URGENSI *CONVENTION ON CYBERCRIME* TAHUN 2001 DALAM RANGKA PEMBENTUKAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DI INDONESIA

Suardi

Abstrak

Implikasi yang ditimbulkan oleh kemajuan teknologi informasi telah berdampak kepada dua aspek dalam perilaku manusia itu sendiri, yang pertama bahwa masyarakat dunia dalam percepatan untuk mendapatkan informasi baik ilmu pengetahuan dan teknologi telah membutuhkan komonokasi teknologi tinggi untuk memberikan informasi tentang perkembangan ilmu pengetahuan dan teknologi dalam berbagai aspek kebutuhan masyarakat dunia. Kedua cenderung kemajuan teknologi informasi telah dijadikan komoditi untuk melakukan kejahatan siber (cybercrime), baik kejahatan berupa hacking, pembobolan kartu keredit melalui situs internet (carding) dan bentuk lain dari kejahatan siber yang tidak dapat dibatasi oleh territorial suatu Negara karena sipat dari media internet yang tidak lagi mengenal batas-batas territorial suatu Negara. Sementara di sisi lain, pelaku kejahatan berada diluar wilayah territorial dan Negara yang menjadi korban tidak dapat mengadili pelaku kejahatan dengan alasan yurisdiksi suatu Negara.

Dengan demikian urgensi Convention cybercrime untuk ditatifikasi sangatlah penting karena di dalamnya telah

menekankan kepada semua Negara untuk melakukan kerjasama internasional dalam memberantas cybercrime yang bersifat global dan tanpa batas itu. Konsekwensi logis dari ratifikasi ini adalah Indonesia harus dapat menyesuaikan segalah aturan perundang-undangannya serta membangun kerjasama internasional baik dalam tehnologi informasi maupun

Kata Kunci : Urgensi Convention on cybercrime dan implikasinya terhadap aturan nasinal Indonesia

A. Latar Belakang

Perkembangan teknologi informasi menjadikan dunia seolah-olah tidak mengenal batas territorial dan menjadikan masyarakat dunia menjadi suatu masyarakat dalam satu lingkup dunia yang satu . Kemajuan tersebut merupakan kontribusi besar yang diberikan oleh hasil teknologi yang diberi nama *Internet*. Sekarang masyarakat dunia dengan begitu mudah dapat berkomunikasi dengan warga negara dunia di belahan dunia yang hanya dengan menekan tombol yang tersedia di internet. Pada level pemerintahan pun membuka situs mereka di internet untuk melayani masyarakatnya yang membutuhkan informasi dalam bentuk *e-govermnet*.

Namun, sisi lain perkembangan teknologi informasi menimbulkan persoalan bagi masyarakat dunia maya. Kemajuan itu membuka peluang bagi munculnya jenis-jenis kejahatan baru yang selama ini kita anggap sebagai suatu hal yang mustahil dapat dilakukan. Tepat kiranya bila dikemukakan satu pernyataan teori bahwa *crime is product of society it self*, masyarakat sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat peradaban suatu masyarakat, maka semakin canggih pula suatu kejahatan yang terjadi dalam masyarakat.[1] Sejauh ini benyak kasus penyalahgunaan Internet untuk tujuan kejahatan yang merugikan Indonesia. Ketika

[1] Ari Juliana Gema, *Cybercrime :Sebuah Fenomena di Dunia Maya*, diakses dari situs www.click legal solution.com pada tanggal 7 maret 2005.

masalah tuntutan kemerdekaan Timor-timur menghangat pada tahun 1997 situs milik Departemen Luar negeri dan TNI dijebol oleh *cracker Porto (*Portugis) yang pro-kemerdekaan. Ketika Pemilihan umum langsung dilakukan di Indonesia situs resmi KPU dijebol oleh *hacker*. Penjebolan situs KPU tersebut menyebabkan berubahnya nama partai peserta pemilu dan jumlah perolehan suara berubah.[2] Pada tahun 2005 situs Departemen Hukum dan Perundang-undangan menjadi sasaran perusakan oleh *cracker* sebagai bentuk protes mereka terhadap kebijakan pemerintah yang menaikan harga BBM.

Kejahatan dengan menggunakan internet dilakukan dengan modus yang lain yaitu melakukan transaksi lewat internet dengan menggunakan kartu kredit orang lain secara melawan hukum. Lembaga intelejen dunia maya internasional, *Versign* melaporkan Indonesia merupakan negara dengan peringkat pertama yang melakukan kejahatan siber (*cybercrime*), kemudian disusul oleh Nigeria dan Pakistan. Pemberian peringkat ini didasarkan pada banyaknya transaksi yang dilakukan dengan melawan hukum yang berasal dari Indonesia. Di kota Bandung sendiri pelaku *cybercrime* yang sampai saat ini telah diadili sebanyak 10 orang. Para pelaku tersebut telah melakukan kegiatan *carding* (pembobolan kartu kredit melalui internet) lebih 200 kali.[3]

Kejahatan siber merupakan kejahatan yang mempunyai karakteristik tersendiri yang berbeda dengan kejahatan konvensional pada umumnya. Perbedaan yang mencolok adalah terletak pada modus dan sarana kejahatan.. Para ahli hukum mengkategorikan kejahatan ini sebagai *White collar Crime*.[4] Oleh karena kekhasan sifatnya tersebut, maka pemberantasan

---

[2] Dalam kasus penjebolan situs KPU ini Polisi melalui unit khusus Cybercrime Polda Metro jaya berhasil menangkap pelaku, yang ternyata seorang mahasiswa salah satu perguruan tinggi di indonesia.

[3] Kompas, *Indonesia peringkat pertaman dalam " Cybercrime"* edisi 4 september 2004.

[4] Ronny Nitibaskara, *Problema Yuridis Cybercrime,* makalah pada seminar tentang *Cyber Law* , diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 juli 2000, hlm.2 dan 5

kejahatan ini harus dilakukan dengan cara yang berbeda yang mengikuti perkembangan teknologi informasi. Dalam konteks Indonesia sampai saat ini belum terdapat pengaturan khusus yang mengatur kejahatan berteknologi tinggi. Oleh karena itu Kebutuhan akan perangkat hukum dan profesionalisme penegak hukum mutlak dibutuhkan dalam memberantas kejahatan ini.

Pada tataran internasional, kejahatan siber telah menyita perhatian masyarakat internasional, karena sifat dari kejahatan ini yang bersifat global dan tanpa batas. Sebuah negara dapat saja menjadi korban dari kejahatan yang dilakukan oleh warga negara lain. Kejahatan *hacking, carding* dan bentuk lain dari kejahatan siber tidak dapat dibatasi oleh teritorial suatu negara karena sifat dari media internet yang tidak lagi mengenal batas-batas teritorial. Sementara di sisi lain, pelaku kejahatan berada di luar wilayah teriotorialnya dan negara yang menjadi korban kejahatan tidak dapat mengadili pelaku kejahatan dengan alasan yurisdiksi suatu negara. Menyadari kondisi demikian maka kerjasama internasional dalam memberantas kejahatan siber merupakan suatu keniscayaan. Menjawab masalah itu, pada tahun 2001 masyarakat Uni Eropa menandatangani suatu konvensi yang mengkriminalisasi kejahatan siber sebagai tindak kejahatan yang harus diberantas dengan hukum nasional negara anggota. Yang menarik dari konvensi ini adalah diperbolehkannya negara di luar anggota Uni Eropa untuk meratifikasi konvensi ini sepanjang negara tersebut mempunyai perhatian yang besar dalam memberantas kejahatan siber. Ketentuan ini memberikan kemungkinan bagi Negara lain termasuk Indonesia untuk meratifikasi Konvensi ini sebagai bagian dari hukum nasional Indonesia dalam usaha pemberantasan kejahatan siber.

B. Identifikasi Masalah

Berdasarkan uraian latar belakang di atas maka dirumuskan permasalahan dalam makalah ini, yang kemudian akan di bahas dalam pembahasan yaitu :

1. Sejauh manakah urgensi *convention on cybercrime* tahun 2001 dalam rangka pembentukan undang-

undang informasi dan transaksi elektronik indonesia ?

2. Apakah implikasi yuridis ratifikasi *Convention on Cybercrime* tahun 2001 bagi hukum nasional Indonesia ?

II. TINJAUAN PUSTAKA

A. Tinjauan Singkat tentang *Cybercrime*

Nazura Abdul Manap memberikan batasan tantang kejahatan siber adalah:

> *...cybercrimes are crimes are commited could extend throught internet online. This means that crimes committed could extend to other counties, which is beyond the Malaysian jurisdiction . Any way, it causes no harm to refer computer crimes are as cybercrimes or vice versa, since they have some impact in law.*[5]

Definisi tersebut berbeda dengan kejahatan computer (*computer crime*). Kejahatan komputer diartikan sebagai:

> " *...computer crime could reasionable include a wide variety crime offences, activities issues. It is also known as a crime committed using a computer as tool and its involves direct contact between the crime and the computer. Forinstance, a dishonest bank clerk who unauthorisedly transfers a custumer's money to a dormant account for his own interest or a person' without permission has obtained acces to other persons computer directly to download information, which in the first place, are cofidental. These situations requare dicect access by the hacker to the first computer. There is no internet line involved, or only limited networking used such as the local area Network.*[6]

---

[5] Nazura Abdul Manap, *Cybercrimes : Problems and Solution Under Malaysian Law,* Makalah pada seminar nasional Money laundring dan cyberrime dalam perspektif penegakan hukum Indonesia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 februari 2001, hal. 3 sebagaimana dikutip dari Budi Raharjo, *Cybercrime... Op.cit hlm.227*

[6] Ibid.

Selanjutnya Nazura Abdul Manap membedakan *cybercrime* dalam tiga tipe :

a. *Cybercrimes against property* meliputi theft berupa *theft of information, theft of property,* dan *theft of services,fraud/cheating, forgery* dan *minshief*
b. *Cybercrimes against persons,* meliputi pornografi, *cybeharassment, cyberstalking, cybertrespass. Cyberstrepass* meliputi *spam E-mail, hacking a web page dan breaking into personal computer*
c. *Cyber-terrorism.*

Kongres PBB tentang pencegahan tindak pidana dan perlakuan terhadap pelakunya yang diadakan pada tahun 2000 membagai dua kategori *cybercrime* yaitu

> *cybercrime in narrow sense (computer sense)* yaitu *any illegal behaviour directed by means of electronic operations that targets the security of computer system and the data prossed by them* dan *cybecrime in a broader sense (computer related crime)* yang meliputi *any illegal behaviour commited by means of or in relation to a computer system network, including such crimes as illegal possession, offering or distributing information by means of computer system or network.*

Konvesi Internasional tentang *Cybercrime* pada tahun 2001 tidak memberikan definisi tentang *Cybercrime*. Dalam konvensi ini hanya memberikan berbagai bentuk *cybercrime* yamg dapat dilarang dalam hukum nasional negara anggota.bentuk perbuatan yang dilarang itu adalah *Illegal acces, illegal interception, illegal interference, system interference, computer related forgery, computer related fraud, offences related to child pornography, offences related to infringments of copyright and related rights.*

Uraian tentang batasan *cybercrime*di atas terlihat bahwa belum ada keseragaman pendapat tentang *cybercrime.* Dalam instrumen hukum internasional tentang *cybercrime* tidak menyebutkan tentang definisi *cybercrime* secara jelas tetapi hanya menyebutkan bentuk-bentuk *cybercrime.*

B. Pemberantasan *Cybercrime* dan permasalahannya di Indonesia

Di Indonesia kejahatan Siber (*cybercrime*) merupakan bentuk kejahatan yang relatif baru, karena pada tahun 1997 Indonesia telah menjadi salah satu negara korban dari *cybercrime* yaitu dengan dirusaknya situs TNI oleh *cracker*. Di samping itu, tidak semua lembaga dapat menggunakan internet sebagai alat komunikasi, hanya beberapa instansi pemerintah dan swasta yang telah memiliki keterampilan dalam bidang teknologi informasi. Sekarang kondisinya mengalami perbedaan, dapat diaktakan hampir semua orang dapat mengakses internet baik melalui internet pribadi maupun melalui warung-warung internet (warnet) yang hampir tersedia di seluruh kota di Indonesia.

Dalam tindak kejahatan konvensional Polisi dapat dengan mudah menangkap pelaku pencurian asalkan ada laporan dari korban dan telah cukup bukti untuk menangkap pelakunya karena perbuatan itu telah diatur dalam KUHP, namun berbeda halnya kalau kejahatan itu dilakukan dengan menggunakan teknologi informasi yang demikian canggih. Para pelaku umumnya susah dilacak keberadaanya karena pelaku dapat melakukan akses internet dimana dan kapan saja untuk melakukan kejahatan. Menyadari kondisi demikian ketersediaan hukum dan kesiapan penegak hukum mutlak dibutuhkan dalam memberantas *cybercrime*.

Meskipun dunia internet merupakan dunia yang bersifat maya, namun perbuatan yang dilakukan melalui media internet merupakan perbuatan nyata yang mempunyai akibat hukum. Perbuatan merusak situs resmi milik orang lain, memasuki situs orang lain dengan melawan hukum, melakukan transaksi dengan internet dengan menggunakan kartu kredit orang lain, prostitusi lewat internet merupakan perbuatan nyata yang dapat merugikan orang lain dan melanggar hukum oleh karena itu, harus diatur oleh hukum demi keamanan aktivitas yang digunakan oleh para *Netizen* di internet. Pengaturan terhadap keamanan internet merupakan tanggung jawab kita bersama sebagai *Netizen* Indonesia, agar kita merasa aman dalam

menggunakan internet dan hak-hak privasi kita terlindungi dalam internet.[7]

Pengaturan kebijakan dalam menjaga keamanan dunia siber (*cyberspace*) harus dilakukan dengan menggunakan kombinasi pendekatan yang dapat dilakukan dalam menjaga keamanan di dunia siber. Menurut Prof. Ahmad M Ramli terdapat tiga pendekatan yang dapat digunakan dalam menjaga keamanan di dunia siber yaitu pendekatan teknologi, sosial budaya dan etika dan terakhir adalah pendekatan hukum.[8]

Pendekatan hukum yang harus dilakukan mengatasi *cybercrime* adalah dengan menentukan bahwa perbuatan-perbuatan yang merugikan orang lain dalam aktivitas internet merupakan tindak kriminal atau yang dikenal dengan istilah kriminalisasi.[9] Upaya kriminalisasi *cybercrime* dalam hukum nasional Indonesia sampai saat ini masih dimuat dalam Rancangan Undang-Undang Informasi dan Transaksi Elektronik (RUU ITE). Lahirnya RUU ini sebagai jawaban atas kondisi obyektif terjadinya kejahatan siber di wilayah Indonesia yang melibatkan warga negara Indoensia sebagai pelakunya maupun sebagai korbannya begitu pula orang asing.[10]

Dalam RUU ITE kriminalisasi kejahatan siber terdapat dalam ketentuan Bab VII pasal 26 sampai pasal 33. Pengadopsian substansi larangan yang terdapat dalam konvensi *cybercrime* dalam RUU ITE tersebut di atas dapat dipahami sebagai upaya pemerintah untuk mengharmonisasikan ketentuan siber nasional dengan ketentuan umum yang berlaku secara internasional. Praktek serupa juga pernah dilakukan oleh Indonesia dalam membentuk undang-undang nomor 26 tahun 2000 tentang pengadilan HAM. Dalam undang-undang ini

---

7 Budi Rahardjo, *Keamanan Internet Tanggung Jawab Kita Bersama,* Makalah lepas dalam situs yang diberikan hak kebebasan oleh penulisnya sebagai publik domain.diakses pada hari rabu tanggal 7 maret 2005.

8 Ahmad M Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*: Bandung, Refika Aditama, cetakan pertama, 2004. hlm.3-4

9 Barda Nawawi Arif, *Kapita Selekta Hukum Pidana,*Bandung, Citra Aditya Bhakti, 2003, hlm.256

10 Penjelasan umum RUU Transaksi elektronik dan Teknologi Informasi.

Indonesia mengambil substansi tentang kejahatan yang dapat diadili oleh Pengadilan HAM yaitu kejahatan kemanusian dan genosida dari ketentuan statuta Roma tentang piagam pembentukan *International Criminal Court.*[11] Dalam kedua konvensi yang diadopsi subtansinya tersebut Indonesia bukanlah menjadi pihak dalam konvensi tersebut.

Semua larangan yang ditentukan dalam Bab VII RUU ITE di atas merupakan kriminalisasi dari fenomena kejahatan siber yang terjadi selama ini. Namun, dalam RUU ini tidak menentukan tentang larangan terhadap kegiatan di internet yang melanggar sendi-sendi moral kehidupan bangsa Indonesia. Kegiatan prostitusi lewat internet berupa penyebaran situs porno yang mengeksploitasi wanita dibawah umur merupakan fenomena riil dalam dunia siber. Begitu pula perjudian melalui internet juga merupakan suatu kenyataan yang terjadi. Seharusnya hal tersebut diatur pula dalam RUU ITE sebagai bentuk proteksi terhadap masyarakat siber dari dampak negatif teknologi informasi . Hal ini disebabkan karena pengguna internet tidak hanya orang dewasa, tetapi juga anak-anak di bawah umur dapat mengakses internet.

Dalam RUU ITE ruang lingkup ditentukan bahwa RUU ITE tidak hanya berlaku dalam wilayah Republik Indonesia, tetapi juga bagi pelaku kejahatan yang melakukan kejahatan di luar wilayah Indonesia yang mempunyai akibat hukum di Indonesia.[12] Penerapan yurisdiksi yang bersifat protektif dalam RUU ITE dapat dipahami sebagai upaya untuk melindungi warga negara Indonesia dan kepentingan nasional jika kejahatan siber itu berakibat terhadap Indonesia. Namun persoalan akan muncul ketika pelaku kejahatan itu bukan WNI, apakah RUU ITE juga berlaku bagi warga negara lain yang berada di luar negeri. Apakah dimungkinkan untuk mengekstradisi pelaku kejahatan untuk diadili Indonesia ? . Hal akan berhadapan pada persoalan asas dari ekstradisi yang melarang untuk mengekstradisi warga negaranya sendiri.

---

[11] Romli Atmasasmita, *Kapita Selekta Hukum Pidana Nasional,* jilid II, Bandung, CV. UTOMO, 2004, hlm 2.

[12] Pasal 3 RUU ITE

Sehingga tidak mungkin sebuah negara akan menyerahkan begitu saja warga negaranya untuk diadili di negara lain.

Masalah lain yang mencuat dari RUU ITE adalah tidak semua bentuk kejahatan siber diatur dalam RUU tersebut, hanya mengatur dua jenis kejahatan yaitu *carding* dan *hacking*, sedangkan bentuk kejahatan siber memiliki fariasi bentuk yang lain misalnya pornografi, *cyberterorisme*, dll. Maka untuk memenuhi kebutuhan akan hukum siber yang spesifik melarang kejahatan siber merupakan salah satu jawaban atas kekosongan hukum selama ini. Perlu diperhatikan dalam konteks penyusunan RUU *Cybercrime* adalah aspek kekhasan yang meliputi kejahatan ini yaitu kejahatan yang berteknologi yang menggunakan sarana teknologi informasi sebagai sarana utamanya. Selain itu yang perlu diperhatikan adalah hukum negara lain yang telah terlebih dahulu mengatur masalah *cybercrime* dalam hukum nasionalnya dan pengaturan organisasi internasional yang berkaitan dengan *cybercrime*. Studi komparatif peraturan perundang-undangan negara lain tentang *cybercrime* merupakan salah satu langkah positif untuk mengatur kejahatan ini misalnya saja Malaysia, Kanada, Australia, Singapura sebagai negara yang telah lebih dahulu mengatur masalah ini. Tentu dengan memperhatikan kekhasan karakter bangsa Indonesia sebagai negara yang menjunjung tinggi nilai-nilai agama dan moral. Memperhatikan ketentuan organisasi internasional yang berkaitan dengan siber juga merupakan salah satu cara yang positif dalam memperkaya khasanah hukum siber Indonesia. Kita dapat mengambil contoh misalnya substansi pengaturan tentang kejahatan siber dalam *convention on cybercrime* 2001 ysng dibentuk oleh Uni Eropa. Dalam konvensi tersebut diatur secara kompherensip tentang kriminalisasi terhadap berbagai macam bentuk kejahatan siber.

III. Urgensi Konvensi Pemberantasan Cybercrime Tahun 2001 Dalam Pembentukan Undang-Undang Teknologi Informasi Indonesia

Menyadari bahwa *cybercrime* merupakan kejahatan yang dilakukan di dunia maya dimana dunia seolah tanpa

batas lagi. Begitu pula pelaku dan korban kejahatan tidak lagi merupakan warga negara dalam satu teritori, tetapi dapat terjadi pelaku dan korban kejahatan merupakan warga negara yang berbeda yang berada pada jarak yang beribu-ribu mil. Sementara itu, faktor yurisdiksi negara dalam konteks mengadili pelaku kejahatan dalam kenyataanya merupakan suatu kenyataan yang masih dipegang teguh oleh negara. Menyadari kondisi yang demikian kerjasama internasional dalam memberantas kejahatan siber ini merupakan salah satu solusi yang dapat diambil dalam memberantas kejahatan siber. Masyarakat Uni Eropa memformulasikan kerjasama internasional itu dalam bentuk perjanjian internasional yaitu Konvensi Kejahatan Siber (*convention on cybercrime*) yang ditandatangani di Kota Budapest, Hongaria pada tanggal 23 November 2001. Konvensi tersebut dilatarbelakangi oleh pertimbangan *pertama* bahwa kemajuan teknologi informasi dewasa ini telah berkembang pesatnya namun disisi lain merupakan sarana yang efektif untuk melakukan kejahatan. Oleh karena itu perlu kerjasama internasional antar negara dalam melindungi kepentingan masyarakat terhadap teknologi informasi dan dalam rangka mengembangkan teknologi informasi. *Kedua*, bahwa suatu kenyataan terjadinya peningkatan penyalahgunaan sistem komputer dan jaringan dan data untuk tujuan tindak pidana. Oleh karena itu diperlukan kerjasama internasional untuk mempercepat proses penyidikan dan penuntutan kejahatan siber. Dan *ketiga*, adanya kenyataan perlunya keseimbangan anatara pelaksanaan dan penegakan hukum dan hak asasi manusia sejalan dengan Konvensi Dewan Eropa untuk perlindungan HAM dan kebebasan fundamental tahun 1950 dan Kovenan PBB tentang hak sipil dan politik 1966 yang memberikan perlindungan kepada setiap orang untuk mengemukakan pendapat tanpa intervesi dari orang lain, kebebasan berkekspresi, termasuk pula kebabasan untuk menerima, menyebarkan informasi dan pendapat.[13]

[13] Ahmad M Ramli, *Cyber Law*...Op.cit. hlm. .24.

Hal yang paling urgen dalam Konvensi *cybercrime* adalah ketentuan tentang adanya kejasama internasional antar negara anggota dalam memberantas kejahatan siber. Kerjasama internasional yang dapat dilakukan oleh negara anggota konvensi dilakukan dalam bentuk ekstradisi maupun *mutual legal assistances*. Dalam hal ekstradisi konvensi menentukan bahwa bahwa perbuatan kriminal yang dilarang dalam konvensi ini (mulai dari pasal 2 sampai pasal 11) adalah kejahatan yang dapat dilakukan ekstradisi. Kejahatan itu diancam dengan hukuman penjara maksimum satu tahun atau dengan hukuman yang lain.[14] Jika antara dua negara yang menjadi anggota tidak terdapat perjanjian ekstradisi, maka antara kedua negara tersebut dapat menjadikan konvensi ini sebagai dasar untuk meminta ekstradisi pelaku kejahatan.

Dalam konteks *Mutual legal assistance* ketentuan konvensi yang penting untuk dicermati adalah ketentuan tentang adanya kerjasama saling membatu antara negara anggota konvensi untuk memberikan bantuan yang diperlukan oleh negara anggota untuk menyelidiki dan mengadili pelaku kejahatan siber. Antara negara anggota konvensi wajib memberikan data yang berkaitan dengan sistem komputer ataupun yang berkaitan dengan alat bukti eletronik yang berhubungan dengan kejahatan siber[15]. Kemudahan-kemudahan yang diberikan oleh konvensi kepada negara anggota merupakan kesempatan baik bagi negara anggota untuk secara bersama-sama memberantas kejahatan siber. Konvensi ini seolah-olah meniadakan lagi batasan yurisdiksi negara yang selama ini dipertahankan. Langkah ini merupakan respon masyarakat internasional terhadap kejahatan siber yang selama ini merugikan masyarakat dunia informasi.

Hal lain yang menarik dari konvensi ini adalah ketentuan final dari konvensi yang memberikan kesempatan kepada negara lain yang bukan merupakan anggota dari Uni

---

[14] Pasal 24 ayat (1) Konvensi *Cybercrime*.

[15] Pasal 25 ayat(1) Konvensi *cybercrime*.

Eropa untuk meratifikasi konvensi ini sepanjang negara tersebut mempunyai konsent untuk membarantas kejahatan siber. Dengan berdasarkan ketentuan ini, kemudian timbul pertanyaan apakah Indonesia harus meratifikasi konvensi ini sebagai salah satu langkah untuk memberantas kejahatan siber yang akhir-akhir ini terjadi ? bahkan menjadikan Indonesia sebagai negara nomor satu yang melakukan kejahatan siber. Menjawab persoalan ini penulis berpendapat patut pertimbangkan konvensi ini sebagai konvensi yang harus diratifikasi Indonesia.

Dasar pemikiran yang diajukan oleh penulis menyarankan agar konvesi ini diratifikasi oleh Indonesia mengingat keuntungan yang akan kita peroleh dari konvensi ini. *Pertama*, dalam konvensi di atur tentang kerjasama internasional untuk memberantas kejahatan siber. Dengan adanya ketentuan ini memberikan keuntungan bagi Indonesia untuk meminta bantuan dari negara anggota lain dalam bentuk *mutual legal assistance*. Kita dapat meminta bantuan negara lain yang mempunyai keunggulan teknologi informasi untuk memberikan bantuan dalam bentuk penyediaan data dan alat bukti elektronik dari negara lain dimana pelaku kejahatan siber itu berada yang merugikan negara Indonesia. Dalam konteks ekstradisi, konvensi juga memberikan kemudahan dimana negara anggota walaupun di antara mereka tidak terdapat perjanjian ekstradisi, jika jenis kejahatan yang dimintakan ekstradisi adalah kejahatan siber yang diatur dalam konvensi maka negara anggota harus mengekstradisi pelaku kejahatan tersebut. Ketentuan ini penting bagi Indonesia mengingat banyaknya tersebar WNI di berbagai belahan dunia yang dapat saja melakukan kejahatan negara lain dan akibatnya di Indonesia.

Kedua, dengan meratifikasi perjanjian ini menumbuhkan kembali kepercayaan masyarakat dunia terhadap Indonesia, mengingat selama ini reputasi Indonesia di bidang Informasi teknologi sangat buruk, dengan meratifikasi Konvensi ini menunjukan kepada masyarakat Internasional adanya keseriusan Indoensia untuk

memberantas kejahatan siber.Disamping itu usaha ratifikasi konvensi ini merupakan usaha untuk menumbuhkan kepercayaan pelaku usaha asing yang menjual produknya ke Indonesia agar mereka mau melakukan jual beli lewat internet dengan masyarakat Indonesia.

IV. Implikasi Ratifikasi Konvensi Pemberantasan Cybercrime tahun 2001 bagi hukum nasional Indonesia

Pengesahan perjanjian internasional yang dilakukan oleh negara terhadap sebuah perjanjian internasional membawa implikasi yuridis tertentu. Umumnya implikasi yuridis adalah lahirnya hak dan kewajiban negara yang ditentukan oleh konvensi. Begitu pula dalam konvensi internasional tentang pemberantasan cybercrime tahun 2001 menimbulkan hak dan kewajiban bagi Indonesia jika Indonesia menjadi pihak dalam konvensi ini. Ada beberapa implikasi yuridis yang lahir dari konvensi ini.

Pertama, kewajiban untuk menyesuaikan semua peraturan perundang-undangan yang mengatur kejahatan siber. Sebagaimana disampaikan di atas bahwa sejauh ini Indonesia belum memiliki hukum positif yang mengatur kejahatan siber dan sejauh ini Indonesia telah menyediakan RUU ITE, maka muatan yuridis yang terdapat dalam RUU siber harus menyesuaiakan dengan ketentuan yang terdapat dalam Konvensi pemberantasan *Cybercrime* tahun 2001.

Kewajiban untuk mengadakan kerjasama internasional dengan negara lain. Hal ini dilakukan mengingat *cybercrime* merupakan kejahatan internasional yang bersifat transnasional, seorang pelaku *cybercrime* dapat saja melakukan *cybercrime* di negaranya yang mengakibatkan kepentingan satu negara maupun beberapa negara dalam waktu yang singkat oleh karena itu pemberantasanya juga membutuhkan kerjasama antar negara dalam memberantas kejahatan ini. Dalam konvensi *cybercrime* diatur berbagai macam bentuk kerjasama internasional dalam memberantas kejahatan ini

yaitu berupa perjanjian ekstradisi dan *Mutual Legal Assistence* antara negara peratifikasi perjanjian ini.

Negara lain yang tidak meratifikasi perjanjian ini tidak mendapatkan kemudahan-kemudahan yang ditentukan oleh konvensi, kecuali antara negara tersebut terdapat perjanjian ekstradisi yang memasukan *cybercrime* sebagai kejahatan yang dapat diekstradisi. Oleh karena itu ketentuan undang-undang ekstradisi Indonesia harus direvisi dengan memasukan kejahatan siber sebagai kejahatan yang dapat diekstradisi (*extradable crime*), begitu pula dengan undang-undang Kerjasama Bantuan Hukum (*Mutual Legal Assistance*) harus memasukan kejahatan siber sebagai obyek pengaturannya.

V. Penutup

Kesimpulan dan Saran

Pada tataran internasioanal kejahatan siber telah diatur dalam *Convention on Cybercrime* tahun 2001. Langkah ini merupakan jawaban atas perangkat hukum dankerjasama internasional yang kontruktif dan intensif dalam usaha pemberantasan kejahatan siber. Dalam RUU ITE Indonesia telah mengakomodir sebagaian kecil dari ketentuan tentang kriminalisasi kejahatan siber. Akibatnya tidak semua kejahatan yang potensial merugikan negara dan korban terakomodir dalam RUU ini.

Jika Indonesia meratifikasi Konvensi Cybercrime berimplikasi pada adanya kewajiban untuk melakukan penyesuaian RUU ITE, Undang-undag Ekstradisi dan Undang-undang Kerjasama Bantuan Hukum (*Mutual Legal Assistance)* yang baru disetujui oleh DPR bersama Pemerintah. Dan adanya kewajiban untuk mengadakan kerjasama Internasional dengan negara lain dalam rangka pemberantasan kejaharan siber.

Melalui tulisan ini penulis menyarangkan kepada pemerintah agar meratifikasi *Convention on Cybercrime* tahun

2001 mengingat adanya keuntungan-keuntungan yang akan kita peroleh jika kita meratifikasi Konvensi ini yaitu adanya kemudahan kerjasama Internasional dan perbaikan citra bangsa di mata masyarakata internasional. Selain itu dalam konteks kerjasama internasional , *cybercrime* harus dianggap sebagai kejahatan yang merugikan umat manusia, oleh sebab itu PBB sebagai organisasi internasional harus memperhatikan persoalan ini sebagai suatu hal yang mendesak untuk diatur dalam hukum internasional dalam bentuk konvensi yang melibatkan seluruh negara anggota PBB.

DAFTAR PUSTAKA

Buku-Buku.

Ahmad M Ramli, *Cyber Law dan HAKI dalam sistem Hukum Indonesia*: Bandung, Refika Aditama, cetakan pertama, 2004.

Agus Raharjo, *Cybercrime* Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Bandung, Citra Aditya Bhakti, 2002 .

Barda Nawawi Arif, *Kapita Selekta Hukum Pidana,*Bandung, Citra Aditya Bhakti, 2003

Budi Agus Riswandi, *Hukum dan Internet di Indonesia*, Yogyakarta, UII Press, 2003

Edmon Makarim, *Kompilasi Hukum Teletmatika*, Jakarta, Raja Grafindo Persada, 2003

Hikmahanto Juwana, *Bunga Rampai Hukum Ekonomi dan Hukum Internasional*, Jakarta, Lentera Hati, 2002.

Mieke Komar Kantaatmadja, at.al. *Cyber law* : Suatu Pengantar, Bandung, ELIPS II, 2002

Romli Atmasasmita, *Pengantar Hukum Pidana Internasional*, Edisi Revisi, Bandung, Refika Aditama, 2000

_____*Pengantar Hukum Pidana Internasional II*, Jakarta, Hecca Mitra Utama, 2004

_____Kapita Selekta Hukum Pidana Nasional, Jilid II, Bandung, CV. UTOMO, 2004

Kumpulan Makalah

Ari Juliana Gema, *Cybercrime :sebuah fenomena di dunia maya*, diakses dari situs www.click legal solution.com pada tanggal 7 maret 2005.

Budi Rahardjo, *Keamanan Internet Tanggung Pawab Kita Bersama,*makalah lepas dalam situs yang diberikan hak kebebasan oleh penulisnya sebagai publik domain diakses pada hari rabu tanggal 7 maret 2005.

Danrivanto Budijanto, *Aspek-Aspek Hukum Dalam Perniagaan Secara Elektronik (E-Commerce)*, Makalan Dalam Seminar Nasional Aspek Hukum Transaksi Perdagangan Via Internet di Indonesia yang diselenggarakan FH UNPAD.

Ronny Nitibaskara, *Problema Yuridis cybercrime*, makalah pada seminar tentang *Cyber Law* , diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 juli 2000, hlm.2 dan 5

Vladimir Golubev, *International Cooperation in Fighting Transnational Computer crime"* diakses dari http/www. *Computer crime research center.* Org. tanggal 20 maret 2005.

Rancangan Peraturan perundang-undangan

Rancangan Undang-undang Teknologi Informasi.

Konvensi Internasional

Convention On Cybercrime, 2001

Convention on Against Transnational Organized Crime ,2000