PENERAPAN HUKUM TERHADAP CYBERCRIME DI ERA DIGITAL

Windah Sari[1], Haifa Nabila Asma[2], Tubagus Tommy Fauzan Cecep[3], David Nugraha Saputra[4]
wndaah.sr@gmail.com[1], haifabilaa8@gmail.com[2], tbtommyfauzanc@gmail.com[3]
UIN Sultan Maulana Hasanuddin Banten

ABSTRAK

Tujuan dari artikel ini adalah untuk memberikan pemahaman yang lebih baik kepada pembaca tentang kejahatan dunia maya. Kelemahan dalam bidang ini dapat berpotensi berubah menjadi bencana global yang membahayakan banyak industri, mulai dari bisnis, perilaku sosial, perlindungan anak, keamanan nasional, dan sistem pemerintahan. Berdasarkan penelitian, media sosial masih sering disalahgunakan oleh pengguna untuk menyebarkan kegiatan kriminal secara daring. Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), banyak pelaku kejahatan siber di platform media sosial yang dapat dijerat dengan tuntutan hukum. baik secara sengaja maupun tidak. Di sisi lain, hukum seharusnya memberikan perlindungan bagi pengguna internet yang berniat baik, sekaligus menerapkan sanksi tegas terhadap pelaku kejahatan dunia maya. Namun, hingga saat ini, sistem hukum kita belum mampu mengatasi secara tuntas semua jenis kejahatan komputer yang terjadi melalui Internet. Proses penyidikan pun dihadapkan pada berbagai kendala, seperti perangkat hukum yang belum memadai, keterampilan penyidik, serta akses terhadap alat bukti dan fasilitas komputer forensik. Oleh karena itu, penegakan hukum terkait kejahatan dunia maya masih dirasa lemah.
Kata Kunci: Teknologi Informasi, Hukum Pidana, dan Kejahatan Dunia Maya.

ABSTRACT

The purpose of this article is to provide readers with a better understanding of cybercrime. Weaknesses in this area can potentially turn into a global disaster that endangers many industries, ranging from business, social behavior, child protection, national security, and government systems. Based on research, social media is still often misused by users to spread criminal activities online. Based on Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), many cybercriminals on social media platforms can be prosecuted. either intentionally or unintentionally. On the other hand, the law should provide protection for internet users with good intentions, while also implementing strict sanctions against cybercriminals. However, until now, our legal system has not been able to completely overcome all types of computer crimes that occur via the Internet. The investigation process is also faced with various obstacles, such as inadequate legal instruments, investigator skills, and access to evidence and forensic computer facilities. Therefore, law enforcement related to cybercrime is still considered weak.
Keywords: *Information Technology, Criminal Law and Cybercrime.*

PENDAHULUAN

Kejahatan siber atau cybercrime telah berkembang menjadi risiko yang signifikan di era digital ini. Evolusi teknologi informasi membawa kemudahan dan kecepatan dalam berbagai aspek kehidupan, tetapi di sisi lain, juga memunculkan peluang bagi tindakan kriminal berbasis teknologi. Di Indonesia telah terkena dampak oleh kemajuan teknologi dan internet pada masyarakat, mulai dari bisnis, pendidikan, hingga kehidupan sehari-hari. Namun, seiring dengan kemajuan ini, kejahatan siber juga semakin marak dan kompleks, mencakup berbagai bentuk, mulai dari pencurian data, penipuan online, peretasan, hingga penyebaran hoaks (Susanto, 2020). Undang-Undang Nomor 19 Tahun 2016 merupakan revisi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008. disahkan untuk menghadapi tantangan hukum dalam dunia maya. UU ITE bertujuan

untuk melindungi masyarakat dari tindakan-tindakan yang melanggar hukum di ranah digital, baik dalam bentuk pencemaran nama baik, penyebaran informasi palsu, hingga pencurian data (Hendro, 2019). Meski telah ada kerangka hukum ini, penerapan UU ITE sering kali menuai kritik dan kontroversi, terutama dalam hal penafsiran pasal-pasal yang dianggap rawan disalahgunakan atau terlalu luas cakupannya (Putra, 2021). Masalah ini menjadi tantangan serius dalam menangani kejahatan siber di Indonesia.

Salah satu tantangan utama dalam penerapan UU ITE adalah bagaimana hukum dapat menyeimbangkan antara perlindungan terhadap korban dan kebebasan individu, termasukhak tentang hak kebebasan berbicara. Menurut Sari (2021), meskipun UU ITE bertujuan untuk melindungi masyarakat, dalam beberapa kasus, undang-undang ini telah digunakan untuk menekan kebebasan berekspresi, khususnya di media sosial. Hal ini menjadi perdebatan yang memerlukan perhatian serius, karena kebebasan berekspresi adalah salah satu pilar penting dalam masyarakat demokratis (Sari, 2021). Pentingnya pengembangan regulasi yang lebih adaptif terhadap perkembangan teknologi juga menjadi sorotan dalam banyak studi. Menurut Setiawan (2020), UU ITE sebagai produk hukum masih memiliki beberapa kelemahan dalam hal fleksibilitas menghadapi perubahan cepat di dunia teknologi. Sifat statis dari undang-undang ini dianggap kurang mampu untuk menghadapi sifat dinamis kejahatan siber yang terus berevolusi, terutama dengan munculnya jenis-jenis kejahatan baru seperti serangan siber berbasis kecerdasan buatan (AI) dan pembajakan data melalui ransomware (Setiawan, 2020). Selain itu, pelaksanaan UU ITE dalam menghadapi kejahatan siber sering kali terhambat oleh keterbatasan infrastruktur teknologi penegak hukum di Indonesia. Supriyadi (2022) mencatat bahwa aparat penegak hukum, terutama di wilayah-wilayah tertentu, masih memiliki keterbatasan dalam hal fasilitas pendukung dan pengetahuan terkait teknologi informasi. Keterbatasan ini menyebabkan proses investigasi dan penegakan hukum menjadi kurang optimal dalam menangani kasus-kasus siber yang memerlukan keahlian khusus (Supriyadi,2022).

Penegakan hukum terhadap kejahatan siber di Indonesia merupakan upaya kolaboratif yang melibatkan sejumlah lembaga, seperti Komisi Pemberantasan Korupsi (KPK), Kejaksaan Agung, dan Kepolisian Negara Republik Indonesia (POLRI). Dalam kaitannya dengan kejahatan dunia maya, POLRI menegakkan peranpenting melalui Direktorat Tindak Pidana Siber Bareskrim Polri, sebuah unit khusus yang didedikasikan untuk menyelidiki dan menangani kejahatan di ranah digital. Sementara itu, Kejaksaan Agung turut berperan dalam proses penuntutan terhadap para pelaku kejahatan siber, memastikan bahwa mereka dihadapkan pada konsekuensi hukum yang sesuai dengan perbuatannya.

Dalam konteks globalisasi yang semakin erat dan tingginya tingkat konektivitas, kerjasama internasional menjadi suatu keharusan dalam menangani ancaman kejahatan siber. Indonesia telah aktif berpartisipasi dalam upaya kolaboratif dengan negara lain, khususnya terkait dengan pembagian data dan bukti elektronik mengenai kejahatan dunia maya, memberikan edukasi kepada aparat penegak hukum mengenai metode investigasi dan penuntutan digital, serta penyusunan regulasi bersama untuk mengatasi tantangan yang dihadapi secara bersama-sama. Melalui upaya kolaboratif ini, diharapkan dapat terwujud lingkungan digital yang lebih aman dan terlindungi bagi masyarakat Indonesia serta komunitas global secara luas.

Reformasi dalam Penegakan hukum kejahatan dunia maya mencakup sejumlah bidang utama yang penting. Pertama dan terutama, sangat penting untuk meningkatkan keamanan teknologi informasi. Untuk mencegah serangan digital pada data yang sangat sensitif dan infrastruktur penting, sistem keamanan dunia maya harus diperkuat. Kedua, upaya untuk meningkatkan literasi keamanan siber di kalangan masyarakat menjadi sebuah kebutuhan mendesak. Hal ini bertujuan agar masyarakat memiliki pemahaman yang lebih

baik mengenai ancaman digital dan mampu meresponsnya dengan tindakan yang bijak dan tepat.

METODOLOGI

Pendekatan penelitian normatif menggunakan model deskriptif digunakan untuk mengkaji beberapa aspek perundang-undangan terkait kejahatan dunia maya. Dokumen (tertulis dan elektronik) dari jurnal, artikel, makalah, dan sumber lain dikumpulkan sebagai bagian dari teknik pengumpulan data. Setelah itu, informasi yang terkumpul dibandingkan dan dipilih untuk disajikan dalam artikel ini. Dengan demikian, diharapkan temuan penelitian penulis akan memberikan kontribusi minimal bagi individu yang ingin menyelidiki masalah hukum dunia maya di Indonesia. Pendekatan legislatif dan pendekatan konseptual adalah metode yang digunakan. Hukum yang berkaitan dengan dunia maya diteliti oleh penulis, dan bahan hukum primer dan sekunder digunakan. Bahan hukum primer adalah bahan hukum yang berasal peraturan perundang undangan yang berkaitan dengan penulisan ini. Adapun bahan hukum sekunder adalah bahan hukum yang berasal dari buku, jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini.

HASIL DAN PEMBAHASAN

Di tengah perkembangan terus-menerus dalam era digital, Di Indonesia, kejahatan dunia maya telah berkembang menjadi perhatian utama. terutama di sektor ekonomi yang rentan. Kejahatan dunia maya mencakup perdagangan gelap, penipuan internet, dan pencurian data pelanggan dan serangan terhadap sistem perbankan semakin meningkat. Tren ini menciptakan dampak yang luas, tidak hanya dalam bentuk kerugian finansial bagi masyarakat, tetapi juga mengancam stabilitas keamanan nasional dan menimbulkan risiko yang signifikan terhadap pertumbuhan ekonomi negara.

Penegakan hukum terhadap kejahatan siber ini dihadapkan pada berbagai tantangan, terutama dalam upaya untuk mengharmonisasikan regulasi yang berkaitan dengan penggunaan internet. Dalam menghadapi ancaman yang semakin kompleks ini, upaya penegakan hukum perlu disesuaikan dan diperkuat agar mampu mengatasi tantangan yang dihadapi dalam lingkungan digital yang terus berubah dan berkembang pesat.

Pada masa kini, praktek Ketika menangani aktivitas ilegal seperti penipuan, perjudian, dan pornografi masih mengacu dalam ketentuan Kitab Undang-Undang Hukum Pidana (KUHP). Meskipun demikian, dengan adanya perkembangan teknologi informasi dan komunikasi yang sedang berlangsung, pola transaksi, pembelian, investasi, serta operasional bisnis telah mengalami perubahan signifikan. Selain itu, pertumbuhan ini memudahkan berkembangnya kejahatan dunia maya, termasuk perdagangan gelap, pencurian data, dan serangan terhadap industri perbankan.

Oleh karena itu, diperlukan tindakan khusus untuk menjaga keamanan jaringan, sistem komputer dan perangkat elektronik, serta data dari berbagai ancaman siber yang ada. Upaya-upaya ini menjadi sangat penting untuk mengatasi hambatan baru yang disebabkan oleh kemajuan teknologi, sehingga sistem hukum perlu terus diperbaharui dan disesuaikan agar mampu menjawab kebutuhan dan tantangan zaman yang terus berubah dengan cepat.

Tujuan utama keamanan siber adalah untuk menjaga ketersediaan, kerahasiaan, dan integritas data sensitif serta untuk mempertahankan infrastruktur TI terhadap intrusi yang dapat membahayakan sistem atau mengakibatkan kerugian besar. Di tengah kompleksitas ancaman yang terus berkembang, kolaborasi antara pemerintah, sektor swasta, dan masyarakat menjadi semakin penting dalam upaya menjaga keamanan dan kedaulatan negara dari potensi ancaman serta gangguan.

Dalam konteks ini, meningkatkan pelatihan dan inisiatif pendidikan keamanan siber menjadi suatu langkah yang strategis. Melalui peningkatan kesadaran dan keterampilan dalam menghadapi ancaman siber, diharapkan masyarakat dapat lebih responsif dan proaktif dalam mengatasi berbagai tantangan yang muncul dalam ranah digital. Upaya ini tidak hanya mencakup pelatihan teknis, tetapi juga penyuluhan tentang pentingnya menjaga keamanan informasi dan melindungi infrastruktur teknologi dari potensi serangan yang merugikan.

Meskipun demikian, fenomena kejahatan siber terus mengalami perkembangan dan meningkat menjadi lebih kompleks Kadang-kadang. Salah satu elemen yang menarik perhatian signifikan adalah cyberbullying yang terjadi melalui media sosial, mengingat pentingnya menjaga keseimbangan antara kebebasan berbicara dan perlindungan korban. Dalam konteks ini, penerapan penegakan hukum pidana dalam kasus cyberbullying memerlukan pertimbangan yang matang, terutama dalam menangani Penghinaan, fitnah, dan ancaman terhadap korban merupakan contoh pelanggaran pengaduan.

Dengan memberlakukan undang-undang dan kebijakan yang ditujukan untuk meningkatkan keamanan siber dan menjaga infrastruktur informasi, pemerintah Indonesia telah dengan tegas menanggapi meningkatnya ancaman kejahatan siber yang kritis. Salah satu langkah konkret yang diambil adalah pendirian Badan Siber dan Sandi Negara (BSSN), sebuah lembaga yang dibentuk secara khusus untuk menghadapi berbagai ancaman dalam ranah digital. Meskipun demikian, tantangan yang dihadapi tetap signifikan, dan upaya Peningkatan kewenangan penegakan hukum dan modifikasi regulasi yang berkelanjutan sangat penting. Hal ini diperlukan untuk menjaga keamanan nasional dan mengurangi kemungkinan kejahatan dunia maya yang mengganggu stabilitas dan keamanan Indonesia.

Selain berfungsi sebagai pencegah atau ancaman, hukuman pidana juga harus memiliki kapasitas untuk menginformasikan dan mengubah pelaku. Sangat penting untuk memajukan gagasan mencari hukuman alternatif sebagai pengganti hukuman pidana perampasan kebebasan. Nama Rudolph B. Schesinger menjelaskan bahwa perbandingan hukum adalah metode penyelidikan untuk memperoleh pengetahuan yang lebih dalam tentang bahan-bahan hukum tertentu. Perbandingan hukum bukanlah perangkat peraturan dan asas-asas hukum serta bukan suatu cabang hukum, melainkan teknik untuk menghadapi unsur hukum asing dari suatu masalah hukum.

Menurut Munir Fuady, perbandingan hukum merupakan sebuah disiplin ilmu dan metode dalam studi hukum yang melibatkan peninjauan lebih dari satu sistem hukum. Pendekatan ini dilakukan dengan menganalisis berbagai kaidah, aturan hukum, yurisprudensi, dan pandangan ahli yang terkemuka dalam berbagai sistem hukum, dengan tujuan untuk mengidentifikasi persamaan dan perbedaan di antara mereka. Dengan demikian, melalui perbandingan tersebut, kita dapat mengambil kesimpulan serta mengembangkan konsep-konsep tertentu, sambil memahami penyebab munculnya persamaan dan perbedaan historis, sosial, analitis, dan normatif. Sesuai dengan klausul dalam Pasal 5 Kitab Undang-Undang Hukum Pidana (KUHP), hukum pidana Indonesia memiliki cakupan yang berlaku bagi setiap warga negara Indonesia yang melakukan tindak pidana tertentu di luar wilayah Indonesia. Adapun tindak pidana yang dimaksud mencakup berbagai perbuatan, antara lain yang berkaitan dengan keamanan negara, pelanggaran terhadap martabat Presiden dan Wakil Presiden, hasutan untuk melakukan tindak pidana, penyebaran tulisan yang bertujuan untuk menimbulkan hasutan, tindakan sengaja untuk membuat diri sendiri atau orang lain tidak mampu memenuhi kewajiban militer, melakukan perkawinan dengan mengetahui bahwa perkawinan yang ada menjadi hambatan yang sah untuk itu, serta berbagai tindak pidana lainnya yang dianggap sebagai kejahatan menurut

Undang-Undang Pidana Indonesia serta diancam dengan pidana oleh negara tempat tindak pidana dilakukan.Di Indonesia, banyak aspek hukum yang memiliki akar dari peraturan-peraturan hukum yang berasal dari Belanda, hal ini dikarenakan proses pembuatan aturan peraturan yang memakan waktu lama dan melibatkan partisipasi dari berbagai elemen masyarakatdi Indonesia. Implementasi hukum di Indonesia seringkali mengambil landasan dari undang-undang atau regulasi yang diwarisi dari sistem hukum Belanda. Namun, seiring dengan perubahan zaman dan evolusi sosial, terjadi revisi-revisi yang dilakukan guna menyesuaikan dengan kebutuhan danperilaku masyarakat Indonesia.Contoh konkret dari adaptasi hukum terhadap perkembangan zaman dapat ditemukan dalam Undang-Undang No. 44 Tahun 2008 tentang Pornografi. Di dalamnya, terdapat ketentuan mengenai tindak pidana yangjuga mencakup aspek kejahatan siber. Pengertian pornografi yang disebutkan dalam Pasal 1 ayat 1 diperluas tidak hanya mencakup materi cetak, tetapi juga mencakup berbagai bentuk media komunikasi, termasuk internet. Begitu pula dengan definisi jasa pornografi yang tercantum dalam Pasal 1 angka 2, yang mencakup layanan yang disediakan melalui internet dan media komunikasi elektronik lainnya

Pengertian Cybercrime

Peraturan perundang-undangan yang mengatur penggunaan teknologi ini juga telah dipengaruhi oleh kemajuan ilmu pengetahuan dan teknologi. Sebuah undang-undang yang dikenal sebagai "hukum dunia maya" diciptakan sebagai respons terhadap meningkatnya jumlah kejahatan yang melibatkan teknologi informasi. Undang-Undang ITE No. 11 Tahun 2008, yang mengatur informasi dan transaksi elektronik, telah berlaku di Indonesia. Diharapkan penerapan Undang-Undang ITE No. 11 Tahun 2008 akan mengurangi kejahatan dunia maya di Indonesia. Mengingat konteks ini, penulis ingin tahu tentang kerangka hukum Indonesia terkait dengan kejahatan dunia maya di era informasi dan masyarakat virtual.

Perkembangan internet dan teknologi informasi lainnya memiliki banyak dampak positif, tetapi juga memiliki dampak negatif, seperti memudahkan pelaku kejahatan melakukan kejahatan, yang semakin meresahkan masyarakat. Kejahatan dunia maya adalah istilah yang digunakan untuk menggambarkan penyalahgunaan yang terjadi di dunia maya. Kejahatan komputer adalah definisi teknis dari kejahatan dunia maya. Jika mengacu pada definisi kejahatan komputer yang sebenarnya, Para ahli belum mencapai konsensus mengenai hal ini. Kata "kejahatan komputer" masih belum banyak digunakan, bahkan dalam bahasa Inggris. Kata "penyalahgunaan komputer", "penyalahgunaan komputer", "penipuan komputer", "kejahatan terkait komputer", "kejahatan yang dibantu komputer", dan "kejahatan komputer" sering digunakan dalam kaitannya dengan kejahatan komputer. Istilah "kejahatan dunia maya" digunakan untuk merujuk pada kegiatan kriminal yang terjadi di dunia maya.

Kejahatan dunia maya didefinisikan oleh Komisi Hukum Inggris sebagai "penipuan komputer," yaitu segala bentuk manipulasi komputer yang dilakukan dengan itikad buruk dengan maksud untuk merugikan pihak lain atau mendapatkan uang atau keuntungan lainnya. Semua jenis kegiatan kriminal terhadap komputer, jaringan komputer, dan penggunanya dapat secara kolektif disebut sebagai kejahatan dunia maya. tradisional berupa tindak pidana pornografi anak yang menggunakan atau dengan bantuan peralatan komputer.

Karakteristik dan Jenis Cybercrime

Globalisasi telah mengubah hampir setiap aspek kehidupan manusia, terutama di negara-negara berkembang seperti Indonesia. Modifikasi hukum juga didorong oleh perubahan yang terjadi. Isu-isu yang muncul ketika hukum berubah termasuk sejauh mana hukum dapat beradaptasi dengan perubahan ini dan bagaimana hukum tidak tertinggal dari

perubahan masyarakat, atau sebaliknya. mengutip pandangan Satjipto Raharjo yang menyatakan bahwa hukum bekerja dengan cara mempertaruhkan perilaku atau hubungan interpersonal seseorang. Demi mempertaruhkan, ia menetapkan bahwa hukum harus menjelaskan kerjanya dalam beberapa cara, termasuk: (1) Menciptakan norma, baik yang membangun hubungan antara individu maupun yang memberikan ketentuan; (2) Menyelesaikan konflik; dan (3) Menjamin kelangsungan kehidupan masyarakat, khususnya dalam hal perubahan sosial. Pandangan Satjipto Raharjo tersebut menegaskan bahwa hukum sebagai amanat rakyat tidak dapat dilepaskan dari perkembangan masyarakat dan karenanya harus beradaptasi dengannya.

Era globalisasi juga turut mendorong perkembangan teknologi informasi yang semakin maju dan jenis-jenis kejahatan baru yang lebih modern dan berbeda dari kejahatan tradisional. Kejahatan yang melibatkan teknologi informasi, atau cybercrime, berbeda dengan kejahatan biasa karena membutuhkan kemampuan khusus. Karena pelakunya adalah para profesional di bidangnya dan ahli dalam menggunakan aplikasi tertentu, kejahatan ini juga dapat dikategorikan sebagai kejahatan kerah putih (Suharyanto, 2013:13). Cybercrime, yang juga disebut sebagai kejahatan transnasional, sering kali terjadi di luar batas negara.

Tantangan Penerapan UU ITE dalam Menangani Kejahatan Siber

Penerapan Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia menjadi salah satu upaya negara dalam menanggulangi kejahatan siber yang semakin kompleks. uu ini telah menjadi landasan hukum yang digunakan untuk mengatur berbagai aktivitas digital, terutama yang melibatkan informasi elektronik, privasi, dan transaksi digital. Meski demikian, implementasinya masih menghadapi berbagai tantangan. Beberapa hambatan yang ditemui dalam penerapan uu ite antara lain adalah isu multitafsir pada beberapa pasalnya, keterbatasan kapasitas teknis aparat penegak hukum, dan kurangnya adaptasi terhadap perkembangan teknologi siber yang pesat. Salah satu isu paling mendasar dalam penerapan uu ite adalah multitafsirnya beberapa pasal, khususnya yang berkaitan dengan pencemaran nama baik dan penyebaran informasi yang dianggap palsu atau menyesatkan. pasal-pasal terkait pencemaran nama baik dalam uu ite, seperti Pasal 27 ayat (3), sering dianggap bias karena dapat ditafsirkan secara subjektif oleh aparat penegak hukum. Pasal tersebut memuat ketentuan yang memungkinkan pelaporan pencemaran nama baik di media sosial atau platform digital lainnya, namun rentan digunakan untuk membatasi kebebasan berekspresi. Hal ini sering menjadi kritik dari masyarakat dan aktivis hak asasi manusia, yang melihat bahwa undang-undang ini dapat digunakan sebagai alat untuk mengkriminalisasi kritik atau opini yang berbeda (Susanto, 2021).

Selain itu, pasal-pasal dalam uu ite yang multitafsir ini juga kerap menimbulkan perbedaan pandangan di antara penegak hukum sendiri. Dalam beberapa kasus, perbedaan interpretasi pasal oleh jaksa dan hakim menyebabkan hasil putusan yang tidak konsisten. Hal ini menimbulkan ketidakpastian hukum yang berdampak pada publik, karena masyarakat menjadi khawatir bahwa aktivitas mereka di ruang digital dapat dianggap sebagai pelanggaran hukum hanya karena interpretasi yang berbeda (Putra & Rahman, 2019). Menurut studi dari Supriyadi (2022), kerancuan ini berdampak negatif pada efektivitas UU ITE dalam menangani kejahatan siber, karena undang-undang yang multitafsir justru menimbulkan ketakutan pada masyarakat yang menggunakan media digital sebagai ruang berekspresi. di samping itu, kejahatan siber seringkali memerlukan penanganan khusus dengan keterampilan teknis yang mendalam, seperti investigasi digital, pengumpulan bukti elektronik, serta pelacakan aktivitas daring. Dalam penerapannya, aparat penegak hukum di Indonesia kerap menghadapi keterbatasan teknis dalam

menanggulangi kejahatan siber, terutama dalam hal pemahaman teknologi yang terus berkembang pesat. Menurut Fajrin (2020), banyak aparat penegak hukum yang belum memiliki pengetahuan memadai mengenai teknik penyelidikan forensik digital, sehingga proses pengumpulan bukti sering kali terkendala dan menyebabkan kasus-kasus kejahatan siber tidak dapat diselesaikan dengan optimal. Keterbatasan teknis ini juga diperparah oleh kurangnya pelatihan khusus yang tersedia bagi aparat penegak hukum. Sementara negara-negara maju memiliki tim penegak hukum khusus yang menangani kejahatan siber, di Indonesia, sumber daya dan pelatihan untuk keahlian tersebut masih minim (Rachman, 2021). Hal ini menghambat efektivitas uu ite dalam memberantas kejahatan siber yang memerlukan keahlian khusus, terutama ketika kasus tersebut melibatkan jaringan internasional atau menggunakan teknologi yang sulit dilacak. Menurut Rachman (2021), untuk mengatasi hal ini, Indonesia perlu meningkatkan kapasitas penegakan hukum siber melalui pelatihan khusus, pengadaan perangkat lunak yang mendukung penyelidikan digital, serta kerja sama internasional dengan negara-negara lain.

Perkembangan teknologi digital sangat cepat, sehingga metode kejahatan siber terus berevolusi, menciptakan tantangan baru bagi penegakan hukum. UU ITE, meski telah direvisi pada tahun 2016, belum mampu sepenuhnya mengakomodasi jenis-jenis kejahatan siber yang lebih canggih, seperti penggunaan kecerdasan buatan untuk serangan siber atau penyebaran malware dalam bentuk baru (Hendro, 2019). Menurut studi Setiawan (2020), UU ITE dirancang sebagai undang-undang yang berlaku umum dan belum secara spesifik mengatur metode metode kejahatan siber yang terus berkembang. Ini menyebabkan UU ITE sering kali tidak dapat menanggapi kejahatan siber yang sifatnya dinamis dan semakin kompleks. Kejahatan siber memiliki sifat lintas batas negara yang memerlukan kerangka hukum yang bersifat global. Namun, UU ITE saat ini belum memiliki peraturan yang memadai untuk mengatasi kejahatan siber lintas batas (Fajrin, 2020). Sebagai contoh, jika pelaku berada di luar negeri, Indonesia sering kali kesulitan untuk membawa kasus kejahatan siber ke pengadilan karena perbedaan yurisdiksi. Dalam hal ini, Supriyadi (2022) menyarankan agar uu ite dilengkapi dengan ketentuan yang mendukung kerja sama internasional dalam menangani kejahatan siber, seperti yang diterapkan di negara-negara Eropa melalui Budapest Convention on Cybercrime. Ketiga tantangan ini menunjukkan bahwa meskipun uu ite bertujuan untuk melindungi masyarakat dari kejahatan siber, efektivitasnya masih terbatas karena berbagai faktor. Multitafsir pasal, keterbatasan teknis aparat, serta kurangnya adaptasi terhadap perkembangan teknologi menjadi kendala serius yang menghambat penegakan hukum di dunia siber. Kondisi ini menimbulkan implikasi penting terhadap keamanan siber di Indonesia dan perlindungan terhadap masyarakat digital. Menurut Susanto (2021), untuk mengatasi tantangan ini, perlu ada pembaruan undang- undang yang lebih adaptif terhadap perkembangan teknologi dan upaya untuk memperkuat kapasitas penegak hukum melalui pelatihan khusus dan kolaborasi internasional. Dengan adanya perubahan dan adaptasi terhadap uu ite, diharapkan undang undang ini dapat lebih efektif dalam menangani berbagai jenis kejahatan siber yang semakin kompleks. Selain itu, upaya edukasi publik tentang etika dan hukum di ruang digital juga menjadi penting agar masyarakat dapat berpartisipasi secara aktif dalam menciptakan lingkungan siber yang aman dan bertanggung jawab.

Upaya penegak hukum Indonesia untuk memerangi pelaku kejahatan dunia maya

Meskipun UU ITE telah disahkan menjadi UU No. 11 Tahun 2008 yang mengatur Informasi dan Transaksi Elektronik, masih terdapat kendala dalam upaya penegak hukum untuk menangkap pelaku kejahatan dunia maya. Isi Pasal 5, yang mengakui informasi, data, dan hasil cetak elektronik sebagai alat bukti yang sah, membahas perluasan alat bukti baru sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia. Menurut

laporan tersebut, undang-undang tersebut memperluas fakta kejahatan dunia maya yang sebelumnya tidak diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Sejumlah faktor terus menghambat kemampuan penegak hukum untuk memerangi pelaku kejahatan dunia maya, termasuk kurangnya personel penegak hukum dalam memberantas peretas dunia maya, minimnya teknologi milik kepolisian, dan kurangnya sumber daya media. Mirip dengan laboratorium kejahatan dunia maya, sebuah alat yang seharusnya dimiliki setiap departemen kepolisian daerah untuk mempercepat penemuan dan perkiraan lokasi peretas saat mereka beraksi. Namun, laboratorium ini hanya tersedia di Markas Besar Kepolisian Nasional dan kepolisian di beberapa kota besar, sehingga terdapat kendala berupa keterlambatan dan tingginya anggaran dalam setiap proses penyidikan kasus kejahatan dunia maya di Indonesia, serta adanya korban yang enggan melaporkan kejahatan yang menimpanya karena alasan privasi, alasan ekonomi, atau korban tidak percaya terhadap keahlian dan dedikasi pihak kepolisian dalam mengungkap kasus tersebut.

Sistem Hukum Pidana Indonesia Memberikan Perlindungan Hukum bagi Korban Kejahatan Siber

Tujuan dari kegiatan penegakan hukum terhadap pelaku kejahatan siber adalah untuk melindungi pengguna dunia maya dari pelaku kejahatan yang menggunakan internet untuk melakukan kejahatannya. Meskipun Indonesia belum memiliki "hukum siber" yang secara eksplisit mengatur kepentingan korban, namun tetap diperlukan tindakan hukum dengan memanfaatkan hukum yang telah ada, termasuk peraturan perundang-undangan, yurisprudensi, dan konvensi internasional yang telah diratifikasi, untuk melindungi kepentingan warga negara Indonesia yang menggunakan dunia maya.

Berbagai upaya dapat diambil untuk menyelesaikan kejahatan Internet, baik secara premetif, preventif, maupun represif. Upaya premetif dapat dijalankan dengan meratifikasi kesepakatan cyber crime internasional kedalam sistem hukum di Indonesia. Salah satu jenis perjanjian internasional adalah Perjanjian Dewan Eropa, yang beberapa ketentuannya telah dimasukkan ke dalam hukum Indonesia. Pengembangan keamanan, peningkatan energi untuk fitur komputer, serta kapasitas dan disiplin untuk menggunakan fitur-fitur tersebut di dunia maya merupakan cara untuk mencegah kejahatan dunia maya. Tindakan individu, nasional, atau internasional dapat digunakan untuk melaksanakan kegiatan-kegiatan tersebut. Sementara itu, tindakan penanggulangan kejahatan dunia maya yang represif dapat dilakukan dengan menangkap pelaku kejahatan sehingga mereka dapat ditangani secara hukum. Dengan mengharuskan pelaku kejahatan untuk memberikan ganti rugi, kompensasi, atau bantuan—yang disediakan oleh Negara—hukum menegakkan kepentingan para korban.

Tujuan dari upaya untuk melindungi korban kejahatan adalah untuk mengganti kerugian yang telah mereka derita. Jika korban terlibat atau ikut serta dalam proses penyelesaian kasus pidana, hal ini akan lebih masuk akal. Dalam tatanan global yang otonom, penegakan hukum merupakan upaya pembangunan berkelanjutan yang berupaya untuk mencapai kehidupan yang aman, tenang, tertib, dan aktif bagi negara dan lingkungannya.

Penegakan hukum pidana ke depannya harus lebih menitikberatkan pada sistem keadilan restoratif karena merupakan cara yang adil untuk menghubungkan pelaku, korban, keluarga pelaku, dan pihak lain yang terkait dengan tindak pidana untuk bekerja sama dalam penyelesaiannya. Hal ini berdasarkan pada keputusan bersama yang menekankan pemulihan pada keadaan semula dan dikeluarkan oleh Ketua Mahkamah Agung Republik Indonesia, Menteri Hukum dan Hak Asasi Manusia (HAM), Menteri Sosial, dan Menteri Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia.

Pengaturan Kejahatan Siber dalam Sistem Peradilan Pidana Indonesia

Meskipun hukum siber tidak secara tegas diatur dalam hukum Indonesia, sejumlah peraturan perundang-undangan, termasuk Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang No. 19 Tahun 2002 tentang Hak Cipta, dan Undang-Undang No. 15 Tahun 2003 tentang Pemberantasan Terorisme, serta Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang dan peraturan tersebut ini telah mengkriminalisasi jenis14 kejahatan dunia maya (cybercrime) dan ancaman hukuman buat setiap pelanggarnya.

Lebih lanjut, Rkhuhp yang terdapat dalam Buku Kedua (Bab VIII): Tindak Pidana yang Membahayakan Keamanan Publik terhadap Orang, Barang, dan Lingkungan Hidup, memuat kebijakan kriminalisasi yang telah dituangkan dalam kategori kejahatan dunia maya. Bagian 5: Tindak Pidana terhadap Informatika dan Telematika Pasal 373–379, yang mengatur tentang pelanggaran akses tidak sah, penyadapan tidak sah, manipulasi sistem dan data, penyalahgunaan nama domain, dan pornografi anak.

Hukum Positif Indonesia Mengatur Kejahatan Dunia Maya

Akademisi hukum terus berdebat tentang kejahatan dunia maya. Hal ini disebabkan karena jenis kejahatan ini masih tergolong baru. Efektivitas hukum pidana positif (KUHP dan KUHAP) dalam menangani kejahatan ini telah didukung dan dikecam. Penegak hukum akan menangkap pelaku kejahatan dunia maya. Kejahatan dunia maya masih dituntut berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP), terutama yang sesuai dengan ketentuan pasal-pasal yang tidak lazim dalam KUHP. Banyak perangkat hukum pidana di luar KUHP yang dapat digunakan untuk menyelesaikan kejahatan melalui penggunaan teknologi ini ketika dianggap tidak cukup untuk mencegah berbagai jenis kejahatan daring. Berbagai pendekatan terhadap berbagai hukum hukum dicakup oleh perangkat ini. Peneliti akan terlebih dahulu meneliti komponen-komponen kejahatan dunia maya yang tercantum dalam KUHP untuk menyelidiki bagaimana kejahatan dunia maya ditangani berdasarkan undang-undang Indonesia. Karena istilah "kejahatan dunia maya" mencakup berbagai macam perilaku, para ahli telah mendefinisikan frasa tersebut dan akan menyarankan jenis-jenis kejahatan dunia maya lainnya. Saat ini, kejahatan seperti kejahatan dunia maya, perdagangan manusia, korupsi, dan kekerasan dalam rumah tangga diatur berdasarkan undang-undang yang berbeda dari KUHP. Kitab Undang-Undang Hukum Pidana berfungsi sebagai acuan untuk melihat unsur-unsur pidana apabila undang-undang berikutnya yang mengatur tindak pidana yang sama tidak menjelaskannya. Menurut hukum pidana, suatu perbuatan jahat dianggap sebagai kejahatan jika dinyatakan demikian dan pelakunya dapat dihukum. "Dapat dihukum" dan "bagian dari kenyataan" adalah kata-kata Belanda untuk "perbuatan pidana," atau "strafbaarfeit."

Berikut tindakan kejahatan dunia maya (cybercrime) yang di atur dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang undang No. 19 Tahun 2016 tentang Perubahan atas Undang undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagai berikut:

1. Perbuatan tercela secara moral. Misalnya, “Setiap orang yang dengan sengaja dan tanpa hak membagikan, mendistribusikan, atau membuat dapat diaksesnya Informasi Elektronik atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan” didefinisikan dalam Pasal 27 ayat (1) Undang-Undang Nomor 11 Tahun 2008. Namun, Undang-Undang Nomor 11 Tahun 2008 tidak mengatur perbuatan membagikan, menerbitkan, atau memproduksi konten informasi atau dokumen elektronik yang tidak bermoral. Kitab Undang-Undang Hukum Pidana digunakan apabila terjadi pelanggaran etika atau kesusilaan melalui media daring.
   Undang-Undang Nomor 11 Tahun 2008 Pasal 27 ayat (1) mengatur tentang informasi

dan transaksi elektronik, termasuk pornografi daring dan prostitusi daring, terkait dengan perbuatan yang menyebarkan kemaksiatan melalui media elektronik. Tindak pidana ini akan jauh lebih berat jika dilakukan terhadap anak di bawah umur. Maraknya situs-situs yang memuat konten pornografi merupakan salah satu masalah yang ditimbulkan oleh kemajuan teknologi informasi melalui internet. Tampaknya saat ini upaya melindungi internet dari gangguan para pedagang hiburan yang menjual pornografi menjadi tantangan yang sangat besar.

2. Perjudian Undang-Undang Informasi dan Transaksi Elektronik Pasal 27 ayat (2) mengatur tentang perjudian daring. Peraturan tersebut selanjutnya menetapkan bahwa: "Setiap orang yang dengan sengaja dan tanpa hak membagikan/mendistribusikan/menyediakan informasi/dokumen elektronik yang memuat konten perjudian.
3. " Ucapan atau penghinaan yang bersifat fitnah Pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 melarang pencemaran nama baik dan penghinaan di dunia maya, dengan menyatakan bahwa "Setiap orang dengan sengaja dan tanpa hak membagikan/menyebarkan/menyediakan informasi elektronik/dokumen elektronik yang memuat muatan penghinaan atau pencemaran nama baik." Pembuat undang-undang menyamakan fitnah dengan penghinaan. Penghinaan merupakan tindakan tersendiri, dan salah satu bentuk penghinaan yang dimaksud adalah fitnah yang dilakukan oleh pembuat undang-undang itu sendiri. Yang mau mengarahkan perbuatan penghinaan dari media internet tersebut sebagai pencemaran. Dalam Bab XVI Buku II mengatur tentang perbuatan penghinaan dan pencemaran. Kejahatan penghinaan terdiri dari penghinaan umum dan penghinaan khusus. Penghinaan umum mengacu pada obyek harga diri dan derajat orang pribadi, meliputi pencemaran nama baik. Di sisi lain, penghinaan khusus adalah penghinaan yang secara terbuka (di depan umum) menargetkan kehormatan, nama baik, atau harga diri seseorang. Kolom komentar di dunia maya dapat berisi tindakan penghinaan atau pencemaran nama baik, terutama saat korban melihat nama, gambar, atau videonya sendiri. Untuk membuat pernyataan atau menghubungkan pernyataan tersebut dengan korban, pelaku juga dapat menulis kata-kata yang merendahkan atau memfitnah di kolom komentar.
4. Spionase siber merupakan salah satu bentuk kegiatan kriminal yang dilakukan dengan membobol sistem jaringan komputer milik target dengan tujuan memata- matai mereka.
5. Pemerasan dan sabotase siber (cyber extortion and sabotage) Data yang terkait dengan program komputer, sistem jaringan komputer, atau internet biasanya diganggu, dirusak, atau dihancurkan untuk melakukan kejahatan semacam ini. Kejahatan semacam ini biasanya dilakukan dengan menanam bom logika, virus komputer, atau program tertentu, yang mencegah data, program komputer, atau sistem jaringan komputer digunakan, berfungsi dengan benar, atau berjalan sama sekali, tetapi memungkinkan penjahat untuk memanipulasinya sesuai kebutuhan.
6. Pelanggaran hak kekayaan intelektual, atau pelanggaran terhadap kekayaan intelektual Metode operasi kejahatan ini adalah dengan menargetkan hak kekayaan intelektual daring milik orang lain.
7. Pelanggaran privasi, Jenis kejahatan ini biasanya menyasar informasi pribadi yang tersimpan dalam formulir komputer. Jika orang lain mengetahuinya, hal ini dapat mengakibatkan kerugian baik materiil maupun immaterial bagi korban, termasuk terungkapnya PIN ATM.

KESIMPULAN

Cybercrime merupakan ancaman nyata bagi keamanan informasi dan ketertiban hukum di era digitalisasi. Mengenai Indonesia, pengaturan mengenai cybercrime melalui Mengenai Informasi dan Transaksi Elektronik, Undang-Undang Nomor 11 Tahun 2008 (UU ITE), beserta perubahan-perubahannya, menjadi dasar hukum yang penting dalam menanggulangi kejahatan di dunia maya. Namun, pelaksanaan dan penegakan hukum terhadap cybercrime masih menghadapi berbagai tantangan, seperti ketidakjelasan norma hukum, kesenjangan kapasitas penegak hukum, serta kompleksitas teknis dari kejahatan yang bersifat lintas batas negara.

Pendekatan hukum pidana terhadap cybercrime di Indonesia cenderung bersifat reaktif dan belum sepenuhnya mampu melindungi korban secara optimal. Selain itu, kerja sama internasional yang belum terkoordinasi secara efektif memperlemah upaya pencegahan dan penindakan kejahatan siber yang transnasional. Oleh karena itu, dibutuhkan langkah- langkah konkret dalam bentuk reformasi regulasi, peningkatan kapasitas kelembagaan, serta penguatan mekanisme perlindungan hak-hak korban.

DAFTAR PUSTAKA

Adinda Lola Sarian. 2024. Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia, Al-Dalil : Jurnal Ilmu Sosial, Politik, dan Hukum 2 (2), 71-72

Azra Salsabilla, Jennifer Angelina. 2024 . Peran Hukum Pidana Dalam Menangani Kejahatan Siber pada Masa Sekarang: Tinjauan Terhadap Undang Undang Informasi Transaksi Elektronik, JERUMI: Journal of Education Religion Humanities and Multidiciplinary, 2 (2), 1550-1552.

Martini Idris, Serlika Aprita, Meirina Nurlani. 2024. PENGATURAN DAN PENEGAKAN HUKUM KEJAHATAN DUNIA MAYA (CYEBER CRIME) : HARMONISASI REVISI UNDANG-UNDANG ITE DAN KUHP, LEXLATA : Jurnal ilmiah ilmu hukum, 401

Miftakhur Rokhman Habibi-Isnatul Liviani. 2020. Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23(2), 413-421

Purnomo. 2018. KEBIJAKAN HUKUM TERHADAP KEJAHATAN CYBERCRIME DI ERA INFORMASI DAN MASYARAKAT VIRTUAL. 78.