I.dn.J.of Law 7(2): 281-287, Juni 2025
DOI: 10.35965/ijlf.v7i2.6240

Indonesian Journal of Legality of Law
e-ISSN : 2477-197X
https://postgraduate.universitasbosowa.ac.id/

KEJAHATAN *CYBERCRIME* DAN PENANGGULANGANNYA DALAM KERANGKA SISTEM HUKUM NASIONAL

Cybercrime and Its Countermeasures Within the Framework of the National Legal System

Hasirudin Hasri*, Mashendra, Hayun, Fias Nurul Nisa
Program Studi Ilmu Hukum Universitas Muhammadiyah Buton
*Email: alifhasirudin@gmail.com

Diterima: 10 April 2025/Disetujui: 30 Juni 2025

ABSTRAK

Kejahatan siber merupakan masalah yang signifikan di Indonesia dan berakar pada hukum global internasional. Meningkatnya kejahatan siber dipengaruhi oleh faktor penyebab yang sulit dibuktikan dengan bukti dalam kasus-kasus kejahatan siber. Ketika internet dapat diakses oleh siapa saja, individu dapat mengejar tujuan apa pun dengan menargetkan upaya mereka. Kejahatan siber adalah masalah yang lazim terjadi dan memerlukan penyelesaian melalui tindakan hukum yang ketat. Untuk mengatasi masalah kejahatan siber di Indonesia, pemerintah telah memberlakukan peraturan dan regulasi khusus yakni Undang Nomor 11 Tahun 2008 yang mengatur Informasi dan Transaksi Elektronik untuk memerangi kejahatan siber yang tidak hanya menangani situs-situs cabul atau pornografi, tetapi juga menetapkan peraturan untuk transaksi elektronik, sehingga memberikan kerangka hukum untuk hukum siber di Indonesia.

Kata Kunci: Kejahatan, *Cybercrime*, Sistem Hukum Nasional

ABSTRACT

Cybercrime is a significant problem in Indonesia and is rooted in international global law. The rise of Cybercrime is influenced by causal factors that are difficult to prove with evidence in Cybercrime cases. When the internet is accessible to anyone, individuals can pursue any goal by targeting their efforts. Cybercrime is a prevalent problem and requires resolution through strict legal action. To address the issue of Cybercrime in Indonesia, the government has enacted specific rules and regulations, namely Law Number 11 of 2008 governing Electronic Information and Transactions to combat Cybercrime that not only addresses obscene or pornographic websites, but also establishes regulations for electronic transactions, thus providing a legal framework for cyber law in Indonesia.

Keywords: *Crime, Cybercrime, National Legal System*

1. PENDAHULUAN

Meningkatnya kompleksitas dan keberadaan kejahatan siber di mana-mana membutuhkan kerangka hukum yang kuat dan fleksibel yang dapat secara efektif mencegah, menuntut, dan mengurangi berbagai bahayanya (Iqbal et al. 2023). Kejahatan siber, yang mencakup berbagai perilaku berbahaya yang dilakukan melalui jaringan digital, menghadirkan ancaman yang cukup besar bagi keamanan nasional, stabilitas ekonomi, dan privasi pribadi. Interkoneksi di seluruh dunia yang dimungkinkan oleh internet secara tidak sengaja telah menumbuhkan iklim yang mendukung tindakan kejahatan siber, sehingga membutuhkan upaya terpadu oleh legislator untuk mengembangkan prosedur dan kerangka kerja hukum yang komprehensif (Esen 2002). Kerangka hukum untuk kejahatan siber terus berubah, ditandai dengan isu-isu seperti komplikasi yurisdiksi, kemajuan teknis yang cepat, dan aspek global ancaman siber (Amoo et al. 2024). penanggulangan hukum yang kuat sangat penting untuk melindungi aset digital, menjaga kepercayaan publik terhadap sistem daring, dan mempromosikan pemanfaatan teknologi yang bertanggung jawab (Iqbal et al. 2023).

Memerangi kejahatan dunia maya dalam kerangka hukum nasional membutuhkan strategi komprehensif yang menggabungkan ketajaman teknologi dengan kecakapan hukum (Hunton 2010). Kualitas bukti digital yang bersifat sementara dan anonimitas yang disediakan oleh platform online menghambat pendekatan penegakan hukum konvensional, sehingga membutuhkan prosedur khusus untuk penyelidikan, atribusi, dan penuntutan (Arshad, Jantan, and Omolara 2019). Sifat internet yang tanpa batas memperparah masalah ini, memungkinkan peretas untuk beroperasi secara global, yang sering kali menghindari pemerintah nasional (Casino et al. 2022).

Dengan kemajuan teknologi, tantangan baru muncul, termasuk eksploitasi teknologi informasi yang jahat, juga dikenal sebagai kejahatan dunia maya, yang dapat merugikan orang lain. Penyusupan kejahatan siber ke dalam infrastruktur

publik pemerintah sangat mengkhawatirkan, karena mengakibatkan kerugian nasional dan mengganggu masyarakat luas. Kejahatan dunia maya adalah bentuk kontemporer dari kejahatan konvensional. Oleh karena itu, hukum publik yang mencakup yurisdiksi, etika aktivitas online, perlindungan konsumen, peraturan antimonopoli, persaingan usaha yang sehat, perpajakan, badan pengatur, perlindungan data, dan kejahatan siber, serta hukum privat yang mencakup hak kekayaan intelektual, e-commerce, kontrak siber, privasi, nama domain, dan asuransi, menjadi kerangka kerja dasar bagi negara untuk memerangi pelanggaran ini.

Jonathan Rosenoer mengkategorikan domain Cyberlaw ke dalam berbagai komponen, termasuk Hak Cipta, Merek Dagang, Pencemaran Nama Baik, Ujaran Kebencian, Peretasan, Virus, Akses Ilegal, Regulasi Sumber Daya Internet, Privasi, Kewajiban untuk Berhati-hati, Pertanggungjawaban Pidana, Masalah Prosedural, Kontrak Elektronik, Pornografi, Perampokan, Perlindungan Konsumen, E-Commerce, dan E-Pemerintahan (Rosenoer 2012).

Darrel C Menthe menegaskan bahwa: "Masyarakat berinteraksi dengan dunia maya dengan dua cara utama: dengan memasukkan informasi ke dalam dunia maya atau dengan mengekstrak informasi dari dunia maya." Dalam hukum dunia maya, ada dua entitas yang berbeda: pengunggah dan pengunduh. Dalam teori ini, pengunggah dan pengunduh berfungsi sebagai agen dalam pengumpulan informasi klasik: pengunggah menyimpan informasi di sebuah lokasi di dunia maya, sementara pengunduh mengaksesnya pada waktu yang berbeda. Mereka tidak perlu mengetahui identitas satu sama lain. Selain itu, pada Kongres PBB ke-X di Wina, Austria pada tahun 2000, wacana kejahatan dunia maya juga diakui sebagai kejahatan yang berhubungan dengan komputer karena memiliki jangkauan akses yang luar biasa. Secara teoritis, Menthe mengemukakan tiga deskripsi teoritis mengenai karakteristik khusus yang terdapat di dunia maya, yaitu;

1) The Theory of the Uploader and the Downloade Penafsiran daripada teori ini adalah suatu negara dapat melarang dalam wilayahnya, kegiatan upload dan download yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk uploading kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk downloading kegiatan perjudian tersebut. Minnesota adalah salah satu negara bagian pertama yang menggunakan jurisdiksi ini.
2) The Theory of Law of The Server Pendekatan ini memperlakukan server Dimana webpages secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah webpages yang berlokasi di server pada Stanford University tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila uploader berada dalam jurisdiksi asing. Kesulitan terhadap bentuk kenyataan pengendalian server.
3) The Theory of Internasional Spaces. Ruang siber dianggap sebagai dimensi keempat. Analogi ini tidak terletak pada kemiripan fisik, tetapi pada karakteristik internasional, khususnya kurangnya kedaulatan. 4 Undang-undang untuk menangkap pelaku terhalang oleh batas-batas yurisdiksi antar negara.

Semakin banyaknya kasus *Cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cybercrime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Penentuan sebagai tindak pidana merupakan kebijakan kriminal, yang menurut Sudarto sebagai usaha yang rasional dari masyarakat untuk menanggulangi kajahatan (Sudarto 2007). Di dalam kebijakan kriminal mencakup kebijakan hukum pidana yang disebut juga sebagai kebijakan penanggulangan kejahatan dengan hukum pidana, karena di samping dengan hukum pidana untuk menanggulangi kejahatan, dapat dengan sarana-sarana non-hukum pidana. Hukum pidana selaku fungsi kontrol sosial digunakan untuk memberantas tindak pidana berbentuk pelanggaran norma terkait penggunaan teknologi informasi yang berpotensi pidana, buat melindungi masyarakat dari bahaya tindak pidana tersebut (Mulya et al. 2021).

Korupsi tidak mustahil diredakan sekiranya semua pihak turut benar-benar komited dalam membasmi. Suatu kejahatan apabila tidak dilakukan pembasmian atau penanggulangan, maka secara kriminologis akan memberikan beberapa dampak buruk, antara lain: (1) meningkatnya kejahatan, baik dari aspek kuantitas maupun kualitas; (2) memunculkan bentuk-bentuk kejahatan baru di luar perhitungan umat manusia, yang bisa saja merupakan derivasi dari "kejahatan konservatif"; dan (3) tidak dapat teridentifikasinya sebuah kejahatan sebagai kejahatan (Mubarok 2019).

Keberhasilan pembangunan suatu negara memerlukan persyaratan ketahanan negara dan dukungan otorisasi masyarakat, yaitu suatu keadaan menghindari gangguan-gangguan dan ancaman-ancaman, termasuk bentuk kejahatan. Seiring dengan kemajuan dan perkembangan ilmu pengetahuan dan teknologi dalam masyarakat, hal ini juga berlaku bagi perkembangan kejahatan (Didenko 2020). Kejahatan yang dilakukan tidak lagi dengan cara tradisional, namun sudah memanfaatkan dan menggunakan peluang yang disediakan oleh kemudahan instrumen modern dengan peralatan yang canggih (Rosenoer 2012). Kejahatan ini merupakan kejahatan baru. Yang dimaksud dengan kejahatan yang berkaitan dengan perkembangan sosial bidang ekonomi dalam masyarakat industri yang pelakunya adalah orang- orang kaya, berilmu, dan terorganisir (termasuk dalam white collar crime).

Mobilitas kejahatan yang tinggi tidak hanya terjadi di dalam satu wilayah, tetapi juga antar wilayah, bahkan lintas wilayah dan lintas batas negara. Modus operasinya menggunakan peralatan yang kompleks untuk memanfaatkan sepenuhnya kelemahan sistem hukum dan peluang sistem manajemen. Korban bukan lagi seorang individu, melainkan penyerangan terhadap suatu kelompok masyarakat, bahkan negara, dan kemungkinan korban juga tidak menyadari jikalau dirugikan (Gosita 2010).

2. METODE

Penelitian ini merupakan jenis penelitian normatif-empiris dengan menggunakan pendekatan kualitatif. Penelitian normatif-empiris merupakan penelitian hukum yang dilengkapi dengan data empirik atau dapat disimpulkan bahwa penelitian normatif-empiris adalah jenis penelitian hukum normatif yang didukung dan dilengkapi dengan data empirik (Irwansyah,

2020). Data empirik tersebut diperoleh dari hasil penelitian yang dilakukan di lapangan. Metode yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mengeksplorasi berbagai aspek peraturan perundang-undangan terkait cyber-crime.

Jenis data yang digunakan dalam penelitian ini terdiri dari 2 (dua) yaitu data primer dan data sekunder. 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 (Effendi and Ibrahim 2020).

Metode pengumpulan data (Sugiyono 2013). dilakukan dengan mengumpulkan dokumen (baik dokumen tertulis maupun dokumen elektronik) dari jurnal, artikel, makalah, dan lain-lain. Data-data yang terkumpul kemudian dibandingkan dan diseleksi untuk ditampilkan dalam penulisan ini. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan cyber law di Indonesia. Pendekatan yang dipergunakan adalah pendekatan perundang-undangan dan pendekatan konseptual (Soekanto 2007).

Setelah keseluruhan data dan informasi yang dibutuhkan dalam terkumpul, peneliti kemudian menggunakan perangkat teori, konsep, atau peraturan perundang-undangan yang berlaku dan relevan untuk menganalisis semua data, baik primer maupun sekunder, hal tersebut dilakukan untuk membahas atau memberikan jawaban terhadap permasalahan yang ditemukan di lapangan. Dengan tujuan agar permasalahan dalam penelitian ini dapat terjawab dengan baik.

3. HASIL DAN PEMBAHASAN

3.1. Pengaturan *Cybercrime* Dalam Sistem Hukum Pidana Indonesia

Dalam *Cybercrime* dunia itu adalah sempit sebab bisa dijangkau dengan singkat dan cepat. Rentannya pelanggaran yang seringkali diakibatkan oleh *Cybercrime* masyarakat awam berpendapat bahkan ada yang sengaja mentafsirkan sulit dijerat hukum karena hukum dan pengadilan di Negara Indonesia tidak mempunyai yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi melalui teknologi secara sahih.

Namun demikian kejahatan yang diakibatkan oleh peralatan teknologi adalah tetap disebut suatu pelanggaran hukum bersifat transnasional yang berdampak pada inplikasi hukum di Indonesia. Maka, setidaknya kita mengacu pada hukum internasional kalau kita menggagas betapa kekuatan hukum berupa Undang-Undang Informasi dan Transaksi Elektronik dan menyelaraskan KUHP. Dalam hukum internasional untuk menemukan yurisdiksi tentang cyberlaw terdapat tiga jenis yurisdiksi antara lain: yurisdiksi untuk menetapkan undang-undang (the jurisdiction to prescribe), yurisdiksi untuk penegakan hukum (the jurisdiction to enforce), dan yurisdiksi untuk menuntut (the jurisdiction to adjudicate) (Hafidz 2014).

Yurisdiksi adalah berlakunya hukum pidana menurut tempat yang sesungguhnya sudah tertera dalam KUHP yang didasarkan pada asas territorial, asas personal (nasional aktif) dan asas perlindungan (nasional pasif) serta asas universal. Karena itu undang-undang khusus di luar KUHP tidak perlu membuat aturan tersendiri kecuali akan mengatur hal khusus yang belum diatur oleh KUHP. Sementara kita melihat dasar Undang-Undang Telekomunikasi, Undang-Undang No. 36 Tahun 1999 Pasal 3, disebutkan bahwa “Telekomunikasi diselenggarakan dengan tujuan untuk mendukung persatuan dan kesatuan bangsa, meningkatkan kesejahteraan dan kemakmuran rakyat secara adil dan merata, mendukung kehidupan ekonomi dan kegiatan pemerintahan, serta meningkatkan hubungan antar bangsa”.

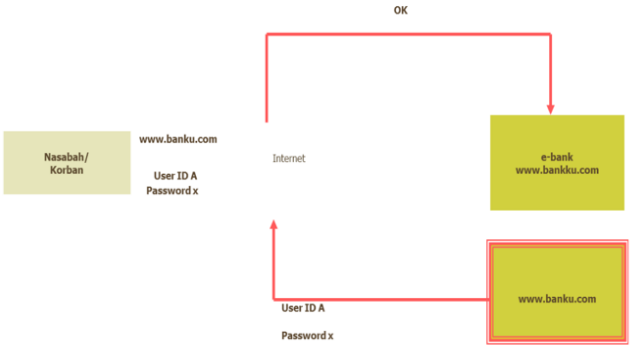
Lahirnya Undang-Undang tersebut telah merubah sistem telekomunikasi di Indonesia yaitu: Telekomunikasi adalah salah satu infrastruktur penting dalam kehidupan berbangsa dan bernegara. Perkembangan teknologi yang sangat pesat tidak hanya terbatas pada lingkup telekomunikasi itu saja, malainkan sudah berkembang pada TI. Dan perkembangan teknologi telekomunikasi dituntut untuk mengikuti norma dan kebijaksanaan yang ada di Indonesia. Artinya bahwa locus itu bisa menjadi catatan hukum penting dalam menguak para pelaku *Cybercrime* yang bergentayangan selama ini. Locus delicate menurut Balck’s Law Dictionaryadalah the place where offense is commiteted: the place where the last event necessary to make the actor liable occurs (Henningsen et al. 2019). Bahwa Locus delicate merupakan tempat dimana suatu tindak pidana terjadi; suatu tempat dimana peristiwa kejadian (tindak pidana) dapat menyebabkan pelaku harus bertanggungjawab.

Persoalanya adalah apakah tindak pidana *Cybercrime* tersebut terjadi di Indonesia atau bukan? Dan peradilan mana yang berhak dan berwenang untuk mengadili suatu perkara tersebut.Oleh sebab itu, disinilah KUHP tentang pidana berperan sesuai dengan perumusannya seperti yang tertera dalam pasal 2-8 KUHP yaitu; apakah pelanggaran pidana tersebut terjadi di muka umum, pekarangan tertentu, atau ditempat yang biasa dilalui orang, atau diatas perahu Indonesia atau kapal Indonesia dan lain sebagainya.Pandangan Utrecht, persoalan locus delicate dalam ilmu hukum pidana bersama dengan yurispundensi hukum pidana membuat tiga maacam teori yang bisa disebut sebagai kekuatan krusial untuk kita coba kupas perlakuan *Cybercrime* yang semakin marak di Indonesia (Utrecht 1966).

Pertama, teori pembuatan materiil. Locus delicatenya adalah tempat dimana pembuat melakukan segala perbuatan yang dapat mengakibatkan delik yang bersangkutan. Karenanya Locus delicate adalah tempat dimana perbuatan yang perlu ada supaya delik dapat terjadi.

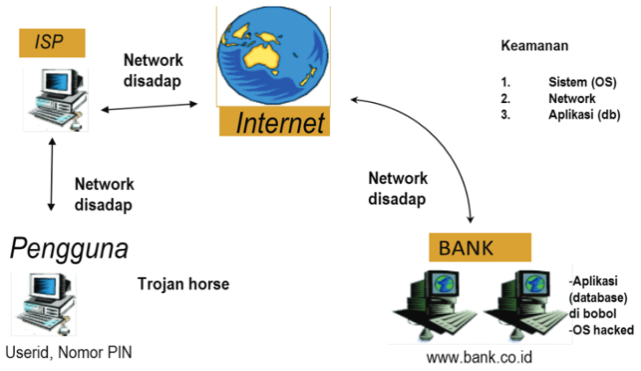
Kedua, teori alat yang dipergunakan. Delik dilakukan di tempat dimana alat yang dipergunakan itu menyelesaikannya. Dan ketiga adalah teori akibat. Disini locus delicate menjadi titik tekan dimana tempat akibat terjadinya. Kemudian perkembangan locus delicatebisa kita lihat dari perbandingan yang dikatakan E.Y Kanter dan Sianturi, bahwa perkembangan pola pikir manusia mencetuskan locus delicatebaru sebagai berikut: pertama, teori tindakan badaniah. Untuk menentukan tempat tindak pidana dibutuhkan teori tindakan badaniah dimana pelaku melakukan suatu tindak pidana, unsur-unsur tindak pidana pada saa itu bagaimana menjadi sempurna. Kedua, teori tempat bekerjanya alat. Locus delicatenya adalah dimana alat yang digunakan bekerja dan telah sempurna atau menimbulkan suatau tindakan pidana. Ketiga, teori akibat dari tindakan. Tempat tindak pidana adalah tempat terjadinya suatu akibat yang merupakan penyempurnaan dari tindak pidana yang telah terjadi. Keempat, teori berbagai tempat tindak pidana. Locus delicatenya adalah gabungan ketiga-tiganya teori atau dua di antara ajaran-ajaran tersebut. Yakni gabungan

antara beberapa teori berikut adalah teori perbuatan, teori alat yang digunakan, dan teori akibat. Disini penulis mencoba menyepakati apakah pendapat perkembangan locus delicate ini bisa menjadi perangkat untuk menelisik bentuk-bentuk tindak pidana dalam *Cybercrime* yang semakin lama semakin berkembang. Sehingga tindak pidana itu tidak terjadi dalam satu tempat saja melainkan di beberapa tempat seperti yang kerap terjadi dalam perlakuan *Cybercrime* lebih lanjut. Kasus typosit (situs palsu) misalnya, locus delicatedalam mencari yurisdis untuk melangkah ke tahap pidana selanjutnya dan untuk mendapatkan pelaku dimana dia berada, di tempat mana dia melakukan kejahatan tersebut. Kinerja kejahatan tersebut kalau kita kerangkakan dari berbagai sumber maka bisa kita lihat pada bagan di bawah ini.

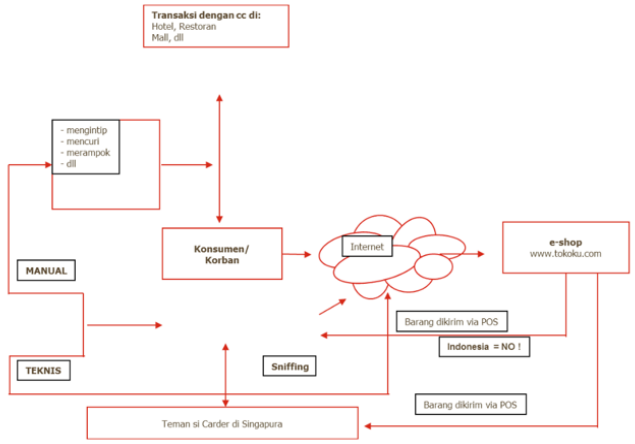


Gambar 1. Kerja dan Tempat Untuk Melakukan Kejahatan Typosit (Situs Palsu)

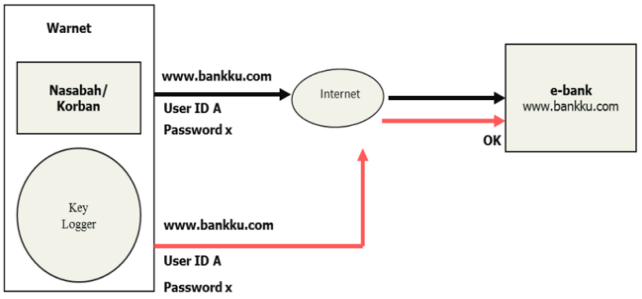
Sedangkan kalau kita mau melihat beberapa contoh kasus lain seperti kejahatan *Cybercrime* yang sering dilakukan melalu jejaring sosial lain seperti key-longger, E-banking, dan carding sebagai berikut.



Gambar 2. Kerja dan Tempat Untuk Melakukan Kejahatan E-banking



Gambar 3. Kerja dan Tempat Untuk Melakukan Kejahatan Carding



Gambar 4. Kerja dan Tempat Untuk Melakukan Kejahatan Key-Longger

Cybercrime dengan jalan demikian kerap terjadi dan jarang bisa ditemukan locus delicatenya. Peran hukum untuk menemukan tindak pidana diperlukan upaya penguatan konstruksi hukum yang sejalan dengan hukum internasional. Mengacu pada Undang-Undang ITE (Informasi Dan Transaksi Elektronik) Nomor 11 Tahun 2008 Presiden Republik Indonesia sebagai berikut: Menimbang:

1) Bahwa pembangunan nasional adalah salah satu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika di masyarakat.
2) Bahwa globalisasi informasi telah menempatkan indonesia sebagai bagian dari masyarakat informasi dan transaksi elektronik di tingkat nasional seentuk hingga pembangunan teknologi informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.
3) Bahwa perkembangan dan kemajuan teknologi informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru.
4) Bahwa penggunaan dan pemanfaatan teknologi informasi harus terus dikem-bangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perun-dang-undangan demi kepentingan nasional.
5) Bahwa pemanfaatan teknologi informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat.
6) Bahwa pemerintah perlu mendukung pengembangan teknologi informasi melalui infrastruktur hukum dan pengaturanya sehingga pemanfaatan teknologi informasi memperhatikan nilai-nilai agama dan sosial budaya masyarakat indonesia.
7) Bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f, perlu membentuk undang-undang tentang informasi dan transaksi elektronik.

Presiden Republik Indonesia dan Dewan Perwakilan Rakyat (DPR) telah memutuskan menetapkan, Undang-undang tentang Informasi Transaksi Elektronik pada tahun 2008 sebagai berikut:

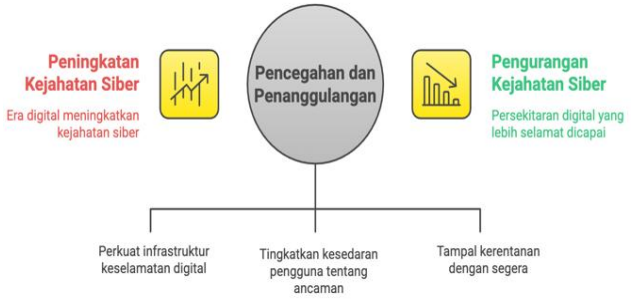
1) Bab I, tentang Ketentuan Umum
2) Bab II, tentang Asas dan Tujuan
3) Bab III, tentang informasi, dokumen, dan tanda tangan elektronik.
4) Bab IV, tentang penyelenggaran dan sertifikasi elektronik dan sistem elektronik.

5) Bab V, tentang transaksi elektroni.
6) Bab VI, tentang domain hak kekayaan intelektual, dan perlindungan hak pribadi.
7) Bab VII, tentang perbuatan yang dilarang.
8) Bab VIII, tentang penyelesain sengketa.
9) Bab IX, tentang peran pemersyaraintah dan Masyarakat.
10) Bab X, tentang penyidikan
11) Bab XI, tentang ketentuan pidana.
12) Bab XII, tentang ketentuan peralihan
13) Bab XIII, tentang ketentuan penutup

Persoalan hukum dalam mencari yurisdis untuk menindak *Cybercrime* adalah bagian dari upaya hukum untuk menguatkan kesepakatan dan sanksi hukum yang telah diputuskan pemerintah pada tahun 2008, sebagaimana Undang-Undang Informasi dan Transaksi Elektronik yang kita gunakan sekarang untuk menjerat para pelaku *Cybercrime* di Indonesia. Namun persoalan cyberlaw tersebut bersifat transnasional-internasional. Relevansi dari hukum tersebut apakah menjadikan Undang-Undang Informasi dan Transaksi Elektronik itu sudah bisa dijadikan alat hukum yang kuat dalam menemukan locus delicatenya yang mencakup yurisdis hukum dalam menangangi merebaknya kejahatan melalui dunia virtual atau penyelewengan terhadap fungsi internet tersebut? Bahwa merebaknya kejahatan yang dilakukan lewat jejaring sosial memang tidak bisa disamakan dengan kejahatan pada umumnya. Kejahatan tersebut cukup sulit dalam tahap penyelesaian nya sebab kejahatan Informasi dan Transaksi Elektronik adalah kejahatan tingkat modern yang syarat dengan kecanggihan sistem komunikasi yang membutuhkan kecerdasan seperangkat teknologi. Untuk memaksimalkan hukum tersebut agar tetap berjalan berdasarkan strandart etik dan hukum maka diperlukan dua hal. Pertama, adalah prinsip hukum. Pemerintah, swasta dan professional adalah unsur keterlibatan utama dalam memantau perkembangan teknologi di Indonesia. Kerjasama dalam memerangi *Cybercrime* antara pemerintah, swasta dan professional bukan hanya menjadi sinergitas melainkan upaya dan kewajiban bersama dalam rangka melindungi negara dari kejahatan yang dilakukan secara modern. Kedua, melakukan tinjauan hukum perundangan nasional yang terkait langsung maupun tidak langsung akibat munculnya persoalan yang ditimbulkan oleh perkembangan transaksi melalui teknologi-internet. Misalnya; Undang-Undang Hak Cipta, Undang-Undang Hak Merk, Undang-Undang Penyiaran, Undang-Undang Informasi dan Komunikasi, Undang-Undang Kontrak, Undang-Undang Perseroan Terbatas, Undang-Undang pidana, Undang-Undang Pajak, Undang-Undang Penanaman Modal Asing dan sebagainya, terkontrol kontinu setiap ada kasus yang diakibatkan oleh *Cybercrime*

3.2. Pencegahan dan Penanggulangan *Cybercrime*

Cybercrime atau kejahatan siber merupakan masalah yang semakin meningkat di era digital saat ini. Dengan kemajuan teknologi dan penggunaan internet yang meluas, kejahatan siber dapat terjadi dalam berbagai bentuk, mulai dari pencurian identitas, penipuan online, hingga serangan malware. Dokumen ini akan membahas langkah-langkah pencegahan dan penanggulangan yang dapat diambil untuk mengurangi risiko dan dampak dari *Cybercrime*.



Gambar 5. Resiko Kejahatan Cyber

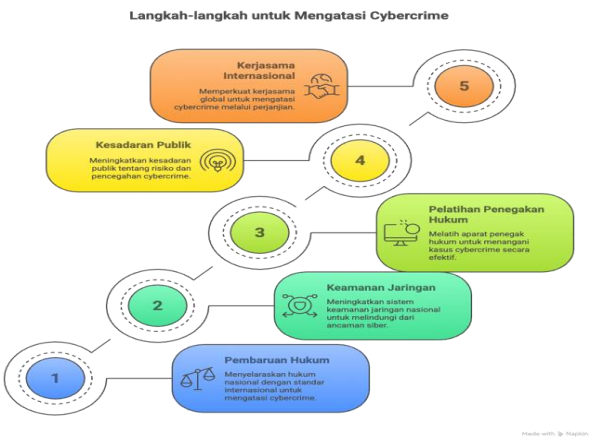
Berdasarkan Gambar 5. upaya pencegahan dan penanggulangan kejahatan siber di era digital. Di satu sisi, era digital menyebabkan peningkatan kejahatan siber, sementara di sisi lain, upaya yang tepat dapat mengarah pada pengurangan kejahatan siber dan terciptanya persekitaran digital yang lebih aman. Untuk mewujudkannya, perlu dilakukan penguatan infrastruktur keamanan digital, peningkatan kesadaran pengguna terhadap ancaman, serta penanganan segera terhadap kerentanan sistem.

Tindak pidana *Cybercrime* memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Kebanyakan dari korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman mereka saat ini, dan yang perlu dilakukan sekarang adalah mencegah kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan tersebut dapat berupa(Arifah 2011):

1) Educate user (memberikan pengetahuan baru tentang Cyber Crime dan dunia internet)
2) Use hacker's perspective (menggunakan pemikiran hacker untuk melindungi sistem anda)
3) Patch system (menutup lubang-lubang kelemahan pada sistem)
4) Policy (menetapkan kebijakan dan aturan untuk melindungi sistem Anda dari orang-orang yang tidak berwenang)
5) IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System)
6) Firewall.
7) AntiVirus.

Beberapa langkah penting yang harus diambil dalam menanggapi *Cybercrime* adalah:

1) Melakukan pembaruan hukum pidana nasional dan hukum acara, sesuai dengan kesepakatan internasional yang terkait dengan kejahatan tersebut.
2) Meningkatkan sistem keamanan jaringan computer nasional sesuai dengan standar internasional.
3) Meningkatkan pengetahuan dan keahlian aparat penegak hukum dalam upaya pencegahan, investigasi, dan penuntutan kasus-kasus yang berkaitan dengan *Cybercrime*.
4) Meningkatkan kesadaran warga negara tentang masalah *Cybercrime* dan pentingnya mencegah kejahatan itu terjadi.
5) Meningkatkan kerjasama dari berbagai negara, baik kerja sama bilateral, regional maupun multilateral dalam upaya mengatasi *Cybercrime*, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan timbal balik (mutual assistance treaties).



Gambar 6. Langkah Langkah Mengatasi Kejahatan Cyber

Gambar 6. tersebut menjelaskan langkah-langkah strategis untuk menghadapi kejahatan siber (*Cybercrime*) secara komprehensif. Langkah pertama adalah pembaruan hukum, yaitu menyelaraskan hukum nasional dengan standar internasional untuk mengatasi *Cybercrime*. Selanjutnya, keamanan jaringan ditingkatkan dengan membangun sistem yang mampu mendeteksi dan mencegah ancaman siber. Langkah ketiga adalah pelatihan penegakan hukum, agar aparat memiliki kemampuan dalam menangani kejahatan siber secara efektif. Peningkatan kesadaran publik menjadi langkah penting untuk mendorong keterlibatan masyarakat dalam pencegahan *Cybercrime*. Terakhir, kerja sama internasional diperkuat untuk mengatasi kejahatan siber yang bersifat lintas negara.

Beberapa contoh dari bentuk penanggulangan yang lain yaitu:

1) IDCERT (Indonesia Computer Emergency Response Team) Salah satu cara untuk membuat masalah keamanan lebih mudah ditangani adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Dengan munculnya "sendmail worm" (sekitar tahun 1988), masalah keamanan semacam ini mulai dikenali di luar negeri, ketika worm menutup sistem email Internet era itu. Selepasnya dibentuk sebuah (CERT) Computer Emergency Response Team, sejak itu di negara lain juga mulai membentuk CERT untuk dijadikan point of contact guna orang untuk mengadukan problem kemanan. IDCERT merupakan CERT Indonesia.
2) Sertifikasi perangkat security Peralatan yang dipakai guna membereskan keamanan harus memiliki tingkat karakteristik. Tentunya peralatan yang digunakan untuk tujuan pribadi berbeda dengan yang digunakan untuk tujuan militer. Tetapi sejauh ini di Indonesia belum ada institusi yang menangani problem evaluasi perangkat keamanan.

4. KESIMPULAN DAN SARAN

Hasil penelitian dapat disimpulkan bahwa *Cybercrime* cukup menyulitkan yurisdiksi hukum tapi bukan berarti tidak bisa ditangani ketika bukti itu ada. Alasan sulitnya adalah; pertama, kegiatan dunia cyber tidak dibatasi oleh teritorial Negara, Kedua, Kegiatan dunia cyber relatif tidak berwujud hingga secara hukum tradisional kadang sulit untuk menemukan bukti yang dapat disebut pembuktian karena data elektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan ke seluruh belahan dunia dalam hitungan detik.Demikian juga dengan apabila ada kejahatan dunia maya, pencurian bandwidth, carding, typosit, dan sebagainya apakah memungkinkan menghadirkan alat bukti dalam konteks cyberspace. Hardware hanya alat yang belum tentu bisa menjamin kepastian yurisdis dan ketetapan bukti hukum yang pasti. Dalam pembahasan perkembangan hukum pidana dimasa mendatang, penanggulangan dan pencegahan *Cybercrime* kudu diimbangi dengan pembenahan serta pengembangan seluruh sistem hukum pidana, yang meliputi pembangunan struktur, budaya, serta substansi hukum pidana. Dalam kondisi demikian, kebijakan hukum pidana menempati posisi yang strategis dalam kemajuan hukum pidana modern.

5. DAFTAR PUSTAKA

Amoo, Olukunle Oladipupo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Femi Osasona, and Benjamin Samson Ayinla. 2024. "The Legal Landscape of *Cybercrime*: A Review of Contemporary Issues in the Criminal Justice System." World Journal of Advanced Research and Reviews 21 (2): 205–17. DOI url: https://doi.org/10.30574/wjarr.2024.21.2.0438

Arifah, Dista Amalia. 2011. "Kasus *Cybercrime* Di Indonesia." Jurnal Bisnis Dan Ekonomi 18 (2).

Arshad, Humaira, Aman Jantan, and Esther Omolara. 2019. "Evidence Collection and Forensics on Social Networks: Research Challenges and Directions." Digital Investigation 28:126–38. https://doi.org/10.1016/j.diin.2019.02.001

Casino, Fran, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, and Constantinos Patsakis. 2022. "SoK: Cross-Border Criminal Investigations and Digital Evidence." Journal of Cybersecurity 8 (1): tyac014. https://doi.org/10.1093/cybsec/tyac014

Didenko, Anton N. 2020. "Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond." Uniform Law Review 25 (1): 125–67. https://doi.org/10.1093/ulr/unaa006

Effendi, Jonaedi, and Johnny Ibrahim. 2020. "Metode Penelitian Hukum Normatif Dan Empiris (Cetakan Ke)." Kencana.

Esen, Rita. 2002. "Cyber Crime: A Growing Problem." The Journal of Criminal Law 66 (3): 269–83.

Gosita, Arif. 2010. "Masalah Korban Kejahatan." BUKU DOSEN-2009.

Hafidz, Jawade. 2014. "Kajian Yuridis Dalam Antisipasi Kejahatan Cyber." Jurnal Pembaharuan Hukum 1 (1): 32–40

Henningsen, Mary Lynn Miller, Kathleen S Valde, Melissa J Entzminger, Daniel T Dick, and L Bryan Wilcher. 2019. "Student Disclosures about Academic Information: Student Privacy Rules and Boundaries." Communication Reports 32 (1): 29–42. https://doi.org/10.1080/08934215.2018.1556312

Hunton, Paul. 2010. "Cyber Crime and Security: A New Model of Law Enforcement Investigation." Policing: A Journal of Policy and Practice 4 (4): 385–95. https://doi.org/10.1093/police/paq038

Iqbal, Muhammad, Samar Raza Talpur, Amir Manzoor, Malik Muneeb Abid, Nazir Ahmad Shaikh, and Sanaullah Abbasi. 2023. "The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan." Siazga Research Journal 2 (4): 273–82.

Mubarok, Zaki. 2019. "Indonesia Legal Analysis of Iuu Fishing and Transnational Organized Fisheries Crimes: Loopholes and Proposed Measures." Indonesian Journal of International Law 17 (1): 113–37. https://doi.org/10.17304/ijil.vol17.1.780.

Mulya, Nurrachman Budi, Kadek Dwi Natasya Pradnyani, Ajeng Laras Wangi, Anggi Anggraeni Nugraha, and Tri Diana Rimadhani. 2021. "Analisis Peningkatan Jumlah Kasus Cyber Attack Di Indonesia Pada Masa Pandemi Covid-19." In Prosiding Seminar Nasional Teknologi Dan Sistem Informasi, 1:241–47. https://doi.org/10.33005/sitasi.v1i1.188

Prof. D. Sugiyono. 2013. "Metode Penelitian Kuantitatif Kualitatif Dan R&D." CV. Alfabeta, Bandung, x+334.

Rosenoer, Jonathan. 2012. CyberLaw: The Law of the Internet. Springer Science & Business Media.

Soekanto, Soerjono. 2007. "Penelitian Hukum Normatif: Suatu Tinjauan Singkat."

Sudarto. 2007. Pidana Dan Hukum Pidana. Ind-Hill.

Utrecht, Ernst. 1966. "Pengantar Dalam Hukum Indonesia." (No Title).

Zainuddin Ali. 2015. Sosiologi Hukum. Sinar Grafika, Jakarta.

Zainuddin Ali. 2014. Metode Penelitian Hukum. Sinar Grafika, Jakarta.