“ TINJAUAN YURIDIS TERHADAP CYBER CRIME”

Ronal / D 101 09 540

Pembimbing I : Achmad Allang S,H. M,H.

Pembimbing II : Harun Nyak Itam Abu S,H. M,H.

Abstrak

Yurisdiksi merupakan refleksi dari prinsip dasar kedaulatan negara, kedaulatan negara tidak akan diakui apabila negara tersebut tidak memiliki jurisdiksi, persamaan derajat negara dimana kedua negara yang sama-sama merdeka dan berdaulat tidak bisa memiliki jurisdiksi (wewenang) terhadap pihak lainnya (equal states dont jurisdiction over each other) dan prinsip tidak campur negara terhadap urusan domestik negara lain. Cyber crime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Cyber crime merupakan kejahatan yang memanfaatkan perkembanagan teknologi komputer khususnya internet.Tujuan penelitian ini adalah untuk mengetahui dengan jelas faktor-faktor yang dominan yang berpengaruh terjadinya pertentangan yuridikasi dalam menyelesaikan kasus cyber crime. Dan untuk mengetahui sistem pembuktian dalam perkara tindak pidana cyber crime.Adapun metode yang digunakan dalam penelitian ini adalah dengan teknik pengumpulan data dengan melakukan observasi, reduksi data dan penyajian data. Dan hasil penelitian ini adalah pada hakikatnya yurisdiksi yang berpotensi untuk mengisi kekosongan hukum dalam pelaksanaan yurisdiksi terhadap tinda-tindak pidana internasional. Hakikat yurisdiksi universal berbeda dengan yurisdiksi yang lain karena tidak memerlukan titik pertautan antara negara yang melakukan /melaksanakan yurisdiksinya dengan pelaku, korban, dan tindak pidana itu sendiri. Kekosongan hukum dapat diatasi dengan diberikannya wewenang oleh hukum internasional kepada setiap negara untuk melaksanakan yurisdiksiuniversal.

Kata Kunci : Cyber Crime Tinjauan Yuridis

1.

PENDAHULUAN

A.Latar Belakang

Fenomena tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi munmcul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagaimana dikemukakan oleh *Ronni R. Nitisbaskara* bahwa: "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Menjawab tuntutan dan tantangan komunikasi global lewat *internet*, Undang-Undang yang diharapkan (*ius konstituendum*) adalah perangkat hukum yang permasalahan, termasuk dampak negatif penyalahgunaan *internet* dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Pada dasarnya teknologi internet merupakan sesuatu yang bersifat netral, dalam artian bahwa teknologi tersebut tidak bersifat baik ataupun jahat. Akan tetapi dengan keluasan fungsi dan kecanggihan teknologi informasi yang terkandung di dalamnya semakin merebaknya globalisasi dalam kehidupan mendorong para pelaku kejahatan untuk menggunakan internet sebagai sarananya. Cyber crime pada saatnya akan menjadi bentuk kejahatan serius yang dapat membahayakan keamanan individu, masyarakat dan negara serta tatanan kehidupan global.

Mengingat bahwa cybercrime tidak mengenal batas negara maka dalam upaya penanggulangannya memerlukan suatu kordinasi dan kerja sama antar negara. Cybercrime memperlihatkan salah satu kondisi yang kompleks dan penting untuk diadakannya suatu kerjasama internasional. Cyber Crime merupakan bentuk prkembangan kejahatan internasional yang cukup menghawatirkan saat ini[1]. Pesatnya perkembangan dibidang teknologi informasi saat ini. Dekatnya hubungan antara informasi dan teknologi jaringan komunikasi telah menghasilkan dunia maya yang amat luas yang bisa disebut dengan teknologi cyberspace. Teknologi ini berisikan kumpulan informasi yang dapat diakses oleh sema orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet, sebagai media penyedia informasi internet juga merupakan sarana kegiatan komunitas komersial terbesar dan terpesat pertumbuhannya.

Ada beberapa hukum positif yang berlaku umum dan dapat dikenakan bagi para pelaku *cyber crime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarananya. Melalui permasalahan yang diuraian diatas, maka peneliti tertarik untuk melakukan penelitian dengan judul **" TINJAUAN YURIDIS TERHADAP CYBER CRIME "**.

B. Rumusan Masalah

1. Bagaimanakah pengaturan yurisdiksi Cyber Crime?

2. Bagaimanakah sistem pembuktian dalam perkata tindak pidana cyber crime ?

II.PEMBAHASAN

A. PENGERTIAN YURISDIKSI

Yurisdiksi merupakan refleksi dari prinsip dasar kedaulatan negara, kedaulatan negara tidak akan diakui apabila negara tersebut tidak memiliki jurisdiksi, persamaan derajat negara dimana kedua negara yang sama-sama

[1] *http://adit-chaky.blogspot.com2011/03/cyber crime-di indonesia.html*

merdeka dan berdaulat tidak bisa memiliki jurisdiksi (wewenang) terhadap pihak lainnya *(equal states dont jurisdiction over each other)* dan prinsip tidak campur negara terhadap urusan domestik negara lain.

Jurisdiction sendiri berasal dari bahasa latin *yurisdictio*, yang terdiri dari dua suku kata yuris berarti kepunyaan menurut hukum, dan *diction* yang berarti ucapan, sabda, sebutan, firman,jadi dapat disimpulkan yurisdiksi berarti :[2]

a. Kepunyaan sendiri yang ditentukan oleh hukum
b. Tidak menurut hukum
c. Kekuasaan menurut hukum
d. Kewenangan menurut hukum

Berdasarkan pengertian yang dikemukakan diatas, termasuk dalam unsur-unsur yurisdiksi negara adalah :

a. Hak, kekuasaan, dan kewenangan,
b. Mengatur (legislatif, eksekutif dan yudikatif)
c. Objek (hal, peristiwa,perilaku, masalah, orang dan benda,
d. Tidak semata-mata merupakan masalah dalam negeri
e. Hukum internasional (sebagai dasar/landasan)

Dalam Kamus Besar Bahasa Indonesia, Yurisdiksi memiliki 2 pengertian yaitu :[3]

1. Kekuasaan mengadili,lingkup kekuasaan kehakiman
2. Lingkungan hak dan kewajiban, serta tanggung jawab di suatu wilayah atau lingkungan kerja tertentu kekuasaan hukum.

Sepanjang menyangkut perkara pidana ada beberapa prinsip yurisdiksi yang dikenal dalam hukum internasinal yang dapat digunakan oleh negara untuk mengklaim dirinya memiliki *judical jurisdiction*. Adapun prinsip-prinsip tersebut ialah :[4]

1. Prinsip Yurisdiksi Teritorial

Menurut Prinsip ini setiap negara memiliki yurisdiksi terhadap kejahatan-kejahatan yang dilakukan didalam wilayah atau teritorialnya.

2. Yurisdiksi Personal

Menurut prinsip yurisdiksi personal, suatu negara dapat mengadili warga negaranya karena kejahatan yang dilakukannya dimana pun juga. Sebaiknya adalah kewajiban negara untuk memberikan perlindungan diplomatik kepada warga negaranya di luar negeri.ketentuan ini telah diterima secara universal.

3. Prinsip Perlindungan

Berdasarkan prinsip ini negara memiliki yurisdiksi terhadap orang asing yang melakukan kejahatan yang sangat serius yang mengancam kepentingan vital negara, keamanan, integritas, dan kedaulatan, serta kepentingan vital ekonomi nrgara, atau suatu negara dapat melaksanakan yurisdiksinya terhadap warga-warga asing yang melakukan kejahatan di luar negeri yang diduga dapat mengancam kepentingan keamanan, integritas dan kemerdekaan negara.

4. Prinsip Universal

Berdasarkan prinsip ini setiap negara memiliki yurisdiksi untuk mengadili pelaku kejahatan internasional yang dilakukan dimana pun tanpa memperhatikan kebangsaan pelaku atau korban.

Apabila kita kaji lebih jauh makna dari Sistem Pembuktian Dalam Hukum Acara Pidana Di Indonesia adalah yang pertama kita harus mendefenisikan apa yang dimaksud dengan sistem, kemudian kita juga harus menjelaskan apa yang dimaksud dengan pembuktian. Menurut Kamus Besar Bahasa Indonesia, sistem adalah perangkat unsur yang secara teratur saling berkaitan sehingga membentuk totalitas atau susunan yang

---

[3] *Departemen Pendidikan Nasional, Kamus Besar Bahasa Indonesia, 2005. Edisi ketiga, Jakarta: Balai Pustaka Hal 1278*

[4] *H.Bachtiar Hamzah, 1997,.Hukum Internasional II. Medan : USU Press. Hal 69*

teratur dari pandangan, teori dan asas.[5] berdasarkan sistem pembuktian pada umumnya dikenal ada tiga teori sistem pembuktian yaitu :

1. Sistem Pembuktian Menurut Undang-undang Secara Positif *(Positif Wettelijke Bewijs Theory)*
2. Sistem Pembuktian Menurut Keyakinan Hakim
3. Sisteem Pembuktian Menurut Undang-Undang Secara Negatif *(Negatif Wettelijke Bewijs Theory)*

Adapun sistem pembuktian yang diatur dalam KUHAP tercantum dalam Pasal 183 yang rumusannya adalah sebagai berikut :

" hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila sekurang-kurangnya dua alat bukti yang sah, ia memperoleh keyakinan suatu tindak pidana banar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya".

B.Pengertian dan Ruang Lingkup Cybercrime

1. Pengertian dan Ruang Lingkup Cybercrime

Cyber crime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime*merupakan kejahatan yang memanfaatkan perkembanagan teknologi komputer khususnya internet. Internet yang menghadirkan *Cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi dibalik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran untuk melakukan aksi kejahatan dunia maya.[6]

Internet telah menciptakan dunia baru yang dinamakan *cybercrime* yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual (tidak langsung dan tidak nyata). Sebagaimana lazimnya pembaharuan teknologi, internet selain memberi manfaat juga menimbulkan sisi negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Dalam jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas.[7]

Berikut ini beberapa pengertian cybercrime menurut para ahli :

a. Andi Hamzah mengartikan kejahatan komputer bukan sebagai kejahatan baru, melainkan kejahatan biasa, karena masih mingkin diselesaikan melalui KUHP.[8]
b. Forester dan Morrison mendefenisikan kejahatan komputer sebagai aksi kriminal dimana komputer digunakan sebagai senjata utama.
c. Girasa mendefenisikan cybercrime sebagai aksi kejahatan yang menggunakan teknologi komputer sebagai komponen utama.
d. *Encyclopedia of crime and justice, New York : Free Press, 1983* : Setiap perbuatan melawan hukum yang memerlukan pengetahuan tentang teknologi

[5] *Kamus Besar Bahasa Indonesia. Op.cit.hal.481*

[6] Adami Chazawi.2005 Tindak Pidana Mengenai Kesopanan, Rajagrafindo Persada, Jakarta.

[7] *Agus Raharjo.2002. Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Citra Aditya Bakti, Bandung: Hal 41*

[8] *Deris Setiawan. 2005. Sistem Keamanan Komputer, PT Elex Media Komputindo, Jakarta. Hal 34*

komputer yang bertujuan untuk dapat melakukan kejahatan yang dapat dikategorikan dalam dua bentuk yaitu penggunaan komputer sebagai alat untuk suatu kejahatan, seperti pemilikan uang secara ilegal, pencurian properti atau digunakan untuk merencanakan suatu kejahatan, komputer sebagai objek dari suatu kejahatan, seperti sabotase, pencurian atau perubahan data-data.[9]

e. *OECD (Organization for economic cooerporation develovment)* : setiap tindakan yang tidak sah, tidak etis atau tidak berdasar pada cukup wewenang, yang melibatkan pemrosesan data otomatis dan /atau transmisi data, dimana defenisi tersebut juga meliputi : kejahatan ekonomi yang berkaitan dengan komputer (penipuan, spionase, sabotase) Pelanggaran privasi individual yang berkaitan dengan komputer dan pelanggaran terhadap kebijakan keamanan nasional dan kendali aliran data antar batas dan integrasi dari prosedur yang berdasarkan komputer dan jaringan komunikasi data atau legitimasi demokratis atau keputusan-keputusan yang berdasarkan komputer.[10]

Cybercrime pada dasarnya tindak pidana yang berkenan dengan informasi, sistem informasi itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya *(transmitter/orginator to recepient).* Menurut Susanto, secara garis besar *cybercrime* terdiri dari dua jenis yaitu :

1. Kejahatan yang menggunakan teknologi informasi sebagai fasilitas.
   Contoh dari aktifitas cybercrime jenis pertama ini adalah pembajakan (copyright atau hak cipta intelektual dan lain-lain), pornografi, pemalsuan dan pencurian kartu kredit *(carding),* penipuan lewat e-mail, penipuan dan pembobolan rekening bank, perjudian online, terorisme, materi-materi internet yang berkaitan dengan zara (seperti penyebaran kebencian etnik dan ras atau agama), transaksi dan penyebaran obat terlarang, transaksi seks dan lain-lain.[11]
2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasran.
   Cybercrime jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sasaran tindak pidana, melainkan menjadikannya sebagai sasaran. Contoh dari jenis-jenis tindak kejahatannya antara lain pengaksesan ke suatu sistem secara ilegal *(hacking),* perusakan situs internet dan server *data (cracking)* serta defacting.[12]

   Sedangkan kualifikasi kejahatan dunia maya *(cybercrime)* sebagaiamana dikutip Barda Nawawi Arief adalah kualifikasi *cybercrime* menurut *Convention on Cybercrime 2001 di BudapestHungaria*, yaitu :

[9] *Ibid. Hal 35*

[11] *Sabartua Tambubolon,2002.Domain Name: Nama Domain, Universitas Pelita Harapan, Jakarta Hal 64*
[12] *Ibid. Hal 65*

1. *Illegal access* yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak
2. *Illegal interception* yaitu sengaja dan tanpa hak mendengar menangkap secara diam-diam pengiriman dan pemancaran data komputer yang bersifat tidak publik ke, dari atau didalam sistem komputer dengan menggunakan alat bantu teknis.
3. Data *interferecence* yaitu data sengaja dan tanpa hak melakukan perusakan, peghapsan, perubahan, atau penghapusan data komputer.
4. *System interferecence* yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap fungsinya sistem komputer.
5. *Misuse of Devices* yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*Acces Code)*
6. *Computer related forgery* pemalsuan (dengan sengaja dan tanpa hak memasukan mengubah,menghapus data autentik menjadi tidak autentik dengan maksud sebagai data autentik)
7. *Computer related Fraud penipuan* (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain denagan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).
8. *Content-Related offonces* Delik-delik yang berhubungang dengan pornografi *anak (Child pornografy)*
9. *Offences related to infringements of copyright and related rights.*[13] Sejarah perkembangan internet tidak dapat dipisahkan dari terjadinya perang dingin antara Uni Soviet dengan Amerika Serikat sesuai Perang Dunia II. Perang dingin tersebut berimplikasi dengan semakin giatnya kedua negara mengembangkan teknologi, dan amerika ikut kemudian mengembangkan teknologinya dengan peruntukan militer. Dalam hal ini dibentuklah *Advanced Research Agency* (ARPA). Tugas pertama yang dibebankan ARPA adalah mengamankan dan melindungi data-data dan sistem komunikasi yang telah dibangun dan tidak dapat dihancurkan.[14]

Saat ini *cybercrime* telah menjadi isu global security pada setiap negara yang menandakan

[13] http://itsmeryd.com/2012/12/cyber-crime-di-Indonesia.html *diakses pada tanggal 10 Agustus 2015*

perlunya pengamanan akses informasi internet khususnya yang berkaitan dengan kejahatan dunia maya yang dapat berpotensi mengancam stabilitas keamanan nasional. Cybercrime menjadi salah salah satu bahan kajian baru dalam ruang lingkup kajian hubungan internasional khususnya dalam hal menganankan kepentingan nasional yang berkaitan dengan menjaga dan meningkatkan stabilitas keamanan nasional. Selaras dengan langkah-langkah pengaman tersebut juga diperlukan upaya mengoptimalkan penegakan hukum terhadap *cybercrime* yang lebih efektif. Penegakan hukum dalam *cyberspace* membutuhkan sinegeri antara masyarakat yang partisifatif dengan aparat penegak hukum yang demokratis, transparan, bertanggung jawab dan berorientasi pada HAM, pada aplikasinya diharapkan dapat benar-benar mewujudkan stabiltas keamanan yang semakin mantap dalam rangka mendukung pembangunan nasional menuju cita-cita nasional.[15]

Problema penegakan hukum di Indonesia nampaknya mulai menghadapi kendala berkaitan dengan perkembangan masyarakat yang kian cepat. Berbagai kasus menggambarkan sulitnya penegakan hukum mencari cara agar hukum nampak sejalan dengan norma masyarakat.[16] Bagaimana pun juga perkembangan teknologi dan informasi, baik itu menguntungkan dan merugikan tidak dapat dilepaskan dengan manusia dan perilakunya dalam kehidupan bermasyarakat. *Cybercrime* adalah salah satu hasil karya den rekayasa manusia dan memenuhi kebutuhan hidupnya ditengah masyarakat yang penuh dengan persaingan dan krisis serta tekanan.[17]

Dalam rangka menanggulangi tindak pidana *cybercrime* perlu diimbangi dengan melakuakan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh dalam suatu bentuk kebijakan legislatif atau yang dikenal dengan kebijakan formulasi. Kebijakan merumuskan dan menetapkan sangksi pidana dalam perundang-undangan, dapat juga disebut sebagi tahap kebijakan formulasi. Kebijakan formulasi mempunyai posisi yang sangat strategis bila dipandang dari keseluruhan kebijakan mengoprasionalisasikan hukum pidana. Pandanagan ini sesuai dengan pendapat Barda Nawawi Arief yang menyatakan bahwa tahap kebijakan legislatif merupakan tahap yang paling strategis dilihat dari mengoprasionalkan sanksi pidana. Pada tahap ini dirumuskan garis kebijaksanaan sistem pidana dan pemidanaan yang sekaligus sebagai landasan legislatif bagi tahap-tahap berikutnya, yaitu tahap perapan pidana oleh badan pengadilan dan tahap pelaksanaan pidana dan oleh aparat pelaksana pidana.[18]

Menurut Barda Nawawi Arief kebijakan formulasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak pidana) menjadi suatutindak pidana (Perbuatan yang

[15]*Heru Soepraptomo 2000 Peranan Komputer dalam industri dan pengaruhnya terhadap bidang hukum, Alumni.Bandung Hal 37*

[16]*Eva Achjani zulfa,2008 ketika jaman meninggalkan hukum, Citra Aditya Bakti.Bandung, hal 46*

[1717]*Hirronymus Jati, Kaum Miskin Mengais Pendapatan Lewat Judi, Rajawali Pers. Jakarta : hal 25*

[18]*Barda Nawawi Arief, 1996. Kebijakan Legislatif Dalam Penanggulangan Kejahatan dengan Pidana Penjara. Badan Penerbit Universitas Diponegoro, Semarang, hal.3*

dapat dipidana). Jadi pada hakekatnya kebijakan formulasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal *(criminal Policy)* dengan menggunakan sarana hukum pidana (Penal) dan oleh karena itu termasuk bagian dari kebijakan hukum pidana *(penal policy),* khususnya kebijakan formulasinya. Selanjutnya menurut Barda Nawawi Arief kebijakan formulasinya bukan sekedar kebijakan menetapkan/ merumuskan/ memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi/ legislasi itu disusun dalam suatu kesatuan sistem hukum pidana (kebijakan legislatif) yangharmonis dan terpadu.[19]

Pendapat lain dikemukakan oleh H.L Packer, bahwa kebijakan formulasi dalam bidang hukum penentensier sangat penting bagi bagi suatu kebijakan pemidanaan *(setencing policy)* yang merupakan salah satu masalah kontriversial saat ini dalam hukum pidana.[20]

Penegakan hukum pada hakikatnya merupakan bagian dari poloitikkriminal yang pada hakikatnya menjadi bagian integral dari kebijakan sosial *(social policy)* kemudian kebijakan ini diimflementasikan kedalam sistem peradilan pidana *(Criminal justice system),* menurut Muladi sistem peradilan pidana mempunyai dimensi fungsional ganda. Disatu pihak berfungsi sebagai sarana masyarakat untuk menahan dan mengendalikan kejahatan pada tingkatan tertentu (crime containtmen system) dilain pihak sistem peradilan pidana juga berfungsi untuk pencegahan sekunder *(Secondary prevention)* yaitu mencoba mengurangi kriminalitas dikalangan mereka yang pernah melakukan kejahatan melalui proses deteksi,pemidanaan dan pelaksanaan pidana.[21]

Sistem peradilan pidana tersebut di dalam oprasionalnya melibatkan subsistem yang bekerja secara koheren, kordinatif dan itegratif, agar dapat mencapai efesiensi dan efektifitas yang maksimal. Oleh karena itu efesiensi maupun efektivitasnya yang sangat tergantung pada faktor-faktor sebagai berikut :[22]

a. Infrastruktur pendukung sarana dan prasarana
b. Propesionalisme aparat penegak hukum dan;
c. Budaya hukum masyarakat.

Terhadap masalah penegakan hukum Soerjono Soekamto mengemukakan bahwa secara konsepsional intidan arti penegakan hukum terletak pada kegiatan menyerasikian hubungan nilai-nilai yang terjabarkan di dalam kaidah-kaidah yang mantap dan mengejewantah sikap tindak sebagai rangkaian penjabaran nilai terhadap akhir, untuk menciptakan memelihara dan mempertahankan kedamaian pergaulan hidup. Sebagai suatu proses penegakan hukum pada kakikatnya merupakan penerapan diskresi yang menyatakan pembuat keputusannya tidak secara ketat diatur oleh kaidah hukum. Akan tetapi mempunyai unsur penilaian

[19] *Barda Nawawi Arief 2003,kapita Selekta Hukum Pidana, PT Citra Aditya Bakti, Bamdung Hal.259*
[20] *H.L packer 1968, The Limits of criminal Sanction, Standfor Unuversity Press, Calipornia, Hal13*
[21] *Muladi,1990. Proyeksi Hukum Pidana Indonesia Dimasa Yang Akan Datang, Pidato Pengukuhan Guru Besar Fakultas Hukum UNDIP, Semarang.hal.21-22*
[22] *Ibid hal. 24*

pribadi demikian menurut Wayn Lafawel.[23]

Sehubungan dengan pandangan diatas menurut Soerjono Soekamto ada beberapa faktor yang mempengaruhi penegakan hukum yaitu :[24]

a. Faktor hukumnya sendiri
b. Faktor penegak hukum
c. Faktor sarana dan fasilitas yang mendukung penegakan hukum
d. Faktor masyarakat
e. Faktor kebudayaan

Kelima faktor diatas mrupakan faktor-faktor yang terkait satu sama lain. Merupakan esensi dari penegakan hukum dan bekerjanya hukum dalam masyarakat. Kaitannya dengan penegakan hukum terhadap tindak pidana *cybercrime*, efesiensi maupun efektifitasnya juga tergantung pada salah satu faktor sebagaimana yang dikemukakan diatas yaitu :

a. Faktor Perundang-Undangan

Meskipun eksistensi pengaturan tindak pidana *cybercrime* tidak hanya dalam undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi juga terdapat didalam Undang-undang khusus lainnya di luar KUHP, namun masih terdapat bentuk-bentuk tindak pidana *cybercrime* yang belum mendapatkan pengaturan, khususnya yang menyangkut penyalahgunaan teknologi canggih. Salah satu asas dalam hukum pidana menentukan bahwa tiada perbuatan yang dapat dihukum pidana dan dan diancam dengan pidana jikalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan perundang-undangan *(asas legalitas).* Maka pengaturan atas tindak pidana *cybercrime* yang masih belum terakomodir dalam perundang-undangan dimaksud sifatnya cukup penting. Menurut Muladi bahwa secara oprasional perundang-undangan pidana mempunai kedudukan strategis terhadap sistem peradilan pidana. Sebab hal tersebut memberikan defenisi tentang perbuatan-perbuatan yang dirumuskan sebagai tindak pidana. Mengendalikan usaha-usaha pemerintah untuk memberantas kejahatan dan memidana sipelaku, memberikan batasan tentang pidana yang dapat diterapkan untuk setiap kejahatan . dengan perkataan lain perundang-undangan pidana yang menciptakan *legislated environment* yang mengatur segala prosedur dan tata cara yang harus dipatuhi didalam berbagai perangkat sistem peradilan pidana.[25]

b. Faktor Penegak Hukum

Keberhasilan misi hukum pidana untuk mengulangi tindak pidana *cybercrime* tidak hanya ditentukan oleh sempurnanya hukum yang dirumuskan dalam hukum positif. Melainkan telah lebih dari itu keberhasilannya sangat tergantung kepada aparat yang melaksanakannya (penegak hukumnya) mulai dari tingkat penyidikan hingga tingkat eksekusi. Hal ini dikarenakan karasteristik yang khas dari tindak pidana *cybercrime* sebagai suatu tindak pidana yang bersifat virtual. Konsekuensinya logisnya, aparat penegak hukum harus memiliki kemampuan lebih dan profesi didalam menagani tindak pidana *cybercrime,* profesionalisme dan keberanian moral aparat penegak hukum hukum dituntut sekaligus

[23] *Soerjono Soekamto.1983. Faktor-faktor yang mempengaruhi Penegakan Hukum, Rajawali Press, Jakarta, Hal,4.*

[25] *Muladi,1995,Kapita Selekta Peradilan Pidana. Badan Penerbit UNDIP, Semarang. Hal23*

diuji untuk melakukan penemuan hukum sehingga tidak ada alasan klasik yang bersembunyi dibalik asas legalilitas sempit bahwa aturan perundang-undangan tidak lengkap atau belum ada perundang-undangan yang mengaturnya.

c. Faktor Infrastruktur Pendukung Sarana Dan Prasarana

Faktor ini dapat dikatakan sebagai tulang punggung penegak hukum terhadap tindak pidana cybercrime. Sebab eksistensinya merupakan penopang keberhasilan untuk menemukan suatu kebenaran materil. Oleh karena itu jalinan kerja sama harmonis antara lembaga penegak hukum dengan beberapa pakar spesialis dibidangnya seperti ahli forensik, fakar telematika serta dana operasional yang menandai adalah merupakan faktor pendukung guna mengadili dan memidana atau pun mempersempit ruang gerak pelaku tindak pidana cybercrime.

d. Faktor Budaya Hukum Masyarakat

Tidak kalah penting dengan faktor-faktor yang lain, faktor budaya hukum masyarakat ini juga memiliki pengaruh dan memainkan peranan penting dalam proses penegakan hukum terhadap tindak pidana cybercrime. Pluralisme budaya hukum ditengah masyarakat merupakan fenomena yang unik dan mengandung resiko yang potensial, sehingga sering kali menempatkan posisi dan profesi aparat penegak hukum kedalam kondisi dilematis yang pada gilirannya dapat menimbulkan ambivalensi[26]dalam pelaksaanan peranan aktualnya.[27]

e. Kerja Sama Internasional

Melakukan kerjasama dalam melakukan penyidikan kasus kejahatan cyber karena sifatnya yang borderless dan tidak mengenal batas wilayah sehinggah kerja sama dan kordinasi dengan aparat penegak hukum negara lain merupakan hal yang sangat penting untuk dilakukan. Pengamanan Sistem Informasi akan memudahkan aparat kepolisian diberbagai belahan dunia melakukan identifikasi dan medapatkan bantuan dari investigator dan negara lain. Kerja sama internasional juga meliputi perjanjian kerja sama diantara negara-negara baik dalam ekstradisi maupun dalam hal pembantuan dalam upaya menghadirkan korban yang berada diluar toritorial negara. Sebagai upaya lebih efektif dan efesiensi waktu hendaknya dalam upaya pembaharuan hukum pemeriksaan korban dan saksi dalam tindak pidana teknologi informasi dapat dilakukan melalui *cara e-mail* atau *mesengge*r yang ditanda tangani dengan tanda tangan digital sebagai sahnya penyidikan, serta pemeriksaan berupa teleconfrence dalam persidangan di pengadilan[28]

Penerapan alat bukti informasi dan data elektronika dalam perundang-undangan sering mengakibatkan multitafsir diantara aparat penegak hukum terutama pada saat pemeriksaan pengadilan. Hal tersebut dikarenakan belum adanya rambu-rambu yang jelas terhadap pengakuan alat bukti tersebut. Konsep Rancangan Unadang-undang KUHP 2000, dimana konsep ini mengalami perubahan

[26]*Ambivalensi adalah perasaan tidak sadar yang saling bertentangan terhadap situasi yang sama atau terhadap seseorang pada waktu yang sama.*
[27]*Ibid 23*

[28]*Barda Nawawi Arief, 1998. Beberapa aspek kebijakan penegakan dan pengembangan hukum pidana, Bandung : PT.Citra Aditya Bakti, Jakarta: 2006.Hal.78*

sampai dengan 2008 telah mengatur alat bukti elektronik yaitu :[29]

Dalam Buku I (ketentuan Umum) Dibuat ketentuan mengenai alat bukti :

1. Pengertian "barang" (Pasal 174/178) yang didalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer.
2. Pengertian "anak kunci" (pasal178/182) yang termasuk kode rahasia, kunci masuk komputer, kartu magnetic, silly dan yang telah diprogram untuk membuka sesuatu. Menurut Agus Raharjo,[30]maksud dari anak kunci ini kemungkinannya adalah password atau kode-kode tertentu seperti privat atau public key infrastructure.
3. Pengertian "surat" (Pasal 188/192) termasuk data tertulis atau tersimpan dalam disket, pita magnetic, media penyimpanan komputer atau penyimpanan data elektronik lainnya.
4. Pengertian "ruang" (pasal 189/193) termasuk bentangan atau terminal komputer yang dapat diaskes dengan cara-cara tertentu. Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau maya atau antara *cyberspace* atau *virtual reality*.
5. Pengertian "masuk" (pasal 190/194) termasuk mengakses komputer atau masuk kedalam sistem komputer.

III. PENUTUP

A. Kesimpulan

1. Yurisdiksi kriminal berlakunya hukum pidana nasional terhadap *cybercrime* tidak cukup dengan menggunakan prinsip yurisdiksi teritorial dan ekstra teritorial yang diakui dalam hukum internasional publik tetapi juga berdasarkan prinsip yurisdiksi yang berlaku terhadap tindak pidana yang dilakukan diluar yurisdiksi negara manapun. Jadi yurisdiksi kriminal berlakunya hukum pidana nasional terhadap *cybercrime* menganut quasi yurisdiksi yaitu menggunakan yurisdiksi teritorial, yurisdiksi ekstra teritorial terhadap cybercrime yang dilakukan didalam yurisdiksi negara lain dan ekstra teritorial terhadap cybercrime yang dilakukan diluar yurisdiksi negara manapun.
2. Sistem pembuktian dalam perkata tindak pidana cyber crime dengan cara perluasan alat bukti dalam KUHAP sebenarnya sudah diatur dalam berbagai perundang-undangan secara tersebar. Dengan demikian *email*, suara, gambar, kode akses, simbol, dan berbagai dokumen elektronik lainnya mempunyai kekuatan pembuktian yang setara dengan alat bukti lainnya yang diatur didalam KUHAP dan dapat digunakan sebagai alat bukti yang sah.

B. Saran

1. Dalam pengaturan yuridiksi *cyber crime* kerja sama internasional sangat penting dalam memberantas tindak pidana cybercrime terutama dalam proses penyelidikan dan penyidikan. Disini perlu ditingkatkan kemampuan sumber daya aparat penegak hukum terutama dibidang *cyber crime* ditingkatkan sarana dan prasarana dalam bidang teknologi informasi dan komunikasi.

---

[29] *Barda Nawawi Arief ,2005. Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan, PT.Citra Aditya Bakti, Bandung, Hal.131-133*

[30] *Agus raharjo 2002.Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,PT.Citra Aditya Bakti, Bandung, Hal.236*

2. Penegak hukum pada sistem pembuktian dalam perkata tindak pidana *cyber crime* harus lebih meningkatkan upaya dengan cara mementingkan efektif dan efesiensi waktu, hendaknya dalam upaya pembaharuan hukum pemeriksaan korban dan saksi dalam tindak pidana teknologi informasi dapat dilakukan melalui *cara e-mail* atau *mesengge*r yang ditanda tangani dengan tanda tangan digital sebagai sahnya penyidikan, serta pemeriksaan berupa *teleconfrence* dalam persidangan dipengadilan, sehingga kejahatan dalam dunia maya bisa berkurang secara perlahan-lahan dan tidak akan meresahkan penggunan internet yang sering berselancar di dunia maya.
3.

DAFTAR PUSTAKA

BUKU :

Abdul Wahid, Kejahatan Mayantara (Cybercrime), Refika Aditama Bandung : 2010

Agus Rahardjo, Cybercrime : Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi, Citra Aditya Bakti, Bandung 2002

Aloysius Wisnubroto, Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer, Universitas Atmajaya, Yogyakarta:1999

Andi Hamzah, Hukum Acara Pidana, Sinar Grafika, Jakarta : 2002

Asril Sitompul, Hukum Internet Pengenalan Mengenai Masalah Hukum Cybercrime,Citra Aditya Bakti, Bandung 2001.

Barda Nawawi Arief, Tindak Pidana Mayantara, Rajawali Pers, Jakarta : 2006
Yahya harahap,Sistem Pembuktian, Sinar Grafika, Jakarta 1998
Soenarko, Teori Sistem Pembuktian, Djambatan, Jakarta,: 2010

Rachman, Maman, dkk. 2008. Filsafat Ilmu. UPT UNNES Press. Semarang

Soetami, A. Siti. 2007. Pengantar Tata Hukum Indonesia. PT Refika Aditama. Bandung

Soehino. 2005. Ilmu Negara. Liberty Yogyakarta. Yogyakarta

Tanya, Bernard L. 2011. Politik Hukum Agenda Kepentingan Bersama. Genta Publishing. Yogyakarta

UNDANG-UNDANG :

Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
Undang-Undang Dasar Negara Republik Indonesia tahun 1945

BIODATA DIRI

Nama	: RONAL
Tempat Tanggal lahir	: PALU, 25 DESEMBER 1990
Alamat	: JLN.UNTAD 1 NO 5
Alamat E-mail	: sittikridhani@gmail.com
No Hand Phone	: 082332573506