**KORELASI Penggunaan Teknologi Dalam Penindakan Cybercrime di Indonesia**

Nasrulloh Ramadani

# Sekolah Tinggi Ilmu Hukum IBLAM, Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450

**Dewic Ratna**

# Sekolah Tinggi Ilmu Hukum IBLAM, Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450

**Abstrak**

Pemahaman kebijakan di bidang hukum pidana terhadap tindak pidana teknoloi informasi mengenai cyber crime dengan melakukan penindakan, penanganan dan juga analisa dari sudut pandang hukum pidana mengenai tindak pidana teknologi sangat berpengaruh terhadap penanganan kasus cyber crime. Baik di masa sekarang dan juga di masa depan. Penelitian ini dilakukan untuk mengetahui korelasi penggunaan teknologi di dalam penindangan cyber crime di Indonesia. Efektifitas dan efisiensi peran teknologi dan juga *virtual police* dalam melakuan penanganan tindakan kejahatan di dunia maya. Metode penelitian ini menggunakan metode normatif yang terfokus kepada kajian dari analisa kaidah hukum dari Peraturan Undang-Undang dengan menggunakan data-data primer dan juga sekunder serta tersier. Faktor kebijakan kriminalitas di dalam dunia maya terus diharmonisasikan dengan makin banyaknya kejahatan di dunia siber yang sekarang sangat maju dan canggih.

**Kata kunci: teknologi, cyber crime, virtual police**

**Abstract**

Understanding of policies in the field of criminal law regarding criminal acts of information technology regarding cyber crime by carrying out prosecution, handling and also analysis from a criminal law perspective regarding technological crimes greatly influences the handling of cyber crime cases. Both in the present and also in the future. This research was conducted to determine the correlation of the use of technology in the prosecution of cyber crime in Indonesia. The effectiveness and efficiency of the role of technology and also virtual police in handling crimes in cyberspace. This research method uses a normative method that focuses on the study of the analysis of the rule of law from laws and regulations using primary data as well as secondary and tertiary. The criminal policy factor in cyberspace continues to be harmonized with the increasing number of crimes in cyberspace which are now very advanced and sophisticated.

Keywords: technology, cyber crime, virtual police

**PENDAHULUAN**

Perkembangan di dunia teknologi dan informasi serta komunikasi sejatinya memberikan kemudahan dan efektifitas serta efisiensi di dalam kehidupan manusia. Semua aspek di dalam kehidupan akan sangat mudah dan juga efektif. Salah satu wujud dari perkembangan di dunia teknologi informasi tersebut adalah media internet yang bisa menghubungkan dunia tanpa adanya batasan (Raodia, 2019). Dan tentu saja hal ini juga memberikan perubahan di sisi sosial, budaya dan juga ekonomi yang cukup signifikan. Perkembangan positif bagi masyarakat tentu saja memberikan kemudahan di dalam semua hal. Mulai dari kepengurusan kependudukan hingga proses transaksi jual beli (Ismail, 2009). Ada positif, tentu ada dampak negatif. Perkembangan di dunia teknologi dan informasi ini memiliki dampak negatif yang tidak boleh dipandang sebelah mata. Dampak yang bisa memberikan kerugian bagi kehidupan masyarakat adalah kejahatan di dunia maya atau biasa disebut dengan *cyber crime* (Wahyudi, 2013)*.* Hal ini muncul dari ketidak sesuaian penggunaan yang bisa memberikan akibat munculnya tindak kejahatan atau kriminal yang akhirnya disebut dengan cyber crime atau kejahatan siber (Nawawi Arief, Kapita Selekta Hukum Pidana, 2003).

Lalu apa kejahatan siber atau cyber crime tersebut? Kejahatan dunia maya ini adalah sebuah fenomena baru yang muncul berupa tindak pidana dimana mampu memberikan dampak langsung dari sisi perkembangan teknologi informasi yang menggunakan media internet sebagai media utama dalam melakukan tindakan kejahatan tersebut. Perkembangan teknologi memudahkan perkembangan di dunia kejahatan. Ditambah lagi masyarakat belum terlalu melek akan perkembangan di dunia informasi dan teknologi tersebut.

Dengan perkembangan teknologi, maka kejahatan juga mengalami perkembangan. Dahulu tindak pidana atau kejahatan adalah sebuah tindakan yang terjadi kontak fisik diantara korban dan juga pelaku kejahatan tersebut. Namun sekarang ini tindak pidana atau kejahatan sudah mengalami transformasi sehingga tidak lagi ada kontak fisik diantara pelaku dan juga korban. Pelaku yang melakukan kejahatan di dunia maya, memakai teknologi seperti internet dan juga alat elektronik lain untuk melakukan kejahatannya tersebut(Indah & Sari, 2021).

Media internet memang bisa memberikan peluang yang positif bagi masyarakat. Namun di sisi lain bisa memberikan kemudahan pula bagi para pelaku untuk melakukan tindakan kejahatan. Apalagi tanpa adanya kontak fisik, membuat para pelaku bisa melakukannya tanpa perlu takut identitasnya terbongkar oleh korban. Kejahatan dunia maya ini lebih tersembungi dan bisa dilakukan menembus ruang dan waktu serta mempunyai jangkauan global yang luas. Hanya dengan jaringan internet dan juga peralatan elektronik yang mumpuni, maka pelaku kejahatan sudah bisa melakukan tindakan cyber crime dan memangsa sang korban(Alhakim & Sofia, 2021).

Perkembangan dunia cyber crime memang semakin pesat dengan semakin banyaknya istilah-istilah yang muncul seperti cyber money laundering, high tech white collar crime hingga online business crime. Di dalam dokumen PBB ada istilah-istilah lain seperti Dogpilling, Dixing hingga Doxware. Belum lagi kejahatan siber yang berhubungan dengan identitas seperti pelecehan seksual hingga roasing dan sextortion. Kejahatan di dunia siber paling banyak terjadi di Amerika Serikat, Inggris, Brazil, Jerman dan juga Spanyol serta India. Indonesia juga terdapat kasus kejahatan siber, namun belum sebanyak kasus di Amerika dan juga Inggris. Indonesia masih berada di luar 20 besar kejahatan siber terbesar di dunia.

Di era 90-an, menjadi kasus pertama atas kejahatan siber yang terjadi di Indonesia. Kasus ini membuat Tjandra Sugiono yang menggunakan nama domain dari Mustika Ratu yaitu [www.mustikaratu.com](http://www.mustikaratu.com) harus berurusan dengan hukum. Tjandra Sugiono terkena dakwaan Pasal 382 bis KUHP dan Pasal 48 ayat (1) Pasal 19 huruf b UU No. 5 Tahun 1999 mengenai Pelarangan Praktik Monopoli dan Persaingan Usaha yang Tidak Sehat. Pengadilan Negeri Jakarta Selatan memutuskan bahwa tidak ada bukti yang kuat sehingga Tjandra Sugiono bebas dari segala tuduhan dan juga dakwaan. Pada tahun 2013, Indonesia mendapatkan pengawasan yang jauh lebih besar dari otoritas tindak kejahatan dunia maya. Dan hasil ini didapat dari survey Akamai Technologies yang menyatakan bahwasanya Indonesia sebagai sumber hacking traffic paling besar di dunia. Bahkan Indonesia mampu mengalahkan China dalam survey tersebut. Hal ini diperkuat dengan data yang berisikan statistik tindak kejahatan dunia maya yang terjadi di tahun 2019 dimana ada sekitar 4.586 laporan yang terjadi hanya dalam kurun waktu 1 tahun saja. Beruntung di tahun 2020, menurun hingga 50% dari total laporan di than 2019.

Laporan-laporan ini lebih didominasi oleh kasus konten *hate speech* atau provokatif yang kerap terjadi di dunia maya seperti media sosial. Kasus ini berada di posisi puncak tindak pidana kejahatan dunia siber. Setelah itu kasus penipuan online dan juga pornografi serta akses ilegal menjadi kasus berikutnya yang memiliki jumlah laporan yang cukup banyak.Kejahatan di dunia siber tentu saja memiliki dampak yang signifikan. Masyarakat beranggapan bahwa Indonesia memiliki KUHP yang tidak bisa menjangkau kejahatan di dunia siber ini dimana merupakan tindak pidana baru. Hal ini yang membuat pemerintah harus mengeluarkan aturan-aturan mengenai kejahatan dunia maya atau cyber crime. Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE yang tertuang dalam Undang-Undang No. 19 Tahun 2016 yang berisi perubahan Undang-Undang No. 11 Tahun 2008

Di dalam melaukan antisipasi kejahatan dunia siber, Rancangan Undang-Undang Kitab Hukum Pidana diperluas guna menjaring kejahatan di dunia maya atau cyber crime sehingga bisa memberikan ketenangan bagi masyarakat, hukuman pidana kepada para pelaku kejahatan dunia siber ini kurang bijak (Widodo, 2015). Hal ini tentu saja dipengaruhi oleh karakteristik dari para pelaku kejahatan dan juga sistem pembinaan yang ada di Lembaga Pemasyarakatan. Praktis tujuan dari pemidanaan yang sesuai dengan Undang-Undang permasyarakatan tidak akan terpenuhi. Opsi lain dari hukuman tersebut adalah pidana kerja sosial dan atau pengawasan kepada para pelaku. Sementara pemikiran dari ada beberapa aspek yang bisa menjadi salah satu upaya dalam penanggulangan kejahatan siber terutama di Indonesia. Dan aspek tersebut terdiri dari:

1. Aspek Pertanggung jawaban pidana
2. Aspek Kriminalisasi
3. Aspek Yuridiksi

Kebijakan kriminalisasi sendiri adalah sebuah kebijakan dalam menetapkan sebuah perbuatan yang bukan merupakan tindakan pidana, namun menjadi sebuah tindak pidana. Kebijakan kriminalisasi ini bisa menetapkan dan juga merumuskan serta memformulasi perbuatan yang bisa termasuk ke dalam ranah pidana (Danuri & Suharnawi, 2017). Upaya dalam pembaharuan di ranah hukum tentu saja tidak bisa dilepaskan dari kebijakan publik di dalam proses pengendalian dan juga pembentukan pola sehingga masyarakat bisa diarahkan dan juga diatur sesuai dengan peraturan perundang-undangan. Dan tentu saja hal ini sangat penting bagi para perancang hukum dan juga kebijakan publik bisa menerbitkan peraturan yang bisa diimplementasikan secara meluas di segala bidang mulai dari sosial, ekonomi dan politik. (Hikmawati, 2016) Berbagai upaya dalam melakukan perlindungan kepada masyarakat dan juga upaya dalam meningkatkan kesejahteraan rakyat menjadi salah satu bagian dari kebijakan yang ditetapkan oleh para pemangku keputusan tersebut. Dan tentu saja upaya-upaya ini juga berhubungan dengan usaha dalam meminimalisir kejahatan. Pentingnya penanggulangan terhadap kejahatan ini tentu harus diintegrasi ke semua kebijakan sosial. Dan hal ini juga dituangkan dalam Kongres PBB ke-5 1975 yang digelar di Geneva .

Munculnya hukum pidana dan implementasinya ke dalam kehidupan masyarakat dalam mengatur warga agar bisa sejahtera, memiliki peran sebagai salah satu langkah kebijakan dalam menentukan suatu langkah yang sangat rasional. Dan tentu saja kebijakan yang diambil tidak bisa dipisahkan dari tujuan dan target dari kebijakan tersebut (Gani & Gani, 2019). Termasuk di dalamnya adalah penanggulangan tindak kejahatan atau kriminalisasi di dunia siber. Perkembangan teknologi informasi menjadi salah satu contoh kebijakan yang ditetapkan oleh pemerintah guna meningkatkan kesejahteraan di lingkungan masyarakat. Salah satunya adalah dengan kehadiran polisi virtual atau *virtual police.* Inovasi ini menjadi salah satu pelengkap dari tim siber milik kepolisian yang memiliki fungsi dan pekerjaan yang cukup mirip. Terdapat perbedaan diantara polisi siber dan *virtual police.* Polisi virtual atau *virtual police* lebih bertugas kepada upaya preventif atas tindak pidana kejahatan di dunia maya. Sementara polisi siber ini akan melakukan upaya penegakan hukum sesuai dengan Undang-Undang. Polisi siber sudah melakukan pendeteksian pelaku yang melakukan pelanggaran terhadap UU ITE tersebut (Situmeang, 2021).

Kebijakan mengenai penanggulangan kejahatan siber menurut pemikiran dari GP Hoefnagels bisa ditempung dengan beberapa cara, yaitu:

1. Penerapan Hukum Pidana sesuai Undang-Undang
2. Pencegahan tanpa menggunakan hukum pidana
3. Mengubah pandangan masyarakat mengenai kejahatan di dunia siber via media massa.

Penerapan hukum pidana ini bisa diklasifikasikan ke dalam penanggulangan dengan jalur penal. Sementara pencegahan tanpa menggunakan hukum pidana dan mempengaruhi pendapat masyarakat ditempuh dengan jalur non penal. Begitu pula dengan pendapat dari bahwa kebijakan kriminal merupakan sebuah usaha yang rasional dan terorganisir dalam penanggulangan kejahatan (Sugiswati, 2011). Kebijakan tersebut dilakukan dengan cara represif melalui sistem hukum pidana dengan pendekatan penal, Bisa pula dengan pendekatan non penal. Pendekatan dengan non penal ini memiliki cakupan di area pencegahan tindakan kejahatan yang cukup luas dan mencakup terhadap kebijakan dan praktek. Pendekatan ini adalah sebuah tindakan preventif seperti kode etik, hukum administrasi hingga pembaharuan di ranah hukum. Dan kebijakan ini memiliki perbedaan disetiap negara yang disesuaikan dengan budaya, sosial, politik dan intelektualitas dari negara tersebut(Sugiswati, 2011).

Sementara pendekatan dengan melalui cara penal tentu saja akan bersinggungan langsung dengan kriminalisasi yang mengatur ruang lingkup dengan sifat bertentangan dengan hukum dan juga sanksi serta pindaha. Sarana kebijakan ini bisa dilakukan dengan sarana penal yang harus melihat tujuan dari kebijakan sosial tersebut. Kebijakan mengenai kriminalisasi yang melalui pendekatan penal, tentu akan bersinggungan dengan tindakan kriminal tersebut dan mengatur ruang lingkup dari hukum pidana baik berupa sanksi dan juga tindakan. Kebijakan kriminalisasi ini tentu harus memperhatikan terhadap kebijakan sosial yaitu *social welfare* dan *social defence* (Hartanto, 2021)*.*

Pendekatan integral yaitu keseimbangan anara sarana penal dan non penal harus terjadi di dalam penanggulangan tindakan kejahatan. Tidak terkecuali dengan kejahatan di dunia siber atau cyber crime. Dari sudut pandang kriminalisasi, kebijakan yang cukup strategis di dalam sarana non penal ini adalah tindakan preventif. Dan kebijakan penal tetap diperlukan sebagai cara penanggulangan kejahatan dimana menjadi salah satu saranan yang menyalurkan rasa tidak puas dan tidak suka dari masyarakat serta kebencian sosial dari masyarakat. (Galih, 2019)

Kebijakan hukum dengan menggunakan sarana penal atau pidana ini bisa dilakukan dengan melakukan proses yang didalamnya terdiri dari 3 tahap yang terdiri dari

1. Tahap formulasi yang merupakan kebijakan legislatif
2. Tahap Aplikasi yang merupakan kebijakan yudikatif dan yudisial
3. Tahap Eksekusi yang merupakan kebijakan eksekutif dan administratif

Dari 3 aspek tersebut maka penegakan hukum dengan sarana penal ini memiliki kandungan 3 kekuasaan yang berasal dari kekuasaan legislatif, yudisial dan juga eksekutif. Kekuasaan yang menerapkan dan merumuskan hukum pidana dari aparat penegak hukum atau pengadilan ini termasuk ke dalam kekuasaan yudisial atau yudikatif. Sementara kekuasaan legislatif ini akan merumuskan perbuatan yang bisa disanksi oleh hukum pidana dengan orientasi terhadap permasalahan pokok di dalam hukum tersebut. Sementara kekuasaan eksekutif bisa melaksanakan hukum pidana dari aparat pelaksana.

Dengan maraknya kejahatan siber, tentu saja keamanan dan pertahanan di ruang siber harus mendapatkan perhatian dan juga perlindungan yang layak. Hal ini tentu saja guna menghindari potensi yang bisa merugikan sisi pribadi dan juga organisasi serta negara. Pertahanan siber tentu menjadi salah satu tindakan dan penanggulangan dengan memaksimalkan teknologi guna mengatasi kejahatan di dunia siber. Pertahanan siber memiliki tingkatan dari lingkup individu, kelompok kerja hingga organisasi yang memiliki skala nasional. Perhatian khusus harus diberikan kepada sektor tersebut yang mengelola sisi infrastruktur yang didalamnya terdapat pertahanan keamanan, energi hingga sistem keuangan dan juga transportasi (Djanggih & Qamar, 2018).

Landasan dari pertahanan siber ini yaitu Undang-Undang No. 3 Tahun 2002 mengenai Pertahanan Negara yang menyatakan bahwasanya pertahanan negara ini memiliki tujuan guna menjaga dan melindungi kedaulatan negara dan juga keutuhan Negara Kesatuan Republik Indonesia. Dan bukan hanya dari sisi keselamatan militer saja. Namun keselamatan nir militer atau non militer juga menjadi perhatian dari pertahanan siber ini. Sementara peraturan Undang-Undang No. 11 Tahun 2008 yang membahas mengenai Informasi dan Transaksi Elektronik menyatakan bahwa pemanfaatan teknologi informasi memerlukan pengamanan dalam rangka menjaga keutuhan bangsa dan juga informasi. Di dalam Undang-Undang ini, semua informasi yang tersaji secara elektronik secara sah diakui di dalam hukum dan juga perbuatan yang berhubungan dengan sistem elektronik tersebut.

**METODE PENELITIAN**

Penelitian menggunakan metode hukum normatif yang akan menitik beratkan kajian melalui analisa kaidah hukum yang dilakukan dengan 3 pendekatan yang terdiri dari pendekatan konseptual dan kasus serta Undang-Undang. Untuk *purposive sampling* atau pengambilan data ini berupa data primer dan sekunder serta data-data tersier. Penelitian ini akan dianalisa secara deskriptif kualitatif dengan perbandingan antara teori dan juga fakta yang ditemukan di lapangan. Pendataan dilakukan dengan studi dokumen dan juga kajian pustaka dengan bahan-bahan data penelitian yang didapatkan selama proses penelitian tersebut.

**HASIL PENELITIAN DAN PEMBAHASAN**

Tindak pidana di bidang teknologi informasi menurut kebijakan hukum pidana dan juga hukum positif, memiliki definisi sebagai tindakan yang melanggar dari ketentuan hukum. Sementara kebijakan hukum pidana sendiri memiliki dasar umum yang berfungsi sebagai pengarahan pemerintah dalam mengelola dan juga mengatur persoalan di tengah masyarakat dan juga permasalahan yang diatur dalam Undang-Undang serta pengaplikasian hukum.

Pemerintah yang didalamnya terdapat aparat penegak hukum tersebut, akan menyelesaikan segala macam permasalahan hukum yang mengatur peraturan perundang-undangan yang memiliki tujuan demi mewujudkan kesejahteraan dan juga keadilan di lingkungan masyarakat. Pemerintah akan mengelola peraturan perundang-undangan tersebut agar bisa diaplikasikan dalam menetapkan keamanan di lingkungan masyarakat (Gani & Gani, 2019). Hukum pidana di Indonesia ini merupakan sebuah sarana yang diciptakan sebagai penanggulangan bentuk kejahatan yang bisa mengatasi semua permasalahan pidana yang mendasar. Hal ini bisa dillihat dengan praktek perundang-undangan yang menampilkan bahwasanya hukum pidana tersebut menjadi salah satu bagian dari kebijakan politik hukum di Indonesia yang bertujuan menjaga keamanan di lingkungan masyarakat. Hukum pidana tersebut digunakan oleh aparat penegak hukum dengan kondisi yang eksistensinya tidak lagi dipermasalahkan di kalangan masyarakat.

Di dalam KUHP yang menjadi sistem peradilan pidana di Indonesia ini memiliki sifat yang konvensional. Dan di dalamnya belum ada perkembangan untuk kejahatan di dunia siber. Ada beberapa peraturang perundang-undangan yang mengatur mengenai kejahatan di dunia siber dan juga berhubungan dengan tindak pidana. Namun berada di luar pengaturan dari Kitab Undang-Undang Hukum Pidana tersebut. Peraturan Perundang-undangan tersebut adalah:

1. UU No. 36 Tahun 1999 mengenai Telekomunikasi
2. UU No. 19 Tahun 2002 mengenai Hak Cipta
3. UU No. 25 Thaun 2003 mengenai Perubahan Undang-Undang No. 15 Tahun 2002 mengenai Tindak Pidana Pencucian Uang
4. UU No. 15 Tahun 2003 mengenai Tindak Pidana Terorisme
5. UU No. 19 Tahun 2016 mengenai Perubahan Undang-Undang No. 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik.

Semakin maraknya kejahatan dunia siber atau cyber crime ini tentu saja membuat pemerintah menerbitkan peraturan yang khususmengatu mengenai tindak pidana teknologi informasi dengan mengeluarkan Undang-Undang No. 19 Tahun 2016. UU ITE ini tentu saja memiliki sebuah harapan yang bisa menjadi kekuatan dalam mengatasi kejahatan dunia siber atau cyber crime. Dari sisi sosiologi, masyarakat memerlukan sebuah peraturan yang bisa menjadi landasan dan acuan hukum yang real dan nyata mengenai peraturan di bidang teknologi informasi tersebut. Sebelum dikeluarkannya Undang-Undang tersebut, peraturan yang ada di lingkungan masyarakat hanya berhubungan dengan dunia informasi dan teknologi semata. Belum ada penjelasan dan penjabaran mengenai sanksi pidana serta penjelasan yang jauh lebih konkrit mengenai dunia tersebut. UU ITE ini mengatur berbagai macam aktifitas masyarakat ketika berinteraksi di dunia maya (Abidin, 2015).

UU ITE sendiri memenuhi syarat sosiologis dan juga filosofis. Kehadiran landasan hukum di bidang filosofis ini terkandung di dalam UUD 1945 pada Pasal 28F yang berisi bahwa setiap masyarakat berhak mendapatkan, mengolah, mencari dan mempunyai serta menyimpan hingga menyampaikan semua informasi dengan menggunakan semua saluran yang tersedia di lingkungan masyarakat tersebut. Tindak kejahatan dunia siber ini dimuat di dalam UU No 19 Tahun 2016 mengenai Perubahan UU No. 11 Tahun 2008 yang terdiri dari (Barda, 2005):

1. Pasal 27 ayat (1) UU No. 11 Tahun 2008, Setiap orang yang melakukan dengan sengaja tanpa hak melakukan pendistribusian dan atau melakukan transmisi sehingga bisa mengakses informasi yang melanggar ketentuan kesusilaan. Namun pada pasal ini tidak ditemukan mengenai kegiatan apa saja yang melanggar muatan kesusilaan Perubahan UU tersebut disebutkan bahwa cyber pornografi dan prostitusi online menjadi muatan yang melanggar kesusilaan (Mudadi & Barda Nawawi, 2010). Dan hukuman pidana akan jauh lebih berat jika terjadi pada anak dibawah umur.
2. Pencemaran nama baik, pencemaran dan penghinaan nama baik tertuang di dalam Pasal 27 ayat (3) UU No. 11 Tahun 2008 yang berbunyi jika setiap orang dengan sengaja dan tanpa hak melakukan pendistribusian dan transmisi yang berisi penghinaan dan pencemaran nama baik dengan diaksesnya informasi dan dokumen elektronik. Tindakan ini bisa ditemukan di dalam kolom komentar media sosial pada ruang siber. Pelaku tindak kejahatan tersebut bisa mendapatkan sanksi pidana
3. Perjudian online, salah satu tindak pidana yang termasuk ke dalam kejahatan siber adalah perjudian online yang diatur di dalam Pasal 27 Ayat (2) UU No. 11 Tahun 2008 yang berbunyi bahwa setiap individu yang dengan sengaja mendistribusi dan mentransmisi sehingga bisa mengakses informasi dan atau dokumen elektronik (Abdul Wahid & Labib, 2005)
4. Cyber stalking, tindakan pidana ini diatur di dalam Pasal 29 yang menyatakan bahwa setiap individu yang dengan sengaja dan tanpa hak mengirim informasi dan atau dokumen elektronik yang berisi ancaman kekerasan dan atau menyebarkan rasa takut kepada pribadi atau individu. Peraturan ini sama halnya dengan peraturan hukum di luar negeri dimana tindakan stalking ini berupa pelecehan, ancaman hingga menimbulkan rasa takut. Mulai dari mail bombs, obsence threatening email.
5. Pemerasan, tindakan pidana ini dituangkan dalam Pasal 27 ayat (4) yang berisi setiap individu yang dengan senagaj dan tanpa hak melakukan pendistribusian dan mentransmisi hingga bisa diaksesnya informasi dan atau dokumen elektronik dengan isi yang bermuatan pemerasan.
6. Ujaran kebencian, tindakan pidana ini diatur di dalam Pasal 28 ayat (2) yang menyatakan bahwasanya setiap individu yang menimbulkan rasa kebencian dan atau permusuhan terhadap individu serta kelompok masyarakat yang berlandaskan SARA.
7. Hoax, Penyebaran berita bohong atau hoax diatur di dalam Pasal 28 ayat (1) yang berbunyi setiap individu yang sengaja dan tanpa sengaja menyebarkan berita bohong serta menyesatkan publik hingga bisa merugikan konsumen dalam kegiatan transaksi elektronik (Suseno S, 2012)
8. Intersepsi, tindakan ni diatur di dalam Pasal 31 yang terdiri dari beberapa perbuatan, yaitu:
   1. Setiap individu yang dengan dan atau tanpa sengaja melawan hukum dan melakukan intersepsi penyadapan atas informasi dan dokumen elektronik dari individu atau lembaga
   2. Setiap individu yang melakukan intersepsi dan melawan hukum yang tidak bersiat publik dari, ke dan di dalam alat elektronik milik pihak lain yang tidak menyebabkan perubahan hingga hilangnya informasi dan atau dokumen elektronik.
   3. Intersepsi yang dilakukan oleh penegakan hukum sesuai permintaan dari aparat penegak hukum, diperbolehkan dilakukan. S
9. Akses ilegal, pada pasal 30 UU No. 11 Tahun 2008 menyebutkan beberapa klasifikasi di dalam akses ilegal tersebut, yaitu:
   1. Setiap individu yang dengan sengaja melawan hukum dengan mengakses alat elektronik milik pihak lain
   2. Setia individu yang dengan sengaja mengakses data elektronik dengan tujuan mendapatkan informasi dan dokumen elektronik
   3. Setiap individu yang mengakses dokumen milik pihak lain dengan cara menjebol dan menerobos hingga melanggar sistem keamanan
10. Kejahatan terhadap informasi Data Interference dituangkan di dalam Pasal 32 UU No. 11 Tahun 2008 yang terdiri dari:
    1. Setiap individu yang melawan hukum dengan mengubah sebuah informasi dan dokumen elektronik milik pihak lain baik individu atau publik
    2. Setiap individu yang melawan hukum dengan melakukan pemindahan data dan informasi tanpa izin
    3. Perbuatan yan bisa mengakibatkan terbukanya rahasia negara yang bisa diakses publik
11. Gangguang terhadap sistem siber tertuang dalam Pasal 33 dimana disebutkan bahwa setiap individu yang melawan hukum dengan tindakan yang bisa mengakibatkan gangguang di ruang siber sehingga tidak bisa bekerja sebagaimana mestinya
12. Penyalah gunaan perangkat, disebutkan di dalam Pasal 34 yang berupa perubahan terhadap sandi di sistem keamanan siber dan juga kode akses yang bisa merugikan pihak lain. Akan tetapi tindakan tersebut tidak termasuk ke dalam ranah pidana jika ditujukan sebagai penelitian dan pengujian sistem elektronik.
13. Pemalsuan dan penipuan yang tertuang dalam Pasal 35 yang menyatakan bahwa setiap individu yang dengan sengaja melakukan manipulasi, pemalsuan hingga perusakan dan juga penipuan informasi dan atau dokumen elektronik yang dianggap sebagai data otentik.

Kejahatan di dunia siber atau disebut pula dengan cyber crime ini memang selalu identik dengan computer crime. Bahkan menurut bahwa cyber crime ini merupakan kejahatan di bidang komputer yang dilakukan secara illegal (Hamzah, 1992). Tindakan ini termasuk ke dalam tindak pidana dengan beberapa klasifikasi yang terdiri dari:

1. Unauthorized access
2. Unauthorized alteration or destruction of data
3. Mengganggu dan merusak operasi komputer
4. Mencegah akses ke dalam komputer.

Klasifikasi kejahatan di dunia maya atau cyber crime ini memiliki beberapa klasifikasi yang ditentukan berdasarkan Convention on Cybercrime di Budapest, Hungaria yang terdiri dari:

1. Illegal Interception

Tindakan ini adalah secara sengaja menangkap pemancaran dan pengiriman data komputer yang bersifat rahasia dan bukan untuk konsumsi publik.

1. Data Interference

Sebuah tindakan yang dilakukan dengan sengaja seperti perusakan hingga penghapusan data-data dan atau dokumen serta informasi elektronik di dalam komputer serta ruang siber.

1. System Interference

Dengan sengaja melakukan gangguan atau rintangan yang menyebabkan sistem komputer tidak bisa berjalan atau berfungsi sebagaimana mestinya.

1. Misuse of Devive

Penyalahgunaan terhadap perlengkapan elektronik seperti program dan password komputer hingga kode akses

1. Computer Related Forgery

Sebuah tindakan pemalsuan yang dilakukan dengan sengaja sehingga mengubah dan menghapus data otentik menjadi tidak otentik sehingga data yang dipalsu menjadi data yang digunakan oleh publik.

1. Computer Related Fraud

Sebuah tindakan pidana penipuan dengan sengaja dan tanpa hak menyebabkan kekayaan dan atau barang dari pihak lain menghilang. Caranya dengan memasukkan dan menghapus data sehingga sistem komputer terganggu dengan maksud mendapatkan keuntngan pribadi.

1. Content Related Offences

Tindakan pidana yang berhubungan erat dengan dunia pornografi bagi anak-anak dibawah umur

1. Offences Related to Infringements of Copyright and Related Rights

Tindak pidana kejahatan siber yang berhubungan erat dengan pelanggaran hak cipta.

Sudah banyak kasus-kasus cyber crime yang ada di Indonesia. Mulai dari kasus pornografi yang cukup banyak kasus di Indonesia hingga penipuan dan juga pencemaran nama baik. Kasus pornografi yang menyeret sejumlah artis menjadi kasus yang sempat heboh ke jagat publik. Bahkan pelaku dan penyebar mendapatkan hukuman sesuai dengan Undang-Undang No. 11 Tahun 2008 tersebut.

Sementara kejahatan seperti Defacing atau perubahan situs milik pemerintah oleh *hacker* yang juga menghebohkan publik. Polisi siber melakukan penelusuran mengenai sosok *hacker* dengan melakukan penyelidikan menggunakan teknologi komputerisasi yang sudah dimiliki oleh aparat penegak hukum. Pelaku yang berasal dari Yogyakarta ini akhirnya berhasil dibekuk dengan cepat oleh polisi siber setelah mendapatkan data-data sang pelaku. Kerja sama *virtual police* dan juga polisi siber memberikan kemudahan dalam penangkapan sang pelaku.Kemudian kasus pencemaran nama baik juga menjadi salah satu kasus yang mencuat. Pencemaran melalui media sosial atau jejaring sosial merupakan kasus yang kerap terjadi dimana berhubungan dengan UU ITE tersebut. Pihak kepolisian melakukan upaya represif untuk melakukan penyelidikan dan penelusuran terkait tindakan pencemaran nama baik tersebut. Begitu pula dengan pencemaran dan berita hoax yang terkait dengan pemerintah dan juga Presiden.

Peran dari *virtual police* dan polisi siber dalam menjaga keamanan di dunia maya memang sangat dibutuhkan. *Virtual police* memiliki peran dalam menyajikan edukasi dan informasi kepada masyarakat mengenai Undang-Undang Informasi dan Transaksi Elektronik. Sementara polisi siber lebih berperan dalam melakukan tindak lanjut mengenai kasus yang beredar di masyarakat yang tidak bisa ditegur dan diperingatkan oleh *virtual police.* Secara aturan maka *virtual police* akan melakukan teguran dan peringatan terlebih dahulu. Setelah itu polisi siber akan melakukan tindakan jika teguran tersebut tidak diindahkan oleh pelaku.

Meski sudah memiliki tim siber dan juga didukung oleh teknologi, ternyata hal ini belum bisa membantu secara maksimal dalam penanggulangan kejahatan di dunia siber. Seringkali di dalam penelusuran dan penyelidikan, tidak diketemukan bukti yang cukup dan juga pelaku tidak terjaring diakibatkan akses yang cukup mudah dilakukan pelaku dengan menggunakan komputer dimana saja tanpa ada saksi. Polisi siber hanya bisa melakukan penelusuran IP Address. Jika pelaku menelusuri dari warnet, tingkat kesulitan untuk melacak akan lebih besar. Pasalnya tidak semua penyedia jasa warnet melakukan registrasi.

Dari penelusuran data-data primer melalui proses wawancara dan juga interview, ada beberapa kendala yang dirasakan oleh pihak penegak hukum yang terdiri dari:

1. Kendala di internal penegak hukum

Kurangnya tim khusus yang menangani permasalahan kejahatan di dunia maya. Ditambah lagi kesulitan dalam mengetahui keberadaan pelaku meski teknologi yang digunakan sudah cukup baik. Apalagi kemudahan pelaku dalam mengakses komputer dari manapun

1. Kendala eksternal

Kurangnya pemahaman dari aparat penega hukum lain mengenai kejahatan dunia siber. Izin dari ketua pengadilan dan juga penuntut umum terkadang tidak maksimal sehingga membuat tim siber sudah kehilangan jejak terlebih dahulu dalam melakukan penelusuran.

Teknologi jelas menjadi salah satu hal yang harus dipersiapkan oleh pemerintah. Bukan hanya membentuk tim khusus siber saja. Namun teknologi seperti pertahanan siber juga harus mendapatkan perhatian. Kementrian Pertahanan dan Tentara Nasional Indonesia mempunyai 2 kepentingan di dalam pengembangan pertahanan siber tersebut. Salah satunya adalah dengan mengamankan semua sistem elektronik dan informasi di lingkungan pemerintah. Jika situs KPU bisa dijebol dengan mudah oleh hacker anak negeri, tentu hacker dari luar Indonesia bisa dengan mudah melakukannya pula.

Kementrian Pertahanan dan Tentara Nasional Indonesia juga mendukung koordinasi pengamanan siber di semua sektor yang sesuai dengan kebutuhan dan juga yang memiliki sifat menjaga rahasia negara. Dari kedua kepentingan tersebut maka dibutuhkan antisipasi dalam kebutuhan pertahanan siber tersebut. Salah satunya adalah kebijakan yang menjadi landasan bagi pertahanan siber seperti pengembangan, koordinasi dan pengoperasian yang meliputi persiapan infrastruktur dan teknologi serta SDM hingga pran dan wewenang di lingkungan pemerintah.

Lembaga pemerintah yang kuat dan juga efektif tentu sangat dibutuhkan di dalam menjalankan perannya di pemerintah serta mendukung pertahanan siber yang mengacu kepada kebijakan-kebijakan di lembaga pemerintah. Teknologi dan juga infrastruktur harus mendukung akan kegiatan pertahanan siber sehingga bisa dilaksanakan dengan efektif dan juga efisien. Di lembaga-lembaga pemerintahan sudah tersedia sumber daya manusia yang terus dilatih agar bisa memiliki pengetahuan dan juga keterampilan khusus di dalam pertahanan siber tersebut.

Ada beberapa prinsip dari pertahanan siber menurut Permenhan No. 82 yang terdiri dari:

1. Mempunyai model pengamanan yang terstruktur dan juga berintegrasi dengan standar dan juga panduan informasi yang sudah ditetapkan oleh lembaga atau institusi yang memiliki wewenang
2. Faktor integritas dan kerahasiaan serta ketersediaan tersebut yang memiliki prinsip dasar akan keamanan informasi
3. Memiliki unsur kebijakan, kelembagaan serta teknologi serta infrastruktur pendukung seperti SDM yang memadai
4. Implementasi dari pertahanan siber ini didukung dengan SDM dengan kualitas, kompetensi dan integritas yang tinggi dan menjunjung kerahasiaan negara
5. Dilakukan dengan cara yang efektif dan efisien sehingga keamanan siber terintegrasi dengan memaksimalkan teknologi terbuka dalam rangka kedaulatan dan juga kemandirian negara
6. Pengamanan dan petahanan siber yang memiliki kategori atau kriteria SDM yang unggul dan berkompetensi
7. Memiliki prinsip tata kelola yang bisa mewujudkan pengawasan di dalam pertahanan siber tersebut
8. Menjamin implementasi pertahanan siber yang aman dan juga bisa menahan serangan dari pihak luar
9. Menghindari kerugian terhadap sistem komputer
10. Mengembangkan kondisi yang bisa menguntungkan pemerintah.

Pertahanan siber ini dimaksudkan untuk mencegah dari tindakan-tindakan kejahatan siber yang bisa saja terjadi kepada lembaga dan juga organisasi pemerintah. Pertahanan siber ini memiliki peran dan juga tugas yang terdiri dari;

1. Menjamin keamanan siber di lingkungan pemerintah dan masyarakat
2. Menjaga sumber daya informasi yang bersifat rahasia milik pemerintah
3. Menjaga keamanan infrastrukrut dan teknologi di lingkungan pemerintah
4. Mendorong partisipasi yang aktif dengan jaringan nasional dan internasional lintas sektor
5. Meningkatkan kemampuan dan penindakan terhadap kejahatan di dunia siber
6. Mengembangkan pertahanan siber yang efektif, efisien dan juga akuntable
7. Memiliki kemampuan dalam menjaga kerahasiaan milik negara dan juga keamanan jaringan strategis
8. Model pusat data dan juga sarana pendukung yang aman dalam menjaga informasi-informasi strategis.

**KESIMPULAN**

Penegakan hukum terhadap kejahatan cyber crime di Indonesia ini belum dilakukan dengan maksimal. Ada berbagai macam faktor yang mempengaruhi terhadap tindakan dan penegakan hukum tersebut. Baik dari sisi hukum, penegak hukum hingga sarana serta fasilitas di dalam penegakan hukum tersebut. Faktor hukum menjadi salahs atu titik lemah penegakan hukum terhadap kejahatan cyber crime di dalam anatomi kejahatan transnasional. Begitu pula dengan faktor penegak hukum.

Pemerintah harus menetapkan aturan hukum yang mengatur mengenai tindak pidana yang jelas dan juga terus diperbaharui seiring perkembangan zaman. Ditambah lagi pemerintah harus melek dengan perkembangan teknologi dan informasi. Pertahanan siber bisa menjadi salah satu langkah untuk melindungi dunia informasi dan teknologi yang tersebar di lingkungan masyarakat.

Pertahanan siber menjadi salah satu pilihan di sisi teknologi untuk mendukung penindakan kejahatan dunia siber di lingkungan pemerintah dan masyarakat. Seiring perkembangan zaman, tentu pemerintah harus melakukan pembaharuan terhadap pertahanan siber di lingkungan lembaga dan organisasi pemerintah agar tindak pidana kejahatan siber tidak menyerang dan mengakses tanpa izin data-data yang bersifat rahasia. Kebijaksanaan kriminalisasi terhadap kejahatan di dunia siber tentu saja harus diharmonisasi agar kejahatan dunia maya bisa dicegah dengan maksimal. Apalagi kejahatan dunia siber ini tidak mengenal batas, teritori dan juga waktu. Masyarakat juga harus mendapatkan informasi dan juga edukasi yang penting di dalam pemahaman antara *virtual police* dan juga polisi siber agar masyarakat bisa mengetahui apa saja klasifikasi di dalam kejahatan siber tersebut.

**Daftar Pustaka**

Abdul Wahid & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama.

Abidin, Z. (2015). “Kejahatan Dalam Teknologi nformasi Dan Komunikasi. *Jurnal Ilmiah Media Processor*, *10*(1), 509–516.

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377–385. https://ejournal.undiksha.ac.id/index.php/jatayu/article/view/38089

Barda, N. (2005). *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia.* PT Raja Grafindo Persada.

Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. *Informasi Komputer Akuntansi Dan Manajemen*, *13*(2), 55–65.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Galih, Y. S. (2019). *YURISDIKSI HUKUM PIDANA DALAM DUNIA MAYA*. *7*(1), 59–74.

Gani, H. A., & Gani, A. W. (2019). Penyelesaian Kasus Kejahatan Internet ( Cybercrime ) dalam Perspektif UU ITE No . 11 TAHUN 2008 dan UU No . 19 Tahun 2016. *Prosiding Seminar Nasional LP2M UNM - 2019*, *11*, 121–129.

Hamzah, A. (1992). *Aspek-aspek Pidana di Bidang Komputer*. Sinar Grafika.

Hartanto. (2021). Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku Cyber Crime Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE). *HERMENEUTIKA: Jurnal Ilmu Hukum*, *5*(2), 196–216. http://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

Hikmawati, P. (2016). Penegakan Hukum Terhadap Undang. Undang No. 11 Tahun 2Oo8 Tentang Informasi Dan Transaksi Elektronik. *Kajian*, *15*(2), 227–252. https://jurnal.dpr.go.id/index.php/kajian/article/view/424

Indah, U., & Sari, P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Mimbar Jurnal Hukum*, *2*(1). www.mustikaratu.com

Ismail, D. E. (2009). CYBER CRIME DI INDONESIA Dian. *INOVASI*, *6*(3), 242–247.

Mudadi & Barda Nawawi, T. (2010). *Teori-teori dan Kebijakan Pidana*. PT. Alumni Bandung.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2), 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Sasi*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Sugiswati, B. (2011). Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi. *Perspektif*, *16*(1), 59. https://doi.org/10.30742/perspektif.v16i1.70

Suseno S. (2012). *Yuridiksi Tindak Pidana Siber*. Refika Aditama.

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.

Widodo. (2015). *Memerangi cybercrime : karakteristik, motivasi, dan strategi penanganannya dalam perspektif kriminologi*. Aswaja Pressindo.