transaksi elektronik, implementasinya menghadapi beberapa hambatan. Beberapa tantangan termasuk hasil pengujian materi di Mahkamah Konstitusi yang mengubah interpretasi hukum, kesulitan dalam penyidikan kejahatan teknologi informasi, dan sifat virtual ruang siber yang memungkinkan penyebaran konten ilegal dengan mudah.(Eryanto, 2023)

Pasal-pasal dalam Undang-Undang ITE, seperti Pasal 27 hingga Pasal 37, mengatur tindakan yang dilarang dan memberikan dasar hukum bagi penegakan hukum terkait dengan cyber crime. Pendekatan punitif dan pendekatan budaya

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

digunakan dalam menangani kasus-kasus tersebut, dengan upaya untuk meningkatkan kesadaran masyarakat dan aparat penegak hukum serta mengembangkan kode etik penggunaan teknologi internet yang baik. Pendekatan Ini diharapkan dapat mengurangi pelanggaran teknologi sebagai langkah pencegahan.(SUJUDI & Ariyanti, 2020)

Efektivitas pengaturan hukum yang saat ini digunakan dalam pengendalian kejahatan cybercrime di Indonesia masih menjadi perdebatan yang relevan dalam konteks perkembangan teknologi informasi.(Himawan et al., 2022)

1. Meskipun terdapat beberapa undang-undang yang mengawasi kejahatan di internet, seperti yang dilakukan oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), pengaturan ini masih belum sepenuhnya efektif dalam mengatasi semua bentuk kejahatan di dunia maya. Meskipun ITE memberikan dasar hukum untuk menindak kejahatan siber, namun perlu dilakukan penyesuaian lebih lanjut dengan perkembangan teknologi.
2. Kendala utama yang dihadapi dalam menanggulangi cybercrime adalah kesulitan dalam penegakan hukum karena sifat lintas batas dari kejahatan tersebut. Pelaku cybercrime sering kali menggunakan teknologi untuk menyamarkan identitas mereka atau beroperasi dari luar negeri, sehingga sulit untuk menentukan yurisdiksi yang tepat dan mengekstradisi pelaku kejahatan.
3. Meskipun terdapat upaya untuk memperkuat regulasi hukum terkait cybercrime, seperti amendemen Undang-Undang ITE, tetapi masih diperlukan kerjasama internasional yang lebih erat dalam pertukaran informasi dan bukti untuk mengungkap dan menindak pelaku kejahatan cybercrime secara efektif.
4. Masyarakat harus lebih menyadari bahaya dan konsekuensi mereka tindak pidana internet, pendidikan mengenai penggunaan teknologi informasi yang aman dan etis juga penting untuk mengurangi jumlah kasus cybercrime di masyarakat.
5. Evaluasi berkala terhadap pengaturan hukum yang ada perlu dilakukan untuk memastikan bahwa undang-undang tersebut tetap relevan dan efektif dalam mengatasi tantangan yang muncul bersamaan dengan kemajuan teknologi informasi. Dengan demikian, pengaturan hukum yang ada harus terus disesuaikan dengan dinamika cybercrime agar dapat memberikan perlindungan yang memadai bagi masyarakat dan pemerintah dalam menghadapi ancaman di dunia maya.

Tantangan utama dalam penegakan hukum tindak pidana cybercrime di Indonesia beserta solusinya

Tantangan utama dalam penegakan hukum tindak pidana cybercrime di Indonesia menghadapi berbagai kompleksitas yang meliputi aspek teknologi, regulasi, kapasitas penegak hukum, budaya, proses peradilan, dan koordinasi antar instansi. Pertama-tama, kecepatan perkembangan teknologi menjadi faktor utama yang menghadirkan tantangan bagi penegakan hukum. Kejahatan siber terus berkembang dengan munculnya modus operandi baru yang sulit diantisipasi oleh regulasi yang ada. Selain itu, keterbatasan ruang lingkup regulasi menjadi kendala serius dalam

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

penegakan hukum cybercrime undang-undang Indonesia tentang Informasi dan Transaksi Elektronik (ITE) berfungsi sebagai peraturan utama masih dianggap belum memadai untuk menjangkau semua jenis kejahatan siber yang terus berkembang.(Farhan et al., 2023)

Keterbatasan kapasitas penegak hukum juga menjadi hambatan yang signifikan. Kurangnya sumber daya manusia yang terlatih dalam bidang teknologi informasi, serta kurangnya akses terhadap teknologi yang memadai, menghambat efektivitas penegakan hukum. Tantangan sosial dan budaya juga mempersulit upaya penegakan hukum cybercrime. Minimnya literasi digital di kalangan masyarakat serta budaya permisif terhadap konten negatif di media sosial menjadi faktor-faktor yang perlu diatasi dalam upaya pemberantasan cybercrime.(Nasution, 2024)

Selanjutnya, mengumpulkan bukti digital dalam kasus cybercrime sering kali menjadi tugas yang sulit dan membutuhkan keahlian khusus. Proses peradilan yang rumit juga menjadi kendala dalam penegakan hukum cybercrime di Indonesia. Proses peradilan yang memakan waktu lama dan rumit dapat memperlambat penanganan kasus dan mengurangi efektivitas penegakan hukum.(Afriyenti, 2022)

Kurangnya koordinasi antar instansi juga menjadi tantangan dalam penegakan hukum cybercrime. Penanganan kasus cybercrime sering kali melibatkan berbagai instansi, namun koordinasi antar instansi belum optimal, sehingga menghambat efisiensi dalam penanganan kasus. Untuk mengatasi tantangan-tantangan tersebut, diperlukan solusi yang komprehensif dan terpadu. Salah satu cara untuk menyelesaikannya adalah dengan merevisi Undang-Undang ITE untuk memperluas ruang lingkup regulasi dan menyesuaikannya dengan perkembangan teknologi. Peningkatan kapasitas penegak hukum juga menjadi kunci dalam mengatasi tantangan ini. Pelatihan dan edukasi bagi aparat penegak hukum perlu ditingkatkan untuk meningkatkan kemampuan mereka dalam mengidentifikasi, menyelidiki, dan menangani kasus cybercrime.(Putra, 2024)

Peningkatan literasi digital di masyarakat juga menjadi solusi yang penting. Edukasi tentang risiko dan bahaya cybercrime, serta cara untuk melindungi diri dari ancaman di dunia digital, harus menjadi komponen utama dari kurikulum sekolah formal dan non-formal. Selain itu, kolaborasi antar pemangku kepentingan, termasuk masyarakat sipil, sektor swasta, akademisi, dan pemerintah juga diperlukan untuk menciptakan lingkungan yang lebih aman dan responsif terhadap ancaman cybercrime. Melalui pendekatan yang holistik dan melibatkan berbagai pihak, diharapkan Indonesia dapat mengatasi tantangan penegakan hukum cybercrime dan menciptakan lingkungan digital yang lebih aman bagi masyarakat secara keseluruhan.(Umami & Yusuf, 2024)

Dalam menghadapi tantangan penegakan hukum terkait tindak pidana cybercrime di Indonesia, sejumlah solusi terbaru telah diusulkan. Pertama, revisi terhadap Salah satu topik utama adalah UU Informasi dan Transaksi Elektronik

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

(ITE). Adapun perbaikan ini dapat memperluas cakupan regulasi dan mengikuti perkembangan teknologi yang terus berubah, sehingga celah hukum yang dieksploitasi oleh pelaku kejahatan siber dapat diminimalkan. Peningkatan kapasitas penegak hukum juga menjadi langkah penting. Aparat penegak hukum perlu diberikan pelatihan dan edukasi yang memadai dalam bidang teknologi informasi, sehingga mereka dapat lebih efektif dalam mengidentifikasi, menyelidiki, dan menangani kasus-kasus cybercrime dengan tepat.

Selain itu, peningkatan literasi digital di kalangan masyarakat juga dianggap sebagai solusi yang penting. Dengan meningkatkan pemahaman masyarakat tentang cybercrime serta mengajarkan perilaku yang bertanggung jawab di ranah digital, diharapkan Masyarakat dapat menjadi lebih berhati-hati saat berinteraksi secara online. Hal ini dapat membantu dalam mengurangi kerentanan masyarakat terhadap serangan cyber dan meningkatkan kesadaran akan potensi risiko yang ada di lingkungan digital.

Kerjasama internasional juga menjadi fokus utama dalam upaya penanggulangan cybercrime. Dengan kerjasama yang erat antar negara, pertukaran informasi dan sumber daya dapat dilakukan secara efektif, sehingga penegakan hukum dapat lebih efektif dalam melacak dan menindak para pelaku kejahatan siber yang sering kali beroperasi lintas negara. Kerjasama ini juga dapat memperkuat mekanisme penegakan hukum global untuk menangani ancaman cybercrime secara lebih holistik dan terkoordinasi.

Pembentukan laboratorium forensik digital juga menjadi solusi yang penting dalam menangani kasus cybercrime. Laboratorium ini diharapkan dapat membantu penegak hukum dalam mengumpulkan dan menganalisis bukti digital dengan lebih efektif, sehingga proses penyelidikan dan pengadilan dapat berjalan dengan lancar dan efisien. Dengan memiliki fasilitas yang memadai, penegak hukum dapat menghasilkan bukti yang kuat dan dapat dipertanggungjawabkan di pengadilan, meningkatkan tingkat keberhasilan dalam penuntutan terhadap pelaku kejahatan siber.

Reformasi dalam sistem peradilan juga menjadi langkah penting dalam penanganan kasus cybercrime. Proses peradilan yang cepat, transparan, dan adil akan memberikan kepastian hukum bagi korban dan memberikan sanksi yang tepat bagi pelaku kejahatan siber. Dengan meningkatkan efektivitas sistem peradilan, diharapkan dapat menimbulkan rasa jera yang lebih kuat terhadap orang-orang yang melakukan kejahatan siber dan menghindari mereka melakukannya lagi.

Terakhir, penguatan koordinasi antar instansi yang terlibat dalam penanganan kasus cybercrime juga menjadi hal yang sangat diperlukan. Dengan koordinasi yang baik, berbagai pihak dapat bekerja sama secara sinergis dalam menangani kasus-kasus cybercrime dengan lebih efektif. Dengan melakukan tindakan ini, harapannya bahwa Indonesia dapat membangun ruang digital yang aman dan tidak terpengaruh oleh

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

aktivitas kriminal online, serta meningkatkan penegakan hukum dan perlindungan korban.

SIMPULAN

Penelitian ini telah menguraikan pengaturan hukum yang berlaku untuk tindak pidana internet di Indonesia serta menunjukkan hambatan penegakan hukum. Temuan menunjukkan adanya kelemahan dalam regulasi yang ada saat ini, terutama terkait dengan keterbatasan sumber daya manusia, fasilitas yang belum memadai, dan anggaran yang terbatas. Untuk mengatasi tantangan ini, langkah-langkah konkret perlu dilakukan untuk meningkatkan efektivitas penegakan hukum cybercrime.

Dalam menghadapi tantangan inipemerintah harus memberi perhatian yang lebih besar pada penegakan hukum cybercrime. Pertama, peningkatan sumber daya manusia dan fasilitas yang diperlukan harus menjadi prioritas untuk meningkatkan kemampuan penegak hukum untuk menangani kasus-kasus terkait cybercrime. Selain itu, alokasi anggaran yang lebih besar juga perlu dipertimbangkan untuk memastikan bahwa lembaga penegak hukum memiliki dana yang memadai untuk melakukan tugasnya dengan efektif. Selain langkah-langkah internal, kerja sama internasional juga merupakan elemen penting dalam penanggulangan cybercrime. Dengan memperkuat kerja sama melalui perjanjian bantuan timbal balik dan ekstradisi, Indonesia dapat lebih efektif menangani kejahatan siber yang berskala global. Dengan demikian, Penelitian ini diharapkan dapat membantu sistem penegakan hukum cybercrime Indonesia dan memperkuat kerjasama internasional dalam menanggulangi ancaman cybercrime yang semakin kompleks dan meluas.

DAFTAR PUSTAKA

Afriyenti, R. R. (2022). *Pelayanan Administrasi Kasus Cyber Crime Pada Direktorat Reserse Kriminal Khusus Polda Riau*. Universitas Islam Riau.

Andika, A. (2022). Agama Dan Perkembangan Teknologi Di Era Modern. *Abrahamic Religions: Jurnal Studi Agama-Agama*, *2*(2), 129–139.

AYUNDA, K. (2023). *Analisis Pengaruh Penggunaan E-Commerce, Media Sosial Dan Sosial Media Marketing Terhadap Usaha Mikro Kecil Menengah (Umkm) Fashion Di Kota Jambi*. UNIVERSITAS JAMBI.

Azzani, I. K., Purwantoro, S. A., & Almubaroq, H. Z. (2023). Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja Paruh Waktu Sebagai Ancaman Negara. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *10*(7), 3556–3568.

Eryanto, R. B. R. (2023). *Kajian Pasal 27 Ayat 3 Undang-Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dikaitkan Dengan Pasal 23 Ayat 2 Undang-Undang No 39 Tahun 1999 Tentang Hak Kebebasan Berekespresi Dalam Kasus Pelanggaran Undangundang Informasi Dan Transaks*. Fakultas Hukum Universitas

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613

Pasundan.

Farah, R. A. (2021). *Perlindungan Hukum Pengguna Internet Banking Terhadap Kejahatan Cybercrime Di Indonesia*. Fakultas Hukum.

Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(6), 8–20.

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.

Hamid, R. (2024). *A*nalisis Yuridis Pertanggungjawaban Pelaku Pidana Yang Bersama Sama Melakukan Tindak Pidana Pencurian Dengan Membawa Senjata Api Secara Ilegal (Studi Kasus: Nomor 121/Pid. Sus/2021/PN. JKT SEL). Universitas Nasional.

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah Dan Hukum*, 40–55.

Himawan, I. S., Wahyuni, S., Hamidin, D., Andriani, A. D., Meidelfi, D., & Khairunisa, Y. (2022). *Etika Profesi Teknologi Informasi Dan Komunikasi*. TOHAR MEDIA.

Jaelani, N. H. (2020). Tinjauan Viktimologis Terhadap Korban Tindak Pidana Cybercrime Illegal Content di Wilayah Hukum Polrestabes Bandung Dihubungkan dengan Undangundang No 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elek. *Varia Hukum*, *2*(1), 65–87.

Lestyaningrum, I. K. M., Trisiana, A., Safitri, D. A., & Pratama, A. Y. (2022). *Pendidikan global berbasis teknologi digital di era milenial*. Unisri Press.

Nasution, Z. A. (2024). Analisis Yuridis Tentang Kebijakan Penegakan Hukum Terhadap Tindak Pidana Cyber Di Indonesia. *Tugas Mahasiswa Fakultas Hukum*, *1*(2).

Parulian, H., & Putranto, R. D. (2022). Pidana Ujaran Kebencian Melalui Media Sosial Ditinjau dalam Perspektif Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). *Jurnal Pendidikan Dan Konseling (JPDK)*, *4*(4), 4909–4919.

Prabowo, I. A., Pomalingo, S., Istiono, W., Muhariya, A., Irmawati, I., Sugianto, C. A., Khairunnisa, K., Pratiwi, M., Ernawati, T., & Setiadi, T. (2023). *SISTEM KOMPUTER DAN INFORMASI*. CV. Gita Lentera.

Putra, J. S. A. A. M. (2024). Melacak Tantangan Peretasan Dalam Perkembangan

Hukum Dunia Maya Di Indonesia. *Belom Bahadat*, *14*(1), 25–40.

Rizkita, A. F. (2023). Kebijakan Hukum Tentang Perjudian Online. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(5), 25–33.

Saputra, A. M. A., Kharisma, L. P. I., Rizal, A. A., Burhan, M. I., & Purnawati, N. W. (2023). *TEKNOLOGI INFORMASI: Peranan TI dalam berbagai bidang*. PT. Sonpedia Publishing Indonesia.

Sawitri, D. (2023). Internet Of Things Memasuki Era Society 5.0. *Jurnal Komputer, Informasi Teknologi, Dan Elektro*, *8*(1).

Setiawan, M. N., Safitri, M., & Lestari, L. (2022). Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia. *DATIN LAW JURNAL*, *3*(2).

Sommaliagustina, D., Citra, H., & Wahyuni, S. (2022). Perlindungan Konsumen E-Commerce Dalam Kerangka Masyarakat Ekonomi Asean (MEA). *Jurnal Penelitian Dan Pengkajian Ilmiah Sosial Budaya*, *1*(1), 149–165.

SUJUDI, M., & Ariyanti, E. (2020). *Kajian Yuridis Pasal 27 Ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Tindak Pidana Siber Kesusilaan*.

Sunaryo, T. (n.d.). *Penemuan Hukum Dalam Proses Peradilan Pidana Di Pengadilan Negeri Pandeglang Berdasarkan Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman*.

Syafrizal, M. (2020). *Pengantar jaringan komputer*. Penerbit Andi.

Umami, E., & Yusuf, H. (2024). Peran Pendidikan Hukum dalam Mencegah Kejahatan Siber di Kalangan Generasi Muda. *Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(2), 1473–1487.

ISSN (Online) 2985-6906

DOI: 10.35905/delictum.v2i2.10613