Pengaturan Terhadap Yurisdiksi *Cyber Crime* Ditinjau dari Hukum Internasional

Galuh Kartiko
Dosen Politeteknik Negeri Malang
Email : galuh_law@yahoo.co.id

Abstract

According to international law, a state have certain boundaries in the case of applying of jurisdiction to case entangling importance of other state. in Indonesia, law of no.11 on 2008 about information and electronic transaction (ITE), section arranging jurisdiction is section 2 embracing ground of subjective territoriality where everyone conducting cybercrime and its impact harm Indonesia can judge in Indonesia. But, in practice, this matter is difficult to done if perpetrator do its crime from outside Indonesia. Except Indonesia follow to ratify convention on cybercrime. Advantage of this convention ratification is Indonesia can braid cooperation with participant in the event of case of cybercrime which harming Indonesia especially if the perpetrator do the cybercrime outside region of Indonesia, position of Indonesia in apply for the extradition of perpetrator will become stronger.
Key Word: cybercrime, jurisdiction, international law

Abstrak

Menurut hukum internasional, negara memiliki batas-batas tertentu dalam menerapkan yurisdiksi untuk kasus yang melibatkan kepentingan negara lain. Salah satu batas tersebut dalam bentuk kewajiban setiap negara untuk menghindari kesulitan negara lain dalam upaya menerapkan yurisdiksi. Hukum Indonesia yang mengatur *cybercrime* adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), bagian mengatur yurisdiksi yang bagian ke-2 mencakup dasar teritorial subjektif bagi setiap orang melakukan *cybercrime* dan dikualifikasi berbahaya di Indonesia . Namun, dalam prakteknya, hal ini sulit untuk dilakukan jika kejahatan dilakukan dari luar Indonesia karena belum tentu setiap negara akan menyampaikan, meskipun UU ITE telah mengikuti ketentuan substantif dalam Konvensi tentang *cybercrime*,kecuali Indonesia ikut meratifikasi Konvensi c*ybercrim*e. Keuntungan Indonesia meratifikasi, Indonesia dapat menjalin kerjasama dengan peserta dalam hal kasus *cybercrime* yang merugikan Indonesia terutama jika pelaku melakukan *cybercrime* di luar wilayah Indonesia, posisi Indonesia dapat mengajukan ekstradisi terhadap pelaku akan menjadi lebih kuat.
Kata kunci: cybercrime, yurisdiksi, hukum internasional

Pendahuluan

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer. (AndiHamzah., 2000 : 23)

Perkembangan yang pesat dalam pemanfaatan jasa internet juga mengundang terjadinya kejahatan.C*ybercrime* merupakan perkembangan dari *computer crime*. Rene L. Pattiradjawane menyebutkan bahwa konsep hukum *cyberspace*, *cyberlaw* dan *cyberline* yang dapat menciptakan komunitas pengguna jaringan internet yang luas (60 juta), yang melibatkan 160 negara telah menimbulkan kegusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi, khususnya perlindungan terhadap milik pribadi. (Rene L. Pattiradjawane, 2000).

John Spiropoulos mengungkapkan bahwa cybercrime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya. (Jhon Sipropoulus, 1999) Hukum yang salah satu fungsinya menjamin kelancaran proses pembangunan nasional sekaligus mengamankan hasil-hasil yang telah dicapai harus dapat melindungi hak para pemakai jasa internet sekaligus menindak tegas para pelaku cybercrime.

Kriminalitas yang menggunakan internet sebagai media atau kerap disebut sebagai *cyber crime* telah melonjak drastis. Hal ini sesuai dengan adagium yang mengatakan bahwa "*crime is product of society itself*", di mana kejahatan dengan modus teknologi informasi ini akan semakin berkembang di dalam masyarakat yang semakin terbiasa dengan dunia maya. Secara sederhana *International Telecommunciation Union* (ITU) mengemukakan bahwa definisi dari *cybercrime* adalah kejahatan yang melibatkan komputer baik sebagai alat, target ataupun

perantara untuk melakukan kejahatan konvensional. ICT (2009: 17) Secara garis besar *cyber crime* terdiri dari beberapa jenis:

a. *Offences against Confidentiality, integrity and Availability of Computer Systems and Data*, adalah kejahatan yang bertujuan untuk mengakses, menyadap data atau system secara illegal. (ITU, 2009: 20-29).
b. *Content Related Offences*, adalah kejahatan komputer yang menggunakan konten dalam komputer untuk kejahatan seperti pornografi, menyebarkan fitnah, Judi .Dll. (ITU,2009 : 29)
c. *Copyright and Trademark Related Offences*, adalah kejahatan yang melanggar hak cipta atau merek dagang, seperti pembajakan. (ITU.,2009 : 41-45)
d. *Computer Related Offences,* adalah kejahatan yang menggunakan sistem komputer untuk mengambil data-data tertentu, seperti identitas, nomor tanda pengenal sampai rekening bank. (ITU.,2009 : 45-51)
e. *Combination Offences* , adalah kejahatan yang memadukan antara *cybercrime* dan kejahatan konvensional seperti *cyberterrorism*, *cyberwarfare*, dan *cyber laundering*. (ITU.,2009 : 51-59)

Permasalahan

Maraknya *cyber crime* disebabkan karena kemunculan internet kini diibaratkan seperti sebuah daerah perbatasan baru (*new frontier*) pada zaman *wildwest*. Wilayah baru ini bebas untuk di eksploitasi dan dieksplorasi tanpa ada hukum yang mengaturnya. (Golose., 2006: 30) Salah satu kesulitan besar dalam menangani masalah cybercrime adalah sifatnya yang sangat Transboundary (lintasbatas). Ia hampir tidak mengenal batas-batas negara. Kejahatan cyber di satu negara dapat dilakukan dari dan melalui negara lain manapun di dunia, dapat menentukan korbannya di belahan dunia manapun, dapat menyembunyikan identitas pelaku melalui sistem komputer yang berlokasi di negara manapun, dan

menyimpan bukti-bukti di negara lain yang jauh. (*Police Reported Statistics*, Catalogue no. 85-558-XIE).

Pembahasan

Penerapan Hukum di *Cyberspace*

Kebebasan Kontra Pengaturan

Kemunculan teknologi komputer yang diikuti dengan lahirnya internet telah membawa sejumlah konsekuensi, salah satunya adalah berupa terbentuknya suatu komunitas atau kelompok sosial baru. Sementara itu seiring dengan perkembangan teknologi komputer (internet) yang begitu pesat, jumlah komunitas tersebut semakin hari semakin bertambah. Akibatnya aktivitas yang terjadi di *cyberspace* yang melibatkan individu-individu yang biasa disebut *Netizen* pun semakin meningkat, baik itu aktivitas yang bersifat positif maupun aktivitas yang bersifat negatif. Berangkat dari fenomena ini, maka sejumlah kalangan menganggap perlu segera diadakannya pengaturan terhadap *cyberspace* beserta aktivitas-aktivitas yang terjadi disana. Dasar pemikirannya adalah hukum, sebagaimana kodratnya diperlukan di *cyberspace* agar aktivitas-aktivitas yang terjadi di atasnya dapat teratur dan terkontrol (UNESCO, 2000: 19). Sehingga tidak terjadi *radikalisme* di *cyberspace*. Kekhawatiran tersebut memang cukup beralasan mengingat akan konsep kebebasan (free access) yang berlaku di *cyberspace*. (www.cyberjurisdiction.net ,diakses pada 16 Mei 2013)

Ide yang diuraikan di atas secara tegas ditentang oleh kalangan, umumya adalah aktivis *cyberspace* yang menjunjung tinggi konsep kebebasan di internet (*cyber-space*) (VivekSood, 2000: 275). Mereka bahkan memandang *cyberspace* sebagai sesuatu yang berada di luar jangkauan negara, maka dari itu negara tidak dapat memberlakukan hukum di*cyberspace*. (UNESCO., 2000 : 219). Konsep kebebasan di *cyberspace* memungkinkan penggunanya dapat mengakses, menyimpan, mengirim informasi atau aktivitas lainnya secara bebas di internet. (VivekSood, 2000: 276). Pandangan ini berlawanan dengan pendapat sebelumnya yang menganggap *cyberspace* “hanyalah” media biasa yang digunakan oleh manusia untuk berkomunikasi, berinteraksi, dan berbisinis.

Kondisi Empiris

Walaupun tidak ada kesepakatan yang secara jelas mengakhiri perseteruan antara dua pendapat di atas, namun kondisi empiris yang ada sekarang setidaknya telah menggambarkan ke arah mana masyarakat hukum internasional berpihak, Sebagian besar cenderung menyetujui gagasan yang mengehendaki adanya pengaturan atau penerapan hukum terhadap *cyberspace* beserta aktivitas-aktivitas yang berlangsung disana. Keberpihakan ini antara lain ditandai dengan kemunculan sejumlah ketentuan hukum mengenai *cyberspace*, baik itu yang berlaku secara internasional maupun nasional. Ketentuan hukum mengenai *cyberspace* atau yang biasa disebut *cyberlaw* diterbitkan oleh sejumlah Negara sebagai reaksi dan antisipasi terhadap ancaman keamanan yang muncul sebagai konsekuensi dari perkembangan teknologi yang begitu pesat.

Secara umum, negara-negara yang telah memiliki *cyberlaw* dapat diklasifikasikan menjadi dua, Kelompok pertama adalah negara-negara yang memutuskan untuk membuat *cyberlaw* khusus. Beberapa negara yang termasuk dalam kelompok ini antara lain Amerika Serikat (Computer Fraud and Abuse Act), Inggris (Theft/Forgery and Counterfeiting Act), dan Singapura (Computer Misuse Act). (Wisnubroto, 2001 :26).

Sementara kelompok kedua adalah negara-negara yang hanya menyisipkan ketentuan mengenai *cyberspace* atau merevisi undang-undang pidana biasa yang ada. Belanda dan Prancis adalah contoh negara yang termasuk dalam kelompok negara kedua ini. 164 Keberpihakan ini semakin diperkuat dengan adanya sejum-lah ketentuan yang dikeluarkan beberapa organisasi internasional seperti PBB, Council of Europe, dan OECD (Organization for Economic Co-Operation Development).

Konsep Yurisdiksi di Cyberspace

Salah satu masalah paling krusial yang diminculkan oleh *cybercrime* adalah masalah yurisdiksi yang berkaitan dengan sejauh mana suatu negara dapat menerapkan kedaulatan hukumnya atau dengan kata lain sejauh mana kemampuan suatu negara menyidangkan suatu perkara bernuansa internasional. Permasalahan yurisdiksi di suatu negara dapat menerapkan kedaulatan hukumnya atau dengan kata lain sejauh mana kemampuan suatu negara menyidangkan suatu perkara bernuansa internasional.

Permasalahan yurisdiksi di *cybercrime* ini selajutnya memunculkan perbedaan pendapat antara dua kubu, perdebatan tersebut pada pertanyaan mengenai bagaimana seharusnya *cyberspace* diatur termasuk juga konsep yurisdiksi yang seharusnya berlaku di *cyberspace*. Kubu pertama menganggap bahwa *cyberspace* cukup diatur dengan hukum serta konsep yang selama ini ada dan digunakan dalam dunia nyata (kubu ini selanjutnya disebut dengan *Cyber-paternalist*). Sementara kubu kedua mempunyai pandangan bahwa *cyberspace* itu dunia yang khas, unutuk itu perlu ada hukum serta konsep tersendiri yang diberlakukan di *cyberspace*. Pandangan ini mencoba memisahkan *cyberspace* dengan dunia nyata (kubu ini selanjutnya disebut dengan *cyber-libertarian*) (Andrew D. Murray, 2007).

Di tengah perdebatan yang alot mengenai hal ini, David R. Johnson mencoba menawarkan empat model yang patut dipertimbangkan sebagai solusi, keempat model tersebut antara lain: (David R. Johnson and David G., 1996)

a) Pelaksanaan kontrol dilakukan oleh badan-badan peradilan yang saat ini ada;
b) Mengadakan kesepakatan internasional mengenai pengaturan *cyberspace*;
c) Membentuk organisasi internasional yang khusus mengatur *cyberspace*;
d) Pengaturan sendiri oleh pengguna internet (*self-governance*).

Internasional yang khusus mengatur segala aspek tetang *cyberspace*. Gagasan ini bisa jadi adalah solusi terbaik bagi masalah ”ketidakjelasan” pengaturan di *cyberspace*. Berkaitan dengan gagasan tersebut, UNESCO dalam terbitannya berjudul “*The International Dimensions of Cyberspace Law*”

berpendapat bahwa tidak dapat dipungkiri bahwa keberadaan sebuah organisasi internasional akan mempunyai peran yang penting dalam perkembangan cyberspace (UNESCO, 2000: 42). Alasan yang mendasari gagasan ini adalah bahwa dengan adanya organisasi internasional ini semua negara dapat menyesuaikan atau menyeragamkan peraturan mengenai segala sesuatu yang berkaitan dengan *cyberspace*.Namun UNESCO dalam hal ini mengingatkan bahwa pembentukan organisasi internasional baru juga memiliki permasalahan-permasalahan yang harus dijawab. Beberapa permasalahan yang dimaksud antara lain berkaitan dengan dasar kewenangan, jaminan obyektivitas, jaminan perlindungan terhadap golongan minoritas, dan sebagainya.(UNESCO., 2000 : 42).

Yurisdiksi Negara Dalam Menangani Kasus Cybercrime

Yurisdiksi Menurut Convention on Cybercrime

Permasalahan yurisdiksi dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa, secara khusus ditempatkan pada pasal tersendiri yakni pada pasal 22.Pasal yang terdiri dari lima ayat tersebut antara lain berbunyi sebagai berikut (CDPC., 25 Mei 2001) :

1. *Each Party shall adopt such legislative and other measures as may benecessary to establish jurisdiction over any offence established in accordancewith Articles through 11 of this Convention, when the offence is committed:*

   a. in its territory; or
   b. on board a ship flying the flag of that Party; or
   c .on board an aircraft registered under the laws of that Party; or

   d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside theterritorial jurisdiction of any State.

2. *Each Party may reserve the right not to apply or to apply only in specificcases or conditions the jurisdiction rules laid down in paragraphs 1.b through1.d of this article or any part thereof.*
3. *Each Party shall adopt such measures as may be necessary to establishjurisdiction over the offences referred to in Article 24, paragraph 1, of thisConvention, in cases where an alleged offender is present in its territory andit does not extradite him or her to another*

Party, solely on the basis of his orher nationality, after a request for extradition.

4. *This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.*
5. *When more than one Party claims jurisdiction over an alleged offence stablished in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*

Terjemahan bebas dari pasal 22 ini adalah :

1. Setiap Negara yang menjadi peserta dalam konvensi ini sebaiknya mengambil langkah-langkah di bidang legislasi dan bidang lainnya yang dianggap perlu untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan yang tercantum dalam pasal 2-11 konvensi ini,dalam hal kejahatan tersebut berlangsung di :

   a. Di wilayah negara tersebut,
   b. Di atas kapal berbendera negara tersebut,
   c. Diatas pesawat yang terdaftar menurut hukum negara tersebut, Kejahatan yang dilakukan oleh warganegaranya, dalam hal perbuatan yang dilakuakan tersebut dikategorikan sebagai tindak kejahatan menurut hukum pidana dimana perbuatan itu terjadi atau jika perbuatan tersebut berlangsung di luar wilayah yurisdiksi negara.
2. Setiap negara berhak untuk memilih apakah akan menerapkan atau tidak ketentuan yurisdiksi dalam bagian 1b-1ds diatas dengan mempertimbangkan kondisi serta kasus tersebut.
3. Setiap peserta dalam konvensi ini sebaiknya mengambil langkah-langkah yang dianggap perlu untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan berdasarkan pasal 24 bagian pertama konvensi ini, dalam hal tersangka berada di wilayahnya dan tidak dilakukan ekstradisi atas dirinya dengan pertimbangan status kewarganegaraannya. Dewan Eropa melalui *Commitee of Experts on Crime in Cyberspace* (PC-CY) sebagai panitia perumus konvensi ini menerbitkan penjelasan resmi mengenai pasal-pasal dalam konvensi tersebut. Penjelasan tersebut dimuat dalam suatu dokumen yang dinamakan *Expalanatoty Report of The Draft Convention on Cybercrime* yang telah disetujui pada bulan November 2001.Pasal 22 ini memuat sejumlah criteria yang mewajibkan setiap pihak dalam konvensi ini untuk menerapkan yurisdiksinya terhadap kejahatan-kejahatan yang disebutkan mulai dari pasal 2 hingga pasal 11 dalam konvensi ini. Kejahatan-kejahatan tersebut antara lain :
   1) Penyadapan secara tidak sah (*illegal interception*),
   2) Memasuki suatu sistem komputer secara tidak sah (*illegal access*),
   3) Intervensi terhadap data (*data intervention*),
   4) Intervensi terhadap sistem (*system interference*),

5) Penyalahgunaan alat (*misuse of device*),
6) Pemalsuan melalui komputer (*computer related forgery*),
7) Penipuan melalui komputer (*computer realted fraud*),
8) Kejahatan pornografi anak (*offences related to child pornography*),
9) Pelanggaran hak cipta dan hak-hak lainnya yang terkait (*offencesrelated to infringements of copyright and related rights*),
10) Segala bentuk percobaan, pembantuan, dan persekongkolan yang berkaitan dengan kejahatan-kejahatan tersebut di atas.(<www.coe.net>, diakses pada tanggal 4 April 2013).

Ayat pertama dalam pasal ini menganut prinsip teritorial, artinya setiap negara yang menjadi pihak dalam konvensi ini berhak mengadili terhadap kejahatan-kejahatan yang tercantum dalam konvensi ini yang dilakukan di wilayahnya.

1. Keberadaan konvensi ini tidak mengesampingkan penerapan yurisdiksi criminal berdasarkan hukum nasional suatu negara.
2. Apabila lebih dari satu pihak mengklaim yurisdiksi atas suatu kejahatan yang terdapat dalam konvensi ini, maka para pihak yang terlibat sebaiknya mengadakan konsultasi dalam menentukan yurisdiksi yang tepat.

Contoh misalnya suatu Negara dapat menerapkan yurisdiksi teritorialnya jika baik pelaku maupun sistem komputer yang diserang berada di wilayahnya atau jika sistem komputer yang diserang berada di wilayahnya, tetapi pelakunya tidak berada di wilayahnya. (<www.coe.net>, diaksespadatanggal 4 April 2013). Pada awal perumusannya, dalam pasal ini juga dipertimbangkan untuk memasukkan klausul yang memungkinkan suatu Negara perserta konvensi menerapkan yurisdiksinya berdasarkan jenis kejahatan dalam konvensi ini yang melibatkan satelit yang terdaftar pada negara tersebut. Namun tim perumus konvensi pada akhirnya menganggap hal ini tidak perlu mengingat kejahatan yang melibatkan satelit bagaimanapun juga selalu berasal dari bumi dan tertuju ke bumi. Dalam hal ini, salah satu dasar penentuan yurisdiksi yang tercantum dalam ayat (1) butir (a) hingga (c) dapat diterapkan oleh suatu negara jika transmisi melalui satelit tersebut berasal atau dilakukan di luar wilayahnya. Sementara ayat (1) butir (d) dapat diterapkan jika kejahatan tersebut dilakukan oleh warganegara

yang bersangkutan dan dilakukan di luar wilayah yurisdiksi negara tersebut. Selanjutnya sempat dipertanyakan juga apakah tepat jika menempatkan negara dimana satelit tersebut terdaftar sebagai penentuan yurisdiksi kriminal, mengingat dalam banyak kasus sebenarnya tidak ada hubungan yang berarti antara kejahatan yang dilakukan dengan negara tempat satelit tersebut terdaftar karena pada dasarnya fungsi satelit hanya sebagai pengirim. (<www.coe.net>, diakses pada tanggal 4 April 2013).

Pasal 22 Ayat 1 butir b dan c menganut prinsip teritorial yang diperluas, dimana dimungkinkan setiap Negara menrapkan yurisdiksinya terhadap kejahatan yang dilakukan di kapal laut yang mengibarkan bendera atau pesawat yang terdaftar menurut hukum negara tersebut. Prinsip ini secara praktek telah dikenal luas dan tercantum dalam beberapa hukum nasional sejumlah negara, khususnya semenjak kapal laut dan pesawat dianggap sebagai perluasan dari yurisdiksi suatu negara. Penerapan ini hanya akan berguna jika kapal laut atau pesawat tersebut berada di luar yurisdiksi negara yang dimaksud.(<www.coe.net>, diakses pada tanggal 4 April 2013). Pasal Ayat (1) butir (d) berisi prinsip nasionalitas yang banyak oleh negara-negara penganut sistem *civil law*. Prinsip ini memungkinkan seorang warga negara diproses menurut hukum negaranya atas suatu perbuatan yang dilakukan di luar wilayah yurisdiksi negara yang bersangkutan. (Ayat (2) memuat ketentuan yang memungkinkan negara peserta konvensi untuk melakukan pengecualian (persyaratan) terhadap ayat (1) butir (b), (c), dan (d).

Sementara pengecualian tersebut tidak diperkenankan terhadap pemberlakuan yurisdiksi teritorial seperti yang tercantum dalam butir a, atau terhadap penerapan yurisdiksi berdasarkan prinsip *autdedereautjudicare* (pengekstradisian atau penuntutan) seperti yang tercantum dalam ayat 3 yakni dalam hal suatu Negara menolak untuk mengekstardisi seorang pelaku kejahatan karena status kewarganegaraannya serta pelaku berada di wilayah negara tersebut. Ketentuan ayat 3 tersebut perlu untuk menjamin bahwa Negara peserta konvensi yang menolak mengekstradisi tetap mempunyai kewenangan untuk melakukan penyelidikan dan prosedur hukum lainnya terhadap warganegaranya, jika ekstradisi tersebut diminta oleh negara peserta konvensi lainnya berdasarkan

syarat-syarat dalam Pasal 24 ayat (6), yang berbunyi bahwa jika permintaan ekstradisi terhadap pelaku kejahatan-kejahatan dalam konvensi ini ditolak dengan alasan status kewarganegaraannya atau pihak yang diminta menganggap mereka mempunyai yurisdiksi terhadap kejahatan tersebut, maka negara yang menolak tersebut harus menyampaikan kepada pihak yang meminta serta memberikan laporan hasil proses yang dilakukan.

Dasar penerapan yurisdiksi yang tercantum dalam ayat 1 tidak bersifat baku, karena dalam ayat (4) disebutkan bahwa negara peserta konvensi diperkenankan untuk mempergunakan jenis yurisdiksi lainnya yang didasarkan pada hukum nasionalnya masing-masing. Dalam hal kasus kejahatan yang melibatkan sistem komputer, terdapat kemungkinan dimana lebih dari satu negara peserta yang mengklaim mempunyai yurisdiksi terhadap kejahatan tersebut. Misalnya, banyak kejahatan seperti serangan virus, penipuan, atau pelanggaran hak cipta yang dilakukan lewat internet dengan korban lebih dari satu negara. Oleh karena itu, untuk menghindari persaingan antar negara dalam hal penegakan hukum, maka negara peserta yang terlibat dalam situasi tersebut dapat mengadakan perundingan untuk menentukan yurisdiksi yang tepat terhadap kejahatan yang dimaksud. Perundingan yang dimaksud tidak bersifat wajib, melainkan hanya dilakukan jika dianggap perlu. Sebagai contoh misalnya salah satu pihak yang memiliki kepentingan atas suatu kejahatan yang melibatkan lebih dari suatu negara telah mendapat pemberitahuan bahwa pihak lain yang juga memiliki kepentingan tidak akan mengajukan tuntutan apa-apa.

Berdasarkan uraian mengenai Pasal 22 beserta penjelasannya di atas, dapat dilihat bahwa *Convention on Cybercrime* ciptaan Dewan Eropa ternyata masih menggunakan konsep yurisdiksi yang selama ini dikenal dan dipergunakan secara internasional. Selain itu, meskipun tidak secara tegas menyatakan dukungan terhadap konsep analogi, konvensi ini cenderung ‘melepaskan’ diri dari konsep pemisahan.Sikap ini dimaklumi, mengingat desakan untuk menciptakan hukum tersendiri terhadap *cyberspace* selama ini masih sebatas wacana yang terus berkembang dan praktis belum ada konsep yang jelas mengenai hal ini. Sementara disisi lain, intensitas kejahatan komputer yang merupakan dampak negatif dari

kecanggihan komputer terus meningkat. Kondisi ini akan berbahaya dan dapat menimbulkan ‘anarkisme’ di *cyberspace* jika tidak segera dibuat suatu produk legislasi yang nantinya berfungsi menertibkan segala aktivitas di *cyberspace*. (Mark D. Rasch., 1996). Lebih jauh lagi, dengan adanya ketentuan mengenai yurisdiksi yang tercantum dalam Pasal 22, maka Negara peserta konvensi mempunyai ‘sandaran’ hukum yang pasti dalam menerapkan yurisdiksinya terhadap *cybercrime* sehingga konflik yang potensial terjadi karena perebutan penerapan yurisdiksi dapat dihindari. Potensi konflik yurisdiksi dapat terjadi jika: (*Convention on Transfer of Proceedings Explanatory Report*, Poin 16)

a) Beberapa Negara mengklaim yurisdiksi terhadap suatu kasus berdasarkan prinsip tempat dimana kejahatan tersebut dilakukan
b) Beberapa Negara mengklaim yurisdiksi berdasarkan prinsip yang berbedabeda (Negara A berdasarkan prinsip Nasionalitas Aktif, Negara B Berdasarkan Nasionalitas Pasif, Negara C berdasarkan teritorialitas).

Dalam *Convention on Cybercrime* tidak diatur mengenai solusi akan hal ini, para Pihak hanya diminta untuk berunding dalam menentukan siapa yang lebih berhak mengklaim yurisdiksi. Namun solusi atas hal ini sudah diatur jauh sebelum pembentukan *Convention on Cybercrime*, yakni pada tahun 1972 pada saat pembentukan *European Convention on Transfer of Proceedings*, dalam *explanatory report* konvensi tersebut disebutkan bahwa Negara yang mengklaim harus membuat sebuah daftar prioritas penentuan yurisdiksi dari prinsip tempat kejahatan dilakukan. ((*Convention on Transfer of Proceedings Explanatory Report*, Poin 18)

Kerjasama Internasional Dalam Mengatasi Konflik Yuirsdiksi

Berbagai cara dilakukan oleh negara-negara untuk menyelesaikan permasalahan yurisdiksi, namun apabila pelaku *cybercrime* berada di luar wilayah negara yang terkena dampak paling besar, maka harus dipikirkan bagaimana cara membawa pelaku tersebut ke negara tersebut. Cara yang biasa ditempuh oleh Negara-negara adalah melalui jalur kerjasama internasional. Berikut adalah

bentuk kerjasama internasional yang ditempuh negara-negara untuk membawa pelaku *cybercrime* agar dapat diadili di negaranya:

. 1. Ekstradisi dan Deportasi
2. Bantuan Timbal Balik (Mutual Legal Assistance)
3. Pengalihan Perkara (*Transfer of Proceedings*)

Pengaturan Mengenai Cybercrime Di Indonesia

Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Secara umum Undang-Undang ini mengatur tentang segala sesuatu mengenai data elektronik dan pemanfaatannya untuk kepentingan umum. Pada awal pembentukannya undang-undang ini menuai banyak kontroversi karena dianggap akan mematikan kebebasan untuk mengekspresikan diri di *cyberspace*. Dalam undang-undang ini secara rinci dijelaskan mengenai segala perbuatan yang digolongkan sebagai *cybercrime*, jenis-jenis perbuatan ini diatur dalam Pasal 27sampai Pasal 37.

Transfer of Proceeding* dalam kasus *Transboundary Cybercrime

Transfer ofproceeding merupakan hal yang baru dalam dunia hukum pidana dan karena konvensi internasional yang mengatur mengenai *transfer of proceeding* hanya satu yaitu *European Convention on Transfer of Proceeding*. Menurut konvensi tersebut kejahatan yang bisa dimintakan *transfer of proceeding* adalah kejahatan yang termasuk dalam ranah hukum pidana. (*Transfer of proceedings Convention* Pasal 1 huruf a) Untuk melihat apakah *cybercrime* termasuk dalam ranah hukum pidana, maka kita harus melihat pengaturan dari beberapa negara Eropa:

Belanda

Peraturan mengenai *cybercrime* di Belanda dimulai tahun 1993 dimana dibentuk satu undang-undang baru yang disebut *Computer Crime Act* (*wetcomputer criminaliteit)* yang lalu diaman deman pada tahun 2006 untuk menyesuaikan

dengan *convention on cybercrime*. (Bert-JaapKoops., 2008) Undang Undang ini merupakan bagian dari Kitab Undang-Undang Hukum Pidana (*wetboek van strafrecht*)

.

Denmark

Di Denmark *cybercrime* diatur dalam Kitab Undang-Undang Hukum Pidana (*strafloven)* dan Undang-Undang Khusus. Bentuk *cybercrime* yang pertama kali diatur dalam KUHP. Denmark adalah kejahatan yang berhubungan dengan data (*datacrime/data kriminalitet*). (Henrik-SpangHansen,IT Law Series., 2008 : 159)

Jerman

Di Jerman *cybercrime* diatur dalam *strafgesetzbuch* (KUHP) yang pengaturannya pertama kali muncul di tahun 1986, adapun jenis *cybercrime* yang diatur adalah *hacking*, pengubahan data, *computer sabotage*, *computer fraud* dan penipuan. (Ulrich Sieber., 2008 : 183) Dari beberapa peraturan mengenai *cybercrime* diatas, maka dapat disimpulkan bahwa *cybercrime* termasuk ke dalam ranah hokum pidana sehingga *transfer of proceeding* dapat dilakukan untuk pelaku *transboundary cybercrime* adapun alasan dan prosedur *transfer of proceeding* adalah sebagai berikut:

Permintaan *Transfer of Proceeding*

Apabila seseorang diduga telah melakukan kejahatan menurut hukum negara peserta, maka sesuai dengan kondisi yang disyaratkan oleh konvensi ini bisa meminta negara peserta lainnya untuk memproses orang tersebut. Adapun kondisi yang memungkinkan seseorang dimintakan untuk diproses di negara peserta lainnya adalah:

a) Apabila terduga tinggal di negara yang dimintakan (*Requested State)*;
b) Apabila terduga merupakan warga negara negara yang dimintakan atau berasal dari negara yang dimintakan;
c) Apabila terduga sedang menjalani hukuman berupa pencabutan kebebasan (kurungan atau penjara);
d) Apabila terduga sedang menjalani proses peradilan atas kejahatan yang sama di negara yang dimintakan;
e) Apabila transfer of proceeding ditujukan untuk lebih memperjelas permasalahan atau bukti yang paling jelas ada di negara yang dimintakan;
f) Apabila penegakan hukum di negara yang dimintakan dirasa mampu untuk merehabilitasi yang bersangkutan;
g) Apabila terduga/terdakwa dipastikan tidak mampu untuk menghadiri persidangan di negara yang meminta;
h) Apabila cara yang lain (ekstradisi) dirasa tidak mampu untuk menghadirkan terduga/tersangka.

Prosedur *Transfer of Proceeding*

1. Permintaan diajukan oleh negara peminta melalui Kementerian Kehakiman ke Kementerian negara yang diminta. (Pasal 13 ayat (1))
2. Apabila permintaan tersebut terkait dengan kasus yang memerlukan aksicepat, maka permintaan dapat diajukan melalui Interpol. (Pasal 12 ayat (2))
3. Apabila negara yang diminta merasa dokumen permintaan yang dilampirkan belum cukup, maka mereka bisa meminta negara peminta untuk melengkapi dokumen tersebut dalam jangka waktu tertentu. (Pasal 14)
4. Setiap permintaan harus disertai dengan dokumen-dokumen hukum yang sah baik berupa dokumen asli maupun salinan yang telah di legalisir, namun apabila tersangka sudah terlebih dahulu ditangkap, maka dokumen tersebut dapat dikirimkan menyusul.

Di Indonesia sendiri memang belum dikenal *Transfer of Proceedings* meskipun kata-kata ini sudah muncul di beberapa Undang-Undang salah satunya adalah Undang-Undang No 1 Tahun 2006 Tentang Bantuan Timbal-Balik (*Mutual Legal Asssitance*) dimana dalam pasal 4 menyebutkan bahwa Undang-Undang ini tidak berlaku untuk *transfer of proceedings* (Undang-Undang Tentang Bantuan Timbal Balik No 1 Tahun 2006, pasal 4). Hal ini sangat disayangkan karena sesuai dengan definisi yang diberikan oleh *European Convention on Transfer of Proceedings*, *transfer of proceedings* itu sendiri adalah bentuk kerjasama yang berbentuk *mutual legal assistance* sehingga dengan pembatasan yang diatur dalam Undang-Undang ini menutup kemungkinan dilakukannya *transfer of proceedings* di Indonesia. Penulis sendiri berpendapat bahwa *transfer of proceedings* seharusnya dapat dilakukan di Indonesia khususnya dalam penanganan kasus *cybercrime*, hal ini didasari atas pengaturan yang ada dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) dimana dalam pasal 43 ayat 8 berbunyi" (Undang-Undang InformasidanTransaki Elektronik, *Loc.cit*, pasal 43 ayat 8

> "*Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.*"

Dari rumusan pasal diatas kata-kata "berbagi informasi dan alat bukti" dengan penyidik negara lain dapat dilakukan salah satunya dengan melakukan *transfer of proceedings* terhadap seseorang yang diduga telah melakukan tindak pidana *cybercrime* yang merugikan Indonesia, hasil dari *transfer of proceedings* tersebut nantinya akan dikirimkan ke Indonesia sebagai acuan untuk penanganan kasus *cybercrime* di masa yang akan datang.

Kesimpulan

Meskipun Undang-Undang Informasi dan Transaksi Elektronik sudah mengikuti ketentuan dalam *Convention on Cybercrime* secara substantif, namun ada baiknya Indonesia ikut meratifikasi *Convention on Cybercrime*. Keuntungan dari meratifikasi konvensi ini adalah Indonesia bisa menjalin kerja sama dengan peserta apabila terjadi kasus *cybercrime* yang merugikan Indonesia terutama jika

si pelaku melakukan *cybercrime* tersebut di luar wilayah Indonesia, posisi Indonesia dalam mengajukan permohonan untuk mengekstradisi pelaku akan menjadi lebih kuat. Keuntungan lain adalah Indonesia dapat menjalin kerjasama di bidang teknologi informasi agar Indonesia tidak ketinggalan dalam penanganan kasus *cybercrime*. Harus ada perubahan peraturan perundang-undangan (amandemen) yang memungkinkan dilakukannya *transfer of proceedings* di Indonesia, salah satunya adalah dengan mengamandemen Undang-Undang Tentang Bantuan Timbal Balik (*Mutual Legal Assistance*) terutama pasal 4 yang memberikan pembatasan bagi dilakukannya *transfer of proceedings* di Indonesia. Setelah pengamandemenan UU tersebut pemerintah bisa mulai membahas prosedur *transfer of proceedings* di Indonesia.

Daftar Rujukan

Andi Hamzah, 2000, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta

Andrew D. Murray,2007. *The Regulation in Cyberspace :Control in the Online Environment*, Routelage& Cavendish.

Bert-JaapKoops, *Cybercrime Legislation in Netherlands*, Netherland Comparative Law Association*Convention on Transfer of Proceedings Explanatory Report*, Poin 16Crime", The National Cybercrime Training Partnership, Introduction.

"*Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police Reported Statistics*", Canadian Centre for Justice Statistics: Catalogue no. 85-558-XIE.

David R. Johnson and David G. Post,1996. *"And How Should The Internet Be Governed?"*, The American Lawyer.

European Committee on Crime Problems (CDPC),2001. "Final Draft Convention on Cybercrime", Strasbourg, 25 Mei

"Expalantory Report of Convention on Cybercrime",2001 Adopted November

ITU, 2009. *Understanding cybercrime guide,* ICT Appliccation dan Cybersecurity Division, hal 17.

Jhon Sipropoulus, 1999, "*Cyber Crime Fighting*, The Law Enforcement Officer's Guide to Online.

Juliet M, Oberding and Treje Norderhaug, "*A Separate Jurisdiction for Cyberspace"*.

Petrus Reinhard Golose,2006. Perkembangan Cyber Crime dan Upaya Penanganannya oleh POLRI, "Buletin Hukum Perbankan dan Kebanksentralan", Vol. 4 no. 2, Agustus ,Jakarta

Rasch, Mark D,1996. *Criminal Law and The Internet*, Computer Law Association

Rene L. Pattiradjawane,2000. "*Media Konverjensi dan Tantangan Masa Depan*", Kompas, 21 Juli

UNESCO.2000.*The International Demension of Cyberspace Law*. Ashgate Publishing Ltd.,England..

VivekSood,2001. *Cyber Law Simplified*, Tata Mc Graw-Hill Publishing Co.Ltd, New Delhi

Wisnubroto, A.L,2001. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Penerbitan Universitas Atmajaya Yogyakarta

<www.coe.net>, diakses pada tanggal 4 April 2013.

<www.cyberjurisdiction.net> ,diakses pada 16 Mei 2013.