ANALISIS TERHADAP CYBER CRIME DALAM KAITANNYA DENGAN ASAS TERRITORIALITAS

Ikhsan Yusda PP
Dosen Jurusan Teknologi Informasi, Politeknik Negeri Padang
ikhsan_yusda@yahoo.com

ABSTRAK

Cyberspace adalah media yang tidak mengenal batas, baik batas-batas wilayah maupun batas kenegaraan, sehubungan dengan dunia maya (Cyber Crime) tentunya akan menimbulkan masalah tersendiri, khususnya berkenaan dengan masalah yurisdiksi. Yurisdiksi merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Hukum Internasional tradisional telah meletakkan beberapa prinsip umum yang berkaitan dengan yurisdiksi suatu negara, salahsatu prinsip itu adalah "Prinsip Teritorial". Berdasarkan prinsip ini setiap negara dapat menerapkan yurisdiksi nasionalnya terhadap semua orang (baik warga negara atau asing), badan hukum dan semua benda yang berada didalamnya. Berdasarkan uraian diatas, dapat dirumuskan pokok masalah sebagai berikut; bagaimanakah Yurisdiksi Hukum Pidana dalam kejahatan di Dunia Maya (Cyber Crime)?, dan bagaimanakah Kebijakan Kriminalisasi Terhadap Cyber Crime (Kejahatan Mayantara)?. Hasil yang didapat dari kajian ini adalah meningkatnya penggunaan internet disatu sisi memberikan kemudahan bagi manusia dalam melakukan aktivitasnya, disisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana. Munculnya kejahatan dengan mempergunakan internet sebagai alat bantunya (Cyber Crime) lebih banyak disebabkan oleh faktor keamanan sipelaku dalam melakukan kejahatan, masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam hal Cyber Crime,

***Kata kunci**: Cyber Space, Cyber Crime, Yurisdiksi, Prinsip Territorialitas, KUHP, Penegakan Hukum.*

ABSTRACT

Cyberspace is a medium that knows no boundaries, both boundaries and limits of the state, with respect to the virtual world (Cyber Crime) will certainly cause problems of its own, particularly with regard to the issue of jurisdiction. Jurisdiction is a reflection of the basic principles of sovereignty, equality state and non-interference principle. International law traditionally has laid some general principles relating to the jurisdiction of a country, one of the main principles are "Territorial Principle". Based on this principle of each country can apply its national jurisdiction against all persons (whether citizens or foreigners), legal entities and all things therein. Based on the description above, the basic problem can be formulated as follows; how the crime Criminal Law Jurisdiction in Cyberspace (Cyber Crime)?, and how Criminalization Policy Against Cyber Crime (Crime mayantara)?. The results obtained from this study is the increasing use of the Internet on the one hand makes it easy for people in their activities, on the other hand makes it easy for certain parties to the crime. The emergence of the Internet as a crime by using the kit (Cyber Crime) caused more by a safety factor sipelaku in committing a crime, the lack of law enforcement officers who have the capability in terms of Cyber Crime.

***Keywords**: Cyber Space, Cyber Crime, Jurisdiction, Territorial Principle, Criminal Code, Law Enforcement.*

1. Pendahuluan

1.1. Latar Belakang Masalah

Peradaban dunia pada masa kini ditandai dengan fenomena kemajuan informasi dan globalisasi yang berlangsung hampir di semua bidang kehidupan. Apa yang disebut dengan globalisasi pada dasarnya bermula dari awal abad ke-20 yakni pada saat terjadi revolusi transportasi bermula dari awal bad ke-20 yakni pada saat terjadi revolusi transportasi dan elektronika yang menyebar luaskan dan mempercepat perdagangan antar bangsa, , disamping pertambahan dan kecepatan lalu lintas barang dan jasa.

Revolusi terjadi diberbagai bidang kehidupan manusia seperti industri, budaya, pendidikan, teknologi, sistem informasi dan lain-lain. Sebagaimana yang pernah terjadi sebelumnya, revolusi kali ini juga membawa perubahan yang cepat dan cenderung mengubah nilai-nilai dan paradigma lama yang baku.

Dalam masa revolusi, kecepatan menjadi faktor yang paling utama, sehingga muncul pernyataan "siapa yang cepat ia yang

dapat", siapa yang unggul dalam kecepatan maka ia akan memenangkan segalanya. Hal ini juga semakin menguatkan hipotesis *The Winner Takes All* yang kurang lebih menyiratkan makna bahwa yang kaya semakin kaya, sementara yang miskin tetap saja miskin. Begitu juga halnya dengan Revolusi Teknologi Informasi.

Revolusi teknologi informasi berawal sejak ditemukannya komputer yang dalam perkembangannya menciptakan suatu dunia tersendiri yang lazim disebut dengan dunia maya. Kemajuan dan perkembangan teknologi, khususnya telekomunikasi, multi media dan teknologi informasi (telematika) pada akhirnya akan mengubah tatanan organisasi dan hubungan sosial kemasyarakatan.

Fenomena baru ini tentunya menimbulkan dampak positif disamping dampak negatif. Kemajuan teknologi informasi memberikan banyak manfaat bagi kehidupan manusia, aktifitas manusia menjadi serba cepat, mudah dan praktis karena mobilitas manusia semakin cepat, jarak tempuh antara satu tempat dan tempat lain menjadi singkat bahkan komunikasi jarak jauh terasa semakin dekat.

Melalui kemajuan teknologi informasi, masyarakat memiliki ruang gerak yang lebih luas. Aktifitas manusia yang semula bersifat nasional telah berubah menjadi internasional, peristiwa yang terjasi disuatu negara dalam hitungan detik sudah dapat diketahui oleh penduduk belahan dunia lainnya, sesuatu yang sebelumnya dianggap mustahil.

Sekalipun kemajuan teknologi informasi memberikan banyak kemudahan bagi kehidupan manusia, tetapi kemajuan inipun secara bersamaan menumbulkan berbagai permasalahan yang tidak mudah ditemukan jalan keluarnya. Salahsatu masalah yang muncul akibat perkembangan teknologi informasi adalah lahirnya kejahatan-kejahatan yang sifatnya "baru" khususnya yang mempergunakan internet sebagai alat bantunya. Lazaim dikenal dengan sebutan kejahatan dunia maya (*Cyber Crime*).

Kata Cyber yang berasal dari kata "*Cybernetics*" merupakan suatu bidang ilmu yang merupakan perpaduan antara robotik, matematika, elektro dan psikologi yang dikembangkan oleh Norbert Wiener ditahun 1948. Salahsatu aplikasi dari cybernetics adalah bidang pengendalian (robot) dari jarak jauh. Dalam hal ini tentunya yang diinginkan adalah sebuah kendali yang betul-betul sempurna (*perfect control*).[1] Karena Budi Raharjo berpendapat bahwa sedikit mengherankan jika kata "*Cyberspace*" yang berasal darikata "*Cyber*" tidak dapat dikendalikan. *Cyberspace* dapat diatur. Meskipun pengaturannya membutuhkan pendekatan yang berbeda dengan cara yang digunakan untuk mengatur dunia nyata.

Cyberspace adalah media yang tidak mengenal batas, baik batas-batas wilayah maupun batas kenegaraan, sehubungan dengan dunia maya (*Cyber Crime*) tentunya akan menimbulkan masalah tersendiri, khususnya berkenaan dengan masalah yurisdiksi.

Yurisdiksi adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum.

Hukum Internasional tradisional telah meletakkan beberapa prinsip umum yang berkaitan dengan yurisdiksi suatu negara, salahsatu prinsip itu adalah "Prinsip Teritorial". Berdasarkan prinsip ini setiap negara dapat menerapkan yurisdiksi nasionalnya terhadap semua orang (baik warga negara atau asing), badan hukum dan semua benda yang berada didalamnya.

Dalam hal penegakan hukum didunia virtual/maya, masalah-masalah yang berkaitan dengan yurisdiksi dan penegakan serta pemilihan hukum yang berlaku terhadap suatu sengketa multi yurisdiksi akan bertambah penting dan kompleks.

Hal ini penting untuk diperhatikan mengingat seringkali disatu sisi kewenangan aparat penegak hukum dibatasi oleh wilayah suatu negara yang berdaulat penuh sebagai batas dari yurisdiksi hukum yang dimilikinya, disisi lain para pelaku kejahatan dapat bergerak bebas melewati batas negara selama dilengkapi dokumen keimigrasian yang memadai, akibatnya sangat sulit bagi

negara untuk mengungkapkan sekaligus menangkap pelaku kejahatan tersebut.

1.2. Masalah Pokok

Berdasarkan uraian yang telah dikemukakan dalam latar belakang masalah diatas, maka penulis merumuskan pokok masalah sebagai berikut :

1. Bagaimanakah Yurisdiksi Hukum Pidana dalam kejahatan di Dunia Maya (*Cyber Crime*)?
2. Bagaimanakah Kebijakan Kriminalisasi Terhadap *Cyber Crime* (Kejahatan Mayantara)?

2. Tinjauan Kepustakaan

Cyber Crime merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. *Cyber Crime* muncul bersamaam dengan lahirnya revolusi teknologi informasi, sebagaimana dikemukakan oleh Ronnni R. Nitibaskara, bahwa: ”Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain dari revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial yang berupa kejahatan (*Crime*), akan menyesuaiakn bentuknya dengan karakter baru tersbut”.

Ringkasnya, sesuatu dengan ungkapan ”Kejahatan merupakan produk dari masyarakatnya sendiri”, (*Crime is product of society its self*)”, habitat baru ini, dengan segala bentuk pola interaksi yang ada didalamnya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan yang lain yang sebelumnya telah dikenal. Kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah ”*Cyber Crime*”.

Belum ada kesatuan pendapat dikalangan para ahli mengenai definisi *Cyber Crime*. Hal tersebut disebabkan kejahatan ini (*Cyber Crime*) merupakan kejahatan yang rleatif baru dibandingkan dengan kejahatan-kejahatan konvensional. Ada yang menerjemahkan dengan kejahatan siber, kejahatan didunia maya, kejahatan virtual, bahkan ada yang tetap mempergunakan istilah aslinya, yaitu, *Cyber Crime* tanpa menerjemahkannya.

Meskipun belum ada kesepahaman mengenai definisi, kejahatan teknologi informasi (*Cyber Crime*), namun ada kesamaan pengertian universal mengenai kejahatan komputer. Hal ini dapat dimengerti karena kehadiran komputer yang sudah mengglobal mendorong terjadinya uveralisasi aksi dan akibat yang dan dirasakan dari kejahatan komputer tersebut. Secara umum yang dimaksud kejahatan komputer atau kejahatan dunia cyber adalah:

”Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau dipergunak tersebut”.

Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer tanpa atau bagian dari jaringan komputer tanpa seizin yang berhak, tindakan tersebut sudah tergolong kejahatan komputer dapat dikelompokkan dalam 2 (dua) golongan, yakni, penipuan data dan penipuan program. Dalam bentuk pertama, data yang tidak syah dimasukkan kedalam sistem jaringan komputer atau data yang seharusnya dientry diubah menjadi tidak valid atau syah lagi. Fokus perhatian pada kasus ini adalah adanya pemalsuan dan atau perusakan data input.

Bentuk kejahatan kedua, yang relatif lebih canggih dan lebih berbahaya adalah apabila seseorang mengubah program komputer, baik dilakukan langsung ditempat komputer tersebut berada maupun dilakukan secara remote melalui jaringan komunikasi data. Pada kasus ini penjahat melakukan penetrasi kedalam sistem komputer dan selanjutnya mengubah susunan program dengan tujuan menghasilkan keluaran (output) yang berbeda dari seharusnya, meski program tersebut memperoleh masukan (input) yang benar.

Bainbridge dalam bukunya kompuer dan hukum dikutip dari Merry Magdalena dan Mas Wigrantoro Roes Setiyadi, membagi beberapa macam kejahatan dengan menggunakan sarana komputer, yaitu:

a. Memasukkan instruksi yang tidak syah, yaitu seseorang memasukkan instruksi secara tidak syah sehingga menyebabkan sistem komputer melakukan transfer uang dari satu rekening ke rekening lain, tindakan ini dapat dilakukan oleh orang dalam atau luar bank yang berhasil

b. memperoleh akses kepada sistem komputer tanpa izin.
c. Perusakan data input, yaitu data yang secara syah dimasukkan kedalam komputer dengan sengaja diubah. Cara ini adalah suatu hal yang paling lazim digunakan karena mudah dilakukan dan sulit dilacak dengan pemeriksaan berkala.
d. Perusakan data, hal ini terjadi terutama pada data output, misalnya; laporan dalam bentuk hasil cetak komputer dirobek, tidak dicetak atau hasilnya diubah.
e. Komputer sebagai pembantu kejahatan, misalnya; seseorang dengan menggunakan komputer menelusuri rekening seseorang yang tidak aktif, kemudian melakukan penarikan dana dari rekening tersebut.
f. Akses tidak syah terhadap sistem komputer atau yang dikenal dengan hacking. Tindakan hacking ini berkaitan dengan ketentuan rahasia bank, karena seseorang memiliki akses yang tidak syah terhadap sistem komputer bank, sudah tentu mengetahui catatan tentang keadaan keuangan nasabah dan hal-hal lain yang harus dirahasiakan menurut kelaziman dunia perbankan.

Kejahatan dalam dunia maya (*Cyber Crime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempergunakan media internet sebagai alat bantu.

Jenis-jenis kejahatan yang masuk dalam kategori *Cyber Crime* diantaranya:

a. *Cyber Terrorism*. Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan teror, ancaman, intimidasi terhadap pihak lain. Dengan memasuki sistem jaringan komputer pihak sasaran;
b. *Cyber Pornography*. Penyebar luasan pornography melalui jaringan internet;
c. *Cyber Stalking*, *Crime of Stalking* melalui penggunaan komputer dan internet;
d. *Hacking*. Penggunaan programming abilitas dengan maksud yang bertentangan dengan hukum;
e. *Cyber-Harrashment*. Pelecehan seksual melalui e-mail;
f. *Carding* (*credit card fraud*).

Mempergunakan berbagai macam aktivitas yang melibatkan kartu kredit. Carding muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Dengan memperhatikan jenis-jenis kejahatan sebagaimana dikemukakan diatas, dapat digambarkan bahwa Cyber Crime memiliki ciri-ciri khusus, yaitu:

a. Non-Violence (tanpa kekerasan).
b. Sedikit melibatkan kontak fisik.
c. Menggunakan peralatan dan teknologi.
d. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.

Apabila memperhatikan ciri-ciri ke-3 dan ke-4, yaitu; menggunakan peralatan dan teknologi serta memanfaatkan jaringan telematika global, maka tampak jelas bahwa *Cyber Crime* dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan tanpa batas. Keadaan ini mengakibatkan tempat terjadinya tindak pidana (*locus delicti*) serta akibat yang ditimbulkan dapat terjadi dibeberapa negara dan melampaui batas-batas terttitorial suatu negara.

3. PEMBAHASAN

3.1. Yuridiksi Hukum Pidana dalam Kejahatan Dunia Maya (Cyber Crime)

Dalam membicarakan masalah yuridiksi diruang maya, Masaki Hamano dalam tulisannya berjudul ”*Comparative Study in the Approach to Jurisdiction in Cyberspace*” mengemukakan terlebih dahulu adanya yurisdiksi yang didasarkan pada prinsip-prinsip tradisional.

Menurutnya ada 3 (tiga) kategori yurisdiksi maka dapat dikatakan bahwa yurisdiksi tradisional yaitu: Yurisdiksi legislatif (legislative jurisdiction), yurisdiksi judisial (Judicial jurisdiction) dan yurisdiksi eksekutif (executive jurisdiction).

Mengacu pada pengertian ketiga yurisdiksi diatas maka dapat dikatakan bahwa yurisdiksi tradisional berkaitan dengan batas-batas kewenangan negara ditiga bidang penegakan hukum, pertama, kewenangan pembuatan hukum substantif, (oleh karena itu disebut yurisdiksi judisial atau aplikatif). Ketiga kewenangan melaksanakan/memaksakan kepatuhan

hukum yang dibuatnya (oleh karenanya disebut juga yurisdiksi eksekutif).

Dalam hal penegakan hukum didunia maya, masalah-masalah yang berkaitan dengan yurisdiksi dan penegakan serta pemilihan hukum yang berlaku terhadap suatu sengketa multi yurisdiksi akan bertambah penting dan kompleks.

Hal ini sangat penting untuk diperhatikan, mengingat seringkali disatu sisi kewenangan aparat penegakan hukum dapat melakukan tugasnya dibatasi oleh wilayah suatu negara yang berdaulat penuh sebagai batas dari yurisdiksi hukum yang dimilikinya, disisi lain pelaku kejahatan dapat bergerak bebas. Melewati batas negara selama dilengkapi dokumen keimigrasian yang memadai, akibatnya sangat sulit bagi negara untuk mengungkapkan sekaligus menangkap pelaku kejahatan tersebut.

Berdasarkan asas uraura dalam Hukum Internasional, setiap negara memiliki kekuasaan tertinggi atau kedaulatan atas orang dan benda yang ada dalam wilayahnya sendiri, oleh karena itu suatu negara tidak boleh melakukan tindakan yang bersifat melampaui kedaulatannya (*act of sovereignty*) didalam wilayah negara lain. Sebab tindakan demikian itu dipandang sebagai intervensi atau campur tangan atas masalah-masalah dalam negara lain, yang dilarang menurut Hukum Internasional.

Akibatnya, apabila diketahui adanya pelaku kejahatan yang melarikan diri atau berada diwilayah negara lain, maka negara yang memiliki yurisdiksi atas sipelaku kejahatan, misalnya, negara tempat kejahatan dilakukan atau negara-negara yang menderita akibat dari kejahatan itu, tidak boleh melakukan penangkapan dan penahanan secara langsung didalam wilayah negara tempat sipelaku kejahatan itu berada. Hal ini sangat wajar karena setiap negara tidak menghendaki wiayahnya dimasuki oleh pihak lain (orang/negara) tanpa seizin dari negara yang bersangkutan. Sedangkan cara yang lazim dipergunakan untuk menangkap pelaku kejahatan yang berada dinegara lain adalah negara yang memiliki yurisdiksi itu meminta kepada negara tempat si pelaku kejahatan itu berada supaya menangkap dan menyerahkan orang tersebut.

Dalam prakteknya yurisdiksi dapat dibedakan antara yurisdiksi perdata dan yurisdiksi pidana, yurisdiksi perdata adalah kewenangan pengadilan suatu negara terhadap perkara-perkara yang menyangkut keperdataan, baik yang siffatnya nasional maupun internasional. Yurisdiksi pidana adalah kewenangan pengadilan suatu negara terhadap perkarra-perkara yang menyangkut kepidanaan, baik yang tersangkut didalamnya unsur asing maupun nasional.

Harus diakui bahwa untuk menerapkan yurisdiksi yang tepat dalam kejahatan-kejahatan didunia maya (*Cyber Crime*) bukan merupakan pekerjaan yang mudah, karena kejahatannya bersifat internasional sehingga banyak bersinggungan dengan sistem hukum negara lain, oleh karena itu perlu ada harmonisasi, kesepakatan dan kerjasam antar warga negara mengenai masalah yurisdiksi ini.

Salahsatu upaya harmonisasi masalah yurisdiksi ini terlihat dalam ”*draft convention of Cyber Crime*” diantara negara-negara Dewan Eropa. Dalam article 22 Draft itu dinyatakan antara lain:

1. Tiap pihak (negara) akan mengambil langkah-langkah legislatif dan langkah-langkah lain yang diperlukan untuk menetapkan yurisdiksi terhadap setiap tindak pidana yang ditetapkan sesuai dengan Pasal 2 sampai Pasal 11 konvensi ini, apabila tindak pidana itu dilakukan:
   a. Didalam wilayah territorialnya; atau
   b. Di atas kapal yang mengibarkan bendera negara yang bersangkutan, atau
   c. Di atas pesawat yang terdaftar menurut hukum negara yang bersangkutan, atau
   d. Oleh seseorang dari warga negaranya, apabila tindak pidana itu dapat dipidana menurut hukum pidana ditempat tindak pidana itu dilakukan diluar yurisdiksi teritorial setiap Negara.
1. Setiap negara berhak untuk tidak menerapkan atau hanya menerapkan aturan yurisdiksi sebagaimana disebut dalam Ayat (1) b – Ayat (1) d Pasal ini dalam kasus-kasus atau kondisi-kondisi tertentu.
2. Tiap pihak (negara) akan mengambil langkah-langkah yang diperlukan untuk menetapkan yurisdiksi terhadap tindak pidana yang ditunjuk dalam Pasal 24 Ayat (1) konvensi ini, dalam hal tersangka berada diwilayahnya dan

3. negara itu tidak mengekstradisi tersangka itu ke negara lain, setelah adanya permintaan ekstradisi.
4. Konvensi ini tidak meniadakan yurisdiksi kriminal yang dilaksanakan sesuai dengan hukum domestik (hukum negara yang bersangkutan).
5. Apabila lebih dari 1 (satu) pihak (negara) menyatakn berhak atas yurisdiksi tindak pidana dalam konvensi ini, maka para pihak yang terlibat akan melakukan konsultasi untuk menetapkan yurisdiksi yang paling tepat untuk penuntutan.

Berdasarkan kasus-kasus yang telah terjadi, nampak bahwa yurisdiksi teritorial banyak dijadikan dasar penanganan kasus *Cyber Crime* dipengadilan, misalnya; di Amerika Syarikat, dengan memperhatikan pada keterbatasan-keterbatasan yang ada dalam KUHP yang berkaitan dengan *Cyber Crime*, maka perlu dikembangkan kemungkinan perluasan yurisdiksi kriminal.

Perluasan yurisdiksi kriminal ini meliputi hak untuk melakukan penuntutan dan penjatuhan pidana atas kejahatan-kejahatan yang dilakukan dalam batas wilayah suatu negara tetapi diselesaikan dalam wilayah negara lain.

Berkaitan dengan hal tersebut, Barda Nawawi Arief menganjurkan menerapkan prinsip-prinsip ”*ubikuitas*” yaitu: prinsip yang menyatakan bahwa delik-delik yang terjadi disebahagian wilayah territorial negara dan sebagian diluar territorial negara, harus dapat dibawa kedalam yurisdiksi negara terkait.

2. Ke*bijakan* Kriminalisasi Terhadap Kejahatan Mayantara (Cyber Crime)

Seiring dengan pesatnya perkembangan perkembangan teknologi informatika telah merubah pola kehidupan, *virtual life* dan *reality life*. Perubahan paradigma ini sebagai akibat dari kehadiran *Cyber Space*, yang merupakan impas dari jaringan komputer global.

Peningkatan jaringan komputer global telah menghancurkan hubungan antar letak geografis dengan:

a. Kewenangan pemerintah untuk memaksakan kontrol atas *online behavior*.
b. Pengaruh online behavior terhadap individu atas barang.
c. Legitimasi pemerintah untuk mengatur febnomena global; dan
d. Kemampuan wilayah untuk memberitahukan kepada orang yang melewati perbatasan mengenai hukum yang berlaku.

Perubahan ini disamping membawa dampak positif juga membawa dampak negatif. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. Kejahatan mengalami metaformosa baik secara kualitas atau kuantitas, paralel dengan perkembangan budaya masyarakat.

J.E Sahetapy telah menyatakan dalam tulisannya, bahwa kejahatan erat kaitannya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya.

Salahsatu dampak negatif sebagai akibat perubahan yang diusung perkembangan teknologi adalah *Cyber Crime*. *Cyber Crime* merupakan suatu bentuk dimensi baru dalam dunia kejahatan. Volodymyr Golubev menyebutnya sebagai ”The new form anti-social behavior”.

Cyber Crime pontesial menimbulkan keriguan pada beberapa bidang, seperti; politik, ekonomi, sosial dan budaya yang signifikan lebih memperhatikan dibandingkan dengan kejahatan yang berintensitas tinggi lainnya dan bahkan pada masa yang akan datang dapat mengganggu perekonomian nasional melalui jaringan infra struktur yang berbasis teknologi elektronik (perbankan, telekomunikasi, satelit, jaringan listrik dan jaringan lalu-lintas penerbangan.

Melihat fenomena ini maka perlu dilakukan upaya untuk pencegahan dan penanggulangan terhadap kejahatan adalah cyber ini. Salahsatu diantara upaya penanggulanngan kejahatan adalah kriminalisasi. Kriminalisasi adalah suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan dapat dipidana).

Berbicara masalah kriminalisasi sesungguhnya terkait erat dengan penyusunan dan kebijakan hukum pidana. Marc Ancel mendefinisikan *penal policy* sebagai *suatu ilmu sekaligus seni yang*

bertujuan untuk memungkinkan peraturan hal positif (dalam hal ini hukum pidana) secara lebih baik.

Dengan demikian dapat disimpulkan bahwa kebijakan hukum pidana juga berkaitan dengan merubah, menambah, menghapus rurausan undang-undang hukum pidana dalam. rangka mewujudkan peraturan hukum pidana yang lebih baik.

Berkenaan dengan pengaturan aktifitas dunia maya (*Cyber Space*) ini kemudian dihadapkan pada persoalan siapakah yang berhak membuat regulasi, melakukan penuntutan dan proses peradilan mengingat *Cyber space* tidak jelas locus-nya. Dan juga melewati batas teritorial negara. Akhirnya ini berkaitan dengan otoritas mana yang berhak mengatur internet.

Mengenai masalah ini, David R. Johnson dan David G. Post dalam artikelnya, "*And how should the internet be governed*?" mengemukakan 4 model yang bersaing, yaitu:

a. Pelaksanaan kontrol yang dilakukan oleh badan peradilan yang ada saat ini.
b. Penguasa nasional melakukan kesepakatan internasional mengenai "*the governance of Cyber space*".
c. Pembentukan suatu organisasi internasional baru yang secara khusus menangani masalah dunia internet.
d. Pemerintahan/pengaturan sendiri oleh para pengguna internet.

Dalam hal ini David R. Johnson dan David G. Post mendukunng model ke-4, ini dikarenakan mereka melihat bahwa dunia nyata dan dunia maya terpisah.

Menurut hemat penulis dunia nyata dan maya (*Cyber spcace*) tidak terpisahkan secara tegas. Artinya aktifitas diinternet walaupun dianggap sebagai suatu aktifitas maya, dalam pengaturannya tidak dapat dilepaskan dari manusia dalam dunia nyata. Ini dikarenakan internet sebagai sebuah teknologi menuntut pesan manusia dalam mengoperasikannya. Manusia dalam alam nyatalah yang bertanggung-jawab atas akibat dari perbuatannya. Dengan demikian aktifitas dalam *Cyber space* tidak dapat terpisahkan dari alam nyata. Regulasi yang berkaitan dengan internet tidak terlepas dari aktifitas manusia pada dunia nyata.

Sebagaimana pengaturannya *cyber law*, pengaturan *Cyber Crime* juga menimbulakn kontroversi. Agus Rahardjo tampaknya cenderung pada pendekatan yang digunakan Muladi dalam membahas kejahatan komputer. Pendekatan-pendekatan itu adalah sebagai berikut:

a. Pendekatan pertama dapat disebut sebagai pendekatan global (*global Approach*) yang menghendaki adanya pengaturan baru yang bersifat umum terhadapkejahatan komputer yang mencakup berbagai bentuk perbuatan berupa manipulasi, perusakan, pencurian dan penggunaan komputer secara melawan hukum dan tanpa kewenangan (*access to data processing system*). Hal ini tampak misalnya pada Swedish Data Act 1973.
b. Pendekatan kedua adalah pendekatan evolusioner (*evolutionary approach*) yang berusaha untuk mengadakan pembaharuan dari amandemen terhadap perumusan kejahatan-kejahatan tradisional dengan menambah objek cara-cara dilakukannya kejahatan komputer dalam perumusannya. Penambahan dalam hal ini dapat berarti modifikasi atau berupa suplementasi. Contohnya adalah; *Penal Code Amandement Act* 1985 di Canada; dan
c. Pendekatan ketiga merupaakn kompromi antaa pendekatan global dan pendekatan evolusioner dilakukan dengan cara mencantumkan komputer didalam kodifikasi Hukum Pidana.

Dalam rangka upaya untuk menanggulangi Cyber Crime maka PBB lewat resolusinya (resolusi kongres PBB VIII/1990 mengenai "*Computer Related Crime*", mengajukan beberapa kebijakan antara lain, mengimbau agar negara anggota PBB untuk mengintensifkan upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan melakukan modernisasi hukum pidana material dan hukum acara pidana.

Berkaitan dengan resolusi Kongres PBB VIII/1990 mengenai "*computer related Crime*" (didalam termasuk *Cyber Crime*) yang menganjurkan untuk modernisasi hukum pidana tersebut, sudah selayaknya bila negara (Indonesia) memperbaharui hukum pidana nasional dalam upaya penanggulangan *Cyber Crime* tersebut.

Dalam modernisasi hukum pidana, atau dengan kata lain menyusun *Cyber Crime law*, Mas Wigrantoro Roes Setiyadi dalam seminar Cyber Crime tanggal 19 Maret 2003 menawarkan beberapa alternatif, yaitu:

a. Menghapus Pasal-Pasal dalam UU terkait yang tidak dipakai lagi (usang).
b. Mengamandemen KUHP.
c. Mensisipkan hasil kajian dalam RUU yang ada.
d. Membuat RUU sendiri ex RUU (Teknologi Informasi).

Upaya tersebut tampaknya telah dilakukan terbukti dengan mulai disusunnya RUU KUHP yang baru (Konsep tahun 2000). Kalau dikaitkan dengan alternatif yang ditawarkan oleh Mas Roes, maka ini sesuai dengan alternatif kedua. Dalam RUU KUHP tersebut didalamnya mengatur regulasi yang mendukung dalam upaya pemberantasan *Cyber Crime*.

4. PENUTUP

4.1. Kesimpulan

Kemajuan teknologi informasi ditandai dengan meningkatnya penggunaan media internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet disatu sisi memberikan kemudahan bagi manusia dalam melakukan aktivitasnya, disisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana.

Munculnya kejahatan dengan mempergunakan internet sebagai alat bantunya (*Cyber Crime*) lebih banyak disebabkan oleh faktor keamanan sipelaku dalam melakukan kejahatan, masih kurangnya aparat penegak hukum yang memiliki kemampuan dalam hal *Cyber Crime*, serta belum adanya peraturan perundang-undangan yang mengatur kejahatan ini.

Mengingat adanya beberapa prinsip yang dianut dalam kitab undang-undang pidana Indonesia, yaitu; prinsip territorial, prinsip nasional, prinsip nasional pasif/prinsip perlindungan dan prinsip universal maka dalam upaya menanggulangi kejahatan didunia maya (*Cyber Crime*). KUHP Indonesia dapat diberlakukan sekalipun daya berlakunya masih bersifat terbatas, untuk beberapa jenis kejahatan.

Oleh karena itu sudah waktunya pemerintah melakukan berbagai upaya guna mencegah semakin meningkatnya kejahatan cyber (*Cyber Crime*) diantaranya melalui peningkatan kuantitas dan kualitas aparat penegak hukum yang menguasai teknologi informasi, meningkatkan sarana pendukung bagi penyelidikan dan penyidikan kejahatan siber (*cyber Crime*). Disamping perlu dilakukan kebijakan kriminalisasi terhadap cyber crime yaitu dengan cara mengadakan perubahan atau mengamandemen KUHP, dan menghapus Pasal yang tidak dipakai dan membuat Undang-undang khusus yang berkaitan dengan teknologi informasi.

4.2. Saran-saran

Berkaitan dengan *Cyber Crime* tersebut maka perlu adanya upaya-upaya untuk mencegah dan penanggulangan terhadapnya. Untuk itu perlu diperhatikan adalah:

1. Segera membuat regulasi yang berkaitan dengan cyber law umumnya dan *Cyber Crime* khususnya.
2. Dalam pengaturan tersebut perlu mempertimbangkan draft internasional yang berkaitan dengan *Cyber Crime*, mengingat kejahatan ini merupakan ”global Crime”. Selain itu juga perlu menerapkan prinsip ”ubukuitas” dalam regulasi tersebut, dikarenakan yurisdiksi kejahatan ini tidak jelas.
3. Sebelum adanya aturan khusus tentang *Cyber Crime* hakim juga aparat penegak hukum lainnya harus ”berani” melakukan ”*rechtsvinding*”.
4. Melakukan perjanjian-perjanjian ekstradisi dengan negara lain.
5. Mempertimbangkan penerapan alat bukti elektronik dalam hukum pembuktian.

DAFTAR PUSTAKA

Agus Rahardjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung, Citra Aditya Bakti, 2002.

Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Cetakan ke satu. Bandung, PT Refika Aditama, 2005.

Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer Lapitalism Communism and Coexistence from a Bitter Past to a Better Prospect*, Boston, Hougton Mifflin Company, 2002.

A. I. Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Yogyakarta. Universitas Atmajaya, 1999.

Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Bandung, Citra Aditya Bakti, 2003.

Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Bandung, Citra Aditya Bakti, 2002.

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*, Bandung, Citra Aditya Bakti, 2003.

Dikdik M. Arif Mansur & Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, Bandung, PT Refika Aditama, 2005.

Huala Adolf, *Aspek-aspek Negara dalam Hukum Internasional*, Jakarta, Rajawali Pers, 1996.

I Wayan Pasthiana. *Ekstradisi dalam Hukum Internasional dan Hukum Nasional Indonesia*, Bandung, Mandar Maju, 1990.

J. G. Starke, *Pengantar Hukum Internasional*, Edisi Kesepuluh, Buku 1, Jakarta, Sinar Grafika, 1977.

Merry Magdalena dan Mas Wigrantoro Roes Setiyadi, *Cyber Law: Tidak Perlu Takut*. Yogyakarta. CV Andi Offset, 2007.

Tubagus Roni Rahman Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi Hukum dan Sosiologis*, Jakarta, Peradaban, 2001.

Hera Sutadi. *Cyber Crime, apa yang bisa diperbuat*, Sinar Harapan, Sabtu 5 April, Jakarta, 2003.