YURISDIKSI DAN *TRANSFER OF PROCEEDING DALAM KASUS CYBERCRIME*

TESIS

AFITRAHIM M.R
1006736236

FAKULTAS HUKUM
UNIVERSITAS INDONESIA
PROGRAM STUDI MAGISTER HUKUM
PROGRAM PEMINATAN HUKUM TRANSNASIONAL
SALEMBA
JULI 2012

YURISDIKSI DAN *TRANSFER OF PROCEEDING DALAM KASUS CYBERCRIME*

TESIS

Diajukan Sebagai Salah Satu Syarat
Guna Memperoleh Gelar Magister Hukum (M.H)

AFITRAHIM M.R
1006736236

FAKULTAS HUKUM
UNIVERSITAS INDONESIA
PROGRAM STUDI MAGISTER HUKUM
PROGRAM PEMINATAN HUKUM TRANSNASIONAL
SALEMBA
JULI 2012

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : **Afitrahim M.R**

NPM : **1006736236**

Tanda Tangan :

Tanggal : **2 Juli 2012**

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :
Nama : Afitrahim M.R
NPM : 1006736236
Program Studi : Magister Ilmu Hukum
Judul Tesis : Yurisdiksi dan *Transfer of Proceeding* dalam *Cybercrime*

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Hukum pada Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Indonesia

DEWAN PENGUJI

Pembimbing/Penguji :Dr Edmon Makarim, S.H, S.Kom,LL.M ( )

Penguji : Hadi R. Purnama S.H.,LL.M ( )

Penguji : Brian Amy Prasetyo,S.H,MLI ( )

Ditetapkan di : Depok
Tanggal : 2 Juli 2012

KATA PENGANTAR

Puji syukur ke hadairat Allah SWT, bahwa dengan rahmat dan hidayahNya, penulis dapat menyelesaikan Tesis ini. Selanjutnya penulis ingin mengucapkan terimakasih pada :

1. Bapak Dr. M. Fadil Rasad Sp. THT, M.kes dan Ibu Dr. Siti Andriani Gazali yang telah dengan sabar membersarkan penulis sehingga dapat mencapai keadaan yang sekarang, untuk adikku Siti Rahmadini, uda doakan semoga cepat lulus dari kuliahnya.
2. Bapak Dr Edmon Makarim, S.H., S.Kom, LL.M selaku pembimbing yang telah meluangkan waktunya untuk membimbing penulis dari segi materi dan penulisan
3. Bang Hadi Rahmat Purnama S.H, LL.M yang selalu bersedia meluangkan waktunya untuk berdiskusi tentang teroi-teori hukum internasional
4. Ibu Prof. Dr. Rosa Agustina S.H., M.H, Ibu Dr. Nurul Elmiyah S.H., M.H., dan Bapak Heru Susetyo S.H., LL.M., M.Si. selaku pembimbing akademis selama menempuh pendidikan di MHUI.
5. Ajun Komisaris Besar Audie S Latuheru selaku Kepala Sub Direktorat IV Bidang *Cybercrime* Reserse Kriminal Khusus Polda Metro Jaya beserta jajaran stafnya yang telah membantu penulis untuk mendapatkan data yang diperlukan dalam tesis ini.
6. Bapak Watijan, Mas Ari dan seluruh staf administrasi Pasca Sarjana Salemba yang telah berjasa mengurus segala keperluan penulis ketika belajar di MHUI
7. Teman-teman seperjuangan Hukum Transnasional MHUI angkatan 2010, Sheila, Nanda, Desy, Deny, Andrian, Mas Pur, Mas Nana, Zul, Ryan, Reka, Dhana, Poppy, Endah, Mira, Marcell, Ario, Akbar, Asrul, Hendra yang telah berbagi suka dan duka dengan penulis selama dua tahun.
8. Teman-teman ”*genk* Onta, Ibnu, Refan , Hizbul Ana, Real , Haekal,Wahyu, dan Bundo, Qory, Rila, Aida, Devin, Sandra, Anggi, Pinka, Citra, Windy, Keket FHUI yang selalu berbagi suka dan duka dengan penulis.
9. Teman-teman PK VI 2004 FHUI baik yang sudah lulus maupun akan lulus, Ncil, Willy, Aji , Arimbi, Luis, Sandi, Sandra, Vareta, Keke, Setiafitri, Desi, Rey, Ricky, Adhi, Josua, Nyoman , Theo, Fitria, Donny , Mimi.
10. Teman-teman angkatan 2004 SMAN 4 Jakarta yang sangat kompak dan tanggap terhadap keadaan angkatan maupun sekolah.
11. Teman-teman angkatan 2001 SMPN 1 Jakarta.

12. Teman-teman angkatan 1998 SDN Godangdia 01 Pagi Jakarta.

Dan berbagai pihak telah membantu penulis untuk menyelesiakan tesis ini. Penulis merasa tesis ini jauh dari sempurna, maka dari itu diperlukan saran dan kritik yang membangun. Pada akhir kata moga moga tesis ini dapat berguna bagi ilmu pengetahuan pada umumnya terutama pada bidang hukum pada khususnya.

Jakarta, 2 Juli 2012

(Afitrahim M.R, S.H)

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Afitrahim M.R
NPM	: 1006736236
Program Studi	: Magister Hukum
Fakultas	: Hukum
Jenis karya	: Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

"Yurisdiksi dan *Transfer of Proceeding* Dalam *Cybercrime*"

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 2 Juli 2012

Yang menyatakan

(Afitrahim M.R , S.H)

Abstrak

Nama : Afitrahim M.R.

Program Studi : Magister Hukum/Hukum Transnasional.

Judul : Yursidiksi dan *Transfer of proceeding* dalam *Cybercrime*

Perkembangan teknologi yang begitu pesat memunculkan berbagai permasalahan di masyarakat. Salah satu akibatnya tersebut adalah terciptanya sebuah media baru untuk berinteraksi yang disebut cyberspace. Di cyberspace orang bebas melakukan apapun tanpa diketahui oleh orang lain karena tidak diketahui asal-usul maupun kewarganegaraan asli seseorang. Hal ini dimanfaatkan oleh sebagian orang untuk melakukan suatu kejahatan yang disebut cybercrime. Telah banyak usaha untuk melakukan pengaturan di cyberspace untuk mencegah terjadinya cybercrime baik oleh hukum internasional maupun hukum nasional. Salah satunya adalah dengan lahirnya Convention on Cybercrime yang dibuat oleh Dewan Eropa (European Council), aspek yang menjadi perhatian khusus dalam konvensi ini adalah masalah yurisdiksi sebuah negara dalam menangani kasus cybercrime karena semua negara tidak senang yurisdiksi negaranya di lampaui oleh negara lain, termasuk Indonesia. Di Indonesia sendiri perngaturan mengenai cybercrime diatur dalam Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Berbagai cara ditempuh oleh negara-negara untuk menyelesaikan permasalah yurisdiksi dalam menangani kasus *cybercrime*, salah satunya adalah *transfer of proceeding* yang telah diatur di Uni Eropa

Kata Kunci :

Hukum Internasional Yurisdiksi, Cybercrime, Dewan Eropa, *Transfer of Proceeding*

Abstract

Name : Afitrahim M.R

Study Program : Law/Transnational Law

Title : Jurisdiction and *Transfer of Proceeding* in *Cybercrime*.

Massive techology development brings various problems in the society. One of the impact is an invention of a new interactve media called *cyberspace*. In *cyberspace* people is free to do anything anonymuously because no one knows your actual profile and citizenship. This is used by a certain people to commit such crime called *cybercrime*. There are many attempt to regulate a rules in *cyberspace*, weather from internatonal law or national law. One of the attempts is created by *Council of Europe* who produce *Convention on Cybercrime* with jurisdiction as one special aspect that is important because none of the country in the world like their jurisdiction violated by other country, inculding Indonesia. In Indonesia *cybercrime* regulation enacts in Law number 11 Year 2008 regarding Information and Electronic Transaction. Various ways have been taken by the states to solving jurisdiction problem specificly in specificly in *cybercrime* case, one of them is *transfer of proceeding* which has been implemented in European Union

Keywords:

International Law, Jurisdiction, *Cybercrime*, Council of Europe, *Transfer of Proceeding*

DAFTAR ISI

Bab 1

Pendahuluan

1.1. Latar Belakang

Teknologi terus dikembangkan dalam rangka mmpermudah manusia melakukan aktifitasnya sehari-hari. Salah satu produk teknologi informasi dan komunikasi kecang gihannya berkembang pesat adalah internet. Para pelaku bisnis, pejabat, pemerintah dan banyak orang di seluruh dunia menggunakan internet sebagai bagian dari bisnis nasional dan internasional serta kehidupan pribadi manusia sehari hari. Eksistensi dari beberapa jenis bisnis justru tidak mungkin berlangsung tanpa adanya internet.[1]

Teknologi informasi dan komunikasi ini pula yang telah mengubah prilaku masyarakat dan peradaban manusia secara global.[2]dengan munculnya internet, seakan muncul jenis dunia baru yang sebelumnya tidak pernah dikenal oleh manusia yaitu dunia maya. Munculnya dunia maya telah mengubah kebiasaan banyak orang terutama dalam kehidupannya terbiasa menggunakan internet. Mulai dari mengubah cara dan sarana transaksi bisnis atau transaksi perbankan, pendidikan sampai ke sektor hiburan.

Perjalanan ruang dan waktu melalui internet telah memaksa ilmu pengetahuan dan teknologi untuk bergerak cepat tak terbendung. Ilmu pengetahuan dan teknologi itu menawarkan sebuah "realitas lain" yang terdapat di dalam dunia simulasi komputer, yang diistilahkan sebagai *cyber space*. Hal ini menimbulkan sebuah "dilema realitas", apakah dunia simulasi dan simulacra (jamak : *simulacrum*) yang harus dipercayai sebagai "realitas yang lain"? Padahal "realitas yang lain" itu adalah sesuatu yang sebelumnya dianggap tak nyata (*nonreal*). Jika diamati sesungguhnya *cyber space* sebagai "realitas yang lain" itu bukan sekedar merupakan realitas semu

[1] Sutan Remy Syahdeni, *Kejahatan tindak pidana computer, (Jakarta: pustaka utama Grafiti, 2009), hal 2*

[2] Ahmad M.Ramli ,*Cyberlaw dan HAKI dalam system hukum Indonesia, (Jakarta :rafika aditama,2004), hal 1*

dan absurd. Ia hampir menyerupai realitas yang nyata dan alamiah. Dalam dunia *cyber*, dapat dilakukan apa saja yang selama ini merupakan aktifitas dunia nyata. Ia dapat dimasuki dan, tidak bisa dibantah, dunia *cyber* memiliki instrumen-instrumen penting yang layak disebut sebagai realitas.[3]

Perkembangan yang begitu pesat dari teknologi informasi ini telah menimbulkan dampak baru dari dunia hukum. 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. [4] 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 sistem secara illegal.[5]

b. *Content Related Offences*, adalah kejahatan komputer yang menggunakan konten dalam komputer untuk kejahatan seperti pornografi, menyebarkan fitnah, Judi .Dll.[6]

c. *Copyright and Trademark Related Offences*, adalah kejahatan yang melanggar hak cipta atau merek dagang, seperti pembajakan.[7]

d. *Computer Related Offences*, adalah kejahatan yang menggunakan sistem komputer untuk mengambil data-data tertentu, seperti identitas, nomor tanda pengenal sampai rekening bank.[8]

[3] Baudrillard, *Simulation*, New York, Semiotex, hal 12
[4] ITU, *Understanding cybercrime guide*, ICT Appliccation dan Cybersecurity Division, 2009, hal 17
[5] ITU, *loc.cit*, hal 20-29
[6] .*Ibid*., hal 29-
[7] *Ibid.*, hal 41-45.

e. *Combination Offences* , adalah kejahatan yang memadukan antara *cybercrime* dan kejahatan konvensional seperti *cyberterrorism,cyberwarfare* dan *cyberlaundering*.[9]

Maraknya *cyber crime* disebabkan karena kemunculan internet kini diibaratkan seperti sebuah daerah perbatasan baru (*new frontier*) pada zaman *wild west*. Wilayah baru ini bebas untuk di eksploitasi dan dieksplorasi tanpa ada hukum yang mengaturnya.[10] Salah satu kesulitan besar dalam menangani masalah *cybercrime* adalah sifatnya yang sangat *Transboundary* (lintas batas). 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.[11]

Salah satu masalah dalam *transbounday cybercrime* adalah yurisdiksi apakah setiap negara berhak mengadili pelaku *cybercrime* yang berasal dari negara lain?. Hal ini tentu perlu di kaji lebih lanjut karena permasalahan yurisdiksi ini bukanlah sesuatu hal yang mudah untuk dipecahkan, hal ini lebih di akibatkan permasalahan yursidiksi berkaitan dengan kedulatan Negara.

Menurut hukum internasional yang selama ini berlaku, suatu negara memiliki batasan-batasan tertentu dalam hal penerapan yurisdiksi terhadap kasus yang melibatkan kepentingan negara lain.[12] Salah satu batasan yang dimaksud misalnya saja berupa kewajiban setiap negara untuk berhati-hati dan sedapat mungkin menghindari munculnya gangguan terhadap negara lain dalam upaya penerapan yurisdiksinya. Meskipun begitu, pada prakteknya hukum internasional tidak dapat memaksakan suatu negara untuk menerapkan suatu konsep yurisdiksi tertentu,

---

[8] *Ibid.*, hal 45-51.
[9] *Ibid.*, hal 51-59.
[10] Petrus Reinhard Golose, Perkembangan Cyber Crime dan Upaya Penangananya oleh POLRI, "Buletin Hukum Perbankan dan Kebanksentralan", Vol. 4 no. 2, Agustus 2006, hal 30
[11] "*Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police Reported Statistics*", Canadian Centre for Justice Statistics: Catalogue no. 85-558-XIE.
[12] Stephen Wilske and Teresa Schiller, "*International Jurisdiction in Cyberspace: Which States May Regulate The Internet.* 50 Fed. Comm. L.J. 117, 171, 1997

bahkan dalam konteks ini setiap negara cenderung diberikan kebebasan dalam menentukan konsep mana yang akan digunakan. Kebebasan tentu saja akan diberikan sepanjang tidak mengancam ketertiban internasional.[13]

Untuk mengatasi permasalahan ini, banyak negara-negara yang telah untuk membahas *cybercrime*. Salah satunya adalah Dewan Eropa (*Council of Europe)* yang telah menghasilkan suatu konvensi internasional tentang *cybercrime* yang dikenal dengan nama The *Council of Europe Convention on Cybercrime* yang dikenal dengan sebutan *Convention on Cybercrime*, konvensi ini di tandatangani di Budapest, Hungaria pada tanggal 23 November 2001. Masalah yang diatur dalam konvensi tersebut meliputi segala aspek yang menyangkut kepentingan negara termasuk masalah yurisdiksi, yang menjadi bahasan utama tulisan ini. Dalam pasal 22 *Convention on Cybercrime* di jelaskan jika negara perserta konvensi dapat menerapkan yurisdiksinya apabila terjadi kejahatan yang di atur dalam pasal 2-11 konvensi ini. Hal ini terlihat mudah, namun pada kenyataannya sulit untuk di lakukan, oleh karena itu negara-negara peserta konvensi lebih memilih untuk menyelesaikan permasalahan yurisdiksi dengan tiga cara (dua dari tiga cara ini diatur juga dalam *Convention on Cybercrime*). Cara-cara tersebut adalah:

1. Ekstradisi dan Deportasi;
2. Bantuan Timbal Balik (*Mutual Legal Assistance*);
3. Pengalihan Perkara (*Transfer of Proceedings*), yang akan dibahas kemudian.

Di tengah perbincangan hangat soal yurisdiksi, muncul usulan bahwa karena sifat *cybercrime* yang sangat *transnational* maka pelaku *cybercrime* bisa di bawa ke Makhamah Internasional (ICC) atau di bentuk satu badan peradilan baru yang disebut

[13] *Ibid.*

International Court or Tribunal for Cyberspace (ICTC).[14] Hal ini di sebabkan karena *cybercrime* dapat menjadi sebuah kejahatan yang serius dan berdampak global, salah satunya dapat digunakan untuk melumpuhkan infrastruktur suatu negara tidak hanya infrastruktur telekomunikasi tapi juga kegiatan perekonomian dan kemasyarakatan. Seperti yang di alami oleh Estonia pada tahun 2007 dimana *cyberattacks* (serangan siber) yang di lakukan oleh *hacker-hacker* Rusia selama tiga minggu menyebabkan terhentinya kegiatan perekonomian Estonia yang sangat bergantung pada jaringan internet.[15] Bahkan perkembangan terbaru ditemukan jika Amerika Serikat dan Israel di duga telah memulai sebuah serangan siber dengan cara mengirimkan *flame trojan stuxnet*, semacam virus ke fasiltas nuklir Iran.[16]Kedua aksi serangan siber diatas menunjukkan jika pada saat ini *cybercrime* telah menjelma menjadi sebuah fenomena global yang tidak boleh di pandang enteng oleh semua negara karena berpotensi memicu terjadinya perang jenis baru yaitu perang di dunia maya (*cyberwarfare*) yang dampaknya lebih serius dari perang konvensional.[17]

Di Indonesia sendiri peraturan perundang-undangan yang mengatur tentang *cybercrime*, adalah Undang-Undang no 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), adapun pasal yang mengatur yurisdiksi adalah pasal 2 yang menganut asas *subjective territoriality* dimana setiap orang yang melakukan *cybercrime* dan dampaknya merugikan Indonesia dapat di adili di Indonesia, namun pada prakteknya hal ini sulit dilakukan apabila pelaku melakukan kejahatannya dari luar wilayah Indonesia karena belum tentu setiap negara mau menyerahkan warganegaranya untuk di adili di Indonesia dan dalam prakteknya penegak hukum juga belum siap untuk menegakkan Pasal 2 tersebut contohnya adalah kasus 170 Warganegara China yang ditangkap oleh Kepolisian karena melakukan penipuan

---

[14] Prof Kraft PhD, *Ideas of establishment of an interntional court of cybercrime*, WCLF papers, 2011. Lihat juga di Stein Scholberg,*Interntional Criminal Court or Tribunal for Cyberspace*, makalah dalam East West Institute (EWI) Cybercrime legal institute, May 2011

[15] http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all, diakses tanggal 12 Juni 2012

[16] http://www.jpost.com/MiddleEast/Article.aspx?ID=273411&R=R1, diakses tanggal 12 Juni 2012

[17] Yang dimaksud perang konvensional adalah setiap perang yang diatur dalam Konvensi Jenewa 1949 dan Protokolnya

melalui internet.[18] Dalam kasus ini mereka ditangkap setelah polisi melacak *IP address* dan melakukan pengintaian di lokasi yang di curigai sebagai markas mereka.[19] Penyelsaian yang di ambil oleh kepolisian adalah melimpahkan berkas mereka ke imigrasi untuk kemudian di deportasi ke negara asalnya.[20]

1.2. Rumusan Permasalahan

1.Bagaimana Hukum internasional mengatur tentang yurisdiksi terutama di bidang *cybercrime*?

2. Bagaimana kemungkinan di gelarnya *transfer of proceeding* dalam kasus *transboundary cybercrime*?

1.3. Tujuan Tesis

1.3.1 Tujuan Umum

Tujuan umum dari Tesis ini adalah menganalisa penerapan teori-teori tentang yurisdiksi menurut hukum internasional dalam kasus *transboundary cybercrime*.

1.3.2. Tujuan Khusus

Selain tujuan umum Tesis ini juga memiliki tujuan khusus yang berfungsi untuk menjelaskan hal-hal yang spesifik diluar tujuan umum, adapun yang menjadi tujuan khusus Tesis ini adalah :

1. Mengetahui bagaimana pendefinisian *cybercrime* dan jenis-jenis *cybercrime* yang diatur dalam kenetuan hukum internasional tentang *Cybercrime*?
2. Mengetahui apakah mungkin dilakukan *transfer of proceeding* dari satu negara ke negara lain

---

[18] http://internasional.kompas.com/read/2011/06/11/10360083/Ratusan.Penjahat.Internet.Dibekuk, diakses tanggal 11 April 2012

[19] Reinhard Hutagaol, *Indonesia Basis Penipuan Internet Internasional*, http://teknologi.kompasiana.com/internet/2011/06/19/indonesia-basis-penipuan-internet-internasional/, diakses tanggal 15 April 2011,

[20] http://www.tribunnews.com/2011/06/10/imigrasi-deportasi-177-wna-pelaku-cyber-crime-besok, diakses tanggal 13 Juni 2012

1.4. Definisi Operasional

Untuk membatasi bahasan yang bergitu luas, Penulis hanya menfokuskan pembahasan Tesis ini pada masalah yurisdiksi yang terkait dengan negara sebagai subjek hukum Internasional dan juga hubungan antara warganegara dengan negara pada umumnya, prinsip-prinsip yang dipakai adalah prinsip-prinsip tentang yurisdiksi yang berkembang dalam hukum Internasional. Prinsip-prinsip tersebut adalah :

a. Subjective Territoriality
b. Objective Territoriality
c. Nationality
d. Passive Nationality
e. Protective Principle
f. Universality

Istilah-istilah yang akan sering ditemui pada Tesis ini adalah istilah di bidang komputer, untuk memudahkan pembaca memahami Tesis ini, maka akan diuraikan beberapa istilah yang sering ditemui :

1. *Offences against Confidentiality, integrity and Availability of Computer Systems and Data*, adalah kejahatan yang bertujuan untuk mengakses, menyadap data atau sistem secara illegal.[21]

2. *Content Related Offences*, adalah kejahatan komputer yang menggunakan konten dalam komputer untuk kejahatan seperti pornografi, menyebarkan fitnah, Judi .Dll.[22]

3. *Copyright and Trademark Related Offences*, adalah kejahatan yang melanggar hak cipta atau merek dagang, seperti pembajakan.[23]

[21] ITU, *loc.cit*, hal 20-29
[22] .*Ibid*., hal 29-41
[23] *Ibid.*, hal 41-45.

4. *Computer Related Offences*, adalah kejahatan yang menggunakan sistem komputer untuk mengambil data-data tertentu, seperti identitas, nomor tanda pengenal sampai rekening bank.[24]

5. *Combination Offences* , adalah kejahatan yang memadukan antara *cybercrime* dan kejahatan konvensional seperti *cyberterrorism,cyberwarfare* dan *cyberlaundering*.[25]

6. *Transfer of Proceedings* adalah kerjasama internasional yang berbentuk *mutual legal assistance* dimana setiap Negara bisa meminta Negara lain untuk memproses seseorang yang diduga telah melakukan tindak pidana.[26]

1.5. Kerangka Teori

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*).[27] Sementara kubu kedua mempunyai pandangan bahwa *cyberspace* itu dunia yang khas, unutuk itu perlu ada

[24] *Ibid.*, hal 45-51.
[25] *Ibid.*, hal 51-59.
[26] *European Convention on Transfer of proceedings Explanatory Report*, poin 26
[27] Andrew D. Murray, *The Regulation in Cyberspace :Control in the Online Environment*, 2007, Routelage & Cavendish

hukum serta konsep tersendiri yang diberlakukan di *cyberspace*. Pandangan ini mencoba memisahkan *cyberspace* dengan dunia nyata (kubu ini selanjutnya disebut dengan *cyber-libertarian*).

Ditengah perdebatan yang alot mengenai hal ini, David R. Johnson mencoba menawarkan empat model yang patut dipertimbangkan sebagai solusi, keempat model tersebut antara lain:[28]

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. Pegaturan sendiri oleh pengguna internet (*self-governance*).

Salah satu tawaran dari Johnson yang cukup menarik adalah ide pembentukan organisasi 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*[29]. 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 obyektifitas, jaminan perlindungan terhadap golongan minoritas, dan sebagainya.[30] Usulan serupa

[28] David R. Johnson and David G. Post, *"And How Should The Internet Be Governed?"*, The American Lawyer, 1996
[29] UNESCO, *The International Demension of Cyberspace Law*. England. Ashgate Publishing Ltd., 2000., hal 42.
[30] *Ibid.*

baru-baru ini di kemukakan oleh Perdana Menteri Rusia, Vladimir Putin yang pada Juni tahun lalu bertemu dengan Hamadoun I.Toure, Sekrertaris Jenderal *International Telecommunications Union* (ITU) dalam pertemuan tersebut beliau menyampaikan usulan agar ITU di berikan mandat oleh PBB untuk dapat mengatur segala aspek yang ada di *cyberspace* termasuk masalah *cybersecurity* dan standarisasi alamat *website*.[31] Hasil pembicaraan ini kemudian di bawa ke Majelis Umum (*general assembly*) PBB pada bulan September dan langsung mendapat dukungan dari Brazil,China dan India. Amerika Serikat menolak dengan tegas usulan ini,sementara negara-negara lain belum bisa memberikan tanggapan.[32] Secara umum terdapat dua aliran yang menginginkan yurisdiksi di *cyberspace* diatur sedemikian rupa, ada yang menginginkannya diatur seperti yurisdiksi terittorial ada juga yang menginginkan dibentuknya yurisdiksi yang khusus dapat diterapkan di *cyberspace*

a. Aliran *Cyber-Paternalist*.[33]

Para pendukung aliran ini pada intinya ingin menekankan bahwa sebenarnya *cyberspace* hanyalah merupakan bentuk elektronik dari ruang biasa yang kita kenal selama ini.[34] Dengan kata lain golongan ini berpandangan bahwa *cyberspace* adalah dunia biasa sebagaimana halnya dengan dunia nyata, karena analogi ini maka di *cyberspace* dapat diterapkan aturan atau konsep yurisdiksi yang selama ini berkembang dalam hukum internasional, terutama dalam hal penanganan tindak pidana.

Menurut hukum internasional yang selama ini berlaku, suatu negara memiliki batasan-batasan tertentu dalam hal penerapan yurisdiksi terhadap kasus yang melibatkan kepentingan negara lain.[35] Salah satu batasan yang dimaksud misalnya saja berupa kewajiban setiap negara untuk berhati-hati dan sedapat mungkin menghindari munculnya gangguan terhadap negara lain dalam upaya penerapan

---

[31] http://www.eutimes.net/2012/05/russia-backs-un-internet-takeover/, diakses tanggal 14 Juno 2012.
[32] *Ibid*,
[33] Murray, *Op.cit*, hal 7-9
[34] Rene L. Pattiradjawane, *"Cyberlaw: Apakah bisa Melindungi Pribadi Pengguna Internet?"*, 2000,
[35] Stephen Wilske and Teresa Schiller, *"op.cit*

yurisdiksinya. Meskipun begitu, pada prakteknya hukum internasional tidak dapat memaksakan suatu negara untuk menerapkan suatu konsep yurisdiksi tertentu, bahkan dalam konteks ini setiap negara cenderung diberikan kebebasan dalam menentukan konsep mana yang akan digunakan. Kebebasan tentu saja akan diberikan sepajang tidak mengancam ketertiban internasional.[36] Secara umum yurisdiksi dibedakan menjadi tiga jenis, yaitu:[37]

1) Yurisdiksi legislatif (*Jurisdiction to prescribe*)

Secara umum yurisdiksi legislatif merupaka kemampuan suatu negara untuk menerapkan hukum nasionalnya terhadap individu dan peristiwa tertentu.[38] Kemampuan ini pada prinsipnya dapat terwujud selama peristiwa yang dimaksud terjadi di wilayahnya atau peristiwa tersebut dilakukan oleh warganegaranya yang berada diluar batas wilayah negara tersebut. Selain itu jenis yurisdksi ini juga dapat dikatakan sebagai titik tolak dalam menetukan penerapan jenis yurisdiksi yang yang lainnya. Artinya untuk menerapkan yurisdiksi yudikatif, maka harus diawali dengan menganalisa yurisdiksi legislatif terlebih dahulu, namun ini tidak perlu dilakukan jika pihak yang bertindak sebagai negara forum berkenan mempergunakan hukum asing. Persyaratan yang sama berlaku juga bila ingin menerapkan yurisdiksi eksekutif.

Dalam menentukan yurisdiksi legislatif , maka terhadap seseorang maupun suatu peristiwa, terdapat 6 (enam) prinsip lain yang dapat dijadikan acuan. Prinsip-prinsip tersebut antara lain :[39]

1. *Subjective territoriality* (territorial subjektif)
2. *Objective territoriality* (territorial objektif)
3. *Nationality* (nasionalitas aktif)
4. *Passive Nationality* (nasionalitas pasif)
5. *Protective Principle* (prinsip perlindungan)
6. *Universality* (universalitas)

[36] *Ibid.*
[37] *Ibid.*
[38] *Ibid.*
[39] *Ibid.*

2) Yurisdiksi yudikatif (*Jurisdiction to adjudicate*)

Yurisdiksi yudikatif merupakan kewenangan suatu negara untuk melakukan proses peradilan terhadap individu atau peristiwa yang mempunyai hubungan yang cukup dengan negara tersebut.[40] Sebagaimana yang disebutkan sebelumnya, penerapan yurisdiksi yudikatif hampir selalu dengan penerapan yurisdiksi legislatif. Hal ini bisa dilihat dari praktek di seluruh dunia bahwa hampir tidak ada pengadilan yang rela memakai hukum pidana negara lain.[41] Dalam kasus kejahatan internasional, penerapan yurisdiksi yudikatif secara normative sangat bergantung pada dimana pelaku kejahatan tersebut berada.

3) Yurisdiksi eksekutif (*Jurisdiction to enforce*)

Yurisdiksi eksekutif mempunyai makna sebagai kewenangan negara untuk meningkatkan kepatuhan terhadap hukum dan kewenangan negara untuk menjatuhkan hukuman bagi yang melanggar hukum. Jenis yurisdiksi ini memiliki kaitan erat dengan yurisdiksi legislatif, maksudnya suatu negara tidak dapat menegakkan hukum nasionalnya begitu saja kecuali negara tesebut memiliki yurisdiksi legislatif atas seseorang atau suatu peristiwa.

Yurisdiksi legislatif terkadang juga menjadi dasar pembenar bagi suatu negara untuk mengambil langkah-langkah yang dianggap perlu dalam rangka penerapan yurisdiksi eksekusinya diwilayah negara lain dengan syarat ada persetujuan dari negara tersebut. Persetujuan yang dimaksud disini adalah persetujuan yang diberuikan oleh pejabat resmi dari negara yang bersangkutan dan langkah-langkah yang dapat diambil antara lain : penahanan, pengiriman surat, pelayanan dokumen, dan penyelidikan.[42]

Sehubungan dengan belum adanya titik temu antara dua kubu yang saling berseteru mengenai konsep yurisdiksi yang akan digunakan terhadap *cyberspace*,

[40] *Ibid.*
[41] *Ibid.*
[42] *Ibid.*

khususnya mengenai *cybercrime*. Maka dengan kondisi tersebut, praktis konsep tradisional seperti yang disebutkan diatas yang selama ini berlaku dalam menentukan yurisdiksi terhadap kasus-kasus kejahatan komputer yang bernuansa internasional. Setidaknya konsep yang tercantum dalam peraturan nasional khusus tentang kejahatan komputer di beberapa negara, yang merupakan dasar hukum yang selama ini digunakan sebelum adanya ketentuan yang bersifat internasional.

b. Aliran *Cyber-Libertarian*.[43]

Aliran ini diperjuangkan oleh kubu yang sebagian besar terdiri dari para akitvis *cyberspace* atau sekumpulan orang yang sehari-harinya memiliki kegiatan yang tidak lepas dari komputer (internet), beberapa diantaranya adalah *hacker*. Dengan melihat komposisi golongan yang mendukung konsep ini, maka dapat dimaklumi kiranya jika mereka secara terang-terangan menolak segala upaya untuk menyamaratakan *cyberspace* dengan dunia biasa atau dengan kata lain mereka merasa dunia mereka terusik dengan keberadaan konsep analogi.

Pemikiran yang menjiwai aliran ini pada dasarnya berangkat dari beberapa teori yag mereka yakini sebagai kekhasan dari *cyberspace* itu sendiri, seperti :[44]

a. Bahwa *cyberspace* adalah media yang terletak tidak di suatu lokasi tertentu.
b. Aktifitas di *cyberspace* tidak ada kaitannya suatu lokasi.
c. *Cyberspace* merupakan sesuatu yang jelas berbeda dengan dunia nyata.

Berangkat dari butir-butir diatas kalangan yang mendukung aliran ini berpendapat bahwa tidak satu pun organisasi atau negara yang pantas mengatur aktifitas di *cyberspace*. Lebih jauh lagi mereka berpandangan bahwa yang berhak mengatur *cyberspace* hanyalah pengguna *cyberspace* itu sendiri.[45] Argumen tersebut muncul berdasarkan dua asumsi sebagai berikut:[46]

---

[43] Murray, *op.cit*, hal 5-7
[44] Dan L. Burk, "*Jurisdiction in a World Without Border*," 1 Va. J.L. & Tech, 1997
[45] *Ibid.*
[46] *Ibid.*

1. Menurut mereka keberadaan *cyberspace* tidak secara serta-merta menyakiti seseorang di wilayah tertentu.
2. Segala upaya untuk mengontrol aktifitas *cyberspace* akan menjadi sia-sia, karena dengan mudah aktifitas tersebut akan berpindah-pindah dari suatu wilayah ke wilayah yang lain.

Pandangan ini mendapat kritikan dari beberapa kalangan, misalnya yang dikemukakan oleh Lawrence Lessig. Beliau berpendapat bahwa alasan-alasan yang dikemukakan oleh penganut konsep pemisahan lebih merupakan alasan dari prespektif normative serta emosional belaka, bukanlah suatu alasan yag bersifat analitis.[47] Contohnya pandangan mereka yang menganggap bahwa *cyberspace* beserta aktifitasnya harus dipisahkan dari dunia nyata.

Jika pandangan ini diasumsikan benar maka orang yang berhubungan di *cyberspace* adalah bukan orang sungguhan. Hal ini jelas seuatu yag masuk akal menurut Lessig karena menurut beliau orang adalah tetap orang baik sebelum atau sesudah ia menjauh dari komputer.[48] Secara ekstrim Lessig selanjutnya menyatakan bahwa *cyberspace* bukanlah suatu "wilayah aman diluar bumi" (*extra terrestrial safety zone*), para penjahat komputer tidaklah aman dari tuntutan pengadilan.[49]

Kritikan lain datang dari Misaki Hamano yang menyatakan bahwa ide pemisahan *cyberspace* dengan dunia nyata dan ide *self-governance* terhadap *cyberspace*, bukan sesuatu yang realistis saat ini. Karena sekalipun kejahatan di *cyberspace* terus menigkat, namun negara-negara cenderung memilih menggunakan konsep lama dibandingkan membuat ketentuan yang baru. Selanjutnya Masaki menambahkan bahwa memang benar jika dikatakan bahwa ada keterbatasan negara

[47] Barda Nawawi Arief, "*Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tidak Pidana Maya Antara*.", Makalah pada seminar nasional dalam rangka penyusunan RUU teknologi informasi tahun 2002, hal 12.
[48] *Ibid.*
[49] *Ibid.*

untuk mengatasi problem yurisdiksi di *cyberspace*, akan tetapi bukan berarti pengguna *cyberspace* bebas dari hukum di dunia nyata.[50]

Salah satu gagasan yang ditawarkan oleh aliran ini adalah dengan menempatkan *cyberspace* sebagai **The 4th International Space** disamping zona Antartika, ruang angkasa (*outer space*), dan zona laut.[51] Degan menempatkan *cyberspace* setara dengan zona-zona khusus lainnya, maka bagi *cyberspace* perlu juga diadakan pengaturan khusus yang didalamnya termasuk juga konsep yurisdiksi khusus yang berlaku di khusus yang berlaku di *cyberspace*. Berkaitan dengan gagasan ini UNESCO dalam terbitannya yang berjudul "The International Dimensions of Cyberspace Law" berpendapat bahwa *cyberspace* dapat mengambil pengalaman yang berharga dari praktek pengaturan di ruang angkasa (outer space), dimana banyak kalangan yang menganggap bahwa pengaturan di ruang angkasa terbilang berhasil, khususnya dalam hal menertibkan upaya pengeksplorasian di zona tersebut.[52] Selain dua aliran diatas menurut Viktor Mayer-Schönberger terdapat tiga pendapat mengenai bentuk pengaturan mengenai siapa yang berhak meregulasi Internet.[53]

1. Pendapat pertama dikenal dengan teori *The State-Based Traditionalist Discourse* mengatakan sebaiknya pihak yang mengatur Internet adalah pemerintah melalui peraturan perundang-undangan. Berdasarkan pendapat ini bentuk pengaturan Internet akan diatur oleh masing-masing negara. Kelebihan teori ini adalah penegakan hukum terhadap pengaturan Internet lebih terjamin. Sementara itu, kelemahan dari pengaturan ini adalah dilupakannya dasar dari Internet yaitu sifat global. Tidak mungkin suatu negara dapat memaksakan

[50] Masaki Hamano, "*Comparative Study I The Approach to Jurisdiction in Cyberspace*" dalam Dharma Adhikari, *International Cyberjurisdiction :Toward The Formulation of Common Laws*, 2002, makalah yang disampaikan dalam Annual Convention Association For Education of Journalism and Mass Communication, Miami Beach Florida, 2002
[51] UNESCO, *op.cit*, hal 38.
[52] *Ibid.*, hal 143.
[53] Viktor Mayer-Schönberger, "The Shape of Governance: Analyzing the World of Internet Regulation", *Virginia Journal of International Law* (Spring *2003*): 607

peraturan negaranya bagi warga negara lain yang menggunakan fasilitas Internet di negaranya.

2. Pendapat kedua mengatakan, Internet sebaiknya diatur oleh masing-masing pihak berdasarkan kebiasaan atau dikenal dengan istilah *The Cyber-Separatist Discourse*. Pendapat ini memisahkan antara kehidupan sosial di dunia nyata dengan kehidupan di dalam *cyberspace*. Berdasarkan pendapat ini sebaiknya pengaturan mengenai Internet tidak usah dilakukan oleh negara, karena tidak akan ada peraturan yang cocok untuk mengatur kemajemukan di Internet. Karena pengaturan Internet menggunakan kebiasaan, para pengguna Internet akan merasa lebih dapat menerima peraturan yang ada. Akan tetapi, kelemahan dari pendapat ini adalah tidak adanya penegakan hukum seandainya terjadi sengket antara para pihak.
3. Pendapat ketiga yaitu aliran *The Cyber-Internationalist Discourse*, mengatakan pengaturan Internet sebaiknya melalui ketentuan internasional. Jadi, ada suatu ketentuan hukum berlaku secara internasional yang mengatur mengenai Internet. Pendapat ini mengarahkan pandangannya kepada usaha untuk mengunifikasikan peraturan Internet. Kelemahan dari aliran ini adalah, tidak semua negara mau mengakui pengaturan mengenai Internet yang berlaku tersebut, karena tiap negara memiliki karakterisitik tersendiri.

c. Yurisdiksi Berdasarkan Hukum Internasional

Begitu banyak pendapat-pendapat tentang yurisdiksi yang berkembang dan dilontarkan oleh berbagai ahli, namun sedikit sekali yang akhirnya diterima oleh hukum internasional sebagai prinsip. Prinsip-prinsip tersebut adalah :

1) *Subjective Territoriality* (territorialitas subjektif)

Subjective territoriality adalah prinsip yang terpenting di dalam hukum internasional.[54] Menurut prinsip ini, keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. Mayoritas negara-negara di dunia, mengadopsi prinsip ini ke dalam perundang-undangan pidananya.[55]

Namun demikian J.G Starke, sebenarnya asas ini bukan merupakan asas umum hukum internasional, tetapi penggunaannya yang khusus sudah menjadi bagian hukum internasional, sebagai akibat dari dua konvensi yang penting yaitu *Geneva Convention for Supression of Counterfeiting Currency* (1929) dan *Geneva Convention of the Illicit Drug Traffic* (1930).[56]

2) *Objective Territoriality* (territorialitas objektif)

Objective Territoriality digunakan pada saat suatu tindakan dilakukan oleh pelaku yang berada di luar wilayah suatu negara, akan tetapi justru akibat paling serius yang timbul karena peristiwa itu berada di dalam wilayah negara yang dimaksud.[57] Asas ini dirumuskan oleh Prof. Hyde, sebagaimana dikutip oleh J.G Starke[58], sebagai berikut :

> *"The setting motion outside of a state of a force which produces as a direct consequence an injurious effect therein justifies a territorial sovereign in prosecuting the actor when he enter its domain*."

Sebagai contoh, misalnya orang yang sedang berada di perbatasan suatu negara kemudian menembak seseorang yang berada di wilayah negara lain.

---

[54] Derrel Menthe, *Jurisdiction in Cyberspace : A Theory of International Spaces*, 4 Mich Tech Review, 1998, hal 2
[55] *Ibid.*
[56] J.G Starke, *Introduction to International Law*, 9th ed, (London: Butterworths, 2000), hal 184.
[57] Darrel Menthe, *op.cit*, nomor 8, hal 2
[58] J.G Starke ,*op.cit*, hal 187.

3) *Nationality* (nasionalitas aktif)

Nationality adalah prinsip yang didasarkan kepada status kewarganegaraan seseorang.[59]Prinsip ini oleh Starke disebut juga prinsip nasionalitas aktif[60], yaitu negara tidak wajib menyerahkan warganegaranya yang melakukan pelanggaran di luar negeri. Artinya, negara dianggap lebih berwenang mengadili daripada negara lain tempat terjadinya kejahatan.

Sebagai ilustrasi, apabila seorang WNI berada di luar negeri, kemudian melakukan hubungan denga negara asing dan kemudian meggerakkan kekuatan asing agar melakukan peyerangan kepada Indonesia, maka berdasarkan pasal 111 ayat (1) KUHP, orang tersebut dapat diadili atau dituntut di pengadilan Indonesia.

4) *Passive Nationality* (nasionalitas pasif)

Prinsip ini sedikit berbeda dengan prinsip *nationality*. Jika prinsip *nationality* melihat status kewarganegaraan pelaku kejahatan sebagai dasar kewenangan melakukan penuntutan, maka prinsip *Passive Nationality* melihat status kewarganegaraan korban.[61]

Pembenaran terhadap prinsip ini adalah bahwa setiap negara berhak melindungi warganegaranya di luar negeri, dan apabila negara territorial tempat pelanggaran itu terjadi tidak menghukum orang yang menimbulkan kerugian itu, maka negara dari korban itu berweang menghukum pelanggar tersebut jika pelaku memasuki wilayahnya.[62] Keberatan terhadap prinsip ini adalah bahwa kepentingan umum negara tidak serta merta terganggu hanya karena salah seorang warganegaranya telah dirugikan.[63]

---

[59] Darrell Menthe,*op.cit,* nomor 9, Hal 2
[60] J.G Starke,*op.cit,* hal 211.
[61] Darrel Menthe,*op.cit,* nomor 10, Hal 2
[62] J.G Starke,*op.cit,* hal 211.
[63] *Ibid.*

Prinsip nasionalitas pasif ini antara lain termuat dalam undang-undang pidana Mexico, Brazil, Itali dan Indonesia. Sedangkan Inggris dan Amerika Serikat tidak mengadopsi prinsip ini ke dalam undang-undang pidananya.[64]

5) *Protective Principle* (prinsip perlindungan)

Hukum Internasional mengakui bahwa setiap negara berwenang menangai kejahatan yang berkaitan dengan keamanan dan integritas, serta kepentingan ekonomi yang cukup vital.[65]*Protective Principle* inilah yang digunakan sebagai dasar memanifestasikan kewenangan tersebut. Prinsip ini biasanya diterapkan gua melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya, terutama apabila korban adalah negara atau pemerintah.[66]

Ada dua alasan yang mendasari prinsip ini, yaitu, *pertama*, akibat kejahatan sangat besar bagi negara yang dirugikan . *Kedua*, jika kewenangan tidak diterapkan oleh negara yang dirugikan, maka pelaku kejahatan bisa lolos karena di negara tempat perbuatan dilakukan, perbuatan yang dimaksud belum tentu merupakan tindak pidana serta ekstradisi juga ditolak karena alasan-alasan politis.[67]Kelemahan terbesar yang menimbulkan penolakan terhadap *protective principle* ini, yaitu negara (korban) itu sendiri yang menentukan perbuatan mana yang membahayakan keamanan, sehingga dapat menimbulkan kesewenang-wenangan

6) *Universality* (universalitas)

Asas ini seringkali juga disebut sebagai asas "*universal interest jurisdiction*".[68] Dahulu asas ini digunakan sebagai dasar kewenangan untuk menangkap dan menghukum para pelaku bajak laut dan kejahatan perang akan tetapi

[64] *Ibid.*
[65] *Ibid.*
[66] Darrel Menthe,*op.cit,* Nomor 11.
[67] J.G Starke,*op.cit,* hal 212.
[68] Ahmad M.Ramli, *op cit*, hal 20

kemudian asas ini telah diperluas sehingga termasuk pula penyiksaan, genosida, dan pembajakan pesawat udara.[69]

Asas *universal interest jurisdiction* ini selayaknya memperoleh perhatian khusus guna penanganan dan penegakkan hukum kasus-kasus *cybercrime*.[70]Hal ini disebabkan karena asas ini memandang kewenangan untuk menangani kejahatan lebih kepada perlindungan terhadap kepentingan-kepentingan tertentu dari negara-negara yang ada di dunia, tanpa perlu mempersoalkan *locus delicti* dan kewarganegaraan pelaku.[71]

1.6. Metode Peneltian

Metode Penelitian yang digunakan dalam Tesis ini adalah penelitian hukum normatif. Alat yang Penulis gunakan adalah bahan-bahan kepustakaan dimana penulis berusaha untuk mendapatkan data-data yang ada hubungannya dan dapat mendukung permasalahan yang dibahas.

Bahan pustaka yang dipergunakan antara lain:

1. Bahan Hukum *primer,* yaitu bahan hukum yang mempunyai kekuatan mengikat yang berhubungan dengan Tesis ini yaitu, *The Council of Europe Convention on Cybercrime, The Council of Europe Convention on Transfer of Proceedings*

2. Bahan Hukum *sekunder*, yaitu bahan hukum yang berupa buku-buku teks, penelusuran internet, artikel ilmiah, jurnal, majalah dan surat kabar, makalah, skripsi maupun tesis.

[69] Menthe,*op.cit*, nomor 12
[70] M. Ramli,*loc.cit*
[71] E.Y Kanter dan S.R Sianturi, *Asas-asas Hukum Pidana Di Indonesia Dan Penerapannya*, Cet.2 (Jakarta: Storia Grafika, 2002), hal 111

3. Bahan Hukum *tertier*, yaitu bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum *primer* dan *sekunder*, yaitu kamus.

Tesis ini termasuk penelitian yang bersifat deskriptif analitis yang memberikan gambaran yang jelas mengenai *cybercrime* dalam penerapan perangkat hukum internasional, teori-teori dan prinsip-prinsip umum terkait, dan peraturan-peraturan nasional Indonesia serta menganalisa penerapan teori-teori tersebut dalam beberapa kasus menggunakan pendekatan preskriptif.

1.7. Sistematika Penulisan Tesis

Sistematika disajikan untuk mempermudah pembaca dalam memahami materi yang akan dibahas selanjutnya dalam Tesis ini. Dengan adanya sistematika ini diharapkan pembaca dapat mengetahui secara garis besar Tesis ini. Tesis ini dapat dibagi dalam 4 bab sebagaimana diuraikan berikut ini :

Bab 1 Pendahuluan

Dalam Bab ini penulis akan menjelaskan mengenai latar belakang permasalahan yang berisi tentang sejarah komputer, internet dan perkembangan terkini mengenainya yang membuat Penulis tertarik untuk menjadikan topik ini sebagai Tesis, lalu dijelaskan pula apa yang menjadi masalah yang akan dibahas dalam Tesis ini agar tidak terlalu luas pembahasannya, selanjutnya diternagkan juga dalam bab ini tentang tujuan umum dan khusus yang ingin dicapai Penulis dengan Tesis ini dan diterangkan pula metode (cara-cara Penulis mendapatkan dan menganalisis data) untuk Tesis ini agar pembaca memahami Tesis ini, pada akhirnya di bab ini diterangkan mengenai sistematika Tesis yang dimaksudkan untuk memandu pembaca mengikuti jalan pikiran Penulis dalam mengupas topik ini.

Bab 2 Teori Umum Mengenai *Cybercrime* dan Yurisdiksi

berisikan tentang tinjauan umum tentang *cybercrime*. Pada bab ini dijelaskan terlebih dahulu mengenai *cyberspace* sebagai media terjadinya *cybercrime*, karena

antara *cyberspace* dan *cybercrime* mempunyai ikatan yang sangat dekat, lalu dijelaskan pula pendefinisian *cybercrime* menurut berbagai sumber baik itu dari ahli hukum maupun ahli komputer. Pada bab ini juga dijelaskan kejahatan atau perbuatan apa yang dapat digolongkan sebagai *cybercrime* dan juga dijelaskan mengenai sasaran dari *cybercrime* tersebut. Lalu akan dijelasakan juga mengenai Deportasi, Ektradisi dan *Mutual Legal Assistance* sebagai salah satu instrumen yang digunakan dalam mengatasi masalah yurisdiksi dalam kasus *transboundary cybercrime*. Dan terakhir akan dibahas juga usulan dari beberapa ahli yang menginginkan di bentuknya sebuah badan peradilan internasional yang khusus menangani kasus *transboundary cybercrime*.

Bab 3 Hasil Penelitian dan Analisa

Adalah inti dari semua permasalahan yang sudah bersifat khusus bab ini berisikan pembahasan mengenai sejarah pengaturan mengenai *cybercrime* di Indonesia dan kasus-kasus *cybercrime* yang melibatkan warganegara asing di Indonesia. Setelah itu akan dianalisa kasus-kasus tersebut dengan teori-teori penentuan yurisdiksi yang berkembang. Terakhir akan di paparkan mengenai kemungkinan diterapkannya *transfer of proceeding* dalam kasus tersebut.

Bab 4 Kesimpulan dan Saran

Berisi kesimpulan dari seluruh pembahasan yang telah diuraikan pada bab-bab sebelumnya, kesimpulan ini adalah merupakan jawaban atas pokok permasalahan yang penulis ajukan dalam bab pertama, selain itu bab ini juga berisi saran-saran yang penulis buat untuk permasalahan yang dibah

BAB 2

Tinjauan Umum Tentang *Cybercrime* dan Yurisdiksi

A.Tinjauan Umum Tentang Cybercrime

2.1. *Cyberspace* Sebagai Media *Cybercrime*

Perkembangan teknologi yang begitu pesat terutama dalam bidang komputer melahirkan sebuah program yang akan menjadi sebuah fenomena dunia. Program ini disebut internet yang berasal dari penelitian yang dilakukan oleh Departemen Pertahanan dan Keamanan Amerika Serikat.

Kelahiran internet diikuti juga dengan munculnya penggunaan istilah baru, salah satunya adalah *cyberspace* (dunia maya). Istilah *cyberspace* pertama kali dipopulerkan oleh William Gibson dalam novel *science fiction* yang berjudul *Neuromancer*[72] pada tahun 1980-an, *cyberspace* didefinisikan sebagai suatu tempat yang tidak berbatas dimana data-data diorganisasikan sedemikian rupa ke dalam suatu lintas media[73]. Sementara definisi dari Ian J. Lloyd mengatakan bahwa *cyberspace* adalah fenomena dunia digital yang telah merasuki segala segi dari kehidupan manusia.[74]

Korelasi *cyberspace* dan *cybercrime* keduanya apabila dianalogikan seperti hubungan antara bumi dan aktifitas manusia, yaitu hubungan antara media dan aktifitas yang berlangsung di atasnya. *Cybercrime* sebagai suatu aktifitas tidak akan terjadi jika tidak ada medianya, yaitu *cyberspace*. Namun penanalogian diatas akan menjadi tidak tepat jika kita kaitkan dengan permasalahan batas teritorial atau wilayah, maksudnya jika di dunia nyata, kita dengan mudah dapat mengidentifikasian tempat (lokasi) berlangsungnya suatu aktifitas seseorang. Maka hal yang sama tidak

---

[72] Mark D.Rasch,*Criminal Law and The Internet*, The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, Computer Law Association,1996, Edmon Makarim.*Kompilasi Hukum Telematika* (Jakarta:Rajagrafindo, 2003), hal 59.

[73] *Ibid.*

[74] *Ibid.*, hal 13, lihat juga di artikel Ian J.Lloyd, *Information and Technology Law*, third edition, (London, Butterworths, 2000).

berlaku di *cyberspace*, karena aktifitas di media terebut tidak seperti yang terjadi di dunia nyata, terlepas dari isu batas wilayah. Permasalahan batas wilayah ini dalam konteks dunia nyata mempunyai arti yang penting, khususnya dalam hal menentukan hukum mana atau hukum apa yang seharusnya diterapkan terhadap suatu peristiwa.[75]

Secara umum *cyberspace* memiliki sejumlah karakteristik yang unik, dimana beberapa diantaranya mempunyai pengaruh besar bagi dunia hukum. Karakterisitik yang dimaksud antara lain sebagai berikut:[76]

1) Tidak ada batasan wilayah (*No geoghraphic limitation/no boundaries*)

Karakteristik dari *cyberspace* yang paling khas adalah tidak adanya batasan wilayah (*no boundaries*). Karakteristik ini muncul dengan didasari argument yang memandang bahwa segala yang terjadi di *cyberspace* merupakan suatu interaksi secara elektronik yang dapat melewati batas negara.[77] Sebagai salah satu contoh dalam hal ini adalah *chatting*, dimana aktifitas tersebut tidak mengenal adanya batasan wilayah. Artinya tidak ada suatu ketentuan yang menyatakan bahwa setiap orang hanya dapat *chatting*[78] dengan orang lain yang masih berada di negara yang sama. Karena pada kenyataannya sesorang yang berasal dari negara Indonesia bebas melakukan *chatting* dengan siapapun dari negara manapun. Berkaitan dengan prinsip *no baoundaries* tersebut, pandangan yang paling ekstrim yang berkembang menyatakan bahwa *cyberspace* tidak terkait dengan multi yurisdiksi, melainkan berkaitan dengan tidak ada yurisdiksi.[79]

---

[75] UNESCO, *op.cit*, hal 128.
[76] *Ibid.*, hal 14.
[77] *Ibid.*
[78] *Chatting* atau *Online-chat* adalah suatu bentuk komunikasi melalui internet dengan cara mengetik teks (*text-based*) dimana dua orang atau lebih saling melakukan percakapan dan balasan yang didapatkan secara langsung seperti sedang berbicara secara langsung, kenyataan yang sebenarnya bahwa orang tersebut berada di tempat yang jauh, biasanya chatting dilakukan melaui sebuah media seperti Internet Relay Chat (IRC) , Yahoo Messangers dan lain lain.
[79] David G.Post, "Anarchy, State and The Internet: An Essay on Law Making in Cyberspace", *Journal of Online Law*, 1995, hal 2.

Mengingat keberadaan yurisdiksi selalu dikaitkan dengan keberadaan suatu hukum, maka pendapat yang diuraikan pada paragraf diatas kurang lebih dapat diartikan bahwa di *cyberspace* pada dasarnya tidak ada hukum yang mengatur (*lawless paradise).*[80] Munculnya pendapat tersebut dan jika di kaitkan karakteristik dari *cyberspace* yaitu *no baoundaries*, maka dapat dikatakan bahwa keberadaan *cyberspace* bersama dengan karakteristiknya telah menyimpang dari konsep penerapan hukum yang umumnya didasarkan kondisi fisik dan wilayah.[81]

2) Penyembunyian Identitas (*Anonymity*)

Karakteristik *cyberspace* yang lain adalah diperkenankannya seseorang memasuki *cyberspace* untuk menyembunyikan identitas aslinya. Dalam hal ini pengguna internet umumnya menyembunyikan identitas aslinya dengan nama samaran (*nickname).*[82] Bahkan tidak hanya nama saja yang dapat disembunyikan di *cyberspace*, tempat asal dan umur adalah hal-hal yang lain yang dapat dimanipulasi di *cyberspace*. Sebagai contoh misalnya Udin seorang warganegara Indonesia berusia 45 tahun tengah melakukan *chatting* dengan pengguna lainnya, dalam kesempatan ini Udin bisa saja mengaku bernama John yang berkewarganegaraan Australia berusia 20 tahun.

Karakteristik *cyberspace* yang satu ini memang memungkinkan setiap orang berimajinasi sepuasnya dalam menentukan identitas yang akan diguakan saat beraktifitas di *cyberspace*. Namun disamping itu, keberadaan karakteristik ini juga mempunyai dampak negatif secara hukum yaitu, setiap orang yang melakukan pelanggaran atau kejahatan di *cyberspace* dapat saja lolos dari jeratan hukum hanya dengan memanipulasi identitas dirinya.

[80] UNESCO, *.op. cit*, hal 219.
[81] *Ibid.*, hal 15.
[82] *Ibid.*

3) Flekisbilitas (*Mobility*)

Karakteristik selanjutnya adalah aktifitas di *cyberspace* merupakan aktifitas yang sangat fleksibel dalam hal ruang gerak (mobilitas).[83] Dengan adanya karakteristikini maka pengguna *cyberspace* dengan bebas dapat memilih tempat dimana ia akan melanjutkan aktifitasnya.

Fleksibilitas ini dapat terjadi karena aktifitas di *cyberspace* yang mengedepankan konsep *online*, tidak harus dilakukan di suatu komputer tertentu secara tetap. Apalagi jika dikaitkan dengan perkembangan jenis komputer yang, semakin canggih, yang ditandai dengan kemunculan *notebook* (komputer jinjing)[84] yang diikuti dengan komputer saku (*pocket computer*) yang memiliki kelebihan dari segi mobilitas.

Dampaknya secara hukum adalah dengan sifat fleksibilitas tersebut, pelaku kejahatan di *cyberspace* dapat saja lolos dari jeratan hukum hanya dengan memindahkan lokasi tempat aktifitas *cybercrime* berlangsung dari satu yurisdiksi ke yurisdiksi yang lain. Mereka dapat pula memilih yurisdiksi suatu negara yang kondisi penegakkan hukumnya lemah, sehingga semaikin membuka peluang untuk lolos dari jeratan hukum.

2.2. *Computer Crime* dan *Cybercrime*

Ilmu pengetahuan dan teknologi telah menghasilkan prasarana yang memudahkan manusia. Salah satu produk dari ilmu pengetahuan dan teknologi adalah teknologi informasi atau yang lebih dikenal dengan teknologi telekomunikasi. Telekomunikasi telah membantu umat manusia berinteraksi dengan sesama umat manusia dengan mudah. Munculnya komputer dan internet membuat komunikasi tidak dibatasi dengan sekat-sekat territori suatu negara.

---

[83] *Ibid.*, hal 16.

[84] Definisi *Notebook* adalah Komputer portabel. Komputer portabel pertama yang mula-mula disebut dengan laptop, sebagai pembeda dengan komputer desktop. komputer ini mempunyai ukuran sebesar buku catatan (notebook) - standar ukurannya dalam ukuran kertas 8,5 x 11 inchi dan ketebalan 1 sampai 2 inchi., Febrian, *op.cit.*

Perkembangan teknologi terutama internet membuat banyak dampak positif bagi kemjuan umat manusia,ini ditandai dengan munculnya berbagai layanan yang dilakukan via internet seperti e-*commerce, e-banking, e-goverment dan e-learning*. Selain dampak positif perkembangan tekologi juga memiliki dampak negatif, dalam hal ini dikaitkan dengan dunia kejahatan, para pelaku biasanya menggunakan intenet untuk melakukan kejahatan yang berhubungan dengan komputer seperti, penipuan kartu kredit dan bursa efek, pornografi anak dan terrorisme, selain itu juga ada kejahatan yang menjadikan komputer sebagai targetnya seperti, *defacing*, *cracking* dan *phreaking*.[85]

2.2.1. *Computer Crime* (Kejahatan komputer)

Beberapa ahli telah mencoba mendefinisikan pengertian dari kejahatan komputer, baik dalam suatu literatur (pengertian kriminologis) atau dalam undang-undang/rancangan undang-undang (pengertian yuridis, sehingga muncul berbagai definisi tentang kejahatan komputer, sesuai dengan kepentingan dan sudut pandang masing-masing). Berikut ini penulis mencoba untuk menguraikan beberapa pengertian mengenai kejahatan komputer sebagai gambaran.

---

[85] Heru Sutadi, "Cybercrime, apa yang bisa diperbuat?", <http://www.sinarharapanbaru.co.id/berita/0304/05/op01.html>, diakses tanggal 15 April 2012 sebagaimana dirujuk oleh Abdul Wahid dan Mohammad Labib *.op.cit.,* hal 27.
Beberapa pengertian dalam kalimat diatas (diambil dari Kamus Komputer dan Teknologi Informasi karangan Jack Febrian, Penerbit Informatika tahun 2007)
Defacing adalah melakukan perubahan pada halaman web depan pada situs-situs tertentu, biasanya aktifitas ini dilakukan oleh para *hacker* atau *cracker* dengan gerakan undergroundnya sebagai sebuah *cyber gang fight* untuk mengganggu informasi yang dimunculkan pada halaman situs yang dimaksud.

Cracking adalah proses menemukan kata kunci rahasia dari data yang telah disimpan dan atau dikirim oleh sistem komputer. Pendekatan umumnya dengan secara terus-menerus menebak password yang ingin di-*crack*. Tujuan password *cracking* adalah untuk membantu user memperoleh kembali password yang hilang/lupa, untuk mendapatkan hak-hak akses ke sebuah sistem, atau sebagai ukuran pencegahan oleh administrator sistem untuk mengecek password-password yang dapat *di-crack* dengan mudah. Istilah password cracking terbatas untuk menemukan kembali satu atau lebih plaintext password dari password yang *di-hack*.

Phreaking adalah proses *hacking* dengan menggunakan telefon

1) Pengertian kejahatan komputer menurut Kadish Sanford dan Morrison (guru besar di *Law University of California*) :

   Service.When people gain unauthorized access to a computer and use the service for their own purpose, the crime is also often describe as theft of computer crime. If the unauthorized use continue for the exteded period, if can result in a conciderable less in term of service value without permission from the employer, employees have established own companies and have used the employers computer for the new company seometimes the employers existing data and programs have been used.[86]

2) Pengertian kejahatan komputer menurut IBM. Inc. Japan (perancangan dan specialis komputer) :[87]

   a. *Crime using computer as a tool of theft, fraud, embezzlement and so forth*
   b. *Crime through computer system, such at tempering stealing, and elimination of the data and programs.*

3) Pengertian kejahatan komputer meurut *Organization of European Community a Development : Any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*.[88]

Dari definisi yang bermacan-macam tersebut bahwa pada dasarnya ada perumusan definisi mengenai kejahatan komputer secara luas yaitu, perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan

[86] Kadish Sanford and May T Morrison, ed., "*Encyclopedia of Crime and Justice*",Law University of California, Berkeley, Volume I, hal 220.
[87] Djoko Sarwoko "Computer Crime sebagai Dimensi Baru Tindak Pidana Ekonomi", *Varia Peradilan Nomor 21 Tahun II*, (Juni 1987), hal 150, tampaknya IBM. Inc. menganut konsep *Computer* dan *Computer System* yang terpisah.
[88] Eddy Djunaidi Karnasudirja, *Yurisprudensi Kejahatan Komputer*, (Jakarta : CV. Tanjung Agung, 1993), hal 3.

merugikan pihak lain; dan perumusan secara sempit yaitu perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih.[89]

Berdasarkan beberapa pendapat diatas dapat ditarik suatu gambaran secara umum mengenai ciri-ciri dari kejahatan komputer:[90]

a) Merupakan kejahatan atau berkaitan dengan komputer dan/atau sistem komputer.
b) Merupakan kejahatan dengan modus operandi dengan cara memperdaya komputer.
c) Perbuatan itu dilakukan secara ilegal, tanpa hak atau tidak etis.
d) Perbuatan tersebut membuat komputer tidak dapat berfungsi secara benar.
e) Perbuatan tersebut mengakibatkan kerugian materiil amupun kerugian imateriil (waktu, nilai, jasa,pelayanan).

Para ahli berusaha membatasi perumusan kejahatan komputer sedemikian rupa agar tidak mengaburkan batas-batas dari kejahatan komputer itu sendiri. Sebab jika kurang hati-hati dalam merumuskan definisi kejahatan komputer, misalnya memberikan rumusan yang sedemikian luasnya agar mampu mencakup seluruh permasalahan kejahatan komputer yang cukup kompleks tanpa memberikan batasan-batasan yang pasti, maka hal itu justru akan mengaburkan pengertian dari kejahatan komputer .

Seandainya kejahatan komputer diartikan sebagai kejahatan yang menyangkut komputer dan peralatan-peralatan yang berhubungan dengan sarana-sarana penunjangnya, maka sebenarnya tidak semua kejahatan yang biasanya disebut kejahatan komputer merupakan kejahatan komputer. Sebagai ilustrasi ketika seseorang mencuri *harddisk* yang kosong (tidak memuat data atau program) dan bermaksud untuk dimilikinya sendiri atau dijual ke orang lain, maka perbuatan orang

[89] A.L Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, (Yogyakarta: Penerbitan Universitas Atma Jaya, 2001), hal 4.
[90] *Ibid.*

tersebut belumdapat digolongkan sebagai kejahatan komputer. Perbuatan tersebut lebih tepat disebut sebagai pencurian biasa seperti yang diatur dalam pasal 362 KUHP. Berbeda ketika seseorang tersebut mencuri *harddisk* itu dengan mengetahui atau setidak-tidaknya menduga bahwa di dalam *harddisk* tersebut terdapat program atau data komputer dan orang tersebut bermaksud memiliki atau menjual kepada orang lain data atau program yang terdapat dalam *disk* tersebut (jadi bukan *harddisk* itu sendiri) atau punya maksud lain misalnya untukbalas dendam atau memperoleh imbalan yang tidak wajar dengan menyandera benda-benda vital tersebut agar suatu pusat komputer tidak dapat menjalankan operasinya, maka perbuatan ini baru bisa disebut sebagai kejahatan komputer.[91]

Berikut beberapa klasifikasi atau kategorisasi mengenai kejahatan komputer dari berbagai pendapat. Jongerius membagi kejahatan komputer dalam kategori sebagai berikut:[92]

a) Manipulasi komputer;
b) Spionase komputer;
c) Sabotase komputer dengan (dengan merusak atau menghancurkan peralatan dan atau sistem jaringan komputer);
d) *Unauthorized Use* (pemakaian secara tidak sah) *Computer*;
e) *Unauthorized Access* (memasuki secara tidak sah sistem komputer.

Dalam suatu studi dari kongres Amerika Serikat terdapat empat kategori kejahatan komputer yaitu :

a) Pemasukan data yang tidak benar (*fraudulent*) kedalam komputer;
b) Pemakaian fasilitas-fasilitas yang berhubungan dengan komputer;
c) Merubah atau merusak informasi atau arsip;
d) Pencurian apakah secara elektronis atau dengan cara-cara lain terhadap uang, fasilitas-fasilitas, dan data yang berharga.

[91] A.L Wisnubroto, *.op.cit*, hal 25 dengan modifikasi kasus oleh penulis.
[92] Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, (Jakarta: Sinar Grafika, 1990), hal 23-24.

Selanjutnya ada klasifikasi lain yang meletakkan sebagaian besar dari kejahatan komputer ke dalam empat kategori:

a) Sabotase dan vandalisme sistem komputer;
b) Penggunaan fasilitas-fasilitas komputer tanpa wewenang sebagai pencurian;
c) Kejahatan terhadap barang (pencurian melalui penggunaan komputer); dan
d) Kejahatan terhadap data (pencurian informasi)

Dalam ensiklopedia tentang kejahatan dan keadilan (*The Encyclopedia of Crime and Justice*) dikemukakan mengenai kategorisasi kejahatan komputer sebagai berikut :

> *It has two main categories. In the first, the computer is a tool of a crime, such as fraud, emblezzement, and theft of property, or is used to plan manage a crime. In a second, the computer is a object of a crime, such as sabotage, theft or alteration of storage data, or theft of it services.*[93]

Tampak bahwa klasifikasi atau kategorisasi kehajatan komputer cenderung bersifat luas, sehingga dalam *The International Handbook on Computer Crime* yang diproduksi pada tahun 1986 menganjurkan untuk membuat kategorisasi kejahatan komputer sebagai berikut:[94]

1) *Computer-related Economic Crime.*

a. *Fraud by computer manipulation.*
b. *Computer espionage and software piracy.*
c. *Computer sabotage.*
d. *Theft of service.*
e. *Unauthorized access to DP system and hacking.*
f. *The computer is a tool for traditional business offences.*

[93]Joshua Dressler *ed.*, *The Encyclopedia of Crime and Justice, edition* 2 October, New York, Macmillian Reference, 2001.
[94] The Hon.. Adrian Roden Q.C., *Computer Crime and The Law*, dalam Criminal Law Journal, 1991, hal 339.

2) *Computer-related Infringements of Privacy*

g. *Use of incorrect data.*

h. *Illegal collection and storage of correct data.*

i. *Illegal disclosure and misuse of data.*

j. *Infringements of formalities of privacy laws.*

3) *Further Abuses*

a. *Offences against state and political interest.*

b. *The extension to offences against personal integrity.*

Dari sekian banyak kategorisasi yang diuraikan diatas, dapat ditarik gambaran secara umum bahwa yang termasuk kejahatan komputer adalah :[95]

1) *Offences against Confidentiality, integrity and Availability of Computer Systems and Data*, adalah kejahatan yang bertujuan untuk mengakses, menyadap data atau sistem secara illegal.[96] Yang termasuk kejahatan jenis ini adalah

a) *Illegal Access;*

b) *Data Espionage;*

c) *Illegal Interception;*

d) *Data Interference;*

e) *System Interference;*

[95]ITU, *loc,cit*, hal 18.
[96] .*Ibid*, hal 20-29

2) *Content Related Offences*, adalah kejahatan komputer yang menggunakan konten dalam komputer untuk kejahatan lain.[97] Yang termasuk kejahatan jenis ini adalah :

    a) *Erotic or Pornographic Material;*

    b) *Child Pornography;*

    c) *Racisim, Hate Speech, Glorification of Violence;*

    d) *Religious Offences;*

    e) *Illegal gambling and Online Games;*

    f) *Libel and Fals Information;*

    g) *Spam and Related Threats;*

    h) *Other Forms of Illegal Content such as*

        1) *Soliciting offers and incitement to commit crimes*;

        2) *Unlaful Sale of Products;*

        3) *Provision of information and instructions for illegal acts*.

3) *Copyright and Trademark Related Offences*, adalah kejahatan yang melanggar hak cipta atau merek dagang, seperti pembajakan.[98]

4) *Computer Related Offences*, adalah kejahatan yang menggunakan sistem komputer untuk mengambil data-data tertentu, seperti identitas, nomor tanda pengenal sampai rekening bank.[99] Yang termasuk kejahatan ini adalah :

[97] .*Ibid*., hal 29-41
[98] *Ibid.*, hal 41-45.
[99] *Ibid.*, hal 45-51.

a) *Fraud and Computer-related Fraud;*

b) *Computer-related forgery;*

c) *Identity Theft;*

d) *Misuse of Device.*

5) *Combination Offences* , adalah kejahatan yang memadukan antara *cybercrime* dan kejahatan konvensional seperti *cyberterrorism*,*cyberwarfare* dan *cyberlaundering*.[100]

2.2.2. *Cybercrime*

Belum terdapat definisi final mengenai *cybercrime*. *Convention on Cybercrime* tidak menganggap terminologi "*cybercrime"* sebagai kata yang urgen untuk didefinisikan. Hanya ada 4 kata yang didefinisikan dalam konvensi tersebut, yaitu "computer system", "computer data", "service provider" dan "traffic data"[101]

Namun jika dilihat dari asal katanya , *cybercrime* secara harfiah berasal dari kata *cyber* dan *crime*. *Cyber* berasal dari kata *cybernetics* yang di dalam *Encyclopedia of Knowledge*, sebagaimana yang dikutip oleh Edmon Makarim[102] adalah :

> *"…is a term formerly used to describe an interdisciplinary approach to the study ofcontrol and communication in animals, humans, machines and orgaizations. The Word…"*

Sedangkan *crime* memiliki arti kejahatan. Secara sederhana definisi kejahatan adalah suatu tindakan yang anti sosial. J.M. Bemmelen memandang kejahatan sebagai suatu tindakan yang menimbulkan kerugian, ketidakpatutan dalam masyarakat,

[100] *Ibid.*, hal 51-59.
[101] Convention on Cybercrime Article 1
[102] Makarim,.*op. cit*, hal 6

sehingga dalam masyarakat terdapat kegelisahan, dan untuk menentramkan masyarakat. Karena itu negara harus menjatuhkan hukuman terhadap si pelaku.

Sementara berdasarkan Edwin H Sutherland dalam bukunya 'Principle of Criminology,' menyebutkan terdapat beberapa unsur kejahatan yang saling bergantung dan saling mempengaruhi. Di antaranya, pertama, terdapat akibat-akibat tertentu yang nyata atau kerugian, dan kedua, kerugian tersebut melanggar undang-undang yang berlaku dan ketiga, dilakukan secara sengaja.[103] Sedangkan definisi dari kejahatan secara internasional adalah :

> *…an "international crime" is an act that is defined as criminal under international law. In most instances, this will be done through international agreements, but customary international law also plays a role. Normally, an act will initially be defined as a crime by an international agreement and then, after the agreement has been ratified by a large number of states and generally accepted even by those states who do not become parties, the act may be regarded as a crime under customary international law. If an act is defined as an international crime under customary.*[104]

Berbagai pihak telah mencoba untuk memberikan definisi tentang *cybercrime*. Ada yang mendefinisikan bahwa *cybercrime* adalah suatu aktivitas yang dilakukan dengan sebuah alat (*PC, laptop, notebook, handphone*) yang terhubung dengan jaringan internet dan aktivitas tersebut melanggar undang undang.[105]

---

[103] Muhammad Istijar, Korupsi Kejahatan Luar Biasa, <www.hokionline>, diakses pada 1 Mei 2012.
[104] John F Murphy," *Civil Liability for the Commision of International Crimes as an Alternative to Criminal Prosecution"*, Harvard Human Rights Journal 9 th edition 2007.
[105] Sutanto, Hermawan Sulistyo, Tjuk Sugiarso,Ed.,*Cybercrime: Motif dan Penindakan*,Cet. 1, (Jakarta:Pensil-324,2005), hal 20.

Sedangkan menurut Goodman & Brenner[106], istilah "*cybercrime*", "*computer crime*", dan "*high-tech-crime*" seringkali digunakan secara bergantian untuk merujuk kepada dua kategori, dimana suatu perbuatan telah dianggap melawan hukum. Dua kategori itu adalah, pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku bisa melakukan akses secara illegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan (*networking*). Kategori kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvensional, misal pencurian, pemalsuan.

Lastwoka dan Hunter mendefinisikan *cybercrime* sama degan apa yang biasanya disebut sebagai *virtual crime* (kejahatan maya), yaitu suatu kejahatan yang dilakukan terhadap komputer atau dengan alat bantu komputer.[107] Sejalan dengan pemikiran Lastwoka dan Hunter *International Telecommunication Union* (ITU) memberikan definisi dari *cybercrime* itu adalah kejahatan yang melibatkan komputer baik sebagai alat, target ataupun perantara untuk melakukan kejahatan konvensional.[108]

2.3. Jenis-jenis Cybercrime

Seperti pengertian *cybercrime*, jenis-jenis *cybercrime* juga berbeda-beda, karena setiap ahli hukum memiliki pandangan yang berbeda-beda, selain itu juga belum ada kesepakatan yang seragam mengenai pengertian *cybercrime* membuat banyaknya perbedaan tersebut. Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan sebagai *cybercrime* diatur dalam Pasal 2-5, adapun jenis tindak pidana tersebut adalah :

---

[106] Marc D. Goodman dan Susan W. Brenner, *The Emerging Consensus On Criminal Conduct in Cyberspace*, hal 10. Diakses melalui situs <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanberner.php>, pada tanggal 1 April 2012.

[107] F.Gregory Lastwoka dan Dan Hunter, *Virtual Crime*, didownload dari situs <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=564801>, pada tanggal 5 Maret 2012.

[108] ITU, *Loc cit*, hal 17

1. *Illegal Access*[109]

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem komputer.[110] Perlindungan terhadap pelanggaran *illegal access* ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada ganguan dan hambatan.

Pasal ini merupakan ketentuan pertama yang mengatur mengenai masalah *cybercrime*. Sebagai contoh dari kejahatan ini adalah *hacking*, *cracking* atau *computer trespassing*. Gangguan jenis ini memberikan akses kepada pelaku terhadap data-data penting (termasuk *password* atau informasi sistem) dan rahasia-rahasia, yang mungkin digunakan untuk membeli barang dengan menggunakan informasi kartu kredit milik orang lain atau mendorong pelaku untuk melakukan bentuk pelanggaran berkenaan dengan komputer yang lebih berbahaya, seperti pemalsuan atau penipuan dengan komputer.[111]

Pemahaman mengenai *access* sebagaimana disebut dalam ketentuan pasal ini, terdiri dari memasuki seluruh atau sebagian dari suatu sistem komputer (*hardware*, bagian-bagian, data yang tersimpan pada sistem yang terpasang, direktori-direktori, lalu-lintas data-data dan data yang berkenaan dengan isi). Namun demikian akses yang dilakukan ini tidak termasuk didalamnya dengan kegiatan mengirimkan *email* atau *file* ke sistem tersebut. *Access* yang dimaksud meliputi kegiatan memasuki sistem komputer lainnya baik yang terkoneksi melalui jaringan komunikasi umum,

---

[109] Diatur dalam Pasal 2 *Convention on Cybercrime*, yang berbunyi :

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

[110] Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), poin ke 44.

[111] Mike Keyser, "The Council of Europe Convention on Cybercrime", (*Journal of Transnational Law and Policy*, volume 12, 2003), hal 300.

tatu terhadap suatu sistem komputer pada jaringan yang sama seperti pada suatu *Local Area Network* (LAN) atau *intranet* dalam suatu organisasi. Cara komunikasi yang dilakukan baik dari satu lokasi tertentu dengan cara *remote* maupun dengan penghubung *wireless* pada jarak yang dekat tidak masalah.[112]

Ketentuan pasal ini juga menerangkan mengenai pentingnya permasalahan tanpa hak yang harus ada pada suatu pelanggaran yang dilakukan . Bukanlah suatu pelanggaran pidana terhadap akses yang disetujui oleh pemilik atau pemegang hak dari suatu sistem atau bagian dari pemilik atau pemegang hak tersebut.[113] Kondisi ini dapat terjadi apabila dibutuhkan pengujian terhadap keamanan suatu sistem.

2. *Illegal Interception*[114]

Menyatakan tidak sah tindakan pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faximile, *email*, atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.

Pengertian *interception* secara teknis dijleaskan dalam *Explanatory Report To The Convention on Cybercrime* yaitu,

> "*Interception by techincal means relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer*

[112] Council of Europe, *.op cit.*, poin ke 46.
[113] Council of Europe,*.op cit.*, poin ke 47.
[114] Diatur dalam pasal 3 *Cybercrime Convention*, yang berbunyi :

> "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

system, or undirectly through the use of electronic eavesdropping or taping devices.Interception may also involving recording."[115]

Salah satu bagian dari pelanggaran yang dimaksud dari ketentuan pasal ini adalah melakukan penahanan komunikasi atau menghambat proses komunikasi dengan menggunakan perangkat elektronik untuk mendengarkan pembicaraan orang lain atau menggunakan peralatan untuk menyadap komunikasi. Klasifikasi ini hanya berlaku pada komunikasi data komputer yang dilakukan secara pribadi, klasifikasi ketentuan ini mengacu pada sifat pemindahan dan sifat dari data yang dipindahkan. Komunikasi yang terjadi dapat melalui hubungan dari komputer ke *printer*, antara dua komputer atau dari orang ke komputer itu sendiri (seperti mengetik dengan keyboard).[116]

3. *Data Interception*[117]

Ketentuan pengerusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicous codes*), *Viruses*, dan *Trojan Horse* ke suatu sistem komputer merupakan pelangagaran menurut ketentuan pasal ini.[118]

Berdasarkan Pasal 4 ayat 1 merupakan tindak pidana apabila dilakukan dengan terencana tindakan merusak, menghapus, memperburuk, mengubah atau mengembangkan suatu data komputer tanpa hak.[119] Ketentuan yang diatur dalam pasal ini berusaha untuk memberi jaminan bahwa data yang dikirimkan melaui

---

[115] Council of Europe,.*op cit.*, poin ke 53.
[116] Keyser, .*loc cit*., hal 301.
[117] Diatur dalam Pasal 4 *Cybercrime Convention* yang berbunyi :
1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
2. *A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.*

[118] Keyser, .*loc cit*., hal 302.
[119] The Convention on Cybercrime, 23 November 2001.

jaringan internet atau pemindahan data yang dilakukan melaui suatu jaringan adalah sama dengan data yang dikirimkan oleh si pengirim. Kepentingan perlindungan hukum dalam pasal ini adalah keutuhan dan berfungsi sebagaimana mestinya penggunaan data komputer yang tersimpan atau program-program komputer.[120]

4.*System Interference* [121]

Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila "*... when committed intentionally, the serious hindering without right of the functioning of a computer system*…", harus dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer.[122]

Pengganguan terhadap sistem dijadikan sebagai tindak pidana bertujuan untuk mencegah *"…the serious hindering without right of the functioning of a computer system…"*[123]

Sebagai contoh adalah serangan *denial-of-service* yang dilakukan dengan teknik *hacking*, pembuatan kode jahat seperti virus. Contoh tersebut dapat memperlambat penggunaan sistem komputer yang mengakibatkan pengguna tidak dapat mengakses suatu *website.*

[120] Council of Europe,.*op cit.*Poin ke 60.
[121]Diatur dalam pasal 5 *Cybercrime Convention* berbunyi

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."*

[122] Council of Europe,.*op cit*, poin 66.
[123] Keyser, .*loc cit*., hal 303.

5.*Misuse of Device*[124]

Misuse of Device diatur dalam Pasal 6 konvensi ini adapun yang termasuk jenis kejahatan ini adalah pencurian ,penyediaan, penjualan dan distribusi dari data komputer yang diperoleh dari sebuah alat.[125] Adapun yang di maksud alat disini adalah *hardware* maupun *software* yang telah di modifikasi untuk mendapatkan akses dari sebuah komputer atau jaringan komputer.[126] Contohnya apabila ada sesorang yang memasukkan *keylogger* dalam jaringan bank untuk mendapatkan data-data nasabah mulai dari alamat sampai ke *password* ATM dan data-data tersebut dijual, digunakan atau didistribusikan untuk kejahatan lain.

International Telecommunications Union (ITU) dalam terbitannya *Understanding cybercrime guide* juga memberikan jenis-jenis kejahatan yang termasuk ke dalam *cybercrime*. Adapin kejahatan-kejahatan tesebut adalah:[127]

---

[124] Pasal 6 berbunyi:

"1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. "

[125] ITU, *loc.cit*, hal 152
[126] Council of Europe,*loc cit* Poin 72
[127]ITU, *loc,cit*, hal 18.

1) *Offences against Confidentiality, integrity and Availability of Computer Systems and Data*, adalah kejahatan yang bertujuan untuk mengakses, menyadap data atau sistem secara illegal.[128] Yang termasuk kejahatan jenis ini adalah

    a) *Illegal Access;*

    b) *Data Espionage;*

    c) *Illegal Interception;*

    d) *Data Interference;*

    e) *System Interference;*

2) *Content Related Offences*, adalah kejahatan komputer yang menggunakan konten dalam komputer untuk kejahatan lain.[129] Yang termasuk kejahatan jenis ini adalah :

    a) *Erotic or Pornographic Material;*

    b) *Child Pornography;*

    c) *Racisim, Hate Speech, Glorification of Violence;*

    d) *Religious Offences;*

    e) *Illegal gambling and Online Games;*

    f) *Libel and Fals Information;*

    g) *Spam and Related Threats;*

    h) *Other Forms of Illegal Content such as*

        1) *Soliciting offers and incitement to commit crimes*;

        2) *Unlaful Sale of Products;*

        3) *Provision of information and instructions for illegal acts*.

3) *Copyright and Trademark Related Offences*, adalah kejahatan yang melanggar hak cipta atau merek dagang, seperti pembajakan.[130]

[128] .*Ibid*, hal 20-29
[129] .*Ibid*., hal 29-41

4) *Computer Related Offences*, adalah kejahatan yang menggunakan sistem komputer untuk mengambil data-data tertentu, seperti identitas, nomor tanda pengenal sampai rekening bank.[131] Yang termasuk kejahatan ini adalah :

   a) *Fraud and Computer-related Fraud;*
   b) *Computer-related forgery;*
   c) *Identity Theft;*
   d) *Misuse of Device.*

5) *Combination Offences* , adalah kejahatan yang memadukan antara *cybercrime* dan kejahatan konvensional seperti *cyberterrorism*,*cyberwarfare* dan *cyberlaundering*.[132]

2.4. Sasaran Cybercrime

Susan W Brenner, *Professor of Law and Technology* dari *University of Dayton School of Law* mempunyai pendapat untuk menggambarkan bentuk-bentuk *cybercrime*. Brenner mengatakan bahwa terdapat berbagai pendekatan dalam merespon *cybercrime* antara lain ada yang menggunakan hukum pidana tradisional, ada yang memodifikasi hukum pidana tradisional dan ada pula yang membutuhkan perumusan suatu hukum pidana yang benar-benar baru.[133] Akan tetapi Brenner mengelompokkan kejahatan-kejahatan tersebut ke dalam kategori : *crimes against persons, crimes against property, crimes against state* dan *crimes against morality*.[134]

Menurut Brenner, empat kategori ini merupakan pembidangan yang lebih tepat untuk menggolongkan kejahatan-kejahatan yang dilakukan dengan cara-cara yang baru tersebut. Pembidangan tersebut adalah sebagai berikut :

---

[130] *Ibid.*, hal 41-45.
[131] *Ibid.*, hal 45-51.
[132] *Ibid.*, hal 51-59.
[133] G-8 Reccomendation, *.op. cit.*, poin ke 14.
[134] G-8 Reccomendation, *.op. cit*, poin ke15.

2.4.1. *Crimes Against Persons* (kejahatan tehadap orang)

Kejahatan ini oleh Brenner dibedakan menjadi dua yaitu, kejahatan seksual dan non-seksual. Kejahatan seksual disini antara lai adalah pornografi. Barangkali pornografi mempunyai intrepretasi yang berbeda-beda di tiap negara, tetapi pornografi yang melibatkan anak dibawah umur (*child pornography)* pada dasarnya telah dikriminalisasi di hampir semua negara.

Sedangkan kejahatan non-seksual terhadap orang dapat terjadi melalui media *cyber*, antara lain berupa *homicide* (menimbulkan kematian bagi orang lain) dan *assault* (menyebabkan cedera atau celaka bagi orang lain). Contoh tersebut antara lain dapat diilustrasikan mengenai seorang hacker yang mampu membobol sistem computer sebuah rumah sakit, dan kemudian memanipulasi daftar obat-obatan berbahaya yang ada di *database* agar dikonsumsikan kepada pasien-pasien yang tidak mengkonsumsi obat-obat berbahaya tersebut. Dengan begitu akan semakin bertambah parah bahkan bisa berakibat tewasnya para pasien tersebut.[135]

2.4.2. *Crimes Against Property* (kejahatan terhadap hak milik)

Kejahatan terhadap hak milik seseorang merupakan kejahatan yang paling popular, bahkan merupakan kejahatan yang paling umum bila dilihat dari prespektif kejahatan konvensional sekalipun. Namun kali ini cara yang dilakukan oleh pelaku adalah dengan memanfaatkan teknologi internet.

Kejahatan terhadap hak milik ini ada beberapa jenis. Brenner memfokuskan tipe kejahatan ini kedalam 3 jenis yaitu *hacking* (pembobolan), *theft* (pencurian) dan *forgery* (pemalsuan)

[135] G-8 Reccomendation, .*op. cit*, poin ke 17.

2.4.3. *Crimes Against State* (kejahatan terhadap negara)

Menurut Brenner, kejahatan terhadap Negara pada dasarnya telah dikriminalisasi oleh berbagai peraturan perundang-undangan pidana yang ada disetiap negara. Bentuk-bentuk kejahatan semacam ini antara lain perbuatan yang secara langsung dapat menghancurkan kekuatan militer Negara (missal sabotase), diarahkan kepada infrastruktur Negara (missal sarana kesehatan, sarana komunikasi), dapat menggangu stabilitas sistem fiskal nasional (missal pemalsuan uang atau surat-surat berharga). Bahkan kejahatan terhadap agama juga dapat dikategorikan ke dalam kejahatan ini.

Kemajuan teknologi komputer, telah meningkatkan jumlah dokumen rahasia yang disimpan dalam format komputer. Dengan demikian, kejahatan terhadap negara semakin mudah dilakukan dengan adanya bantuan teknologi informasi sekarang.

2.4.3. *Crimes Against Morality* (kejahatan terhadap moral)

Brenner beranggapan bahwa teknologi computer telah memberikan peluang yang cukup besar bagi tindakan-tindakan yang dapat dianggap bertentangan dengan moralitas. Walaupun pada dasarnya kejahatan terhadap moral ini telah dikriminalisasi oleh undang-undang pidana tradisional, tetapi dengan fasilitas teknologi komputer, perbuatan amoral semakin mudah dilakukan.Oleh Brenner tindakan-tindakan amoral itu diberi contoh antara lain perjudian *on-line*, iklan dan perdagangan prostitusi, penyebarluasan materi-materi pornografi.

2.5. *Cybercrime* Sebagai Kejahatan Transnasional

Kejahatan merupakan delik menurut hukum *(rechtsdelicten*), yaitu perbuatan yang bertentangan dengan tertib hukum. Menurut *Memorie Van Toelichting*/memori penjelasan, kejahatan adalah perbuatan yang dinyatakan sebagai tindak pidana bahkan menurut hukum, dalam hal perbuatan tersebut sudah mengandung ancaman pidana bahkan sebelum dinyatakan demikian oleh pembuat undang-undang, bahkan sifat melawan hukum dari perbuatan tersebut sudah disadari meskipun tidak

disebutkan oleh pembuat undang undang. Menurut jan Remmelink tidak satupun suatu tindak pidana berdasarkan suatu system pengertian tertentu dapat dikategorikan sebagai kejahatan atau pelanggaran, yang menentukan dalah makna kebendaan hukum yang tersentuh oleh tindak pidana, ruang lingkup pelanggaran hukum yang terjadi, bagaimana perbuatan itu terjadi, namun demikian meskipun pelanggaran tidak berbeda dengan kejahatan, tetapi dari system kuantitatif pelanggaran kurang berat dari kejahatan.[136]

Perkembangan teknologi informasi dan telekomunikasi yang sangat siginifikan menciptakan suatu "dunia baru" yang sering dikenal dengan istilah *cyberspace*. *Cybercrime* merupakan modus atau bentuk baru dari kejahatan yang terjadi di *cyberspace* akibat dari penyalahgunaan jaringan computer atau internet.

Cybercrime sebagai bentuk kejahatan jika di kaji dari aspek kriminologi dapat dilihat dari beberapa sudut pandang atau teori yaitu: [137]

1) Teori Anomali :

Teori ini berpijak dari adanya suatu keadaan "*normless"* yang terjadi di tengah masyarakat yaitu keadaan "*total absence of norms"* dalam terjemahan bebasnya terjadi kekosongan hukum ditengah-tengah masyarakat khususbya yang berhubungan dengan pengaturan tentang *Cybercrime*. Kekosongan hukum bukanlah dalam artian tidak ada sama sekali hukum yang mengaturnya, namun terjadi ketidakmampuan norma khusunya norma hukum termasuk perangkat hukum yang ada untuk mengatur dan mengontrol perilaku dari individu (*inability of norms to control or regulate)*, hal ini disebabkan oleh ketidakmampuan hukum yang ada untuk menjangkau atau mengatur kejahatan yang terjadi di *cyberspace*. Hukum yang ada yang dibuat pada masa lampau khususnya KUHPidana sangat kurang memadai untuk menghadapi *cybercrime*, bahkan peraturan perundang-undangan yang dibuat juga tidak sepenuhnya merepresenatsikan kebutuhan akan penegakkan hukum dalam dunia

[136] Jan Remmelink,*Hukum Pidana*, Gramedia Pustaka Utama, Jakarta, 2003, Hal 67-68
[137] Abdul Wahid dan Muhammad Labib,*Kejahatan Mayantara (Cybercrime)*, (Cet 1,PT Refika Aditama), Bandung, 2005,Hal 78-87

cyber/telematika. Kekosongan hukum ini dimanfaatkan ataupun mendoroang serta menjadi celah bagi para pelaku untuk melakukan kejahatan di *cyperspace*.

2) Teori Perbedaan Asosiasi (*Differential Association)*

Cybercrime adalah kejahatan yang memanfaatkan teknologi informatika dan telekomunikasi yang canggih, dan para pelaku biasanya adalah orang-orang yang mahir dalam bidang telematika, sehingga untuk dapat memasuki dunia *cyber* dan bahkan melakukan *cybercrime*, seseorang harus belajar terlebih dahulu. Oleh karena itu *cybercrime* dapat dikatakan sebagai kejahatan hasil proses belajar pelaku baik secara otodidiak maupun belajar kepada para pakarnya. Pelaku harus belajar karena kejahatan ini dilakukan dengan memanfaatkan teknologi informatika dan telekomunikasi canggih yang tidak dapat dilakukan oleh orang sembarangan.

3) Teori Kontrol Sosial (*Control Social*)

Menurut teori ini setiap orang dapat melakukan kejahatan, dapat mencuri, membunuh, merampok, memakai narkoba, dan sebagainya, namun yang menjadi pertanyaan utama adalah mengapa masih ada orang yang mampu bertahan untuk menaati norma ketika banyak yang melanggar norma itu, banyak tekanan, kesempatan dan bujuk rayu untuk melakukan, ternyata masih ada orang yang mau melakukannya

Oleh karena itu masih ada yang bertahan berarti mereka yang melakukan kejahatan karena kurangnya control atas diri mereka baik itu control pribadi maupun control sosial. Control pribadi adalah bagaimana seseorang mampu mengontrol dirinya sendiri agar tidak melakukan perbuatan yang menyimpang dalam mencapai keinginannya sedangkan control sosial adalah kemampuan kelompok sosial atau lembaga masyarakat untuk melaksanankan norma atau peraturan agar dapat berlaku secara efektif.

Pelaku *cybercrime* biasanya melakukan kejahatannya seorang diri atau bersifat tertutup hanya pribadi atau setidaknya kelompoknya saja yang tahu sehingga

bersifat privat atau ekslusif, akibat yang timbul juga tidak seketika dan tidak menimbulkan ketakutan yang besar bahkan banyak kejahatan *cyber* yang tidak di sadari oleh korbannya. Sehingga control pribadi pelaku sangat kurang karena respon korban terhadap *cybercrime* sangat lambat dan tidak menghebohkan. Dalam konsep negara sebagai suatu masyarakat, maka ketika hukum dan aparat penegaknya (negara) tidak mampu merespon *cybercrime* maka control sosial terhadap kejahatan tersebut makin lemah. Hal ini yang mendukung tumbuh kembangnya *cybercrime*.

Melalui perkembangan paradigm sistem komunikasi yang bersifat global menimbulkan suatu fenomena pemikiran yang dahulu bersifat lokal ataupun nasional menjadi bersifat internasional, sehingga dalam waktu seketika *cybercrime* menjelma sebagai kejahatan dunia maya yang memanfaatkan jaringan telematika global, kejahatan yang dapat di lakukan dimana saja dan kapan saja serta meinimbulkan dampak negatif kemana saja berskala internasional. Oleh karena itu *cybercrime* menjadi kejahatan dengan pelaku, korban, tempat terjadinya perbuatan pidana (*locus delictie*), serta akibat yang ditimbulkan dapat terjadi pada dan atau di beberapa negara.

Cybercrime sebagai kejahatan internasional memiliki beberapa karakteristik unik tertentu yaitu :[138]

1) Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang /wilayah siber (*cyberspace),* sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.

2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.

3) Perbuatan tersebut mengakibatkan kerugian materiil maupun immaterial (waktu, nilai, jasa, uang, barang , harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional.

[138] Ary Juliano dalam Abdul Wahid dan Muhammad Labib,*Op.cit,* Hal 26

4) Pelakunya dalah orang yang menguasai penggunaan internet beserta aplikasinya.

5) Perbuatan tersebut sering dilakukan secara transnasional /melintasi batas negara.[139]

Selain karena karakteristiknya *cybercrime* itu sendiri ada beberapa faktor pendukung perkembangan *cybercrime* yaitu :[140]

1) Biaya pembelian komputer, telepon seluler dan penggunaan internet semakin murah dan terjangkau sehingga pengguna komputer dan internet sangat cepat pertumbuhannya.

2) Semakin mudahnya memperoleh akses jaringan informasi dan komunikasi termasuk internet seperti pemasangan *Wi-fi* (*wireless fidelity)* yang makin banyak dan tersebar di tempat-tempat umum serta banyaknya warung internet dengan biaya pemakaian yang murah.

3) Banyak informasi yang dapat diperoleh dari internet, baik itu informasi berita dari berbagai belahan dunia maupun informasi ilmu pengetahuan dari berbagai disiplin ilmu.

4) Mengakses internet dapat dilakukan dari manapun bahkan darintempat yang tersembunyi dari penegak hukum dan korban bahkan dari luar kota dan luar negeri.

5) Pengakses/pengguna internet bersifat anonym (tidak diketahui siapa yang menggunakan jasa internet tersebut), tidak mudah dilacak karena tidak ada kewajiban pengguaan identitas yang sebenarnya pasa saat memasuki *cyberspace*.

[139] *Ibid.*
[140] Sutan Remy Syahdeni,*Kejahatan dan Tindak Pidana Komputer*,2009,Jakarta, Grafiti, Hal 47-78

6) Bukti-bukti elektronil/digital (*electronic or digital evidence)* mudah di hapus atau diubah menggunakan komputer lain ditempat lain.

7) Penegak hukum masih kesulitan mengendalikan penggunaan internet.

Modernisasi konvergensi informatika dan komunikasi yang mendorong lahirnya era globalisasi dewasa ini menimbulkan perubahan kehirdupan manusia menjadi berdasarkan pemikiran bersifat globa dengan segala kompleksitasnya. Perubahan pola pemikiran tersebut mengakibatkan perbuhan sistem nilai yang menuntut terjadinya perubahan norma-norma kehidupan sosial dan hukum yang baru. Perubahan tersebut meliputi perubahan struktur hubungan hukum, substansi pengaturan hukum dan budaya hukum. apabila perubahan itu tidak terjadi atau terwujud maka akan menimbulkan bahaya terhadap ketentraman kehidupan dalam pelbagai kehidupan sosial, semua keadaan menjadi serba tidak pasti, tidak tertib dan tidak terlindungi dengan semestinya. Perubahan tersebut timbul serta merta sebagai akibat kompleksitas dan heterogenitas hubungan antar manusia sebagai makhluk sosial yang semakin intens dengan semakin modernnya teknologi informatika dan telekomunikasi.[141]

2.6. Hukum Acara (*Procedural Law*) Dalam *Convention on Cybercrime*

Selain mengatur tentang hukum yang mengatur tentang jenis-jenis *cybercrime* (*substantive law*), *Convention on Cybercrime* juga mengatur mengenai hukum acara (*procedural law*) yang di butuhkan dalam menangani kasus-kasus *cybercrime*. Hal ini mengingat keberadaan pelaku yang tidak harus hadir dalam tempat kejadian perkara dalam kasus *cybercrime* sehingga investigasi harus dilakukan dengan cara yang berbeda dari investigasi yang konvensional.[142] Dalam konvensi ini ditaur beberapa cara untuk melakukan investigasi dan batasan-batasan yang harus dilaksanakan dalam

[141] Muladi,*Hak Azasi Manusia dalam Politik dan Sistem peradilan Pidana*,Kapita Selekta Sistem Peradilan Pidana,Badan Penerbit Universitas Diponegoro,Semarang,2002, Hal 57
[142] ITU, *op.cit*, hal 170

investigasi tersebut. Yang termasuk *procedural law* dalam *convention on Cybercrime* adalah:[143]

1.*Safeguard*

Safeguard yang di maksud dalam Pasal 15 *Convention on Cybercrime* adalah batas-batas yang harus di hormati dalam melakukan investigasi *cybercrime*, maksudnya disini setiap orang boleh melakukan investigasi *cybercrime*, namun harus melihat hukum domestik terlebih dahulu terutama soal prosedur dan tata cara melakukan investigasi terutama yang berkaitan dengan *cybercrime*. Misalnya untuk melakukan penyadapan terhadap data elektronik ada negara yang mewajibkan penyidik atau pihak pihak yang bekepentingan untuk memperoleh izin dari pengadilan. *Safeguard* diperlukan agar sebuah investigasi *cybercrime* tidak menjadi terlalu luas dan akhirnya meyebabkan pelanggaran Hak Asasi Manusia (HAM). Adapun *safeguard* yang dapat dilakukan dalam kaitannya dengan *Convention on Cybercrime* meliputi:[144]

a) Pengawasan

b) Aplikasi batasan kesalahan

c) Pembatasan prosedur terkait dengan lingkup dan waktu

2.*Expedited Preservation and Disclsoure of Stored Computer Data* & *Data Retention*

Pembahasan kedua prosedur ini dijadikan satu karena saling berkaitan dan tidak jauh berbeda dari segi definisi. Persamaan dari kedua prosedur diatas adalah sama-sama merupakan tindakan untuk mencegah data yang akan digunakan untuk menjerat pelaku *cybercrime* di hapus dan menyebabkan pelaku tidak dapat dilacak. Perbedan yang mendasar adalah dalam *data preservation* data tersebut sudah tersimpan dalam waktu yang cukup lama dalam sebuah jaringan, dan data tersebut

[143] *Ibid*, hal 173-207
[144] *Convention on* Cybercrime, Pasal 15 subparagraf 2

harus di jaga agar tidak berkurang atau tidak berubah sebaliknya dalam *data retention* data tersebut baru saja ada atau terjadi lalu disimpan. Dengan kata lain *data retention* adalah aktivitas penyimpanan data tapi *data preservation* adalah aktivitas untuk menjaga data aman.[145] Dalam *Convention on Cybercrime* hanya *Expedited preservation and disclosure of stored computer data* yang secara sepsifik diatur dalam Pasal 16 ditambah Pasal 17 yang mengatur tentang *Expedited preservation and partial disclosure of traffic data*. Inti dari kedua pasal ini sama yaitu *Internet Service Provider* (ISP) wajib untuk menyimpan data mereka dalam waktu tertentu dan di haruskan untuk menyimpan dan melindungi data atau trafik data yang diminta oleh pihak yang berwenang untuk dipakai menjerat pelaku *cybercrime*.[146]

3.*Production Order*

Prosedur ini berhubungan dengan permintaan data yang dimiliki oleh perorangan, dalam *cybercrime* hal ini dimungkinkan karena bisa saja pelaku mengakses dan melakukan kejahatan tersebut melalui komputer milik orang lain ataupun komputer publik (misalnya di warnet). Jika ada data atau bukti yang tersimpan di dalam komputer tersebut, maka penyidik tidak bisa serta merta menyita komputer tersebut di karenakan milik pribadi, atau data yang bisa di jadikan bukti terdapat di dalam *server* milik ISP yang di dalamnya ada data-data rahasia milik pelanggannya (no kartu kredit, jaminan sosial, dll. Dalam prosedur yang diatur dalam Pasal 18 *Convention on Cybercrime* memuat dua kewajiban yaitu:[147]

a) Setiap orang (termasuk ISP) wajib untuk meyerahkan data yang dimilikinya

b) Setiap orang wajib untuk menyerahkan data spesifik yang dimilikinya

[145] *Council of Europe,op cit*, poin 151
[146] ITU, *op.cit*, hal 179
[147] *Ibid*, hal 191-192

3.*Search and Seizure of Stored Computer Data*

Prosedur ini adalah yang umum dilakukan oleh negara-negara apabila menangani kasus *cybercrime*, yang biasanya dilakukan pertama kali oleh negara-negara adalah dengan menyita perangkat komputer yang di curigai dipakai untuk melakukan *cybercrime*, hal ini diatur dalam pasal 19 ayat 1 *Convention on Cybercrime* yang menyatakan jika penyidik dapat melakukan pencarian dan penyitaan data di :[148]

a) Jaringan komputer atau *server* yang terhubung dengan banyak komputer

b) Tempat penyimpanan independen seperti CD-ROM atau disket

Namun pelaku sekarang lebih cerdik untuk mengakali hal tersebut dengan menyimpan data tersebut di internet (*cloud computing*).[149] Tantangan lain yang di hadapi oleh penyidik adalah apabila ternyata penyitaan *hardware* atau komputer yang di maksud belum cukup untuk menjerat pelaku artinya penyidik harus mencari bukti lain yang seringkali bisa merusak data tersebut, hal ini dapat diatasi dengan apa yang diatur dalam Pasal 19 ayat 3 yang berbunyi:[150]

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

[148] *Convention on Cybercrime*, Pasal 19 ayat 1
[149] *Ibid*, hal 187
[150] *Convention on Cybercrime*, Pasal 19 ayat 3

Ayat 3 ini menjelaskan kepada kita jika penyidik bisa menyita data yang sama dari yang telah didapat sebelumnya seperti yang di jelaskan dalam ayat 1 dan 2 , termasuk untuk kasus dimana data tersebut tidak dapat digandakan. Sehingga *hardware* yang digunakan untuk menyimpan data tersebut juga harus di sita.[151]

4.*Real Time Collection of Traffic Data*

Traffic data adalah data yang di dapat ketika komputer melakukan komunikasi dari asal ke tujuan.[152] Yang dimaksud komunikasi di sini apabila kita mengakses suatu *website* maka komputer akan melakukan koneksi dengan *server website* tersebut untuk kemudian membawa kita ke halaman awal *website*. Hal ini juga diatur dalam *Convention on Cybercrime* sebagai salah satu cara untuk mendapatkan bukti yang bisa digunakan untuk menjerat pelaku *cybercrime*. Dalam Pasal 20 ada dua cara untuk mendapatkan *traffic data* tersebut, dua cara tersebut adalah:[153]

a) ISP wajib menginstall satu program yang memungkinkan penyidik untuk langsung mengakses dan mengambil data yang diperlukan

b) ISP wajib untuk menyerahkan data yang diminta atas permintaan penyidik

5.*Interception of Content Data*

Seperti yang sudah di jelaskan di atas penerapan prosedur ini harus dilakukan dengan hati-hati dengan memperhatikan *safeguard* karena prosedur ini memberikan kewenangan penyidik untuk melakukan penyadapan kepada pelaku yang diduga melakukan *cybercrime.* Adapun yang biasanya di sadap adalah: [154]

a) Isi dari *email* pelaku

b) Situs yang diakses oleh pelaku

[151] *Council of Europe*, poin 196
[152] ITU, *op.cit*, hal 195
[153] *Ibid*, hal 196
[154] *Ibid*, hal 198

c) Percakapan via chat room atau VoIP

Dalam *Explanatory Report Convention on Cybercrime*, pasal 20 yang mengatur tentang hal ini sangat sedikit di bahas karena penerapannya tergantung dengan kondidi *safeguards* yang diatur dalam hukum negara tempat penyadapan itu akan dilakukan.

B.Yurisdiksi.

2.7. Penerapan Hukum di *Cyberspace*

Sebelum memasuki bahasan utama mengenai yurisdiksi, penulis merasa perlu diulas mengenai penerapan hukum di *cyberspace*. Di dalam penerapan hukum ini terdapat perdebatan yang alot antara ide kebebasan di dalam *cyberspace* dengan desakan perlunya pengaturan (hukum) di dalam *cyberspace*. Pertentangan kedua kubu ini menjadi cikal-bakal perdebatan mengenai penerapan yurisdiksi di *cyberspace*. Pertentangan kedua kubu ini menjadi cikal-bakal perdebatan mengenai penerapan yurisdiksi di cyberspace.

2.7.1. Kebebasan Kontra Pengaturan

Kemuculan 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 aktifitas yang terjadi di *cyberspace* yag melibatkan individu-individu yang biasa di sebut *Netizen*[155] pun semakin meningkat, baik itu aktifitas yang bersifat positif maupun aktifitas yang bersifat negatif

Berangkat dari fenomena ini, maka sejumlah kalangan menganggap perlu segera diadakannya pengaturan terhadap *cyberspace* beserta aktifitas-aktifitas yang terjadi disana. Dasar pemikirannya adalah hukum, sebagaimana kodratnya diperlukan

[155] Vivek Sood, *Cyber Law Simplified*, (New Delhi: Tata McGraw-Hill Publishing Co.Ltd, 2001), hal 38, kata netizen ini berasal dari gabungan antara kata internet dan citizen.

di *cyberspace* agar aktifitas-aktifitas yang terjadi diatasnya dapat teratur dan terkontrol[156], sehingga tidak terjadi *radikalisme* di *cyberspace*. Kekhawatiran tersebut memang cukup beralasan mengingat akan konsep kebebasan (free access) yang berlaku di *cyberspace*.[157]

Ide yang diuraikan diatas secara tegas ditentang oleh kalangan, umumya adalah aktivis *cyberspace* yang menjunjung tinggi konsep kebebasan di internet (*cyberspace*).[158] Mereka bahkan memandang *cyberspace* sebagai sesuatu yang berada di luar jangkauan negara, maka dari itu negara tidak dapat memberlakukan hukum di *cyberspace*.[159] Konsep kebebasan di *cyberspace* memungkinkan penggunanya dapat mengakses, menyimpan andakan, mengirim informasi atau aktifitas lainnya secara bebas di internet.[160] Pandangan ini berlawanan dengan pendapat sebelumnya yang menganggap *cyberspace* "hanyalah[161]" media biasa yang digunakan oleh manusia untuk berkomunikasi, berinteraksi dan berbisinis.[162]

2.7.2. Kondisi Empiris

Walaupun tidak ada kesepakatan yang secara jelas mengakhiri perseteruan antara dua pendapat diatas, namun kondidi empiris yang ada sekarang setidaknya telah menggambarkan kearah mana masyarakat hukum internasional berpihak. Sebagian besar cenderung menyetujui gagasan yang mengehendaki adanya pengaturan atau penerapan hukum terhadap *cyberspace* beserta aktifitas-aktifitas 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 atisipasi

---

[156] UNESCO,*Op.cit*, hal 19.
[157] Juliet M, Oberding and Treje Norderhaug, *"A Separate Jurisdiction for Cyberspace"*, <www.cyberjurisdiction.net> , diakses pada 16 Mei 2012.
[158] Vivek Sood, *op.cit*, hal 275.
[159][159] UNESCO, *op.cit*, hal 219/
[160] Vivek Sood, *op.cit*, hal 276.
[161] Maksud dari pendapat ini adalah *cyberspace* dianggap sama dengan media penyampai informasi umum, seperti media cetak.
[162] *Ibid.*

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).[163]

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 sejumlah ketentuan yang dikeluarkan beberapa organisiasi internasional seperti PBB, Council of Europe, dan OECD (Organization for Economic Co-Operation Development).

2.8. Perdebatan Mengenai 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

[163] Wisnubroto,*op.cit.* , hal 26.
[164] *Ibid.*

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 selajutnya disebut dengan *cyber-libertarian*).[165]

Ditengah perdebatan yang alot mengenai hal ini, David R. Johnson mencoba menawarkan empat model yang patut dipertimbangkan sebagai solusi, keempat model tersebut antara lain:[166]

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

Salah satu tawaran dari Johnson yang cukup menarik adalah ide pembentukan organisasi 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*[167]. 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

[165] Murray, *op cit*
[166] David R. Johnson and David G. Post,*op.cit*
[167] UNESCO, *op.cit*, hal 42.

dimaksud antara lain berkaitan dengan dasar kewenangan, jaminan obyektifitas, jaminan perlindungan terhadap golongan minoritas, dan sebagainya.[168]

2.8.1.Aliran *Cyber-Paternalist.*[169]

Konsep ini pada intinya ingin menekankan bahwa sebenarnya *cyberspace* hanyalah merupakan bentuk elektronik dari ruang biasa yang kita kenal selama ini.[170] Dengan kata lain golongan ini berpandangan bahwa *cyberspace* adalah dunia biasa sebagaimana halnya dengan dunia nyata, karena analogi ini maka di *cyberspace* dapat diterapkan aturan atau konsep yurisdiksi yang selama ini berkembang dalam hukum internasional, terutama dalam hal penanganan tindak pidana.

Menurut hukum internasional yang selama ini berlaku, suatu negara memiliki batasan-batasan tertentu dalam hal penerapan yurisdiksi terhadap kasus yang melibatkan kepentingan negara lain.[171] Salah satu batasan yang dimaksud misalnya saja berupa kewajiban setiap negara untuk berhati-hati dan sedapat mungkin menghnidari munculnya gangguan terhadap negara lain dalam upaya penerapan yurisdiksinya. Meskipun begitu, pada prakteknya hukum internasional tidak dapat memaksakan suatu negara untuk menerapkan suatu konsep yurisdiksi tertentu, bahkan dalam konteks ini setiap negara cenderung diberikan kebebasan dalam menentukan konsep mana yang akan digunakan. Kebebasan tentu saja akan diberikan sepajang tidak mengancam ketertiban internasional.[172] Secara umum yurisdiksi dibedakan menjadi tiga jenis, yaitu:[173]

---

[168] *Ibid.*
[169] Murray, *op.cit*, hal 7-9
[170] Rene L. Pattiradjawane, *Op cit*,
[171] Stephen Wilske and Teresa Schiller, *op.cit,*
[172] *Ibid.*
[173] *Ibid.*

1) Yurisdiksi legislatif (*Jurisdiction to prescribe*)

Secara umum yurisdiksi legislatif merupaka kemampuan suatu negara untuk menerapkan hukum nasionalnya terhadap individu dan peristiwa tertentu.[174] Kemampuan ini pada prinsipnya dapat terwujud selama peristiwa yang dimaksud terjadi di wilayahnya atau peristiwa tersebut dilakukan oleh warganegaranya yang berada diluar batas wilayah negara tersebut. Selain itu jenis yurisdksi ini juga dapat dikatakan sebagai titik tolak dalam menetukan penerapan jenis yurisdiksi yang yang lainnya. Artinya untuk menerapkan yurisdiksi yudikatif, maka harus diawali dengan menganalisa yurisdiksi legislatif terlebih dahulu, namun ini tidak perlu dilakukan jika pihak yang bertindak sebagai negara forum berkenan mempergunakan hukum asing. Persyaratan yang sama berlaku juga bila ingin menerapkan yurisdiksi eksekutif.

Dalam menentukan yurisdiksi legislatif , maka terhadap seseorang maupun suatu peristiwa, terdapat 6 (enam) prinsip lain yang dapat dijadikan acuan. Prinsip-prinsip tersebut antara lain :[175]

1. *Subjective territoriality* (territorial subjektif)
2. *Objective territoriality* (territorial objektif)
3. *Nationality* (nasionalitas aktif)
4. *Passive Nationality* (nasionalitas pasif)
5. *Protective Principle* (prinsip perlindungan)
6. *Universality* (universalitas)

2) Yurisdiksi yudikatif (*Jurisdiction to adjudicate*)

Yurisdiksi yudikatif merupakan kewenangan suatu negara untuk melakukan proses peradilan terhadap individu atau peristiwa yang mempunyai hubungan yang cukup dengan negara tersebut.[176] Sebagaimana yang disebutkan sebelumnya, penerapan yurisdiksi yudikatif hampir selalu dengan penerapan yurisdiksi legislatif.

[174] *Ibid.*
[175] *Ibid.*
[176] *Ibid.*

Hal ini sangat masuk akal mengingat hampir tidak ada pengadilan yang rela memakai hukum pidana negara lain.[177] Dalam kasus kejahatan internasional, penerapan yurisdiksi yudikatif secara normative sangat bergantung pada dimana pelaku kejahatan tersebut berada.

3) Yurisdiksi eksekutif (*Jurisdiction to enforce*)

Yurisdiksi eksekutif mempunyai makna sebagai kewenangan negara untuk meningkatkan kepatuhan terhadap hukum dan kewenangan negara untuk menjatuhkan hukuman bagi yang melanggar hukum. Jenis yurisdiksi ini memiliki kaitan erat dengan yurisdiksi legislatif, maksudnya suatu negara tidak dapat menegakkan hukum nasionalnya begitu saja kecuali negara tesebut memiliki yurisdiksi legislatif atas seseorang atau suatu peristiwa.

Yurisdiksi legislatif terkadang juga menjadi dasar pembenar bagi suatu negara untuk mengambil langkah-langkah yang dianggap perlu dalam rangka penerapan yurisdiksi eksekusinya diwilayah negara lain dengan syarat ada persetujuan dari negara tersebut. Persetujuan yang dimaksud disini adalah persetujuan yang diberuikan oleh pejabat resmi dari negara yang bersangkutan dan langkah-langkah yang dapat diambil antara lain : penahanan, pengiriman surat, pelayanan dokumen, dan penyelidikan.[178]

Sehubungan dengan belum adanya titik temu antara dua kubu yang saling berseteru mengenai konsep yurisdiksi yang akan digunakan terhadap *cyberspace*, khususnya mengenai *cybercrime*. Maka dengan kondisi tersebut, praktis konsep tradisional seperti yang disebutkan diatas yang selama ini berlaku dalam menentukan yurisdiksi terhadap kasus-kasus kejahatan komputer yang bernuansa internasional. Setidaknya konsep yang tercantum dalam peraturan nasional khusus tentang kejahatan komputer di beberapa negara, yang merupakan dasar hukum yang selama ini digunakan sebelum adanya ketentuan yang bersifat internasional.

[177] *Ibid.*
[178] *Ibid.*

2.8.2. Aliran *Cyber-Libertarian*.[179]

Konsep ini diperjuangkan oleh kubu yang sebagian besar terdiri dari para akitvis *cyberspace* atau sekumpulan orang yang sehari-harinya memiliki kegiatan yang tidak lepas dari komputer (internet), beberapa diantaranya adalah *hacker*. Dengan melihat komposisi golongan yang mendukung konsep ini, maka dapat dimaklumi kiranya jika mereka secara terang-terangan menolak segala upaya untuk menyamaratakan *cyberspace* dengan dunia biasa atau dengan kata lain mereka merasa dunia mereka terusik dengan keberadaan konsep analogi.

Pemikiran yang menjiwai konsep ini pada dasarnya berangkat dari beberapa teori yang mereka yakini sebagai kekhasan dari *cyberspace* itu sendiri, seperti :[180]

a. Bahwa *cyberspace* adalah media yang terletak tidak di suatu lokasi tertentu.
b. Aktifitas di *cyberspace* tidak ada kaitannya suatu lokasi.
c. *Cyberspace* merupakan sesuatu yang jelas berbeda dengan dunia nyata.

Berangkat dari butir-butir diatas kalangan yang menawarkan konsep pemisahan berpendapat bahwa tidak satu pun organisasi atau negara yang pantas mengatur aktifitas di *cyberspace*. Lebih jauh lagi mereka berpandangan bahwa yang berhak mengatur *cyberspace* hanyalah pengguna *cyberspace* itu sendiri.[181] Argumen tersebut muncul berdasarkan dua asumsi sebagai berikut:[182]

1. Menurut mereka keberadaan *cyberspace* tidak secara serta-merta menyakiti seseorang di wilayah tertentu.
2. Segala upaya untuk mengontrol aktifitas *cyberspace* akan menjadi sia-sia, karena dengan mudah aktifitas tersebut akan berpindah-pindah dari suatu wilayah ke wilayah yang lain.

Pandangan ini mendapat kritikan dari beberapa kalangan, misalnya yang dikemukakan oleh Lawrence Lessig. Beliau berpendapat bahwa alasan-alasan yang

[179] Murray, *op cit*, hal 5-7
[180] Dan L. Burk, *op.cit*
[181] *Ibid.*
[182] *Ibid.*

dikemukakan oleh penganut konsep pemisahan lebih merupakan alasan dari prespektif normatif serta emosional belaka, bukanlah suatu alasan yag bersifat analitis.[183] Contohnya pandangan mereka yang menganggap bahwa *cyberspace* beserta aktifitasnya harus dipisahkan dari dunia nyata.

Jika pandangan ini diasumsikan benar maka orang yang berhubungan di *cyberspace* adalah bukan orang sungguhan, bahkan benda pun adalah benda fiktif. Hal ini jelas seuatu yag masuk akal menurut Lessig karena menurut beliau orang adalah tetap orang baik sebelum atau sesudah ia menjauh dari komputer.[184] Secara eksterem Lessig selanjutnya menyatakan bahwa *cyberspace* bukanlah suatu "wilayah aman diluar bumi" (*extra terrestrial safety zone*), para penjahat komputer tidaklah aman dari tuntutan pengadilan.[185]

Kritikan lain datang dari Misaki Hamano yang menyatakan bahwa ide pemisahan *cyberspace* dengan dunia nyata dan ide *self-governance* terhadap *cyberspace*, bukan sesuatu yang realistis saat ini. Karena sekalipun kejahatan di *cyberspace* terus menigkat, namun negara-negara cenderung memilih menggunakan konsep lama dibandingkan membuat ketentuan yang baru. Selanjutnya Masaki menambahkan bahwa memang benar jika dikatakan bahwa ada keterbatasan negara untuk mengatasi problem yurisdiksi di *cyberspace*, akan tetapi bukan berarti pengguna *cyberspace* bebas dari hukum di dunia nyata.[186]

Salah satu gagasan yang ditawarkan oleh kubu ini adalah dengan menempatkan *cyberspace* sebagai **The 4th International Space** disamping zona Antartika, ruang angkasa (*outer space*), dan zona laut.[187] Degan menempatkan *cyberspace* setara dengan zona-zona khusus lainnya, maka bagi *cyberspace* perlu juga diadakan pengaturan khusus yang didalamnya termasuk juga konsep yurisdiksi khusus yang berlaku di khusus yang berlaku di *cyberspace*. Berkaitan dengan

[183] Barda Nawawi Arief, *op,cit*, hal 12.
[184] *Ibid.*
[185] *Ibid.*
[186] Masaki Hamano,*op.cit.*
[187] UNESCO, *op.cit*, hal 38.

gagasan ini UNESCO dalam terbitannya yang berjudul "The International Dimensions of Cyberspace Law" berpendapat bahwa *cyberspace* dapat mengambil pengalaman yang berharga dari praktek pengaturan di ruang angkasa (outer space), dimana banyak kalangan yang menganggap bahwa pengaturan di ruang angkasa terbilang berhasil, khususnya dalam hal menertibkan upaya pengeksplorasian di zona tersebut.[188] Selain dua aliran diatas menurut Viktor Mayer-Schönberger terdapat tiga pendapat mengenai bentuk pengaturan mengenai siapa yang berhak meregulasi Internet.[189]

1. Pendapat pertama dikenal dengan teori *The State-Based Traditionalist Discourse* mengatakan sebaiknya pihak yang mengatur Internet adalah pemerintah melalui peraturan perundang-undangan. Berdasarkan pendapat ini bentuk pengaturan Internet akan diatur oleh masing-masing negara. Kelebihan teori ini adalah penegakan hukum terhadap pengaturan Internet lebih terjamin. Sementara itu, kelemahan dari pengaturan ini adalah dilupakannya dasar dari Internet yaitu sifat global. Tidak mungkin suatu negara dapat memaksakan peraturan negaranya bagi warga negara lain yang menggunakan fasilitas Internet di negaranya.

2. Pendapat kedua mengatakan, Internet sebaiknya diatur oleh masing-masing pihak berdasarkan kebiasaan atau dikenal dengan istilah *The Cyber-Separatist Discourse*. Pendapat ini memisahkan antara kehidupan sosial di dunia nyata dengan kehidupan di dalam *cyberspace*. Berdasarkan pendapat ini sebaiknya pengaturan mengenai Internet tidak usah dilakukan oleh negara, karena tidak akan ada peraturan yang cocok untuk mengatur kemajemukan di Internet. Karena pengaturan Internet menggunakan kebiasaan, para pengguna Internet akan merasa lebih dapat menerima peraturan yang ada. Akan tetapi, kelemahan dari pendapat ini adalah tidak adanya penegakan hukum seandainya terjadi sengket antara para pihak.

[188] *Ibid.*, hal 143.
[189] Viktor Mayer-Schönberger, *Op.cit,* hal 607

3. Pendapat ketiga yaitu aliran *The Cyber-Internationalist Discourse*, mengatakan pengaturan Internet sebaiknya melalui ketentuan internasional. Jadi, ada suatu ketentuan hukum berlaku secara internasional yang mengatur mengenai Internet. Pendapat ini mengarahkan pandangannya kepada usaha untuk mengunifikasikan peraturan Internet. Kelemahan dari aliran ini adalah, tidak semua negara mau mengakui pengaturan mengenai Internet yang berlaku tersebut, karena tiap negara memiliki karakterisitik tersendiri.

2.9. Yurisdiksi Berdasarkan Hukum Internasional

Begitu banyak pendapat-pendapat tentang yurisdiksi yang berkembang dan dilontarkan oleh berbagai ahli, namun sedikit sekali yang akhirnya diterima oleh hukum internasional sebagai prinsip. Prinsip-prinsip tersebut adalah :

2.9.1. *Subjective Territoriality* (territorialitas subjektif)

Subjective territoriality adalah prinsip yang terpenting di dalam hukum internasional.[190] Menurut prinsip ini, keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. Mayoritas negara-negara di dunia, mengadopsi prinsip ini ke dalam perundang-undangan pidananya.[191]

Namun demikian J.G Starke, sebenarnya asas ini bukan merupakan asas umum hukum internasional, tetapi penggunaannya yang khusus sudah menjadi bagian hukum internasional, sebagai akibat dari dua konvensi yang penting yaitu *Geneva Convention for Supression of Counterfeiting Currency* (1929) dan *Geneva Convention of the Illicit Drug Traffic* (1930).[192]

[190] Derrel Menthe, *op.cit,* hal 1
[191] *Ibid.*
[192] J.G Starke, *op.cit*

2.9.2. *Objective Territoriality* (territorialitas objektif)

Objective Territoriality digunakan pada saat suatu tindakan dilakukan oleh pelaku yang berada di luar wilayah suatu negara, akan tetapi justru akibat paling serius yang timbul karena peristiwa itu berada di dalam wilayah negara yang dimaksud.[193] Asas ini dirumuskan oleh Prof. Hyde, sebagaimana dikutip oleh J.G Starke[194], sebagai berikut :

> *"The setting motion outside of a state of a force which produces as a direct consequence an injurious effect therein justifies a territorial sovereign in prosecuting the actor when he enter its domain*."

Sebagai contoh, misalnya orang yang sedang berada di perbatasan suatu negara kemudian menembak seseorang yang berada di wilayan negara lain.

2.9.3. *Active Nationality* (nasionalitas aktif)

Nationality adalah prinsip yang didasarkan kepada status kewarganegaraan seseorang.[195]Prinsip ini oleh Starke disebut juga prinsip nasionalitas aktif[196], yaitu negara tidak wajib menyerahkan warganegaranya yang melakukan pelanggaran di luar negeri. Artinya, negara dianggap lebih berwenang mengadili daripada negara lain tempat terjadinya kejahatan.

Sebagai ilustrasi, apabila seorang WNI berada di luar negeri, kemudian melakukan hubungan denga negara asing dan kemudian meggerakkan kekuatan asing agar melakukan peyerangan kepada Indonesia, maka berdasarkan pasal 111 ayat (1) KUHP, orang tersebut dapat diadili atau dituntut di pengadilan Indonesia.

---

[193] Darrel Menthe, *op.cit*, nomor 8,hal 2
[194] J.G Starke ,*op.cit*, hal 187.
[195] Darrell Menthe,*op.cit*, nomor 9, hal 2
[196] J.G Starke,*op.cit*, hal 211.

2.9.4. *Passive Nationality* (nasionalitas pasif)

Prinsip ini sedikit berbeda dengan prinsip *nationality*. Jika prinsip *nationality* melihat status kewarganegaraan pelaku kejahatan sebagai dasar kewenangan melakukan penuntutan, maka prinsip *Passive Nationality* melihat status kewarganegaraan korban.[197]

Pembenaran terhadap prinsip ini adalah bahwa setiap negara berhak melindungi warganegaranya di luar negeri, dan apabila negara territorial tempat pelanggaran itu terjadi tidak menghukum orang yang menimbulkan kerugian itu, maka negara dari korban itu berweang menghukum pelanggar tersebut jika pelaku memasuki wilayahnya.[198] Keberatan terhadap prinsip ini adalah bahwa kepentingan umum negara tidak serta merta terganggu hanya karena salah seorang warganegaranya telah dirugikan.[199]

Prinsip nasionalitas pasif ini antara lain termuat dalam undang-undang pidana Mexico, Brazil, Itali dan Indonesia. Sedangkan Inggris dan Amerika Serikat tidak mengadopsi prinsip ini ke dalam undang-undang pidananya.[200]

2.9.5. *Protective Principle* (prinsip perlindungan)

Hukum Internasional mengakui bahwa setiap negara berwenang menangai kejahatan yang berkaitan dengan keamanan dan integritas, serta kepentingan ekonomi yang cukup vital.[201]*Protective Principle* inilah yang digunakan sebagai dasar memanifestasikan kewenangan tersebut. Prinsip ini biasanya diterapkan gua melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya, terutama apabila korban adalah negara atau pemerintah.[202]

---

[197] Darrel Menthe,*op.cit*, nomor 10, hal 2
[198] J.G Starke,*op.cit*, hal 211.
[199] *Ibid.*
[200] *Ibid.*
[201] *Ibid.*
[202] Darrel Menthe,*op.cit*, Nomor 11.

Ada dua alasan yang mendasari prinsip ini, yaitu, *pertama*, akibat kejahatan sangat besar bagi negara yang dirugikan . *Kedua*, jika kewenangan tidak diterapkan oleh negara yang dirugikan, maka pelaku kejahatan bisa lolos karena di negara tempat perbuatan dilakukan, perbuatan yang dimaksud belum tentu merupakan tindak pidana serta ekstradisi juga ditolak karena alasan-alasan politis.[203]Kelemahan terbesar yang menimbulkan penolakan terhadap *protective principle* ini, yaitu negara (korban) itu sendiri yang menentukan perbuatan mana yang membahayakan keamanan, sehingga dapat menimbulkan kesewenang-wenangan

2.9.6. *Universality* (universalitas)

Asas ini seringkali juga dusebut sebagai asas "*universal interest jurisdiction*".[204] Dahulu asas ini digunakan sebagai dasar kewenangan untuk menangkap dan menghukum para pelaku bajak laut dan kejahatan perang akan tetapi kemudian asas ini telah diperluas sehingga termasuk pula penyiksaan, genosida, dan pembajakan pesawat udara.[205]

Asas *universal interest jurisdiction* ini selayaknya memperoleh perjatian khusus guna penanganan dan penegakkan hukum kasus-kasus *cybercrime*.[206]Hal ini disebabkan karena asas ini memandang kewenangan untuk menangani kejahatan lebih kepada perlindungan terhadap kepentingan-kepentingan tertentu dari negara-negara yang ada di dunia, tanpa perlu mempersoalkan *locus delicti* dan kewarganegaraan pelaku.[207]

---

[203] J.G Starke,*op.cit*, hal 212.
[204] Ahmad M.Ramli, *Cyberlaw dan HaKI Dalam Sistem Hukum Indonesia*, cet-1 (Bandung: PT Refika Aditama, 2004), hal 20
[205] Menthe,*op.cit*, nomor 12
[206] M. Ramli,*loc.cit*
[207] E.Y Kanter dan S.R Sianturi, *Asas-asas Hukum Pidana Di Indonesia Dan Penerapannya*, Cet.2 (Jakarta: Storia Grafika, 2002), hal 111

2.10. Teori Yurisdiksi Menurut Doktrin

Yurisdiksi dalah salah satu masalah serius yang dihadapi oleh penegak hukum jika berhadapan dengan kasus *cybercrime* yang melibatkan warganegara asing, karena banyaknya kepentingan yang bermain disana, tidak hanya kepentingan negara sendiri, namun juga kepentingan negara lain terhadap warganegaranya sendiri. Sudah banyak ahli yang mencoba memberikan solusi atas penentuan yurisdiksi di *cyberspace* salah satunya adalah Juliet M. Oberding, seorang *lawyer* asal Amerika Serikat yang menyatakan bahwa yurisdiksi di *cyberspace* harus berbeda dengan yurisdiksi pada umumnya karena itu beliau menyarankan jika hukum yang mengatur di *cyberspace* termasuk yurisdiksi haruslah:[208]

1. Diatur dan ditegakkan oleh komunitas yang berada di *cyberspace* (*cybercommunity*);
2. Hukum di *cyberspace* tidak bisa diaplikasikan ke dunia nyata (*Real Life)* dan sebaliknya;
3. Hukum di *Real Life* harus bekerja dua kali karena harus membuat aturan baru untuk mengontrol *cyberspace*

Salah satu usul yang menarik untuk penentuan yurisdiksi dalam kasus *cybercrime* datang dari Susan W Brenner dalam buku *IT Law Series Vol 11 Cybercrime and Jurisdiction*, beliau mengatakan bahwa untuk memjawab permasalahan utama dalam kasus cybercrime yang bersifat *cross-border* ada 7 (tujuh) komponen yang bisa digunakan oleh negara untuk mengklaim yurisdiksi atas sebuah kasus *cybercrime*. Ketujuh komponen tersebut adalah :[209]

---

[208] Juliet M. Oberding, *op.cit*

[209] Susan W Brenner ,*Chapter 17, The Next Step :Prioritizing Jurisdiction*,IT Law Series Vol 11 :*Cybercrime and Jurisdiction*, 2006, Leiden, Asser Press, Hal 330-346

2.10.1. Tempat Kejahatan Dilakukan

Menurut Brenner ini merupakan faktor utama dilakukan suatu negara untuk mengklaim bahwa negara tersebut memiliki yurisdiksi atas suatu kasus, namun hal ini biasanya dilakukan dengan menerapkan asas territorialitas dengan faktor-faktor seperti:[210]

a. Lokasi tempat dilakukannya kejahatan;
b. Lokasi dimana alat berada;
c. Lokasi dimana pelaku berada;
d. Lokasi dimana akibat berada;
e. Lokasi dimana ada hal-hal yang berhubungan dengan kejahatan tersebut.

Namun dalam kasus *cybercrime* hal ini dapat menimbulkan kebingungan jika ada dua negara atau lebih yang mengklaim yurisdiksi atas suatu kasus karena pelaku *cybercrime* dapat melakukan kejahatannya berulang-ulang dengan menggunakan berbagai IP dari seluruh dunia

2.10.2. Tempat Dimana Pelaku Ditangkap

Komponen yang berikut ini dapat digunakan dengan menerapkan asas universalitas yang merupakan salah satu asas dalam hukum internasional bahwa setiap negara berhak mengadili setiap orang dalam hal yang bersangkutan melakukan apa yang di sebut sebagai kejahatan internasional, namun hal ini agak sulit di lakukan mengingat sebagian besar negara belum memiliki peraturan perundangan yang memadai untuk mengadili pelaku *cybercrime*

[210] *Ibid*, Hal 5

2.10.3. Akibat

Komponen ini agaknya lebih bisa diterima karena melihat sebuah kasus *cybercrime* dari akibat yang ditimbulkan, maka apabila terjadi serangan virus misalnya yang menyerang beberapa negara maka, negara yang di rugikan dapat mengklaim yurisdiksi atas kasus tersebut, namun yang menjadi polemic disini adalah ukuran dari sebuah kerugian apakah dapat dinilai dari materi (uang) atau tidak.

2.10.4. Nasionalitas (kewarganegaraan)

Untuk komponen yang berikut ini dapat dibagi menjadi dua bagian, yaitu kewarganegaraan korban dan kewarganegaraan pelaku

a) Kewarganegaraan Korban

Kewarganegaraan korban dapat di gunakan untuk mengklaim yurisdiksi atas suatu kasus, namun dalam hal *cybercrime* yang harus dipertanyakan apakah kewarganegaraan tersebut adalah kewarganegaraan asli si korban atau kewarganegaraan berdasarkan IP yang digunakan pada saat *online*.

b) Kewarganegaraan Pelaku

Komponen yang satu ini memang dapat digunakan, hanya saja negara asal pelaku harus menjamin kepada negara korban bahwa mereka akan mengadili pelaku dengan seadil-adiilnya karena merasa “bertanggung jawab” atas kejahatan yang di lakukan oleh wargangaranya.

2.10.5. Kekuatan Dari Kasus Tersebut

Komponen ini harus diajukan oleh Jaksa Penuntut Umum dalam dokumen yang menyatakan bahwa mereka mempunyai kasus yang cukup kuat (dalam hal bukti,saksi, dll) untuk mengadili pelaku di negaranya.

2.10.6. Pemidanaan

Lamanya pemidanaan juga dapat di jadikan salah satu komponen untuk menentukan yurisdiksi dalam kasus *cybercrime*. Misalnya apabila hukuman untuk *hacking* di negara A adalah 5 tahun penjara dan di negara B adalah 3 tahun penjara, maka negara A yang dapat mengklaim yurisdiksi atas kasus tersebut, namun jangan sampai lamanya pemidanaan justru menjadi hukuman yang berlebihan bagi pelaku

2.10.7. Keadilan dan Kenyamanan

Yang dimaksud dengan keadilan disini adalah negara yang berhak mengklaim yurisdiksi atas suatu kasus *cybercrime* adalah negara yang dianggap memiliki sistem peradilan yang adil dan tidak memihak (imparsial) dan juga paling nyaman bagi saksi untuk hadir dalam persidangan (minimal melalui *video conference*).

2.11. Yurisdiksi Negara Dalam Menangani Kasus Cybercrime

Masalah yurisdiksi merupakan masalah yang pelik dan seringkali menimbulkan konfilik kepentingan antar dua negara. Untuk membantu pembaca memhami lebih dalam mengenai yurisdiksi, maka pembahasan akan dibagi menjadi dua bagian yaitu :

1. Yurisdiksi menurut Convention on Cybercrime
2. Kerjasama Internasional Dalam Mengatasi Konflik Yurisdiksi

2.11.1. Yurisdiksi Menurut Convention on Cybercrime

Permasalahan yurisdiksi dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa, secara khusus ditempatkan pada pasal tersendiri yakini pada pasal 22. Pasal yang terdiri dari lima ayat tersebut antara lain berbunyi sebagai berikut[211] :

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

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with 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 the territorial jurisdiction of any State.*
2. *Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.*
3. *Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her 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 established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*[212]

[212] 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. Diatas kapal berbendera negara tersebut,
    c. Diatas pesawat yang terdaftar menurut hukum negara tersebut,
    d. 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 kewarganegarannya.

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 kritreria 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 (*offences related to infringements of copyright and related rights*),
10) Segala bentuk percobaan, pembantuan, dan persekongkolan yang berkaitan dengan kejahatan-kejahatan tersebut diatas.[213]

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. Sebagai

---

4. Keberadaan konvensi ini tidak mengenyampingkan penerapan yurisdiksi kriminal berdasarkan hukum nasional suatu negara.
5. Apabila lebih dari satu pihak mengkalim yurisdiksi atas suatu kejahatan yang terdapat dalam konvensi ini, maka para pihak yang terlibat sebaiknya mengadakan konsultasi dalam menentukan yurisdiksi yang tepat.

[213] "Expalantory Report of Convention on Cybercrime", Adopted November 2001. <www.coe.net>, diakses pada tanggal 4 April 2012.

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.[214] 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 ayai (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.[215]

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 terdafatar 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 diluar yurisdiksi negara yang dimaksud.[216] Pasal Ayat (1) butir (d) berisi prinsip nasionalitas yang banyak oleh negara-negara penganut sistem *civil law*. Prinsip ini

[214] *Ibid.*
[215] *Ibid.*
[216] *Ibid.*

memungkinkan seorang warganegara diproses menurut hukum negaranya atas suatu perbuatan yang dilakukan diluar wilayah yurisdiksi negara yang bersangkutan.[217]

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 *aut dedere aut judicare* (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 kewarganegaraanya 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.[218]

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.[219] 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

[217] *Ibid.*
[218] *Ibid.*
[219] *Ibid.*

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.[220]

Berdasarkan uraian mengenai Pasal 22 beserta penjelasannya diatas, 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 natinya berfungsi menertibkan segala aktivitas di *cyberspace*.[221] 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 :[222]

a) Beberapa Negara mengklaim yurisdiksi terhadap suatu kasus berdasarkan prinsip tempat dimana kejahatan tersebut dilakukan

[220] *Ibid.*
[221] Mark D. Rasch, *loc.cit*
[222] *Convention on Transfer of Proceedings Explanatory Report*, Poin 16

b) Beberapa Negara mengklaim yurisdiksi berdasarkan prinsip yang berbeda-beda (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 di minta untuk berunding dalam menentukan siapa yang lebih berhak mengklaim yurisdiksi. Namun solusi atas hal ini sudah diatur jauh sebelum pembentukan *Convention on Cybercrime*, yakini pada tahun 1972 pada saat pembentukan *European Convention on Transfer of Proceedings*, dalam *explanatory report* konvensi tersebut di sebutkan bahwa Negara yang mengklaim harus membuat sebuah daftar prioritas penentuan yurisdiksi dari prinsip tempat kejahatan dilakukan.[223]

2.11.2. 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 di tempuh negara-negara untuk membawa pelaku *cybercrime* agar dapat diadili di negaranya:

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

2.10.2.1. Ekstradisi dan Deportasi

Ketika pembahasan mengenai penentuan yurisdiksi negara mana yang berwenang untuk melakukan pentuntutan terhadap pelaku kejahatan maka selanjutnya

[223] *Ibid*, poin 18

yang harus dilakukan bagaimana melakukan ekstradisi terhadap pelaku kejahatan tersebut. Indonesia sejak tahun 1979 telaj memiliki Undang Undang No 1 tahun 1979 tentang ekstadisi dan telah menjalin hubungan diplomatik dan membuat perjanjian ekstradisi dengan banyak negara yang kemudian disahkan dalam bentuk Undang-Undang.

Ekstradisi adalah penyerahan oleh suatu negara kepada negara yang meminta penyerahan seseorang yang disangka atau dipidana karena melakukan suatu kejahatan diluar wilayah negara yang menyerahkan dan didalam yurisdiksi wilayah negara yang meminta penyerahan tersebut karena berwenang untuk mengadili dan memidananya.[224] Syarat-syarat permintaan ekstradisi yaitu:[225]

1.Permintaan ekstradisi hanya akan di pertimbangkan apabila memenuhi syarat :

1) Bahwa telah ada perjanjian ekstradisi sebelumnya atau setidak tidaknya didasarkan hubungan baik dan negara RI menghendakinya (pasal 2);
2) Yang dapat di ekstradisi adalah tersangka pelaku kejahatan atau tersangka pelaku perbantuan terhadap kejahatan yang di Indonesia maupun di negara peminta perbantuan tersebut dapat dipidana (Pasal 3);
3) Ekstradisi dapat dilakukan terhadap kejahatan yang tekah disebutkan dalam UU No 1 Tahun 1979 atau dalam perjanjian ekstadisi Indonesia dengan negara peminta atau terhadap kejahatan lain yang tidak diatur sebelumnya namun berdasarkan kebijaksanaan negara yang diminta dapat di lakukan ekstradisi (Pasal 4).

2.Surat permintaan ekstradisi harus diajukan secara tertulis melalui sluran diplomatik kepada Menteri Hukum dan HAM Republik Indonesia untuk diteruskan kepada Presiden.

[224] UU No 1 Tahun 1979 tentang Ekstadisi, Pasal 1
[225] *Ibid*, Pasal 22 dan 23

3.Surat Permintaan ekstradisi bagi orang yang dimintakan ekstrdisinya untuk menjalani pidana harus disertai:

1) Lembaran asli atau salina otentik dari putusan pengadilan yang berupa pemidanaan yang sudah mempunyai kekuatan hukum tetap.
2) Keterangan yang diperlukan untuk menetapkan identitas dan kewarganegaraan orang yang dimintakan ekstardisinya.
3) Lembaran asli atau salinan otentik dari surat perintah penahanan yang dikeluarkan oleh pejabat yang berwenang dari negara tersebut.

Syarat permintaan ekstradisi bagi orang yang disangka melakukan kejahatan harus disertai:

1) Lembaran asli atau salinan otentik dari surat perintah penahanan yang dikeluarkan oleh pejabat yang berwenang dari negara penerima.
2) Uraian dari kejahatan yang dimintakan ekstradisi, dengan menyebutkan waktu dan tempat kejahatan dilakukan dengan di sertai bukti tertulis yang diperlukan.
3) Teks ketentuan hukum dari negara peminta yang dilanggar atau hal demikian tidak mungkin, isi dari hukum yang diterapkan.
4) Keterangan-keternangan saksi di bawah sumpah mengenai pengetahuannya tentang kejahatan yang dilakukan.
5) Keterangan yang diperlukan untuk menentukan identitas dan kewarganegaraan orang yang dimintakan ekstradisinya.
6) Permohonan penyitaan barang-barang bukti, bila ada dan diperlukan

Apabila Menteri Hukum dan HAM memandang bahwa surat yang dikrimkan tersebut kurang memenuhi syarat pasal 22 dan 23 maka pejabat yang berwenang dari negara peminta diberikan waktu untuk melengkapinya dan setelah Menteri Hukum dan HAM RI memandang bahwa persyaratannya telah lengkap mala surat permintaan

ekstradisi dan kelengkapannya di serahkan ke Kepala Kepolisian RI dan Jaksa Agung RI untuk dilakukan pemeriksaan.

Pemeriksaan terhadap orang yang dimintakan ekstradisi di Indonesia melalui prosedural sebagai berikut:[226]

1) Apabila orang yang hendak di ekstradisi ditahan karena adanya oermintaan dari negara peminta maka tersangka langsung dilakukan pemeriksaan terhadap tersangka atas dasar keterangan dan bukti dari negara peminta, hasil pemeriksaan dibuat dalam Berita Acara (BA) dan segera diserahkan kepada Kejakasaan RI setempat dan selambat-lambatnya 7 hari setelah menerima BA tersebut, kejaksaan dengan mengemukakakn alasannya secara tertulis, menerima Pengadilan Negeri setempat (tempat ditahannya tersangka) untuk memeriksa dan menetapkan bisa atau tidak tersangak tersebut di ekstradisi, dan siding pengadilan dilakukan terbuka kecuali Ketua Sidang menganggap perlu siding tertup, dalam siding tersebut pengadilan memeriksa:
    a. Identitas dan kewarganegaraan tersangka;
    b. Memeriksa kejahatan yang dipersangkakan apakah termasuk dalam kategori kejahatan yang pelakunya dapat diekstradisikan;
    c. Apakah hak penuntutan atau hak melakasanakan putusan pengadilan sudah atau belum kadaluarsa;
    d. Apakah terhadap kejahatan yang dilakukan tersangka telat atau belum dijatuhi putusan pengadilan yang mempunyai kekuatan hukum tetap;
    e. Apakah kejahatan yang diancamkan terhadap tersangka diancam dengan pidana mati atau tidak, karena Indonesia dapat menolak melakukan ekstradisi apabila ancaman hukuman terhadap kejahatan yang dilakukan adalah hukuman mati.
    f. Apakah tersangka sedang diperiksa di Indonesia untuk kejahatan yang sama.

[226] *Ibid*, Pasal 25

2) Selanjutnya berdasarkan hasil pemeriksaan tersebut pengadilan menetapkan apakah yang bersangkutan dapat atau tidak di ekstradisi dan hasil penetapan tersebut di serahkan ke Menteri Hukum dan HAM untuk di serahkan ke Presiden dengan pertimbangan-pertimbangan Menteri Hukum dan HAM, Menteri Luar Negeri, Jaksa Agung RI dan Kepala Kepolisian RI, selanjutnya berdasarkan seluruh pertimbangan di atas Presiden memutuskan dapat atau tidak orang tersebut di ekstradisi.

3) Apabila permintaan ekstradisi berasal dari negara yang sebelumnya tidak memiliki perjanjian ekstradisi dengan Indonesia, maka permintaan ekstradisi diajukan melalui saluran diplomatik, selanjutnya Menteri Luar Negeri menyampaikan permohonan ekstradisi tersebut beserta pertimbangannya kepada Menteri Hukum dan HAM, selanjutnya Menteri Hukum dan HAM melaporkan kepada Presiden dan Presiden memerintahkan kepada Menteri Hukum dan HAM untuk melakukan proses pemeriksaan sebagaimana lazimnya, hasil pemeriksaan dan putusan pengadilan negeri, pertimbangan Menteri Hukum dan HAM dan Menteri Luar Negeri memutuskan dapat atau tidaknya tersangka di ekstradisi, apabila Presiden tidak menyetujui permintaan ekstradisi maka Menteri Hukum dan HAM diminta Presiden untuk memberitahukan kepada Menteri Luar Negeri agar memberitahukan penolakan tersebut ke negara peminta.
4) Apabila dalam waktu bersamaan ada 2 (dua) negara yang meminta ekstradisi terhadap seseorang berkenaan dengan kejahatan yang sama atau berbeda, maka Presiden dapat menolak atau mengabulkan permintaan ekstradisi tersebut dengan mempertimbangkan:

a) Berat ringannya kejahatan;
b) Tempat dilakukannya kejahatan;
c) Waktu mengajukan permintaan ekstradisi
d) Kewarganegaraan orang yang diminta; dan

e) Kemungkinan di ekstradisikan orang yang diminta oleh negara peminta keapa negara lain.

5) Apabila seseorang di sangka melakukan kejahatan atau harus menjalani pidana karena melakukan kejahatan yang dapat diekstradisikan ke dalam yurisdiksi negara Republik Indonesia, dimana tersengka diduga berada di negara asing maka atas pemintaan Jaksa Agung Republik Indonesia, atau Kepala Kepolisian Republik Indonesia, Menteri Hukum dan HAM Republik Indonesia, atas nama Presiden dapat meminta ekstradisi melalui saluran diplomatik dan apabila orang tersebut telah diekstradisikan maka tersangka dapat segera dibawa ke Indonesia dan diserahkan kepada instansi yang berweanang.

Pasal 24 *Cybercrime Convention* juga mengatur tentang pelaksanaan ekstradisi sebagai berikut :[227]

[227] *Cybercrime Convention*, Pasal 24 yang berbunyi:

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

1. a) Artikel ini berlaku untuk ekstradisi antar negara untuk tidak piudana yang ditetapkan sesuai dengan pasal 2sampai dengan 11 konvensi ini untuk tindak pidana, asalkan mereka dapat dihukum menurut hukum kedua belah pihak untuk jangka waktu maksimum minimal satu tahun, atau dengan hukuman yang lebih berat.

   b) Apabila hukuman minimum berbeda sebagaimana yang ditetapkan perjanjian yang disapakati berdasarkan Undang-Undang yang sama atau perjanjian timbale balik atau perjanjian ekstradisi, termasuk Konvensi Eropa tentang Ekstradisi (ETS NO 24), yang berlaku antara dua atau lebih negara, hukuman minimal yang diterapkan adalah pengaturan tersebut atau perjanjian yang berlaku.

2. Tindak pidana yang diuraikan dalam ayat 1 pasal ini dianggap sebagai kejahatan yang dapat diekstradisi dalam setiap perjanjian ekstradisi yang ada antara para pihak. Para pihak harus memasukkan tindak pidana tersebut

---

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

sebagai tindak pidana yang dapat diekstradisi dalam setiap perjanjian ekstradisi yang di sepakati antara mereka.

3. Jika negara yang membuat ekstradisi bersyarat pada adanya suatu perjanjian menrima permintaan ekstradisi dari pihak lain yang tidak memiliki perjanjian ekstradisi, ia dapat mempertimbangkan konvensi ini sebagai dasar hukum bagi ekstradisi sehubungan dengan tindak pidana sebagaimana yang dimaksud dalam ayat 1 pasal ini.

4. Pihak yang tidak membuat ekstradisi bersyarat pada saat adanya suatu perjanjian harus mengakui tindak pidana sebagaimana dimaksud dalam ayat 1 pasal ini.

5. Ekstradisi harus tunduk pada persyaratan yang di sediakan oleh hukum pihak yang diminta atau dengan perjanjian ekstradisi yang berlaku, termasuk alasan yang partial diminta dapat menolak ekstradisi.

6. Jika ekstradisi tindak pidana sebagaimana yang dimaksud dalam ayat 1 pasal ini ditolak sedmata-mata atas dasar kewarganegaraan orang yang dicari, atau karena pihak yang diminta menganggap bahwa ia memiliki yurisdiksi atas pelanggaran yang terjadi, pihak yang diminta wajib mengajukan kasus tersebut atas permintaan negara peminta kepada pihak yang berwenang untuk tujuan penuntutan dan wajib melaporkan hasil akhir kepada pihak peminta pada waktunya. Negara yang berwenang harus mengambil keputusan dan melakukan penyelidikan serta proses dengan cara yang sama seperti untuk setiap pelanggaran lainnya yang sabanding dengan hukum negara tersebut.

7. a) Setiap pihak wajib, pada saat penandatanganan atau ketika menyarahkan instrumen ratifikasi, penerimaan, persetujuan atau aksesi, berkomunikasi dengan Sekeretaris Jenderal Dewan Eropa nama dan alamat setiap otoritas yang bertanggung-jawab untuk membuat atau menerima permintaan ekstradisi atau penangkapan sementara dengan tudak adanya perjanjian.

b) Sekretaris Jenderal Dewan Eropa harus membentuk dan terus memperbaharui daftar otoritas yang ditunjuk oleh para pihak. Setiap pihak wajib memastikan bahwa rincian di daftarkan pada register adalah benar pada setiap saat.

Selain melalui esktradisi sering sekali pemulangan warganegara asing menggunakan mekanisme deportasi. Pengusiran atau deportasi adalah tindakan mengeluarkan orang asing dari wilay Indonesia karena keaberadaannya tidak dikehendaki.[228] Dalam Undang-Undang Keimigrasian dikenal adanya istilah tindakan keimigrasian yaitu tindakan administrative dalam bidang keimigrasian diluar proses pengadilan yang dilakukan terhadap orang asing yang berada di wilayah Indonesia yang melakukan kegiatan berbahaya atau patut diduga akan berbahaya bagi keamanan dan ketertiban umum, tidak mengahormati atau menaati peraturan perundang-undangan yang berlaku.

Adapun yang termasuk tindakan keimigrasian adalah:[229]

1. Pembatasan, perubahan atau pembatalan izin keberadaan;
2. Larangan untuk berada di suatu atau beberapa tempat tertentu di wilayah Indonesia;
3. Keharusan untuk bertempat tinggal di suatu tempat tertentu di wilayah Indonesia;
4. Pengusiran atau deportasi dari wilayah Indonesia atau penolakan masuk ke wilayah Indonesia.

2.11.2.2. *Mutual Legal Assistance*

Bantuan Hukum Timbal Balik atau Biasa juga juga dikenal dengan Bantuan Timbal Balik dalam Masalah Pidana (selanjutnya dapat juga disebut *Mutual Legal Assistance* atau MLA) merupakan satu bentuk kerjasama memerangi kejahatan yang

[228] UU No 9 Tahun 1982 Tentang Keimigrasian, Pasal 1 Butir 16
[229] *Ibid*, Pasal 42

dikenal dari mekanisme hukum yang timbul dalam pergaulan masyaratak internasional. Perserikatan Bangsa-Bangsa (PBB) melalui lembaganya yaiyu UNDOC (*United Nation Office on Drugs and Crime)* memberikan pengertian bahwa MLA adalah prosedur kerjasama internasional dimana Negara-negara mengajukan dan menerima bantuan dalam mengumpulkan alat bukti alat bukti yang akan digunakan dalam penyeldikan dan penuntutan kasus-kasus kejahatan dalam melacak, membekukandan menyita hasil kejahatan yang diperoleh.[230] Selain memberikan definisi PBB bahkan telah meyusun suatu model perjanjian di bidang Bantuan Timbal Balik dalam Masalah Pidana ini yang dikenal dengan *United Nations Model Treaty (UN Model Treaty).*[231] Dalam model tersebut disampaikan pembatasan bahwa bantuan timbal balik bukan berarti bantuan untuk mengadili dan juga bukan bantuan hukum.[232] *UN Model Treaty* menggunakan istilah "*Mutual Assistance"* bukan "*Mutual Legal Assistance*". Atas perbedaan istilah ini, dijelaskan dalam *UN Model Treaty* bahwa kedua istilah tersebut sering digunakan bergantian meskipun dalam system hukum tertentu kedua istilah itu bisa berbeda arti. *UN Model Treaty* sendir menggunakan istilah "*Mutual Assistance"* dalam mamual tersebut, akan tetapi setiap Negara dapat menggunakan istilah manapun yang sesuai dengan sistem hukum mereka. Prinsip-prinsip utama dalam *Mutual Legal Assistance* adalah:[233]

1. Prinsip Kerjasama

   Prinsip kerjasama internasional dalam kasus kasus khusus merujuk pada kerjasama hukum atau peradilan. Prinsip kerjasama biasanya diatur dalam perjanjian atau instrumen legal antara beberapa Negara atau pengaturan khusus dua Negara. Kerjasama yang diatur berbeda-beda, kadang hanya

---

[230] Peter Langseth, *United Nations Handbook on Practical Anti Corruption Measures for Prosecutors dan Investigators* (Vienna;UNDOC,2004), Hal 120.
[231] UNDOC, *Revised Manuals on the Model Treaty on Extradition and the Model Traety on Mutual Legal Assistance in Criminal Matters*, dihasilkan oleh Intergovermental Expert Group of Meeting, yang diselenggarakan oleh UNDOC bekerjasama dengan AIDP, ISISC dan OPCO di Siracusa, Italia Tanggal 6-8 Desember 2002, http://www/undoc.org/pdf/model_treaty_extradition_revised_manual.pdf,
[232] *Ibid*, Hal 66
[233] Afitrahim M.R, Yurisdiksi menurut *Convention on Cybercrime*

mengatur hal-hal umum, namun tidak menutup kemungkinan mengatur hal-hal khusus.

2. Prinsip timbal-balik (resiprositas) atas dasar hubungan baik

   Pada umumnya bantuan timbal balik didasarkan pada hukum acara pidana, perjanjian yang dibuat antar Negra, konvensi seta kebiasaan internasional. Namun hal ini tidak selalu dituangkan dalam perjanjian formal, hubungan baik sering dijadikan dasar untuk memberikan bantuan timbal balik walaupun antar kedua Negara belum memiliko perjanjian timbal-balik formal

Menurut Siswanto Sunarso, *Mutual Legal Assistance*, yakni suatu perjanjian yang bertumpu pada permintaan bantuan yang berkaitan dengan penyelidikan, penyidikan, penuntutan, pemeriksaan di depan sidang pengadilan, dan lain-lain, dari Negara Diminta dengan Negara Peminta.[234] Sedangkan menurut Undang-Undang Nomor 1 Tahun 2006, yang dimaksud Bantuan Timbal Balik Dalam Masalah Pidana adalah: permintaan bantuan kepada negara asing berkenaan dengan penyidikan, penuntutan dan pemeriksaan di sidang pengadilan.[235] Peraturan MLA ini dibuat dengan tujuan untuk memberikan dasar hukum bagi Pemerintah RI dalam meminta dan/atau memberikan bantuan timbal balik dalam masalah pidana dengan Negara asing.

Berdasarkan definisi yang diberikan Undang-Undang tersebut maka dapat diperoleh unsur dari Bantuan Timbal Balik dalam Masalah Pidana yaitu:

1. Bantuan yang diterima maupun yang diajukan adalah bantuan yang terkait kepada hal-hal yang terkait perbuatan kejahatan dalam lingkup hukum pidana;

---

[234] Siswanto Sunarso, *Ekstradisi dan Bantuan Timbal Balik dalam Masalah Pidana: Instrumen Penegakan Hukum Pidana Internasional*, (Jakarta:Rineka Cipta,2009), Hal 133

[235] Indonesia,*Undang-Undang Tentang Bantuan Timbal Balik Dalam Masalah Pidana*, UU NO 1, LN No 18, Tahun 2006, TLN No 4607, Pasal 3 ayat 1.

2. Bantuan terkait kepada prosedur hukum acara pidana di Indonesia (penyidikan, penuntutan, dan pemeriksaan di siding pengadilan);
3. Bantuan harus diajukan dan diterima secara resmi melaui mekanisme hubungan pemerintahan antar Negara (*government to government*); dan
4. Bantuan yang diajukan harus menaati ketentuan hukum Negara yang dimintakan bantuannya.

a) Bentuk *Mutual Assistance*

Penjelasan UU MLA menegaskan bahwa asas atau prinsip bantuan timbal balik dalam masalah pidana dalam UU MLA adalah didasarkan pada ketentuan hukum acara pidana, perjanjian antar negara yang dibuat, dan konvensi dan kebiasaan internasional.bantuan timbal balik tersebut dapat dilakukan berdasarkan suatu perjanjijan atau resiprositas.[236] Perjanjian MLA tersebut dapat berupa perjanjian bilateral maupun multilateral.

Perjanjian bilateral adalah suatu perjanjian yang diadakan oleh dua negara saja dan mengatur soal-soal khusus yang menyangkut kepentingan kedua belah pihak. Sedangkan perjanjian multilateral adalah perjanjian yang diadakan banyak negara yang pada umumnya merupakan perjanjian terbuka (*open verdrag)* dimana hal-hal yang diaturnya pun lazimnya yang menyangkut kepentingan umum yang tidak terbatas pada kepentingan pihak-pihak yang mengdakan perjanjian tetapi juga menyangkut kepentingan yang bukan peserta perjanjian itu sendiri. Perjanjian ini digolongkan pada perjanjian "*law making treaties"* atau perjanjian yang membentuk hukum.[237] Prinsip resiprositas ini artinya apabila belum ada perjanjian, makan bantuan dapat dilakukan atas dasar hubungan baik.

Sampai saat ini Pemerintah Indonesia telah memiliki 4 (empat) perjanjian bilateral di bidang MLA, yaitu :

[236] *Ibid*, Pasal 5
[237] Mochtar Kusumaatmadja,*Pengantar Hukum Internasional*, (bandung :Binacipta, 1996) , Ha; 115.

1. Indonesia-Australia, ditandatangani tahun 1995, sebagaimana telah disahkan dengan Undang-Undang Nomor 1 Tahun 1999 tentang Pengesahan Perjanjian antara Republik Indonesia dan Australia mengenai Bantuan Hukum Timbal Balik dalam Masalah Pidana (*Treaty Between The Republic of Indonesia and Australia on Mutual Legal Assistance in Criminal Matters*).

2. Indonesia-RRC, ditandatangani tahun 2002, sebagaimana di sahkan denga Undang-Undang Nomor 8 Tahun 2006 tentang tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik Rakyat China mengenai Bantuan Hukum Timbal Balik dalam Masalah Pidana (*Treaty Between The Republic of Indonesia and The People's Republic of China on Mutual Legal Assistance in Criminal Matters*).

3. Indonesia-Korea Selatan, ditandatangani 30 Maret 2002, sampai saat ini proses ratifikasi

4. Indonesia-Hongkong, ditandatangani oleh Jaksa Agung RI pada tanggal 3 April 2008, saat ini dalam proses ratifikasi.

Di samping perjanjian bilateral, perjanjian multilateral yang berlaku di Indonesai juga berisikan persyaratan tentang adanya MLA diantara semua pihak yang melakukan perjanjian. Sampai saat ini pemerintah Indonesia telah memiliki perjanjian multilateral di bidang MLA, yaitu ASEAN MLA TREATY, yang ditandatangani tanggal 29 November 2004, sebagaimana telah di sahkan dengan Undang-Undang Nomor 15 Tahun 2008 tentang Pengesahan *Treaty on Mutual Legal Assistance in Criminal Matters* (Perjanjian Tentang Bantuan Timbal Balik Dalam masalah Pidana).

Akan tetapi, pengaturan MLA ini tentu tidak mengurangi pelaksanaan kerjasama yang telah dilakukan melalui *International Criminal Police Organization* (INTERPOL). Organisasi yang berpusat di prancis ini, beranggotakan kepolosian dari berbagai negara di dunia dan memiliki sistem pertukaran informasi sendiri. Dengan demikian polisi suatu negara dapat meminta atau menerima informasi kejahatan

melalui Interpol tanpa harus melalui saluran diplomatik (*diplomatic channel)*. Sistem ini mempunyai kelebihan yang memeprcepat pertukaran informasi diantara polisi di seluruh dunia. Sebaliknya, karena permintaan bantuan ini tidak dilakukan secara resmi melalui pemerintah , kerjasama ini mempunyai keterbatasan. Sebagai contoh informasi yang di terima melalui Interpol umumnya tidak bisa di gunakan di depan pengadilan karena tidak ada pengesahan atas dokumen, bukti ataupun pernyataan. Namun adakalanya pengadilan memperbolehkan informasi tersebut digunakan sebagai bukti di depan pengadilan jika pihak terdakwa atau kuasa hukumnya tidak menolak penggunaan informasi tersebut di pengadilan. Seandainya bisa di prediksi bahwa pihak terdakwa akan menolak infomrnasi tersebut, maka pihak polisi atau jaksa dapat mengajukan permohonan resmi yaitu MLA.

b. Jenis Permintaan Bantuan

Dibawah peraturan MLA di kalsfikasikan 2 (dua) jenas permintaan yaitu:

1) Permintaan Bantuan dari Pemerintah RI[238]

Menteri Hukum dan HAM RI dapat mengajukan permintaan bantuan kepada negara asing secara langsung atau melalui saluran diplomatik (melalui Kementrian Luar Negara), berdasarkan permohonan dari Kepala Kepolisian RI dan Jaksa Agung RI atau Ketua Komisi Pemberantasan Korupsi (khusus Tindak Pidana Korupsi). Permintaan bantuan dari Pemerintah Indonesia harus dalam bentuk tertulis yang berisikan :[239]

1) Identitas dari instansi yang meminta
2) Pokok masalah dan hakekat dari penyidikan, penuntutan atau pemeriksaan di siding pengadilan yang berhubungan dengan permintaan tersebut, serta nama dan fungsi institusi yang melakukan penyidikan, penuntutan dan proses peradilan.

[238] *Ibid*, Bab II
[239] *Ibid*, Pasal 10

3) Ringkasan dari fakta-fakta yang terkait kecuali permintaan bantuan yang berkitan dengan dokumen yuridis.
4) Ketentuan UU uang terkait, isi pasal dan ancaman pidananya.
5) Uraian tentang bantuan yang diminta dan rincian mengenai prosedur khusus yang dikehendaki termasuk kerahasiaan.
6) Tujuan dari bantuan yang diminta
7) Syarat-syarat lain yang ditentukan oleh negara yang diminta

2) Permintaan Bantuan Kepada Pemerintah RI

Setiap negara asing dapat mengajukan permintaan bantuan kepada Pemerintah RI secara langsung atau melalui saluran diplomatik. Isi dari permintaan tersebut harus dalam bentuk tertulis yang dapat dibuat dalam bahasa negara peminta dan/atau bahasa inggris serta dibuat terjemahannya dalam Bahasa Indonesia. Permintaan bantuan tersebut haruslah memuat:[240]

1) Maksud permintaan bantuan dan uraian mengenai bantuan yang diminta
2) Instansi dan nama pejabat yang melakukan penyidikan, penuntutan atau pemeriksaam di siding pengadilan yang terkait dengan permintaan tersebut.
3) Uraian tindak pidana, tingkat penyelesaian perkara, ketentuan Undang-Undang, isi pasal dan ancaman hukumannya.
4) Uraian mengenai perbuatan atau keadaan yang disangkan sebai tindak pidana, kecuali dalam hal permintaan banyuan untuk melaksanakan penyampaian surat.
5) Putusan pengadilan yang bersangkutan dan penjelasan bahwa putusan tersebut telah memperolah kekuatan hukum tetap, dalam hal permintaan bantuan untuk menindaklanjuti putusan pengadilan.

[240] *Ibid*, Pasal 28 ayat 1.

6) Rincian mengenai tat cara atau syarat-syarat khusus yang dikehendaki untuk dipenuhi, termasuk informasi apakah alat bukti yang diminta untuk didapatkan perlu di buat di bawah sumpah atau janji.
7) Jika ada persyaratan mengenai kerahasiaan dan alasan untuk itu.
8) Batasan waktu yang dikehendaki dalam melaksanakan permintaan tersebut.

Selain itu, sejauh diperlukan dan dimungkinan juga harus dimuat:[241]

1) Identitas, kewarganegaraan dan domisili dari orang yang dinilai sanggup memberikan keterangan atau pernyataan yang terkait dengan suatu penyidikan, penuntuan dan pemeriksaan di siding pengadilan;
2) Uraian mengenai mengenai keterangan atau pernyataan yang diminta untuk didapatkan;
3) Uraian mengenai dokumen atau alat bukti lainnya yang diminta untuk didapatkan;
4) Informasi mengenai pembiayaan dan akomodasi yang menjadi kebutuhan dari orang yang diminta untuk diatur kehadirannya di negara asing tersebut.

Persyaratan diatas merupakan persyaratan pokok. Dalam pelaksanaannya dimungkinkan ada penambahan persyaratan lain di samping persyaratan pokok sebagaimana tersebut diatas. Tidak semua permintaan bantuan dapat dipenuhi. Permintaan bantuan kepada Pemerintah Indonesia ada yang ditolak dan ada yang dapat ditolak. Permintaan bantuan ditolak dalam hal:[242]

1) Permintaan bantuan terkait dengan suatu penyidikan, penuntuan dan pemeriksaan di siding pengadilan atau pemintaan terhadap orang atas tindak pidana yang dianggap sebagai:

[241] *Ibid*, Pasal 28 ayat 2.
[242] *Ibid*, Pasal 6

a) Tindak pidana politik, kecuali pembunuhan atau percobaan pembunuhan terhadap kepala negara/kepala pemerintahan, terorisme; atau
b) Tindak pidana berdasarkan hukum militer;

2) Permintaan bantuan berkaitan dengan suatu penyidikan, penuntutan dan pemeriksaan di siding pengadilan atau pemidanaan terhadap orang atas tindak pidana yang pelakunya terlah dibebaskan, diberi grasi atau telah selesai menjalani pemidanaan;
3) Permintaan bantuan berkaitan dengan suatu penyidikan, penuntutan dan pemeriksaan di siding pengadilan atau pemidanaan terhadap orang atas tindak pidana yang jika dilakukan di Indonesia tidak dapat dituntut.
4) Permintaan bantuan diajukan untuk menuntut atau mengadili orang karena alasan suku, jenis kelamin, agama, kewarganegaraan atau pandangan politik.
5) Persetujuaan pemnerian bantuan akan merugikan kedaulatan, keamanan, kepentingan dan hukum nasional
6) Negara asing tidak dapat member jaminan bahwa hal yang dimintakan bantuan tidak digunakan untuk penanganan perkara yang dimintakan.
7) Negara asing tidak dapat memberikan jaminan pengembalian barang bukti yang diperolah berdasarkan bantuan apabila diminta.

Berdasarkan uraian diatas, makan permintaan ditolak hanyalah untuk keadaan tertentu saja dan bersifat mutlak, ketika ada permintaan mengenai lingkup tersbut, mutlak akan ditolak. Selain kondisi tertentu yang menyebabkan permintaan bantuan ditolak, terdapat juga kondisi dimana permintaan bantuan dapat ditolak. Dapat ditolak artinya penolakan bukanlah yang mutlak, dapat saja dengan pertimbang dan kajian yang lebih mendalam. Menteri Hukum dan HAM sebagai pemegang otoritas pusat akan memberikan pertimbangan tersebut. Permintaan bantuan dapat ditolak jika:[243]

[243] *Ibid*, Pasal 7

1) Permintaan bantuan berkaitan dengan suatu penyidikan, penuntutan dengan pemeriksaan di siding pengadilan atau pemidanaan terhadap orang atas tindak pidana yang jika dilakukan di wilayah Indonesia, bukan merupakan tindak pidana; orang atas tindak pidana yang jika dilakukan diluar wilayah Indonesia, bukan merupakan tindak pidana; orang atas tindak pidana yang terhadap orang tersebut diancam pidana mati.
2) Persetujuan pemberian bantuan dimana atas permintaan bantuan tersebut akan merugikan suatu penyidikan, penuntutan dan pemeriksaan siding pengadilan di Indonesia, membahayakan keselamatan orang atau membebani kekayaan negara.

Dalam *Convention on Cybercrime* sudah mengatur segala hal yang berkaitan dengan *Mutual Legal Assistance* antara para pihak secara khusus untuk kasus *Cybercrime*, ada pun ketentuan umum/*general rules* mengenai MLA adalah :[244]

[244] Convention on Cybercrime,*op.cit*, Pasal 25 yang berbunyi :

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or

1) Para pihak harus mengadakan perjanjian timbal balik untuk memperluas segala kemungkinan yang bertujuan untuk investigasi atau proses peradilan terkait kejahatan komputer atau pengumpulan data elektronik dalam kejahatan pidana.

2) Pihak harus mengadopsi peraturan perundang-undangan atau hal lain yang diperlukan untuk mencakup segala kewajiban yang diatur dalam pasal 27 sampai 35.

3) Para pihak dalam hal keadaan yang memaksa dapat meminta pihak lain untuk mempercepat prosedur bantuan timbal balik baik melalui fax, email yang telah dijamin validitas dan keamanannnya (termasuk penggunaan enkripsi).

4) Kecuali ditentukan dalam konvensi ini, perjanjian timbal balik harus di lakukan sesuai dengan kondisi yang diperjanjikan antar kedua belah pihak.

5) Sejalan dengan konvensi ini para pihak di perbolehkan untuk membuat perjanjian *dual criminality*

Selain itu juga diatur tentang permohonan timbal balik apabila tidak ada perjanjian timbal balik seperti yang diatur dalam Pasal 27 :[245]

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

---

denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

[245] *Ibid*, Pasal 27

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Apabila tidak ada perjanjian timbal balik antar para pihak maka ketentuan pasal 2 sampai 9 konvensi ini berlaku, selain itu para pihak diharuskan untuk membentuk suatu badan (*central authority)* yang berwenang untuk mengatur segala sesuatu yang berhubungan denga perjanjian timbal balik. Hal terakhir yang di atur adalah mengenai perjanjian timbal balik yang khusus yang terkait dengan *cybercrime*, adapun perjanjian tersebut adalah mengenai:

1) Berkenaan untuk melakukan tindakan pencegahan, yang terdiri dari :[246]

   a) Melakukan penyimpanan data di komputer;[247]
   b) Melakukan penyimpanan data trafik[248]

2) Berkenaan dengan kewenangan untuk memeriksa yang terdiri dari :[249]

   a) Akses ke data komputer:[250]
   b) Akses ke data komputer dari luar negeri;[251]
   c) Akses untuk mengambil data secara real time;[252]
   d) Akses untuk melakukan *data interception*;[253]

[246] *Ibid*, Chapter III, Section 3, Title 1
[247] *Ibid*,Pasal 29
[248] *Ibid*,Pasal 30
[249] *Ibid*,*loc.cit*, Title 2
[250] *Ibid*, Pasal 31
[251] *Ibid*,Pasal 32
[252] *Ibid*,Pasal 33
[253] *Ibid*,Pasal 34

2.11.2.3. *Transfer of Proceedings*

Transfer of proceedings atau pengalihan perkara merupakan hal baru dalam sistem peradilan pidana internasional. Di dalam praktek sendiri baru ada satu konvensi yang mengatur mengenai ini yaitu *European Convention on The Transfer of Proceedings in Criminal Matters*, dalam konvensi ini tidak disebutkan dengan jelas apa definisi dari *Transfer of proceedings* itu, namun dalam *explanatory report* di sebutkan jika *transfer of proceedings* adalah *Transfer of Proceedings* adalah kerjasama internasional yang berbentuk *mutual legal assistance* dimana setiap Negara bisa meminta Negara lain untuk memproses seseorang yang diduga telah melakukan tindak pidana.[254] Yang dimaksud dengan proses atau *proceedings* adalah kegiatan yang dilakukan oleh penegak hukum untuk menegakkan hukum.[255] Jadi dapat di simpulkan jika *transfer of proceedings* adalah bentuk kerjsama internasional dimana sebuah Negara meminta Negara lain untuk menerapkan hukum acara pidananya kepada seseorang yang diduga telah melakukan tindak pidana.

Kunci dari penerapan bentuk kerjasama ini adalah kompetensi yang diatur pasal 2 ayat 1 menyebutkan jika negara peserta konvensi harus mempunyai kompetensi untuk memproses semua kejahatan dimana hukum negara peserta lainnya dapat digunakan.[256] Lalu untuk menghindari adanya *ne bis in idem* konvensi ini juga mengaturnya di pasal 3 yang berbunyi :[257]

"*Any Contracting State having competence under its own law to prosecute an offence may, for the purpose of applying this Convention, waive or desist from proceedings against a suspected person who is being or will be prosecuted for the same offence by another Contracting State. Having regard to Article 21, paragraph 2, any such decision*

---

[254] *European Convention on Transfer of proceedings Explanatory Report*, poin 26
[255] *Canada Uniform Court Jurisdiction and Transfer of Proceedings Act*, Pasal 1
[256] European Council, *Convention on The Transfer of Proceedings in Criminal Matters*, Pasal 2 ayat 1 berbunyi:
"*For the purposes of applying this Convention, any Contracting State shall have competence to prosecute under its own criminal law any offence to which the law of another Contracting State is applicable"*
[257] *Ibid*,Pasal 3

to waive or to desist from proceedings shall be provisional pending a final decision in the other Contracting State."

Dalam pasal ini di nyatakan bahwa negara peserta konvensi harus mengesampingkan segala proses hukum kepada seseorang yang telah di proses untuk kejahatan yang sama di negara peserta konvensi lainnya.

1. Permintaan Transfer of Proceeding

Apabila seseorang diduga telah melakukan kejahatan menurut hukum negara peserta, maka sesuai dengan kondisi yang di syaratkan oleh konvensi ini bisa meminta negara peserta lainnya untuk memproses orang tersebut.[258] Adapun kondisi yang memungkinkan seseorang dimintakan untuk diproses di negara peserta lainnya adalah :[259]

a) Apabila terduga tinggal di negara yang dimintakan (*Requested State)*;
b) Apabila terduga merupakan warganegara 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 di rasa mampu untuk merehabilitasi yang bersangkutan;
g) Apabila terduga/terdakwa di pastikan tidak mampu untuk mengahadiri persidangan di negara yang meminta;
h) Apabila cara yang lain (ekstradisi) dirasa tidak mampu untuk menghadirkan terduga/tersangka

[258] *Ibid*, Pasal 6
[259] *Ibid*, Pasal 8

2. Prosedur *Transfer of Proceedings*

1) Permintaan diajukan oleh negara peminta melalui Kementrian Kehakiman ke Kementrian negara yang diminta.[260]
2) Apabila permintaan tersebut terkait dengan kasus yang memerlukan aksi cepat, maka permintaan dapat di ajukan melalui Interpol.[261]
3) Apabila negara yang diminta merasa dokumen permintaan yang di lampirkan belum cukup, maka mereka bisa meminta negara peminta untuk melengkapi dokumen tersebut dalam jangka waktu tertentu.[262]
4) Setiap permintaan harus di sertai 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 dikrimkan menyusul.[263]

Dalam *Convention on Cybercrime* tidak ada pasal yang mengatur mengenai *Transfer of Proceedings*, namun jika kita melihat kembali definisi yang terdapat dalam *Convention on Transfer of Proceedings* bahwa *Transfer Proceedings* itu sendiri adalah bentuk kerjasama internasional yang berbentuk *Mutual Legal Assistance*. Maka Aturan umum (*General Rules*) mengenai *Mutual Legal Assistace* yang terdapat dalam pasal 25 *Convention on Cybercrime* dapat berlaku untuk *Transfer of Proceedings*.

2.12. Mahkamah Pidana Internasional

2.12.1. Landasan Yuridis Terbentuknya Mahkamah Pidana Internasional

Landasan yuridis makhamah pidana internasional adalah Statuta Rima tentang makhamah pidana internasional. Statuta ini merupakan hasil dari konferensi diplomatik berkuasa penuh PBB mengenai pendirian makhamah pidana internasional yang dilaksanakan pada tanggal 17 Juli 1 1998 di kota Roma, Italia. Statuta Roma di setujui oleh 120 negara dari 148 negara peserta konferensi, sedangkan sisanya adalah

[260] *Ibid*, Pasal 13 ayat (1)
[261] *Ibid*,Pasal 12 ayat (2)
[262] *Ibid*,Pasal 14
[263] *Ibid*, Pasal 15 ayat (1)

21 negara abstain dan 7 negara menolak. Indonesai dan Amerika Serikat termasuk dari negara peserta konferensi yang menolak menandatangani Statuta Roma.

Penolakan yang dilakukan Indoneaia adalah didsarkan salah satu alasan yang sangat prinsipil yaitu karena dalam Statuta Roma tidak diterapkan asas komplementaritas antara yurisdiksi kriminal makhamah internasional terhadap yurisdiksi nasional/negara terhadap suatu tindak pidana internasional. Indonesia berpendapat bahwa makhamah pidana internasional hanya menjadi pelengkap dari pelaksanaan sistem peradilan pidana nasional bukannya sebagai suatu sistem yang lebih tinggi dari sistem peradilan pidana nasional.[264]

Menurut pasal 126 Statuta Romam yaitu bahwa Statuta Roma akan mulai berlaku pada hari pertama dari bulan setelah 60 (enam puluh) hari setelah tanggal penyimpanan/*deposit* 60 (enam puluh) instrumen ratifikasi, penerimaan, persetujuaan atau pengikutsertaan. Sampai tanggal 7 September 2000, Statuta Roma belum dapat dimulai berlaku katena belum mencapai jumlah ratifikasi seperti yang diatur dalam pasal 126, yaitu hanya 91 negara yang menandatangani dan hanya 5 negara yang telah meratifikasinya.

2.12.2. Struktur Orgainsasi Makhamah Pidana Internsional

Struktur organisasi Makhamah Pidana Internasional sebagaimana yang diatur dalam pasal 34 Statuta Roma terdiri dari 6 Organ yaitu :

1. Kepresidenan (*The Presidency)*;
2. Divisi Banding (*An Appeals Division)*, Divisi Persidangan (*A Trial Division)*, Divisi Persidangan Pendahuluan (*A Pre-Trial Division)*;
3. Kantor Jaksa Penuntut (*The Office of The Prosecutor)*
4. Panitera (*The Registry)*.

[264] Departemen Luar Negeri Republik Indonesia,*"Posisi Indonesia Terhadap Pembentukan Makhamah Pidana Internasional"*, Juli 1998, Hal 23

1. Kepresidenan (*The Presidency*)

Pada saat terbentuknya Makhamah Pidana Internasional, siding majelis negara pihak statuta makhamah pidana internasional memilih kandidat hakim-hakim makhamah pidana internasional untuk masa tugas 3 (tiga) tahun dan hanya dapat dipilih lembali untuk 1 (satu) periode saja.

Para hakim yang dipilih harus menjadi anggota penuh waktu dari makhamah pidana internasional dan harus selalu hadir untuk pelaksanaan tugas mereka. Setiap kandidat hakim harus dipilih dari orang orang yang memiliki karakter moral yang tinggi, tidak memihak dan intergritas yang memenuhi kualifikasi yang di persyaratkan di negara masing masing sebagai pejabat peradilan tertinggi. Selain itu ketiap kandidat hakim harus benar-benar memiliki kompetensi dalam bidang hukum pidana han hukum acara pidana, dan pengalaman-pengalaman yang televan yang penting dalam beracara perkara pidana baik sebagai haikm, jkasa penuntut, advokat atau kapasitas lainnya yang sejenis. Kandidat hakin juga harus benar benar mempunyai kompetensi yang relevan dalam bidang hukum internasional seperti hukum humaniter internasional dan hukum Hak Asasi manusia dan pengalaman yang luas dalam kapasitas profesi hukum yang professional yang relevan dengan tugas peradilan makhamah pidana internasional.

Sesuai dengan pasal 38 Statuta Roma, setelah hakim-hakim telah dipilih, para hakim tersebut memilih kandidat presiden makahamah internasional internasional beserta wakil presiden pertama dan wakil presiden kedua dimana kandidatnya adalah hakim yang telah diangkat oleh siding majelis negara peserta statuta makahmah pidana internasional, berdasarkan suarta mutlak para hakim untuk masa tugas selama 3 (tiga) tahun atau sampai berakhirnya masa tugasnya sebagai hakim. Preseiden dan wakilnya dapat dipilih kembali hanya untuk satu periode saja.

Kepresidenan adalah suatu lembaga yang mempunyai tugas untuk menjalankan dan mengkoordinasikan kegiatan sehari-hari dari makhamah pidana internasional. Kepresiden dipimpin oleh seorang presiden dan satu orang wakil

presiden pertama dan wakil presiden kedua. wakil presiden pertama akan bertindak sebagai presiden dalam hal presiden tidak hadir/tidak berada atau dibatalkan/didiskualifikasi. Begitu pula dengan wakil presiden kedua akan bertindak sebagai wakil presiden pertama dalam hal wakil presiden pertama tidak hadir/tidak berada atau dibatalkan/didiskualifikasi.

Menurut pasal 38 ayat 3 Stauta Roma, Presiden, wakil presiden pertama dan kedua mempunyai tugas untuk mendirikan dan menjalankan kantor kepresidenan yang bertangung jawab terhadap :[265]

a) Adminstrasi makhamah yang baik kecuali terhadap kantor penuntut umum;

b) Fungsi lainnya yang diberikan kepadanya menurut Satuta Roma.

2. Divisi Banding (*An Appeals Division),* Divisi Persidangan (*A Trial Division),* Divisi Persidangan Pendahuluan (*A Pre-Trial Division)*;

Presiden beserta wakil presiden pertama dan wakil presiden kedua mempunyai tugas untuk menysusun organisasi makhamah pidana internasional kedalam divisi-divisi sebagaimana diatur dalam pasal 36 huruf (b) yaitu :[266]

a) Divisi Banding;

b) Divisi Persidangan; dan

c) Divisi Persidangan Pendahuluan.

Divisi banding anggotanya terdiri dari lima hakim yaitu presiden, dan empat hakim lainnya, divisi persidangan tidak kurang dari enam hakim dan divisi persidangan pendahuluan tidak kurang dari enam hakim. Penugasan/penempatan hakim dalam divisi-divisi tersebut harus didasarkan pada sifat dasar dari fungsi yang akan dilaksanakan oleh masing masing divisi, kualifikasi dan pengalaman hakim-hakim yang dipilih/ditugaskan untuk makhamah internasional, dengantetap

[265] Statuta Roma pasal 38 ayat 3
[266] *Ibid*,Pasal 36 huruf b

memperhatikan bahwa setiap divisi harus terdiri dari kombinasi yang layak ahli hukum pidana dan hukum acara pidana serta hukum internasional. Khusus untuk divisi persidangan dan divisi persdiangan pendahuluan, komposisi hakim harus mengutamakan hakim-hakim dengan pengalaman persidangan perkara pidana.

Setelah penugasan hakim-hakim kepada setiap divisi tersebut maka dibentuklah majelis hakim untuk setiap masing masing divisi dimana majelis tersebut mempunyai tugas untuk menjalankan fungsi peradilan makhamah yang diberikan kepada masing masing divisi.

Majelis banding terdiri dari seluruh hakim divisi banding. Sedangkan fungsi majelis persidangan harus dijalankan oleh tiga hakim divisi persidangan dan fungsi majelis persidangan pendahuluan harus di jalankan oleh tiga atau satu hakim pada divisi tersebut berdasarkan statuta dan hukum acara dan pembuktian.

Menurut pasal 39 ayat 2 huruf ©, makhamah pidana internasional dapat mendirikan lebih dari satu majelis persdangan maupun satu majelis persidangan pendahuluan dalam hal efisiensi manajemen beban kerja makhamah pidana internsional.

3. Kantor Jaksa Penuntut (*The Office of The Prosecutor)*

Menurut pasal 42 ayat (1) Statuta Roma, kantor jaksa penuntut harus bertindak secara independen sebagai organ yang terpisah dari makhamah pidana internasional dimana bertanggung jawab untuk menerima penyerahan berkas dan informasi pendukung mengenai tindak pidana yang masuk dalam yurisdiksi makhamah pidana internasional, dan bertanggung jawab untuk menguji atau menilai berkas dan informasi tersebut serta melakukan investigasi dan penuntutan atau dakawaan dihadapan makhamah pidana internasional. Setiap anggota dari kantor jaksa penuntut tidak dapat melakukan penyelidikan atau bertindak atas instruksi yang berasal dari pihak luar.

Menurut pasal 42 ayat (2) Statuta Roma, kantor jaksa penuntut dikepalai oleh seorang jaksa penuntut yang mempunyai kewenangan penuh terhadap majamen dan administrasi kantor jaksa penuntut termasuk staf, fasilitas dan prasarana lainnya dari kantor jaksa penuntut tersebut.

Jaksa penuntut dalam tugas sehari-harinya dibantu oleh satu atau lebih deputi jaksa penuntut yang ditugaskan untuk melaksanakan setiap tindakan yang ditugaskan jaksa penuntut berdasarkan Statuta Roma. Kewarganegaraan dari jaksa penuntut dan deputi jaksa penuntut harus kewarganegaraan yang berbeda satu sama lain, tidak boleh dari satu negara.

Jaksa penuntut dan deputi jaksa penuntut harus mempunyai karakter moral yang tinggi, kompetensi yang baik dan pengalaman praktik yang luas mengenai penuntutan atau persidangan perkara pidana. Selain itu mereka harus memiliki pengetahuan yang baik sekali serta fasih dalam salah satu bahasa kerja makhakamah internasional.

Jaksa penuntut dipilij dengan sistem pemungutan suara rahasia berdasarkan suara mayoritas mutlak dari anggota siding majelis negara peserta statuta roma. Setelah jaksa penuntut dipilih dan diangkat, kemudian dilakukan pemilihan deputi jaksa penuntut dimana daftar kandidiat tersebut diajukan oleh jaksa penuntut yang telah dipilih, dengan cara dan prosedur pemilihan yang sama dengan pemilihan jaksa penuntut.

Baik jaksa penuntut atau deputi jaksa penuntut tidak boleh ikut serta atau terlibat dalam kegiatan apapun yang mana terlibat akan menggangu atau mencampuri fungsi-fungsi dari fungsi penuntutannya atau mempengaruhi keyakinan dalam independensinya. Selain itu mereka juga tidak boleh terlibat dalam bidang prkerjaan profesi umumnya.

Pasal 42 ayat (7) mengatur bahwa presiden makhamah pidana internasional dapat membebaskan jaksa penuntut dan deputi jaksa penuntut atas permintaan dari

yang padanya untuk bertugas dalam kasus tertentu. Selain itu juga, jasa penuntut dan deputi jaksa penuntut tidak boleh untuk ikut serta dalam segala hal apabila ketidakberpihakannya mungkin layak diragukan/dipertanyakan atas dasar alasan apapun. Jaksa penuntut dan deputi jaksa penuntut harus didiskualifikasikan atau dibatalkan dari suatu kasus/perkara apabila sebelumnya mereka telah terlibat dalam kapasitas apapun terhadap perkara yang dihadapkan kepada makahamah pidana internasional atau pada tingkat nasional melibatkan orang yang sedang diinvestigasi atau sedang di dakwa.

Permasalahan mengeni pembatalan/didiskualifikasi jaksa penuntut atau deputi jaksa penuntut akan diputuskan dan diselesaikan oleh majelis banding. Orang yang sedang diinvestigasi atau di dakwa pada setiap saat dapat meminta pembatalan jaksa penuntutan atau deputi jaksa penuntut berdasarkan alasan tersebut. Jaksa penuntut dan deputi jaksa penuntutan yang dimintakan pembatalannya mempunyai hak untuk menjelasakan pendapatnya mengenai usulan pembatalan mereka.

4. Kantor Panitera (*The Registry)*.

Menurut pasal 43 ayat (1) Statuta Roma, kantor panitera harus bertangung jawab menangani aspek non judicial administrasi dan pelayanan makhamah pidana internasional, tanpa mengurangi fungsi dan kewenangan jaksa penuntut berdasarkan 42 Statuta Roma.

Kantor panitera dikepalai oleh pantera yang menjadi petugas administratif utama dari makhamah pidana internasional dan harus menjalankan fungsi-fungsinya dibawah kewenangan dari presiden makhamah pidana internasional.

Panitera dan deputi panitera harusnlah orang orang yang memiliki karakter moral yang tinggi, mempunyai kompetensi yang tinggi dan mempunyai pengetahuan yang baik serta fasih dalam salah satu bahasa kerja makhamah pidana internasional.

Menurut pasal 43 ayat (3) panitera dipilih oleh para hakim makhamah pidana internasional dengan memperhatikan rekomendasi majelis siding negara peserta

statuta. Apabila diperlukan, para hakim makhamah pidana internasional dapat memilih dan mengangkat seorang deputi panitera atas rekomendasi panitera.

Panitera mempunyai masa tugas selama 5 (lima) tahun dan dapat dipilih kembali untuk satu periode saja dan harus menjalankan tugas dengan penuh waktu. Begitu pula dengan deputi panitera mempunayi masa tugas selama 5 (lima) tahun atau lebih pendek sebagaimana diputuskan oleh suara mayoritas mutlak para hakim dan dapat dipilih kembali apabila deputi panitera benar-benar dibutuhkan.

Paintera, berdasarkan pasal 43 ayat (6) mempunyai tugsa untuk menyusun unit korban dan saksi dimana unit ini berfrungsi untuk menyediakan atau memberikan, dalam kaitannya dengan konsultasi dengan kantor jaksa penuntut, tindakan-tindakan perlindungan dan penyusunan keamanan, pemberian nasihat dan asistensi yang layak lainnya bagi saksi-saksi dan para korban yang tamil didepan makhamah pidana internasional, serta pihak lainnya sebagai akibat dari dilakukannya kesaksian oleh saksi-saksi.

2.12.3. Kejahatan Internasional yang dapat diadili di Makhamah Kriminal Internasional (ICC)

Tindak pidana internasional atau *international crimes*, baik menurut perjanjian-perjanjian internasional maupun di dalam hukum kebiasaan internasional, belum ada ketentuan yang jelas hingga sat ini. Hal tersebut disebabkan adanya perdebatan seputar penetapan peristilahannya yang dapat berdampak luas, dalam hal substansi dan subjeknya.[267]

Sudah sejak abad ke-18, masyarakat bangsa-bangsa mengenal dan mengakui kejahatan perompak di laut sebagai kejahatan internasional yang dikenal sebagai *piracy de jure gentium*.[268] Kejahatan tersebut dianggap sangat merugikan

[267] Romli Atmasasmita, *Pengantar Hukum Pidana Internasional*, (Bandung: Refika Aditama, 2003), hlm.35

[268] istilah *Piracy de jure gentium* merupakan istilah yang dipergunakan pada Zaman Romawi Kuno terhadap para pembajak laut yang dianggap sebagai pelaku kejahatan, mengancam bangsa Romawi yang saat itu menggunakan hukum yang disebut dengan *Jure Gentium* atau hukum nasional terhadap

kesejahteraan bangsa-bangsa pada saat itu dan dianggap sebagai musuh bangsa-bangsa. *Piracy de jure gentium* kemudian ditetapkan sebagai kejahatan internasional karena merupakan satu-satunya tindak kriminal murni.

Defenisi tentang tindak pidana internasional atau kejahatan internasional (*international crimes*) menurut Bassiouni sebagai berikut:[269]

"Tindak pidana internasional adalah setiap tindakan yang telah ditetapkan di dalam konvensi-konvensi multilateral dan yang telah diratifikasi oleh negara-negara peserta, sekalipun di dalamnya terkandung salah satu dari kesepuluh karakteristik pidana"

Bassiouni lebih lanjut menjelaskan kesepuluh karakteristik yang dimaksudkan, sebagai berikut:

1. *Explicit recognition of proscribed conduct as constituting an international crime or a crime under international law*. (pengakuan secara eksplisit atas tindakan-tindakan yang dipandang sebagai kejahatan berdasarkan hukum internasional).

2. *Implicit recognition of the penal nature of the act by establishing a duty to prohibit, prevent, prosecute, punish or the like* (pengakuan secara implisit atas sifat-sifat pidana dari tindakan-tindakan tertentu dengan menetapkan suatu kewajiban untuk menghukum, mencegah, menuntut, menjatuhi hukuman atau pidananya).

3. *Criminalization of the proscribed conduct* (kriminalisasi atas tindakan-tindakan tertentu).

4. *Duty or right to prosecute* (kewajiban atau hak untuk menuntut).

---

negara kekuasaan Romawi. Lihat, Eddy O.S. Hiariej, *Pengantar Hukum Pidana Internasional* (Jakarta: Airlangga, 2009), hlm. 49.

[269] Romli Atmasasmita, *Op.Cit*, hlm. 37.

5. *Duty or right to punish the proscribed conduct.* (kewajiban atau hak untuk memidana tindakan tertentu).

6. *Duty or right to extradite* (kewajiban atau hak untuk mengekstradisi).

7. *Duty or right to cooperate in prosecution, punishment, including judicial assistance in penal proceeding*. (kewajiban atau hak untuk bekerjasama di dalam proses pemidanaan).

8. *Establishment of a criminal jurisdiction basis* (penetapan suatu dasar-dasar yurisdiksi kriminil).

9. *Reference to the establishment of an international court* (referensi pembentukan suatu pengadilan internasional).

10. *Elimination of the defense of superiors orders* (penghapusan alasan-alasan perintah atasan).

Dilihat dari perkembangan dan asal-usul tindak pidana internasional ini, maka eksistensi tindak pidana internasional dapat dibedakan dalam:[270]

1. Tindak pidana internasional yang berasal dari kebiasaan yang berkembang di dalam praktik hukum internasional.

2. Tindak pidana internasional yang berasal dari konvensi-konvensi internasional.

3. Tindak pidana internaisonal yang lahir dari sejarah perkembangan konvensi mengenai hak asasi manusia.

Tindak pidana internasional yang berasal dari kebiasaan hukum internasional adalah tindak pidana pembajakan atau *piracy*, kejahatan perang atau *war crimes*, dan tindak pidana perbudakan atau *Slavery.* Tindak pidana internasional yang berasal dari konvensi-konvensi internasional ini secara historis dibedakan antara tindak pidana

[270] *Ibid*,hlm. 40.

internasional yang ditetapkan di dalam satu konvensi saja dan tindak pidana internasional yang ditetapkan oleh banyak konvensi.

Tindak pidana internasional yang lahir dari sejarah perkembangan konvensi mengenai hak asasi manusia merupakan konsekuensi logis akibat Perang Dunia II yang meliputi bukan hanya korban-korban perang mereka yang termasuk *combatant*, melainkan juga korban penduduk sipil (*non-combatant*) yang seharusnya dilindungi dalam suatu peperangan. Salah satu tindak pidana internasional ini ialah *crimes of genocide* sesuai dengan Deklarasi Perserikatan Bangsa-Bangsa (PBB) Tanggal 11 Desember yang menetapkan genosida sebagai kejahatan menurut hukum internasional.[271]

Penetapan tindak pidana internasional atau *International crimes* itu diperkuat dalam Piagam Mahkamah Militer Internasional di Nuremberg atau *the International Military Tribunal* yang dibentuk segera setelah Perang Dunia II terakhir (1946). Mahkamah ini ditetapkan oleh negara pemenang Perang Dunia II (Amerika Serikat, Inggris, Prancis, serta Rusia) dan memiliki yurisdiksi atas tiga golongan kejahatan:

1. *Crimes against peace* atau kejahatan atas perdamaian, yang diartikan termasuk persiapan-persiapan atau pernyataan perang agresi.

2. *War crimes* atau kejahatan perang atau pelanggaran atas hukum-hukum tradisional dan kebiasaan dalam peperangan.

3. *Crimes against humanity* yakni segala bentuk kekejaman terhadap penduduk sipil selama peperangan berlangsung.

Dalam naskah rancangan ketiga Undang-Undang Pidana Internasional atau *the International Criminal Code* Tahun 1954, telah ditetapkan 13 kejahatan yang dapat dijatuhi pidana berdasarkan hukum internasional sebagai kejahatan terhadap perdamaian dan keamanan seluruh umat manusia. Ketiga belas tindak pidana ini adalah sebagai berikut:

[271] *Ibid*

1. Tindakan persiapan untuk agresi dan tindakan agresi.
2. Persiapan penggunaan kekuatan bersenjata terhadap negara lain.
3. Mengorganisasi atau memberikan dukungan persenjataan yang ditujukan untuk memasuki wilayah suatu negara.
4. Memberikan dukungan untuk dilakukan tindakan terorisme di negara asing.
5. Setiap pelanggaran atas perjanjian pemabatasan senjata yang telah disetujui.
6. Aneksasi wilayah asing.
7. *Genocide* (genosida).
8. Pelanggaran atas kebiasaan dan hukum perang.
9. Setiap pemufakatan, pembujukan, dan percobaan untuk melakukan tindak pidana tersebut pada butir 8 di atas.
10. *Piracy* (Pembajakan).
11. *Slavery* (Perbudakan).
12. Apartheid.
13. *Threat and use of force against internationally protected persons.*

Dalam naskah rancangan Undang-Undang Pidana Internasional atau *The International Criminal Code* Tahun 1979 yang disusun oleh *The International Association of Penal Law*, telah dimasukkan jenis tindak pidana lainnya, seperti: lalu lintas perdagangan narkotika illegal (*illicit drug trafficking*), pemalsuan mata uang (*counterfeiting*), keikutsertaan di dalam perdagangan budak, penyuapan (*bribery*), dan pengambilan harta karun negara tanpa izin.

Berdasarkan internasionalisasi kejahatan dan karakterisktik kejahatan internasional, dalam konteks hukum kejahatan internasional, kejahatan internasional memiliki hirarki atau tingkatan. Sampai dengan tahun 2003 atas dasar 281 konvensi internasional sejak tahun 1812, ada 28 kategori kejahatan internasional. 28 kejahatan internasional tersebut adalah:[272]

[272] Eddy O.S. Hiariej, *Op.Cit*.Hlm. 55.

1. *Aggression.*
2. *Genocide.*
3. *Crimes against humanity.*
4. *War crimes.*
5. *Unlawful possession or use or emplacement of weapons.*
6. *Theft of nuclear materials.*
7. *Mercenaries.*
8. *Apartheid.*
9. *Slavery and slave-related practices.*
10. *Torture and other forms of cruel, inhuman, or degrading treatment.*
11. *Unlawful human experimentation.*
12. *Piracy.*
13. *Aircraft hijacking and unlawful acts against international air safety.*
14. *Unlawful acts against the safety of maritime navigation and the safety of platforms on high seas.*
15. *Threat and use of force against internationally protected persons.*
16. *Crimes against United Nations and associated personnel.*
17. *Taking of civilian hostages.*
18. *Unlawful use of the mail.*
19. *Attacks with explosives.*
20. *Financing of terrorism.*
21. *Unlawful traffic in drugs and related drug offenses.*
22. *Organized crime.*
23. *Destruction and/or theft of national treasures.*
24. *Unlawful acts against certain internationally protected elements of the environment.*
25. *International traffic in obsence materials.*

26. *Falsification and counterfeiting.*
27. *Unlawful interference with submarine cables.*
28. *Bribery of foreign public officials*.

Berdasarkan 28 kategori kejahatan internasional tersebut, M. Cherif Bassiouni membagi tingkatan kejahatan interasional menjadi tiga.[273]

Pertama, kejahatan internasional yang disebut sebagai *international crimes* adalah bagian dari *jus cogens*.[274] Tipikal dan karakter dari international crimes berkaitan dengan perdamaian dan keamanan manusia serta nilai-nilai kemanusiaan yang fundamental. Terdapat sebelas kejahatan yang menempati hirarki teratas sebagai *international crime,* yakni:

1. *Aggression.*
2. *Genocide.*
3. *Crimes against humanity.*
4. *War crimes*
5. *Unlawful possession or use or emplacement of weapons.*
6. *Theft of nuclear materials.*
7. *Mercenaries.*
8. *Apartheid.*
9. *Slavery and slave-related practices.*
10. *Torture and other forms of cruel, inhuman, or degrading treatment.*
11. *Unlawful human experimentation.*

Kedua, kejahatan internasional yang disebut sebagai *international delicts.* Tipikal dan karakter *international delicts* berkaitan dengan kepentingan internasional yang dilindungi meliputi lebih dari satu negara atau korban dan kerugian yang timbul

[273] *Ibid*,Hal. 56
[274] *Jus Cogens* adalah hukum pemaksa yang tertinggi dan harus ditaati oleh bangsa-bangsa beradab di dunia sebagai prinsip dasar umum dalam hukum internasional yang berkaitan dengan moral. Lihat, Eddy O.S. Hiariej, *ibid*,hal. 50.

berasal dari satu negara. Ada tiga belas kejahatan internasional yang termasuk dalam *international delicts*, yaitu:

1. *Piracy.*
2. *Aircraft hijacking and unlawful acts against international air safety.*
3. *Unlawful acts against the safety of maritime navigation and safety of platforms on the high seas.*
4. *Threat and use of force against internationally protected person.*
5. *Crimes against United Nations and associated personnel.*
6. *Taking of civilian hostages.*
7. *Unlawful use of the mail.*
8. *Attacks with explosive.*
9. *Financing of terrorism.*
10. *Unlawful traffic in drugs and related drug offenses.*
11. *Organized crime*
12. *Destruction and/or theht of national treasures.*
13. *Unlawful acts against certain internationally protected elements of the environment.*

Ketiga, kejahatan internasional yang disebut dengan istilah *international infraction.* Dalam hukum pidana internasional secara normatif, *international infraction* tidak termasuk dalam kategori *international crime* dan *international delicts*. Kejahatan yang tercakup dalam *international Infraction* hanya ada empat, yaitu:

1. *International traffic in obsence materials.*
2. *Falsification and counterfeiting.*
3. *Unlawful interference with submarine cable.*
4. *Bribery of foreign public official.*

2.12.4. *Cybercrime* Sebagai Kejahatan Internasional

Cybercrime sudah berkembang mejadi fenomena yang bersifat global, serangan siber (*cyberattacks*) dapat menimpa siapa saja yang beroperasi di *cyberspace*, namun apabila serangan-serangan tersebut terjadi secara berulang-ulang dan yang di serang adalah objek vital dari sebuah negara (kantor pemerintahan, bank dan lain-lain) lalu diketahui jika serangan tersebut dilakukan dari negara lain atas inisiatif negara tersebut, maka timbulah apa yang di sebut perang di dunia maya (*cyberwarfare*). Menurut Richard Clarke dalam bukunya *cyber war*, *cyberwarfare* adalah perbuatan yang dilakukan oleh suatu negara untuk menembus komputer atau jaringan komputer negara lain dengan tujuan untuk menyebabkan kerusakan atau ganguan (*actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption*).[275]

Cyberwarfare merupakan jenis *cybercrime* yang memungkinkan sebuah negara melakukan penyusupan ke sistem komputer atau jaringan komputer negara lain tanpa terdeteksi, *cyberwarfare* biasanya mengunakan teknik-teknik yang sudah dikenal seperti *hacking, phising, defacing* dan lain-lain, namun perbedaannya adalah caranya yang terkoordinasi, seperti perang pada umumnya dimana ada serangan pertama, kedua, ketiga dan seterusnya hingga mendapatkan hasil yang dinginkan tercapai. Perbedaan lain antara *cyberwarfare* dan perang konvesional adalah dari segi korban, jika dalam perang biasa yang menjadi korban adalah manusia (makhluk yang bernyawa), dalam *cyberwarfare* yang menjadi korban adalah sistem infrastruktur telekomunikasi dan teknologi suatu negara. Dampak yang di timbulkan oleh *cyberwarfare* dapat lebih serius karena dengan menggangu sistem komputer suatu negara dapat menghentikan seluruh kegiatan perekonomian dan pemerintahan.[276]

---

[275] Richard Clake dalam Max Blumenthal *"International Humanitarian Law on Cyberwarfare"*, Proceedings of The National Conference On Undergraduate Research (NCUR) 2011 Ithaca College, New York 2011

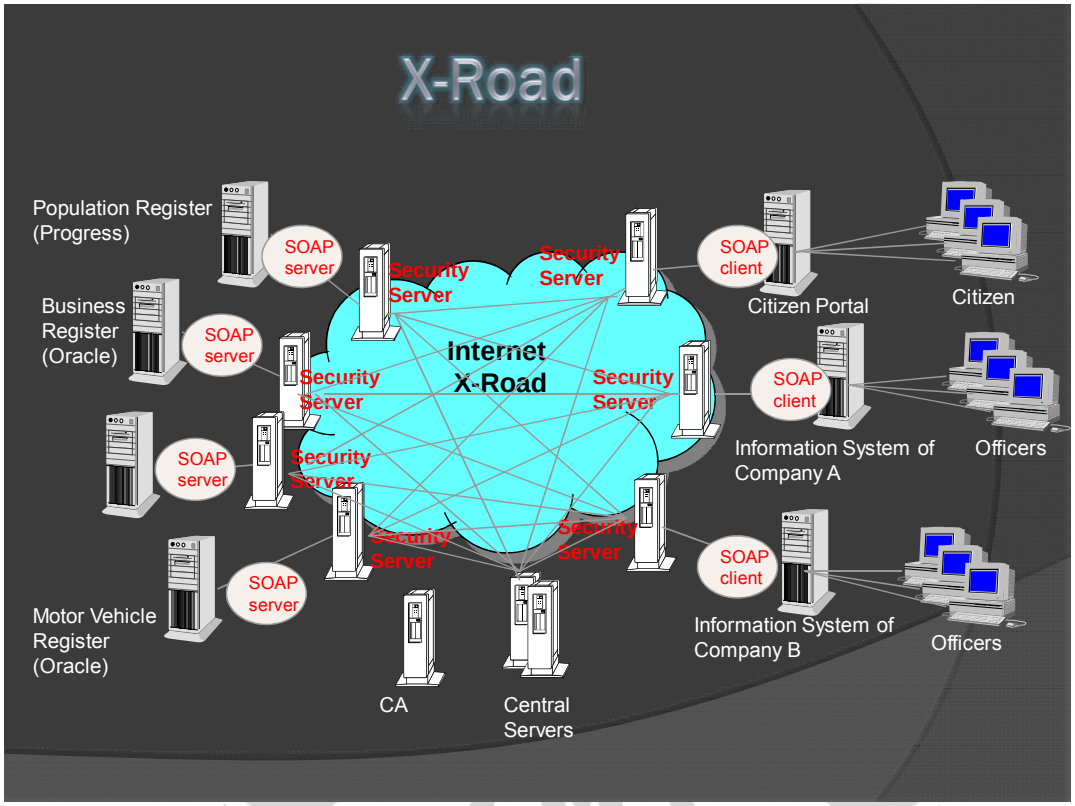
[276] Netherlands Advisory Council of International Affairs Advisory Report No 77,AIV/22, CAVV December 2011, hal 21

2.12.4.1. Kasus *Cyberwarfare* Estonia 2007[277]

Salah satu kasus *cyberwarfare* yang terkenal adalah *cyberwarfare* yang dialami oleh Estonia. Estonia adalah sebuah negara yang terletak di Eropa Utara, negara ini di sebut *wired country* karena maju dalam hal infrastruktur elektronik khususnya yang berkaitan dengan sistem pemerintahan serta merupakan negara pertama yang menerapkan *e-Voting* dalam pemilihan umum pada tahun 2005.

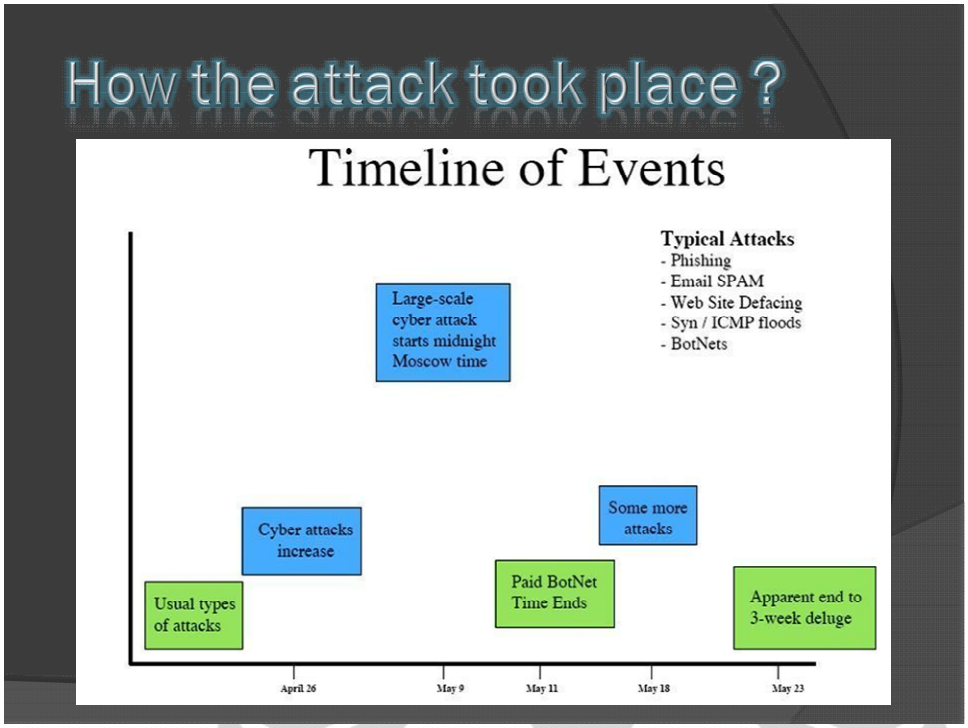
Estonia mulai tahun 2001 mengembangkan sistem interkoneksi data penduduk yang di sebut *X-Road*, dimana setiap warganegaranya bisa mengakses data kependudukan dan bank hanya dengan menggunakan Kartu Tanda Penduduk (KTP) mereka. Sistem ini tersusun atas beberapa bagian (*layer*) dimana setiap bagian memiliki sistem pengamanan tersendiri yang bekerja dari beberapa perangkat *server* yang terpisah. Fungsi dari *server* pengaman ini adalah untuk mengenkripsi dan mengdeenkripsi data, menyimpan informasi (*log*), dan mengamankan data dari *unauthorized users*, adapun koneksi antar *server* pengaman ini di enkripsi dengan *public key infrastructure*. Apabila ada *server* yang rusak maka harus di ganti dengan perstujuan dari *X-Road Certification Authority*. Satu hal lagi yang unik dari *X-Road* ini adalah untuk mencari data kita hanya perlu mengetikkan kode khusus yang di sebut *Simple Object Access Protocol* (SOAP). Cara kerja dari sistem *X-Road* ini bisa di lihat pada gambar 1.

[277] Estonia Cyberattacks 2007 Slide Powerpoint http://africaasia.net/AAF_2009_11_23_Senegal_Dakar/Estonia_cyber_attacks_2007_latest.ppt, diakses tanggal 14 Juni 2012



Gambar 1 Infrastruktur X Road Estonia

Kasus *cyberwarfare* di Estonia ini bermula pada tahun 2007 ketika pemerintah Estonia memindahkan sebuah patung yang merupakan tugu peringatan perang dunia kedua yang didirikan oleh pemerintah Uni Soviet dati Talinn (Ibukota Estonia) ke lokasi yang lebih terpencil. Hal ini membuat pemerintah Estonia di kecam dan berbagai unjuk rasa di gelar baik di Talinn maupun di Moskow (Ibukota Rusia), bahkan Kedutaan Besar Estonia di Moskow di blokade oleh massa. Tidak hanya di dunia nyata (*Real Life*), protes juga bermunculan di dunia maya yang akhirnya berujung kepada serangan siber ke sejumlah situs pemerintah, bank dan sarana umum lainnya pada tanggal 26 April 2007. Serangan ini berlangsung selama tiga minggu. Kronologi seranang siber terhadap Estonia bisa dilihat pada gambar 2.



Gambar 2 Kronologi *cyberattacks* Estonia

Secara garis besar serangan siber di Estonia ini dapat di bagi menjadi tiga bagian

a. Serangan Pertama

Terjadi pada tanggal 27 April 2007, dimana Konstantin Golokov, seorrang aktifis Moldova pro-kremlin mengorganisasikan serangan *Denial of Service* (DDos) terhadap situs pemerintah Estonia dan *Internet Service Provider* (ISP).

b. Serangan Kedua

Terjadi pada tanggal 30 April 2007, situs *livejournal* memposting daftar yang memuat *email* dari seluruh deputi parlemen dan meminta para *user* situs tersebut untuk mengirimkan email secara berulang-ulang, hal ini menyebabkan *server* yang menagani email tersebut jebol dan berhenti beroperasi selama 2 hari.

c. Serangan Ketiga

Terjadi antara tanggal 3 sampai 9 Mei 2007 dimana berbagai situs yang beroperasi di Estonia mengalami *defacing* dengan menggunakan berbagai alat seperti *SQL Injections*

Dampak yang ditimbulkan oleh serangan-serangan ini sungguh luas bagi negara sekecil Estonia, dari segi infrastruktur elektronik dampak yang ditimbulkan adalah:

a) Routers damaged.
b) Routing tables changed.
c) DNS servers overloaded.
d) Email servers mainframes failure, and etc

Sedangkan dari segi pelayanan publik serangan tersebut menyebabkan berhenti beroperasinya:

a) Kantor Kepresidenan dan Parlemen Estonia
b) Semua Kantor Kementrian Estonia
c) Kantor Partai Politik
d) Tiga Kantor Berita
e) Dua Bank Terbesar
f) ISP milik pemerintah
g) Perusahaan Telekomunikasi Pemerintah

Melihat sungguh luasnya dampak yang ditimbulkan oleh *cyberwarfare* yang dilakukan kepada Estonia membuktikan pada kita bahwa *cybercrime* bukan lagi bisa dianggap sebagai kejahatan biasa, namun sudah mencapai tingkatan yang luar biasa. Beberapa ahli berpendapat bahwa *cybercrime* khususnya *cyberwarfare* adalah bentuk

baru dari konflik.[278] Bahkan Netherlands Advisory Council of International Affairs Advisory dalam laporannya tahun 2010 menghubungkan antara *cyberattacks* dengan prinsip *jus ad bellum* dan *jus in bello* yang terdapat dalam Hukum Humaniter Internasional[279] Perdebatan yang muncul saat ini adalah mengenai perlu tidaknya sebuah aturan internasional khusus mengenai *cyberwarfare* dibentuk untuk melindungi korban yang terkena dampak ini seperti yang di atur dalam konvensi Jenewa.

2.12.5. Wacana Pembentukan Makhamah Internasional Khusus *Cybercrime*

Semakin banyaknya kasus *cybercrime* terutama yang bersifat *transboundary* dan kasus *cyberwarfare* Estionia membuat beberapa pihak membuat usulan untuk dibuatnya sebuah lembaga peradilan yang khusus menangani kasus *cybercrime*, pada tahun 2010 ada empat working group yang membahas tentang respon hukum internasional terhadap *cybercrime*, termasuk mekanisme peradilan internasional, empat working grup tersebut adalah:[280]

1) *United Nations Congress on Criminal Prevention and Criminal Justice*, yang di bentuk oleh PBB dimana pertemuan pertamanya di laksanakan di Vienna tanggal 17-21 Januari 2011, dalam pertemuannya mereka mengedepankan topik "*with a view to examening options to strengthen existing and to propose new national and international legal or other responses to cybercrime*"

2) *East West Institute* (EWI), yang beranggotakan ahli-ahli *cybercrime* dan *cybersecurity*, dalam pertemuan pertama mereka di Brussels tanggal 1-2 Oktober 2010 mengetengahkan topik "*develop a consensus-building set of proposals related to international law"*

[278] Jonathan A. Ophard ,*Cyberwarfare and The Crime of Agression : The Need of Individual Accountability on Tomorrow's Battlefield*, Duke Law & Techology Review, 2010, hal 3-6
[279] Netherlands Advisory Council, *op.cit*, hal 20-26
[280] Stein Schjolberg, *op.cit*, hal 4-5

3) Working Group yang di bentuk oleh Amerika-Serikat dan Uni Eropa dalam *US-EU Summit* bulan November 2010 mengedepankan topik *" advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards and become parties."*

4) Working Group yang dibentuk oleh Pertemuan Menteri Hukum dan Jaksa Agung negara Persemakmuran (*commonwealth)* yang membahas mengenai *"review the practical implications of cybercrime in the Commonwealth and identify the most effective means of international co-operation and enforcement, taking in to account, amongst others, the Council of Europe Convention on Cybercrime, without duplicating the work of other international bodies."* Dan juga membahas *"the best practice, educational material and training programme for investigators, prosecutors and judicial officers."*

Dari semua working group diatas ada satu proposal yang cukup menarik untuk di bahas yakini usulan dari Judge Stein Schjolberg dari Norwegia yang muncul pada pertemuan *East West Institiute*. Beliau dengan mantap mengusulkan dibentuknya peradilan internasional khusus *cybercrime* yang disebut *International Court or Tribunal for Cyberspace* (ICTC) bahkan beliau membuat draf konvensi pembentukan ICTC. Adapun yang menjadi argumen utama perlunya dibentuk ICTC adalah bahwa *Cybercrime* dapat digunakan untuk menimbulkan dampak yang serius seperti melumpuhkan infrastruktur telekomunikasi suatu negara.[281] Seperti yang dialami oleh NASDAQ (Bursa saham Amerika Serikat) pada tahun 2010 dimana selama 24 jam situsnya di blok oleh *hacker* dan menimbulkan kepanikan di lantai bursa.[282]

[281] *Ibid*, Hal 7
[282] http://www.huffingtonpost.com/2012/02/14/nasdaq-bats-hacker-attack_n_1277447.html, diakses tanggal 25 Mei 2012

2.12.5.1. Kejahatan Yang Dapat Diadili oleh ICTC dan Yurisdiksi ICTC

Salah satu permasalahan yang serius dalam sebuah peradilan internasional adalah penentuan jurisdiksi apakah sebuah peradilan internasional berwenang untuk mengadili sebuah perkara, namun sebelum menuju ke pembahasan tersebut kita harus melihat apa saja jenis-jenis kejahatan yang dapat diadili di ICTC, dalam draft konvensi pembentukan ICTC dalam pasal 3 dan 4 di sebutkan bahwa kejahatan yang dapat diadili oleh ICTC adalah :[283]

a) illegal access
b) illegal interception
c) data interference
d) system interference
e) misuse of devices
f) forgery
g) fraud
h) offences related to child pornography
i) spam
j) identity theft

Sedangkan untuk permasalahan yurisdiksi ini Judge Schjolberg mengusulkan bahwa kasus yang bisa diadili oleh ICTC hanyalah kasus *cybercrime* yang termasuk :[284]

- Kejahatan yang disebut dalam *Convention on Cybercrime* (Pasal 3 dan 4 yang dijelaskan diatas);
- *Cyberattacks* yang masif dan terkoordinasi untuk menyerang infrastruktur yang penting dan vital dalam telekomunikasi dan informasi. (Pasal 8 Draf Konvensi ICTC)

[283] Schjolberg,*op..cit*,Hal 27
[284] *Ibid*,Hal 18

2.12.5.2. Organ-Organ Dalam ICTC

Dalam draft konvensi ICTC Judge Scholberg juga dengan detail menjabarkan tentang organ-orang yang perlu dibentuk di dalam ICTC tersebut adapun komposisi organ di usulkan oleh Judge Schjoberg:[285]

1. **Judges Chambers**

   Chambers atau perkumpulan hakim adalah badan utama dalam ICTC adapun chambers ini terdiri dari 16 hakim penuh waktu. Adapun hakim-hakim ini harus memiliki karakter dan moral yang baik dan bisa berlaku adil, selain itu mereka harus memiliki pengalaman di bidang hukum internasional dan hukum pidana.[286] Hakim-hakim ini kemudian di bagi-bagi kedalam dua divisi yang terdiri dari :[287]

   a. **Divisi Peradilan Tingkat Pertama**

      Divisi ini terdiri dari 9 hakim, dimana untuk satu kasus dapat di tugaskan minimal 3 hakim untuk menjadi majelis

   b. **Divisi Banding**

      Divisi ini terdiri dari 7 hakim dimana minimal 3 hakim yang dapat di tugaskan untuk menjadi majelis

2. **Jaksa Penuntut**

   Jaksa penuntut memiliki tanggung jawab untuk menuntut setiap kejahatan yang terjadi di *cyberspace* sepanjang sesuai dengan ketentuan di konvensi ini. Jaksa penuntut dipilih oleh Sekretaris Jenderal PBB dan bertugas selama 4 tahun. Jaksa penuntut ini merupakan badan yang terpisah dan bertindak secara independen dari chambers.[288]

---

[285] *Ibid*, Hal 25
[286] *Ibid*, Hal 31
[287] *Ibid*, Hal 30
[288] *Ibid*, Hal 32

3. Panitera

Panitera bertugas untuk menjalankan administrasi dalam ICTC untuk kelancaran sebuah kasus. Panitra dipilih oleh Sekretaris Jenderal PBB dengan rekomendasi dari ketua *chambers* dan bertugas selama 4 tahun.[289]

2.12.5.3. Penyedilikan dan Penyidikan dalam ICTC

Penyelidikan dan penyidikan dalam kasus *cybercrime* apalagi yang bersifat *transboundary* sangatlah sulit terutama terbentur dengan kedaulatan sebuah Negara. Untuk mengatasi hal tersebut Judge Schojlberg mengusulkan untuk mellimpahkan kewanangan tersebut kepada dua badan yaitu:[290]

a.INTERPOL

INTERPOL di yakini sebagai salah satu badan kerjasama internasional yang cukup berhasil untuk pertukaran informasi mengenai pelaku kejahatan. Dalam hal *cybercrime* INTERPOL sejak tahun 1990 secara berkala sudah mengadakan berbagai *working group* di seluruh dunia untuk membahas hal ini, bahkan *working group* di eropa mengambangkan apa yang disebut INTERPOL IT Crime Manual dan INTERPOL juga telah mengambangka sistem pertukaran informasi khusus *cybercrime* yang di sebut I-24/7. Perkembangan terakhir pada tahun 2010 dalam salah satu pertemuannya INTERPOL akan meluncurkan sebuah sistem pertukaran informasi *cybercrime* global yang baru bernama INTERPOL Global Complex (IGC). Kantor pusat IGC ini berada di Singapura dan akan resmi beroperasi pada tahun 2014.[291]

[289] *Ibid*, Hal 33
[290] *Ibid*,Hal 17
[291] *Ibid*, Hal 22

b GVT (*Global Virtual Taskforce*)

GVT adalah sebuah badan independen yang bertugas untuk mengembangkan strategi untuk mencegah *cybercrime*. Badan ini terdiri dari *stakeholder-stakeholder* seperti ahli IT, ekonomi, kalangan akademisi dari seluruh dunia yang dapat berperan untuk mengembangkan strategi dalam menghadapi *cybercrime* yang berkembang sangat cepat. Dalam hal penyelidikan dan penyidikan INTERPOL dapat meminta bantuan kepada GVT untuk memberikan saran atau keterangan mengenai sebuah kasus.

Usulan dari Judge Schjolberg ini sangat menarik untuk dibahas dalam forum yang lebih luas terutama dalam hal jenis-jenis *cybercrime* yang dapat di adili oleh ICTC. Menurut penulis alangkah baiknya untuk memasukkan pasal yang spesifik mengenai *cyberwarfare* karena rumusan pasal 8 dalam draft konvensi ini masih bersifat luas dan berpotensi menimbulkan penafsiran yang berbeda-beda.

Bab 3

Hasil Penelitian dan Analisa

3.1. Sejarah pengaturan mengenai *Cybercrime* di Indonesia

Apabila kita berbicara mengenai peraturan perundang-undangan yang mengatur tentang *cybercrime* di Indonesia, bisa dibilang kita masih sangat tertinggal karena baru satu peraturan yang mengatur secara spesifik mengenai *cybercrime*, yaitu Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Pada awalnya hanya ada pengaturan mengenai telekomunikasi melalui Undang-Undang No. 3 tahun 1989 yang kemudian diamandemen dengan dikeluarkannya Undang-Undang No. 36 Tahun 1999 tentang hal yang sama. Setelah itu perkembangan peraturan yang mengatur mengenai *cybercrime* terus berkembang.

Untuk memudahkan pemahaman maka pembahasan akan dibagi menjadi dua bagian yaitu :

1. Sebelum berlakunya UU Informasi dan Transaksi Elektronik.
2. Sesudah berlakunya UU Informasi dan Transaksi Elektronik.

3.1.1. Sebelum Berlakunya Undang-Undang Informasi dan Transaksi Elektronik

Pada pembahasan ini penulis akan fokus kepada Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi. Alasan kenapa penulis hanya akan fokus kepada satu undang-undang karena undang-undang ini adalah merupakan undang-undang pertama yang mengatur tentang *cybercrime*.

3.1.1.1 Undang-Undang Telekomunikasi

Undang-undang ini mengatur tentang segala hal mengenai telekomunikasi. Hal yang pertama kali diatur dalam undang-undang ini adalah tentang siapa saja yang berhak menyelenggarakan telekomunikasi sesuai dengan peruntukkannya, pihak-pihak yang berhak menyelenggarakan komunikasi adalah :[292]

1. Penyelenggara Jasa Telekomunikasi

Penyelenggara jasa telekomunikasi adalah penyelenggaraan telekomunikasi untuk memenuhi kebutuhan masyarakat. Badan penyelenggara untuk jasa telekomunikasi dalam negeri (domestik) adalah PT. Telkom dan Badan Penyelenggara untuk jasa telekomunikasi luar negeri (internasional) adalah PT. Indosat. Badan Usaha Milik Negara tersebut diberi wewenang untuk yang menyelenggarakan jasa telekomunikasi, seperti telepon, telex, faksimili, dan sebagainya, maupun jasa telekomunikasi berupa jasa-jasa nilai tambah (*value added service*). Badan lain di luar badan penyelenggara, baik dalam bentuk Badan Usaha Milik Swasta (BUMS), Badan Usaha Milik Daerah (BUMD) maupun Koperasi juga berhak untuk menyelenggarakan jasa telekomunikasi non dasar. Sedang untuk menyelenggarakan jasa telekomunikasi dasar, badan lain dapat bekerjasama dengan PT Telkom dan atau PT Indosat. Bentuk kerjasama antara badan penyelenggara dan badan lain ini telah diatur dalam Peraturan Pemerintah Nomor 8 tahun 1993, yaitu dapat berbentuk Kerjasama Operasi (KSO), usaha patungan dan kontrak manajemen.

2. Penyelenggaraan Telekomunikasi untuk Keperluan Khusus

Penyelenggaraan telekomunikasi untuk keperluan khusus adalah penyelenggaraan telekomunikasi yang dilakukan oleh instansi pemerintah tertentu, perorangan atau badan hukum untuk keperluan khusus atau untuk keperluan sendiri.Telekomunikasi khusus dapat dilakukan oleh instansi pemerintah tertentu atau badan hukum (perseroan terbatas atau koperasi) yang ditentukan berdasarkan hukum.

[292] Indonesia Undang-Undang No. 36 Tahun 1999, Pasal 8-10.

Telekomunikasi khusus diselenggarakan berdasarkan ijin yang ditetapkan oleh Direktur Jenderal Pos dan Telekomunikasi.
Ijin penyelenggaraan telekomunikasi khusus hanya diberikan Badan Hukum apabila wilayah tersebut belum tersedia atau belum terjangkau fasilitas telekomunikasi yang dapat disediakan oleh badan penyelenggara atau badan lain.Telekomunikasi untuk keperluan khusus hanya dapat diselenggarakan dengan mempertimbangkan kerahasiaan dan jangkauan atau pengoperasiannya perlu bentuk sendiri. Penyelenggara telekomunikasi untuk keperluan khusus adalah Instansi pemerintah tertentu untuk pelaksanaan tugas khusus, perseorangan atau, badan hukum.

3. Penyelenggaraan Telekomunikasi untuk Keperluan Pertahanan dan Keamanan

Berdasarkan Peraturan Pemerintah Nomor. 4 tahun 1992 tentang Penyelenggaraan Telekomunikasi untuk Keperluan Pertahanan dan Keamanan Negara diatur bahwa penyelenggaraan telekomunikasi untuk keperluan pertahanan dan keamanan negara (Hankamneg) diselenggarakan oleh Dephankam dan/atau ABRI. Penyelenggaraan diperuntukan bagi pertahanan keamanan negara bukan merupakan penyelenggaraan jasa telekomunikasi.

Undang-undang ini merupakan amandemen dari undang-undang sebelumnya, yaitu UU No 3 tahun 1989 dan menjadi undang-undang pertama yang memasukkan *cybercrime* sebagai salah satu pelanggaran di dalam bidang telekomunikasi. Pengaturan mengenai *cybercrime* pada undang-undang ini diatur dalam Pasal 38 dan Pasal 40 yang berbunyi[293]

[293]*Ibid.*, Pasal 38 dan 40.

Pasal 38

"Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi".

Pasal 40 :

"*Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melaiui jaringan telekomunikasi dalam bentuk apapun*"

Berdasarkan penjelasan Pasal 38 perbuatan yang dapat digolongkan sebagai perbuatan yang dapat menyebabkan ganguan telekomunikasi adalah :[294]

a. Tindakan fisik yang dapat menimbulkan kerusakan suatu jaringan telekomunikasi sehingga jaringan tersebut tidak dapat berfungsi sebagaimana mestinya;
b. Tindakan fisik yang menyebabkan hubungan telekomunikasi tidak berjalan sebagaimana mestinya;
c. Penggunaan alat telekomunikasi yang tidak sesuai dengan persyaratan teknis yang berlaku;
d. Penggunaan alat telekomunikasi yang bekerja dengan gelombang radio yang tidak sebagaimana mestinya sehingga menimbulkan gangguan terhadap penyelengaraan telekomunikasi lainnya;
e. Penggunaan alat bukan telekomunikasi yang tidak sebagaimana mestinya sehingga menimbulkan pengaruh teknis yang tidak dikehendaki suatu penyelenggaraan telekomunikasi.

[294]*Ibid.*, Penjelasan Pasal 38.

Sedangkan menurut penjelasan Pasal 40 yang dimaksud dengan *Cyberspy* adalah ”**kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah**”[295]

Dari penjelasan pasal 38 dan 40 tersebut dapat kita simpulkan bahwa yang diatur dalam undang-undang ini adalah salah satu perbuatan yang termasuk dalam kategori *cybercrime* yaitu *illegal interception*[296] terhadap kegiatan telekomunikasi yang mengakibatkan proses telekomunikasi menjadi terhambat.

Mengenai pengaturan tentang yurisdiksi dalam undang-undang ini tidak disebutkan secara gamblang pada pasal tertentu, namun dari pengaturan Pasal 44 dapat disimpulkan bahwa apabila terjadi pelanggaran terhadap gangguan telekomunikasi maka yang diterapkan adalah hukum Indonesia. Bunyi Pasal 44 adalah :[297]

i. *Selain Penyidik Pejabat Polisi Negara Republik Indonesia, juga Pejabat Pegawai Negeri Sipil tertentu di Iingkungan Departemen yang Iingkup tugas dan tanggung jawabnya di bidang telekomunikasi, diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-undang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang telekomunikasi.*

ii. *Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang :*
    a. *melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang telekomunikasi;*
    b. *melakukan pemeriksaan terhadap orang dan atau badan hukum yang diduga melakukan tindak pidana di bidang telekomunikasi;*

[295] *Ibid.*, Penjelasan Pasal 40.
[296] Cybercrime Convention , Article 3, lihat juga pendapat dari Goodman & Brenner, GIPI dalam Bab 2 tulisan ini.
[297] Indonesia, *loc.cit*, Pasal 44.

c. *menghentikan penggunaan alat dan atau perangkat telekomunikasi yang menyimpang dari ketentuan yang berlaku;*
d. *memanggil orang untuk didengar dan diperiksa sebagai saksi atau tersangka;*
e. *melakukan pemeriksaan alat dan atau perangkat telekomunikasi yang diduga digunakan atau diduga berkaitan dengan tindak pidana di bidang telekomunikasi;*
f. *menggeledah tempat yang diduga digunakan untuk melakukan tindak pidana di bidang telekomunikasi;*
g. *menyegel dan atau menyita alat dan atau perangkat telekomunikasi yang digunakan atau yang diduga berkaitan dengan tindak pidana di bidang telekomunikasi;*
h. *meminta bantuan ahli dalam rangka pelaksanaan tugas penyidikan tindak pidana di bidang telekomunikasi;*
i. *mengadakan penghentian penyidikan*

iii. *Kewenangan penyidikan sebagaimana dimaksud pada ayat (2) diliaksanakan sesuai dengan ketentuan undang-undang Hukum Acara Pidana*

Dari pengaturan tentang yurisdiksi diatas maka dapat disimpulkan bahwa undang-undang ini menganut prinsip *objective territoriality* (teritorial objektif), hal ini bisa dilihat dari perumusan Pasal 38 yang menyatakan bahwa setiap orang dilarang untuk melakukan perbuatan yang dapat menggangu komunikasi. Berarti yang dilihat dari Pasal ini adalah akibat dari perbuatan yang dapat mengakibatkan terganggunya komunikasi tanpa melihat tempat dilakukannya kejahatan tersebut.[298]

3.2. Sesudah Berlakunya Undang-Undang Informasi dan Transaksi Elektronik

Dalam sub-bab ini dijelaskan mengenai peraturan yang mengatur mengenai *cybercrime* sesudah berlakunya UU ITE. Secara spesifik akan difokuskan pada pembahasan terhadap dua undang-undang, yaitu :

[298] J.G Starke, *.op cit*, hal 184.

1. Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
2. Undang-Undang No 14 Tahun 2008 tentang Keterbukaan Informasi Publik
3.

3.2.1. Undang-Undang Informasi dan Transaksi Elektronik

Secara umum Undang-Undang ini mengatur tentang segala sesuatu mengenai data elektronik dan pemanfaatannya untuk kepentingan umum. Pada awal pembentukkannya 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 di atur dalam Pasal 27 sampai Pasal 37. Hanya saja untuk pembahasan ini akan dijelaskan beberapa pasal yang terkait dengan *Covention on Cybercrime*. Pasal-pasal tersebut berbunyi :

Pasal 27

i. *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.*

ii. *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.*

iii. *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.*

iv. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 27 memiliki tiga unsur yang sama yaitu unsur setiap orang, unsur dengan sengaja dan tanpa hak, dan unsur mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan atau Dokumen Elektronik. Ayat yang perlu diperhatikan adalah ayat (3) karena hal ini bisa mengakibatkan seorang pengguna internet atau Blogger dapat dituduh mencemarkan nama baik.[299] Seperti yang dialami oleh seorang ibu rumah tangga bernama Prita Mulyasari yang sempat ditahan hanya gara-gara menuliskan sebuah surat pembaca di salah satu forum di internet.[300] Karena surat pembaca ini Prita dilaporkan ke polisi karena dituduh mencemarkan nama baik Rumah Sakit OMNI Internsional dalam dakwaan yang dibacakan di Pengadilan Negeri Tangerang Jaksa penuntut umum membidik Prita dengan tiga dakwaan alternatif. Pertama, Prita dijerat dengan Pasal 45 Ayat (1) jo Pasal 27 Ayat (3) UU ITE.[301]Sementara untuk dakwaan kedua dan ketiga, jaksa menggunakan KUHP, yaitu Pasal 310 Ayat (2) dan 311 Ayat (1). Ketiga pasal dalam dakwaan itu mengatur masalah pencemaran nama baik dan penghinaan.[302]

---

[299] Anggara, UU ITE merupakan ancaman bagi bloger indonesia, <http://anggara.org/2008/03/26/uu-informasi-dan-transaksi-elektronik-adalah-ancaman-serius-bagi-bolger-indonesia/>, diakses tanggal 1 Juni 2012.

[300]RS OMNI dapatkan pasien dari hasil lab fiktif, <http://suarapembaca.detik.com/read/2008/08/30/111736/997265/283/rs-omni-dapatkan-pasien-dari-hasil-lab-fiktif >, diakses tanggal 2 Juni 2012.

[301] Pasal 45 ayat UU ITE berbunyi :

i. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

ii. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

iii. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

[302]Prita Mulyasari Hari Ini Didakwa , www.hukumonline.com, diakses pada tanggal 31 Mei 2012.

Kelanjutan dari kasus ini adalah hakim telah menerima eksepsi dari pihak Prita dan membebaskan Prita dari segala tuntutan.

Pasal 28

i. *Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.*

ii. *Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).*

Pasal 28 memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, unsur menyebarkan. Sama seperti pasal sebelumnya, yang membedakannya hanyalah isi dari apa yang disebarkan. Pada ayat (1) yang disebarkan adalah informasi yang dapat mengakibatkan kerugian konsumen, sedangkan pada ayat (2) yang disebarkan adalah informasi yang berisi SARA dengan tujuan untuk menimbulkan kebencian atau permusuhan. Pasal ini juga krusial bagi seorang pengguna internet karena dengan mudahnya seorang pengguna internet melakukan tindakan tersebut baik secara langsung maupun tidak langsung.[303]

Pasal 30

i. *Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.*

ii. *Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun*

[303] Anggara, *op.cit.*

dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik

iii. *Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.*

Pasal ini memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, dan unsur mengakses komputer atau sistem elektronik. Dapat disimpulkan bahwa Pasal ini mengatur tentang larangan setiap orang untuk tidak melakukan *illegal access* dengan cara apapun (*hacking, cracking* maupun *cyber trespassing*). Sama seperti yang diatur dalam *Convention on Cybercrime* dalam pasal 2[304] yang dimaksud dengan *access* yang dimaksud meliputi kegiatan memasuki sistem komputer lainnya baik yang terkoneksi melalui jaringan komunikasi umum, tatu terhadap suatu sistem komputer pada jaringan yang sama seperti pada suatu *Local Area Network* (LAN) atau *intranet* dalam suatu organisasi. Cara komunikasi yang dilakukan baik dari satu lokasi tertentu dengan cara *remote* maupun dengan penghubung *wireless* pada jarak yang dekat tidak masalah.[305]

Pasal 31

i. *Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau*

[304] Pasal 2 *Convention on Cybercrime*, yang berbunyi :

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

[305] Council of Europe, *.op cit*., Poin 46.

Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

ii. *Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.*

iii. *Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang - undang.*

iv. *Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.*

Pasal ini memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, dan unsur melakukan intersepsi atau penyadapan atas sebuah komputer atau sistem elektronik. Dapat disimpulkan bahwa pasal ini melarang setiap orang untuk melakukan *illegal interception*. Maksud dari Pasal ini sama dengan yang diatur dalam Pasal 3 *Convention on Cybercrime*.[306] Salah satu bagian dari pelanggaran yang dimaksud dari ketentuan pasal ini adalah melakukan penahanan komunikasi atau

[306]Pasal 3 *Cybercrime Convention*, yang berbunyi :

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."*

menghambat proses komunikasi dengan menggunakan perangkat elektronik untuk mendengarkan pembicaraan orang lain atau menggunakan peralatan untuk menyadap komunikasi. Klasifikasi ini hanya berlaku pada komunikasi data komputer yang dilakukan secara pribadi, klasifikasi ketentuan ini mengacu pada sifat pemindahan dan sifat dari data yang dipindahkan. Komunikasi yang terjadi dapat melalui hubungan dari komputer ke *printer*, antara dua komputer atau dari orang ke komputer itu sendiri (seperti mengetik dengan *keyboard*).[307]

Pasal 32

i. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Pasal ini memiliki unsur setiap orang, unsur dengan sengaja, unsur tanpa hak, unsur mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik. Dapat disimpulkan bahwa pasal ini mengatur tentang larangan untuk melakukan *data interception* seperti yang diatur dalam Pasal 4 *Convention on Cybercrime.*[308] Ketentuan yang diatur dalam pasal ini berusaha untuk memberi jaminan bahwa data yang dikirimkan melaui jaringan internet atau pemindahan data yang dilakukan melaui suatu jaringan adalah sama dengan data yang dikirimkan oleh si pengirim. Kepentingan perlindungan hukum dalam pasal ini adalah keutuhan dan berfungsi

[307] Keyser, .*loc cit*., hal 301.

[308] Pasal 4 *Cybercrime Convention* yang berbunyi :

i. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

ii. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

sebagaimana mestinya penggunaan data komputer yang tersimpan atau program-program komputer.[309]

Mengenai yurisdiksi dalam undang-undang ini diatur dalam Pasal 2, yang berbunyi :

> *"Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang‐Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia"*

Dari perumusan pasal diatas dapat disimpulkan bahwa undang-undang ini menganut prinsip *objective territoriality* (teritorial objektif) karena yang lebih dilihat adalah akibat dari perbuatan yang ditimbulkan karena perbuatan yang di sebutkan dalam pasal-pasal tersebut

3.2.2. Undang-Undang Keterbukaan Informasi Publik

Dalam undang-undang ini terdapat ketentuan yang dapat dilihat sebagai suatu *cybercrime*. Hal ini berlaku apabila sebuah informasi publik di sebarkan melalui publik di sebarkan melalui *cyberspace*. Pasal-pasal tersebut adalah :[310]

Pasal 54

ii. *Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf a, huruf b, huruf d, huruf f, huruf g, huruf h, huruf i, dan huruf j dipidana dengan pidana penjara paling lama 2 (dua)*

[309] Council of Europe,.*op cit.* Poin 60
[310] Indonesia UU No 14 Tahun 2008, pasal 54-55

tahun dan pidana denda paling banyak Rp10.000.000,00 (sepuluh juta rupiah).

iii. *Setiap Orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf c dan huruf e, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp20.000.000,00 (dua puluh juta rupiah).*

Pasal 55

i. *Setiap Orang yang dengan sengaja membuat Informasi Publik yang tidak benar atau menyesatkan dan mengakibatkan kerugian bagi orang lain dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau denda paling banyak Rp5.000.000,00 (lima juta rupiah).*

Dalam pasa-pasal ini jika kita kaitkan dengan jenis-jenis *cybercrime* menurut *Convention on Cybercrime* maka terdapat dua perbuatan yaitu, *illegal access*[311] yang terdapat dalam pasal 54 yang melarang setiap orang yang tanpa hak mengakses informasi publik yang tidak seharusnya dia peroleh. Perbuatan selanjutnya yang termasuk *cybercrime* adalah *data interception*[312] yang diatur dalam pasal 55 yang

[311]Pasal 3 *Cybercrime Convention*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

[312] Pasal 4 *Cybercrime Convention* yang berbunyi :

i. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
ii. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

melarang setiap orang untuk membuat sebuah informasi publik yang tidak benar dengan cara apapun.

3.3. Statistik Kasus Cybercrime yang ditangani di Indonesia

Cybercrime telah dikenal secara internasional sebagai ruang umum kelima setelah darat, laut, udara dan ruang angkasa, oleh karena itu dalam pemikiran internasional sangat dibutuhkan langkah-langkah koordinasi, kerja sama dan hukum diantara semua bangsa untuk menyadarkan masyarakat internasional bahwa perlunya tanggapan global global atas ancaman *cybercrime* yang bersifat global. Ancaman *cybercrime* di dunia maya bersifat masif dan terkoordinasi dalam menyerang infrastruktur komunikasi dan informasi vital negara-negara, sehingga diperlukan segera respon dunia internasional untuk mengatasi *cybercrime* guna mewujudkan perdamaian , keadilan dan keamanan.

Semua negara setidaknya pernah mengalami *cyberattack* atau serangan di dunia maya baik yang kecil maupun besar, termasuk di Indonesia yang berpenduduk 150 juta orang, perkembangan dunia teknologi informasi terutama internet yang saat ini sudah dapat di akses di sebagian besar wilayah Indonesia dengan menggunakan kabel fiber optik, jaringan nirkabel baik melalui jaringan *Wireless Fidelity* (Wi-Fi) maupun modem, membuat semua orang rentan untuk mengalami *cybercrime*. Kasus *cybercrime* di Indonesia sudah mucul sejak lama dan trennya semakin meningkat, hal ini bisa dilihat dalam tabel-tabel dibawah ini:

Tabel 1. Data Penangananan Perkara *Cybercrime* di POLDA Metro Jaya Tahun 2006

No	Jenis Kejahatan	P21	SP3	Dilimpahkan	Proses	Jumlah
1	Pelanggaran Hak Cipta	3	2	0	1	6
2	Pelanggaran UU Telekomunikasi	1	1	0	1	3
3	Pencemaran Nama	1	5	0	1	7

	Baik via Internet					
4	Pencurian Data	0	1	0	1	2
5	Penggelapan via Internet	0	0	0	2	2
6	Penipuan via Internet	3	9	2	3	17
7	Permusuhan di Muka Umum	1	0	0	0	1
	Total	9	18	2	9	38

Tabel 2. Data Penangananan Perkara *Cybercrime* di POLDA Metro Jaya Tahun 2007

No	Jenis Kejahatan	P21	SP3	Dilimpahkan	Proses	Jumlah
1	Ancaman via SMS	0	0	0	1	1
2	Kejahatan Keusilaan	0	0	0	2	2
3	Pelanggaran Hak Cipta	3	0	0	1	4
4	Pelanggaran UU Telekomunikasi	0	0	0	1	1
5	Pencemaran Nama Baik via Internet	1	3	0	1	5
6	Pencurian Data	1	2	1	1	5
7	Penggelapan via Internet	0	0	0	1	1
8	Penipuan	0	1	1	2	4
9	Perbuatan Tidak	0	0	4	1	5

	Menyenangkan via Internet					
10	Perjudian via Internet	2	0	0	0	2
	Total	7	6	6	11	30

Komentar:

Pada dua tabel pertama yang memuat data penanganan kasus *cybercrime* tahun 2006 dan 2007 dapat disimpulkan jika kasus *cybercrime* di Indonesia sudah mulai berkembang, namun penangananya belum terlalu maksimal karena setiap kasus yang di proses masih menggunakan KUHP sebagai dasar hukumnya dikarenakan UU ITE pada saat itu masih berupa RUU dan belum berlaku.

Tabel 3. Data Penangananan Perkara *Cybercrime* di POLDA Metro Jaya Tahun 2008

No	Jenis Kejahatan	P21	SP3	Dilimpahkan	Proses	Jumlah
1	Memudahkan Pencabulan	1	0	0	1	1
2	Pelanggaran Hak Cipta	1	2	0	3	6
3	Pelanggaran UU Telekomunikasi	0	0	0	1	1
4	Pemalsuan	0	0	0	2	2
5	Pencemaran Nama Baik	0	5	0	11	16
6	Pencurian Data	0	0	0	6	6
7	Penghinaan	0	1	0	0	1
8	Penipuan	0	2	1	17	20

9	Penipuan via Internet (*cyberfraud)*	4	0	0	5	9
10	Perbuatan Tidak Menyenangkan	0	0	2	1	3
11	Penyadapan Telepon	0	0	0	1	1
12	Perjudian via Internet	1	0	0	0	1
	Total	7	10	3	48	67

Komentar:

Berdasarkan tabel diatas pada tahun 2008 yang merupakan tahun dimana UU ITE sudah mulai berlaku, jumlah yang melaporkan kasus *cybercrime* semakin banyak dan mencapai puncaknya, hal ini di sebabkan para korban merasa optimis dengan adanya UU ITE kasus mereka bisa diselesaikan

Tabel 4. Data Penangananan Perkara *Cybercrime* di POLDA Metro Jaya Tahun 2009

No	Jenis Kejahatan	P21	SP3	Dilimpahkan	Proses	Jumlah
1	Melampaui dan Menjebol Sistem Pengamanan	0	0	0	1	1
2	Melanggar Kesusilaan via Internet	0	0	0	1	1
3	Pencemaran Nama Baik via Internet	0	0	0	11	11

4	Pengancaman Melalui email	0	0	0	1	1
5	Pengerusakan Situs Berita	0	0	0	1	1
6	Penipuan via Internet	0	0	0	10	10
	Total	0	0	0	25	25

Komentar:

Pada tahun 2009 memang jumlah pelapor tidak sebanyak tahun 2008, namun yang harus menjadi perhatian adalah semakin kompleksnya kasus yang terjadi seperti merusak situs berita (*defacing*) dan menjebol dan melampaui sistem pengamanan (*cracking*)

Tabel 5 Data Penanganan Perkara *cybercrime* di POLDA Metro Jaya Tahun 2010

NO	JENIS KEJAHATAN	P21	SP3	DILIMPAH	PROSES	JUMLAH
1	Kejahatan terhadap Kesusilaan dan Kesopanan	0	0	0	1	1
2	Pemalsuan dokumen	0	0	0	2	2
3	Pencemaran nama baik melalui internet	0	0	3	9	12
4	Pencurian data email	0	0	0	2	2
5	Pencurian pulsa	0	0	0	1	1
6	Penipuan melalui internet	0	0	0	15	15

7	Penghinaan melalui internet	0	0	0	1	1
8	Percabulan via internet	0	0	0	1	1
9	Penjebolan email / Penggunaan email tanpa ijin pemilik	0	0	0	1	1
	Total	0	0	3	**33**	**36**

Tabel 6 Penanganan Kasus *Cybercrime* di Polda Metro Jaya Tahun 2011

No	Jenis Kejahatan	P21	SP3	Dilimpahkan	Proses	Jumlah
1	Pencurian Data					40
2	Penipuan (Internet & Ponsel)					310
3	Penggelapan					9
4	Pemalsuan Data/Situs					27
5	Pelanggaran UU Hak Cipta					5
6	Pelanggaran UU Telekomunikasi					10
7	Pencemaran Nama Baik Melalui Internet					75
8	Kejahatan Keusilaan					12
9	Perbuatan Tidak Menyenangkan (Internet & Ponsel)					21
10	Pengancaman Melalui Internet					12
	Total	46	112	289	648	521

3.4. Kasus *Cybercrime* yang melibatkan Warganegara Asing di Indonesia serta Analisa Kasus

Meskipun banyak kasus *cybercrime* yang terjadi di Indonesia, namun kasus *cybercrime* yang melibatkan warganegara asing yang masuk ke kepolisian dapat

dihitung dengan jari. Dalam tulisan ini penulis akan mengangkat dua kasus *cybercrime* yang melibatkan Warganegara asing di Indonesia. Dalam analisa kasus yang akan dipaparkan, penulis akan melakukan analisa penentuan yurisdiksi berdasarkan doktrin yang telah di jelaskan dalam bab sebelumnya

3.4.1. Kasus Penipuan "Mama Minta Pulsa" (Pelaku :Warganegara China dan Taiwan)

Kasus ini mencuat pada tahun 2011, dimana Badan Reserse Kriminal (Bareskrim) Polri, berhasil membekuk 170 Warganegara Asing yang terdiri dari 73 Warganegara China dan 97 Warganegara Taiwan di sebuah rumah di Kawasan Bumi Serpong Damai ,Tangerang.[313] Setelah di telusuri lebih jauh ternyata mereka melakukan berbagai macam penipuan, termasuk penipuan via SMS "mama minta pulsa", adapun modus kejahatan ini adalah dengan berpura-pura mengirimkan SMS yang seolah-olah pelaku adalah Mama/Ibu dari korban biasanya isi SMSnya adalah seperti dibawah ini:

"**Beliin dulu mama pulsa As 20rb di nomor baru mama, ini nomor nya 085294176xxx secepatnya penting sekali, nanti mama ganti uang nya sekarang mama tunggu** "

Jika tidak sadar korban yang mengira bahwa itu benar-benar Mama/Ibunya akan langsung mentransfer pulsa yang di inginkan kepada nomor tersebut, ketika di cek kepada Mama/Ibu korban,korban akan sadar kalau sudah tertipu. Langkah yang diambil oleh Kepolisian Republik Indonesia dalam menyelsaikan kasus ini adalah dengan menyerahkan kasus tersebut ke Imigrasi untuk mendeportasi para pelaku.[314]

[313] http://news.detik.com/read/2011/06/09/211211/1657155/10/wna-yang-ditangkap-kasus-cybercrime-capai-177-orang?nd992203605, diakses tanggal 3 Juni 2012
[314] http://news.detik.com/read/2011/06/10/113324/1657463/10/177-wna-pelaku-scamming-akan-dideportasi-sabtu?nd992203605, diakses tanggal 4 Juni 2012

Analisa Kasus

1) Tempat Kejahatan Dilakukan

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN China dan WN Taiwan melakukan kejahatan mereka di Indonesia

2) Tempat Dimana Pelaku Ditangkap

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN China dan WN Taiwan berhasil ditangkap di Indonesia, tepatnya di BSD, Tangerang

3) Akibat

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN China dan WN Taiwan akibat kejahatan yang pelaku lakukan terbesar berada di Indonesia

4) Nasionalitas (kewarganegaraan)

a.Kewarganegaraan Korban

Dalam kasus penipuan "mama minta pulsa" korban yang melapor lebih banyak WN Indonesia

b.Kewarganegaraan Pelaku

Dalam kasus penipuan "mama minta pulsa" pelaku adalah WN China dan WN Taiwan

5) Kekuatan Dari Kasus Tersebut

Dalam kasus penipuan "mama minta pulsa" kekuatan dari kasus tersebut berada di Indonesia karena bukti, akibat dan korban berada di Indonesia.

6) Pemidanaan

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN China dan WN Taiwan, penulis tidak dapat menemukan peraturan baik dari China dan Taiwan yang mengatur mengenai lamanya hukuman untuk penipuan, oleh karena itu penulis berasumsi jika lamanya pidana yang di ancamkan kepada pelaku di Indonesia lebih berat daripada di China dan Taiwan

7) Keadilan dan Kenyamanan

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN China dan WN Taiwan melakukan kejahtan mereka di Indonesia jadi demi keadilan maka pelaku harus diadili di Indonesia, juga dari segi kenyamanan saksi yang lebih mudah di hadirkan karena persidangan yang berlangsung di Indonesia

3.4.2. Kasus Penipuan *Online* (Pelaku :Warganegara Nigeria dan Kamerun)

Kasus ini terjadi tahun 2009 dimana pelaku yang terdiri dari David (WN Nigeria), Timoty (WN Nigeria), dan Phillip (WN Kamerun) berusaha melakukan *email scamming* (penipuan melalui email) dengan cara mengirmkan email kepada calon korbannya yang isinya bahwa mereka telah memenangkan uang $1.000.000 (Satu Juta Dollar) yang diadakan oleh Yahoo!. Drs. M Oda Sugarda, yang menjadi korban menyatakan jika pelaku mengharuskan ia membayar uang sejumlah Rp 462.108.048(Empat Ratus Juta Seratus Delapan Ribu Empat Puluh Delapan Rupiah) untuk biaya pengurusan bank, notaris, pengacara dan asuransi.[315] Namun setelah korban mentransfer uang tersebut hadiah tidak kunjung diterima, tapi pada 4 Maret 2011, pelaku menghubungi korban untuk membicarakan penyerahan *cash-box* hadiah yang akan diterima korban, setelah mengadakan pertemuan di salah satu mall di Jakarta Utara, korban yang merasa curiga karena tidak melihat *cash-box* yang

[315] http://jakarta.tribunnews.com/2012/03/20/menipu-via-online-3-wna-ditangkap, diakses tanggal 4 Juni 2012

dijanjikan melapor ke sekuriti mal dan pelaku di bawa ke Polsek Kelapa Gading.[316] Kasus ini masih ditangani oleh Polsek Kelapa Gading.

Analisa:

1) Tempat Kejahatan Dilakukan

Dalam kasus penipuan email pelaku yang terdiri dari WN Nigeria dan WN Kamerun melakukan kejahatan mereka di Indonesia

2) Tempat Dimana Pelaku Ditangkap

Dalam kasus penipuan email pelaku yang terdiri dari WN Nigeria dan WN Kamerun berhasil ditangkap di Indonesia, tepatnya di Jakarta Utara

3) Akibat

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN Nigeria dan WN Kamerun akibat kejahatan yang pelaku lakukan terbesar berada di Indonesia

4) Nasionalitas (kewarganegaraan)

a.Kewarganegaraan Korban

Dalam kasus penipuan email korban adalah WN Indonesia

b.Kewarganegaraan Pelaku

Dalam kasus penipuan email pelaku adalah WN Nigeria dan WN Kamerun

[316] http://www.merdeka.com/peristiwa/3-wn-afrika-tipu-wni-rp-462-juta.html, diakses tanggal 4 Juni 2012

5) Kekuatan Dari Kasus Tersebut

Dalam kasus penipuan email kekuatan kasus tersebut adalah di Indonesia karean bukti, akibat dan korban berada di Indonesia.

6) Pemidanaan

Dalam kasus penipuan email pelaku yang terdiri dari WN Nigeria dan WN Kamerun, penulis tidak dapat menemukan peraturan baik dari Nigeria dan Kamerun yang mengatur mengenai lamanya hukuman untuk penipuan, oleh karena itu penulis berasumsi jika lamanya pidana yang di ancamkan kepada pelaku di Indonesia lebih berat daripada di Nigeria dan Kamerun

7) Keadilan dan Kenyamanan

Dalam kasus penipuan "mama minta pulsa" pelaku yang terdiri dari WN Nigeria dan WN Kamerun melakukan kejahtan mereka di Indonesia jadi demi keadilan maka pelaku jarud diadili di Indonesia, juga dari segi kenyamanan saksi yang lebih mudah di hadirkan karena persidangan yang berlangsung di Indonesia

Untuk lebih memudahkan pembaca memahami hubungan komponen dengan kasus di atas maka penulis akan memaparkannya dalam bentuk tabel di bawah ini

Tabel 5 Hubungan Komponen Penentuan Yurisdiksi dengan Kasus *Cybercrime* di Indonesia

No	Komponen	Kasus 1:	Kasus 2 :
		Penipuan Mama Minta Pulsa (Pelaku :WN China & Taiwan)	Kasus Penipuan email (Pelaku : WN Nigeria & Kamerun)
1	Tempat Dilaksanakannya Kejahatan	Indonesia	Indonesia

2	Tempat Pelaku Ditangkap	Indonesia	Indonesia
3	Akibat	Indonesia	Indonesia
4	Nasionalitas Pelaku: Korban:	 China & Taiwan Indonesia	 Nigeria & Kamerun Indonesia
5	Kekuatan dari Kasus	Indonesia	Indonesia
6	Pemidanaan	Indonesia: Maksimal 6 Tahun China :N/A Taiwan :N/A	Indonesia: Maksimal 6 Tahun Nigeria :N/A Kamerun :N/A
7	Imparsialitas dan Kenyamanan	Indonesia	Indonesia
	Penyelesaian	Deportasi	Proses

3.5. *Transfer of Proceeding* dalam kasus *Transboundary Cybercrime*

Seperti yang sudah di kemukakan pada bab sebelumnya bahwa *transfer of proceeding* 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*, maka penulis akan berpatokan kepada konvensi tersebut. Menurut konvensi tersebut kejahatan yang bisa dimintakan *transfer of proceeding* adalah kejahtan yang termasuk kedalam ranah hukum pidana.[317] Untuk melihat apakah *cybercrime* termasuk kedalam ranah hukum pidana, maka kita harus melihat pengaturan dari beberapa negara Eropa:

1. Belanda

Peraturan mengenai *cybercrime* di Belanda dimulai tahun 1993 dimana dibentuk satu undang-undang baru yang di sebut *Computer Crime Act* (*wet computercriminaliteit)* yang lalu diamandeman pada tahun 2006 untuk menyesuaikan

[317] *Transfer of proceedings Convention* ,Pasal 1 huruf a

denga *convention on cybercrime*.[318] Undang undang ini merupakan bagian dari Kitab Undang-Undang Hukum Pidana (*wetboek van strafrecht*)

2. 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 (*data crime/data kriminalitet*).[319]

3. Jerman

Di Jerman *cybercrime* di atur 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.[320]

Dari beberapa peraturan mengenai *cybercrime* diatas, maka dapat disimpulkan bahwa *cybercrime* termasuk kedalam ranah hukum pidana sehingga *transfer of proceeding* dapat di lakukan untuk pelaku *transboundary cybercrime* adapun alasan dan prosedur *transfer of proceeding* adalah sebagai berikut:

1. Permintaan *Transfer of Proceeding*

Apabila seseorang diduga telah melakukan kejahatan menurut hukum negara peserta, maka sesuai dengan kondisi yang di syaratkan oleh konvensi ini bisa meminta negara peserta lainnya untuk memproses orang tersebut.[321] Adapun kondisi yang memungkinkan seseorang dimintakan untuk diproses di negara peserta lainnya adalah :[322]

a) Apabila terduga tinggal di negara yang dimintakan (*Requested State)*;

[318] Bert-Jaap Koops, *Cybercrime Legislation in Netherlands*,Netherland Comparative Law Association
[319] Henrik-Spang Hansen,IT Law Series, Hal 159
[320] Ulrich Sieber, *Ibid*, Hal 183
[321] *Ibid*, Pasal 6
[322] *Ibid*, Pasal 8

b) Apabila terduga merupakan warganegara 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 di rasa mampu untuk merehabilitasi yang bersangkutan;
g) Apabila terduga/terdakwa di pastikan tidak mampu untuk mengahadiri persidangan di negara yang meminta;
h) Apabila cara yang lain (ekstradisi) dirasa tidak mampu untuk menghadirkan terduga/tersangka

2. Prosedur *Transfer of Proceeding*

1. Permintaan diajukan oleh negara peminta melalui Kementrian Kehakiman ke Kementrian negara yang diminta.[323]
2. Apabila permintaan tersebut terkait dengan kasus yang memerlukan aksi cepat, maka permintaan dapat di ajukan melalui Interpol.[324]
3. Apabila negara yang diminta merasa dokumen permintaan yang di lampirkan belum cukup, maka mereka bisa meminta negara peminta untuk melengkapi dokumen tersebut dalam jangka waktu tertentu.[325]
4. Setiap permintaan harus di sertai 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 dikrimkan menyusul

[323] *Ibid*, Pasal 13 ayat (1)
[324] *Ibid*,Pasal 12 ayat (2)
[325] *Ibid*,Pasal 14

Di Indonesia sendiri memang belum di kenal *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*[326]. Hal ini sangat di sayangkan karena sesuai dengan definisi yang di berikan 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 di lakukannya *transfer of proceedings* di Indonesia. Penulis sendiri berpendapat bahwa *transfer of proceedings* seharusnya dapat di lakukan di Indonesia khususnya dalam penanganan kasus *cybercrime*, hal ini di dasari atas pengaturan yang ada dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) dimana dalam pasal 43 ayat 8 berbunyi"[327]

"Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja 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 seserorang yang diduga telah melakukan tindak pidana *cybercrime* yang merugikan Indonesia, hasil dari *transfer of proceedings* tersebut nantinya akan di kirimkan ke Indonesia sebagai acuan untuk penanganan kasus *cybercrime* di masa yang akan datang

[326] Indonesia, Undang-Undang Tentang Bantuan Timbal Balik No 1 Tahun 2006, pasal 4
[327] Indonesia, Undang-Undang Informasi dan Transaki Eelektronik, *Loc.cit*, pasal 43 ayat 8

Bab 4

Kesimpulan dan Saran

4.1.Kesimpulan

1. Pengaturan terhadap yurisdiksi dalam hukum internasional khusus mengenai *cybercrime* diatur dalam *Convention on Cybercrime*. Permasalahan yurisdiksi dalam *Convention on Cybercrime* yang dibuat oleh Dewan Eropa, secara khusus ditempatkan pada pasal tersendiri yakini pada pasal 22. Pasal yang terdiri dari lima ayat tersebut antara lain mengatur sebagai berikut
    a. Yurisidiksi suatu negara harus diterapkan apabila tindak pidana terjadi di tempat-tempat yang disebutkan.
    b. Negara boleh memilih apakah akan menerapkan yurisdiksinya apabila tindak pidana terjadi di luar wilayahnya.
    c. Apabila tidak ada ekstradisi maka Negara harus mengambil langkah-langkah yang diperlukan.
    d. Konvensi ini tidak mengesampingkan penerapan hukum nasional .
    e. Apabila dua negara mengklaim yurisdiksi atas sebuah tindak pidana, maka disarankan kedua negara tersebut mengadakan konsultasi.

    Berdasarkan uraian mengenai Pasal 22 beserta penjelasannya diatas, 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 natinya berfungsi menertibkan segala aktivitas di *cyberspace*. 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. Apabila terjadi konflik yurisdiksi biasanya negara-negara menempuh cara kerjasama internasional untuk menyelesaikannya, tiga hal tersebut adalah:

a.Ekstradisi dan Deportasi

b.*Mutual Legal Assistance* atau bantuan timbal balik

c.*Transfer of Proceeding*

Cybercrime dapat menjelma menjadi sebuah kejahatan serius hal ini di tunjukkan dengan munculnnya kasus *cyberattacks* yang terjadi di Estonia pada tahun 2007, serangan tersebut menyebabkan terhentinya seluruh kegiatan pemerintahan dan perekonomian di Estonia. Kasus ini mendorong Judge Stein Schjolberg mengusulkan perlunya di bentuk suatu mahkamah internasional yang khusus menanganai kasus-kasus di *cyberspace* yang bernama *Interntional Court or Tribunal on Cyberspace*.

2.Penentuan yurisdiksi dalam kasus *transboundary cybercrime* bermacam-macam namun tujuh komponen yang diajukan oleh Susan Brenner dapat dijadikan pertimbangan untuk menentukan yurisdiksi terhadap satu kasus *transboundary cybercrime*, ketujuh komponen tersebut adalah

a.Tempat kejahatan dilakukan

b.Tempat ditangkapnya pelaku

c.Akibat dari kejahatan tersebut

d.Nasionalitas atau kewarganegaraan (pelaku dan korban)

e.Kekuatan dari kasus tersebut

f.Pemindanaan

g.Imparisalitas dan kenyamanan

Analisa terhadap hubungan antara ketujuh komponen tersebut dengan kasus *transboundary cybercrime* yang terjadi di Indonesia, menunjukkan jika terjadi sebuah kasus yang melibatkan warganegara asing di Indonesia penegak hukum, terutama Jaksa cenderung menyelesaikan kasus tersebut dengan cara non-hukum (ekstradisi dan deportasi) seperti yang terjadi dalam kasus Penipuan "mama minta pulsa" yang pelakunya adalah warganegara China dan Taiwan. Di Eropa *Transfer of proceedings* yang merupakan hal baru dalam menyelsaikan konfik yurisdiksi antar negara dapat dilakukan dalam hal penanganan kasus *cybercrime* hanya saja terbatas pada kasus kasus yang termasuk ke dalam ranah hukum pidana. Sementara di Indonesia Sendiri *Transfer of Proceedings* tidak dimungkinan dilakuakn karena Undang-Undang No 1 Tahun 2006 Tentang Bantuan Timbal Balik, tidak mengikut sertakan *transfer of porceedings* sebagai salah satu bidang yang dapat di lakukan perjanjian timbal balik.

4.2.Saran

1. 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*.

2. 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 Pustaka

I. Buku, Artikel, Makalah dan Jurnal.

Atmasasmita,Romli *Pengantar Hukum Pidana Internasional*, (Bandung: Refika Aditama, 2003)

Arief Mansur, Dikdik M. dan Elisatris Gultom. *Cyber Law-Aspek Hukum Teknologi Informasi*, Cet.1. Bandung. PT Refika Aditama, 2005.

Baudrillard, *Simulation*, New York, Semiotex

Barry, Colin. *the Future of Cyberterrorism*, Crime and Justice International, March 1997.

Blumenthal, Max *"International Humanitarian Law on Cyberwarfare"*, Proceedings of The National Conference On Undergraduate Research (NCUR) 2011 Ithaca College, New York 2011

Brenner Susan W. ,*Chapter 17, The Next Step :Prioritizing Jurisdiction*,IT Law Series Vol 11 :*Cybercrime and Jurisdiction*, Leiden, Asser Press, 2006,

Burk, Dan L. *Jurisdiction in a World Without Border*. <www.cyberjurisdiction.net> , diakses tanggal 5 Mei 2012.

Connoly, Chris. *An Introduction to Internet Content Regulation in Asia and the Pacific*. Galexia intelligence reports, articles, papers, conferences and seminars. <www.galexia.com>, diakses pada tanggal 10Juni 2012.

Departemen Luar Negeri Republik Indonesia,*"Posisi Indonesia Terhadap Pembentukan Makhamah Pidana Internasional"*, Juli 1998

Dressler, Joshua. *ed. The Encyclopedia of Crime and Justice, edition* 2. New York. Macmillian Reference, 2001.

Granville, Johanna. *The Transnational Dimension of Cybercrime and Terrorism*. British Journal of Criminology volume .43, 2003.

Graycar, Adam. *Cybercrime: Old Wine in New Bottles?*. Makalah disampaikan dalam seminar dengan tema *Cybercrime* di Centre for Crimnology, The University of Hongkong, tanggal 24 Februari 2000.

Gregory Lastwoka, F and Dan Hutter. *Virtual Crime*. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=564801>, pada tanggal 5 Maret 2012.

Goodman, Mark D. and Susan W. Brenner. *The Emerging Consensus On Criminal Conduct in Cyberspace*. <http://www.lawtechjournal.com/articles/2002/03_020625_goodmanberner.php>. Diakses pada tanggal 1 April 2012.

Hariyanti Chandra, Francisca. *Internet:Information Superhighway*, Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah V1 di Semarang, 4-8 September 1995.

Hamano, Masaki. *Comparative Study I The Approach to Jurisdiction in Cyberspace"*.dalam Dharma Adhikari, *International Cyberjurisdiction :Toward The Formulation of Common Laws*, 2002

Hamzah, Andi. *Aspek-aspek Pidana di Bidang Komputer*. Jakarta. Sinar Grafika, 1990.

Hiariej, Eddy, O.S, *Pengantar Hukum Pidana Internasional* (Jakarta: Airlangga, 2009)

Istijar, Muhammad. *Korupsi Kejahatan Luar Biasa*.<www.hokionline>, diakses pada 30 Juni 2009.

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

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

Keyser, Mike. *The Council of Europe Convention on Cybercrime*. Journal of Transnational Law and Policy, volume 12, 2003.

Kraft PhD, *Ideas of establishment of an interntional court of cybercrime*, WCLF papers, 2011

Langseth,Peter *United Nations Handbook on Practical Anti Corruption Measures for Prosecutors dan Investigators*,Vienna;UNDOC,2004

Lloyd, Ian J. *Information and Technology Law*. third edition. London. Butterworths. 2000.

Kanter, E.Y dan S.R Sianturi. *Asas-asas Hukum Pidana Di Indonesia Dan Penerapannya*, Cet.2. Jakarta. Storia Grafika, 2002.

Karnasudirja. Eddy Djunaidi. *Yurisprudensi Kejahatan Komputer*. Jakarta. CV. Tanjung Agung, 1993.

Kusumaatmadja,Mochtar,*Pengantar Hukum Internasional*, Bandung :Binacipta, 1996

Nawawi Arief, Barda. *Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tidak Pidana Maya Antara*. Makalah pada seminar nasional dalam rangka penyusunan RUU teknologi informasi.

Netherlands Advisory Council of International Affairs Advisory Report No 77,AIV/22, CAVV December 2011

Makarim, Edmon. *Kompilasi Hukum Telematika*, cet kedua. Jakarta. Rajagrafindo, 2003.

Mayer-Schönberger,Viktor "The Shape of Governance: Analyzing the World of Internet Regulation", *Virginia Journal of International Law* ,2003

Menthe, Darrel. *Jurisdiction in Cyberspace : A Theory of International Spaces*. 4 Mich Tech Review, 1998

Muladi,*Hak Azasi Manusia dalam Politik dan Sistem peradilan Pidana*,Kapita Selekta Sistem Peradilan Pidana,Badan Penerbit Universitas Diponegoro,Semarang,2002

Murphy, John F. *Civil Liability for the Commision of International Crimes as an Alternative to Criminal Prosecution*. Harvard Human Rights Journal 9 th edition 2007

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

Oberding, Juliet M. and Treje Norderhaug. *A Separate Jurisdiction for Cyberspace*. <www.cyberjurisdiction.net> , diakses pada 16 Mei 2012.

Ophard Jonathan A. ,*Cyberwarfare and The Crime of Agression : The Need of Individual Accountability on Tomorrow's Battlefield*, Duke Law & Techology Review, 2010

Pattiradjawane. Rene L. *Cyberlaw: Apakah bisa Melindungi Pribadi Pengguna Internet?*. <www.kompas.com>,

Post, David G. *Anarchy, State and The Internet: An Essay on Law Making in Cyberspace*. Journal of Online Law, 1995.

Purbo, Onno W. Sejarah Internet, <www.ilmukomputer.com> , diakses pada tanggal 15 Maret 2009.

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

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

Ramli, Ahmad M. *Cyberlaw dan HaKI Dalam Sistem Hukum Indonesia*, cet-1. Bandung. PT Refika Aditama, 2004.

Remmelink, Jan ,*Hukum Pidana*, Gramedia Pustaka Utama, Jakarta, 2003

Remy Syahdeni, Sutan, *Kejahatan tindak pidana Komputer,* Jakarta. Pustaka utama Grafiti, 2009

Reinhard Golose, Peter. *Perkembangan Cybercrime dan Penanganannya di Indonesia oleh POLRI*. Makalah disampaikan pada seminar nasional mengenai "Penanganan *Cybercrime* di Indonesia ke Arah Pengembangan Kebijakan Menyeluruh dan Terpadu", tanggal 10 Agustus 2006.

Roden, Adrian. *Computer Crime and The Law*. Criminal Law Journal, 1991.

Sanford, Kadish and May T Morrison. *ed.Encyclopedia of Crime and Justice*",Law University of California, Berkeley, Volume I.

Sarwoko, Djoko. *Computer Crime sebagai Dimensi Baru Tindak Pidana Ekonomi*. Varia Peradilan Nomor 21 Tahun II, Juni 1987.

Starke, J.G. *Introduction to International Law*. 9th ed. London. Butterworths, 2000

Scholberg,Stein *Interntional Criminal Court or Tribunal for Cyberspace*, East West Institute (EWI) Cybercrime legal institute, May 2011

Sudirman, Ivan dan Romi Satria. *Sejarah Komputer*. Makalah disampaikan pada Training Ilmu Komputer,bahan didownload dari <www.ilmukomputer.com>,

Sunarso, Siswanto *Ekstradisi dan Bantuan Timbal Balik dalam Masalah Pidana: Instrumen Penegakan Hukum Pidana Internasional*, Jakarta:Rineka Cipta,2009

Sood, Vivek. *Cyber Law Simplified*. New Delhi. Tata McGraw-Hill Publishing Co.Ltd, 2001.

Sutadi, Heru. *"Cybercrime, apa yang bisa diperbuat?"*, <http://www.sinarharapanbaru.co.id/berita/0304/05/op01.html>, diakses tanggal 15 April 2012.

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

Wahid, Abdul dan Muhammad Labib,*Kejahatan Mayantara (Cybercrime)*, (Cet 1,PT Refika Aditama), Bandung, 2005

Wilske, Stephen and Teresa Schiller. *International Jurisdiction in Cyberspace: Which States May Regulate The Internet*. 50 Fed. Comm. L.J. 117, 171, 1997

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

II. Konvensi Internasional dan Peraturan Perundang-undangan.

Council of Europe, *Convention on Cybercrime*.

Indonesia, Undang-Undang Ekstradisi No 1 Tahun 1979, Lembaran Negara No. 2 Tahun 1979, Tambahan Lembaran Negara No. 3130

Indonesia, Undang-Undang Keimigrasian No 9 Tahun 1982 , Lembaran Negara No. 33 Tahun 1982, Tambahan Lembaran Negara No. 3474

Indonesia, Undang-Undang Tentang Telekomunikasi No. 36 Tahun 1999, Lembaran Negara No. 154 Tahun 1999, Tambahan Lembaran Negara No. 3881

Indonesia,Undang-Undang Tentang Bantuan Timbal Balik Dalam Masalah Pidana, UU No 1 Tahun 2006, Lembaran Negara No 18, Tahun 2006, Tambahan Lembaran Negara No 4607

Indonesia, Undang-Undang Tentang Informasi dan Transaksi Elektronik No 11 Tahun 2009, Lembaran Negara No. 58, Tambahan Lembaran Negara No 4843

Indonesia, Undang-Undang Tentang Keterbukaan Informasi Publik No. 14 Tahun 2008, Lembaran Negara No. 61 Tahun 2008, Tambahan Lembaran Negara No. 4846

III. Sumber Lainnya

Gobal Internet Policy Initiative. *Trust and Security in Cyberspace :The Legal and Policy Framework for Adressing Cybercrime*, 2005.

Information Warfare Monitor.*Tracking GhostNet : Investigating a Cyber Espionage Network*, 29 March 2009.

Prita Mulyasari Hari Ini Didakwa , www.hukumonline.com, diakses pada tanggal 12 Juni 2012.

RS OMNI dapatkan pasien dari hasil lab fiktif, <http://suarapembaca.detik.com/read/2008/08/30/111736/997265/283/rs-omni-dapatkan-pasien-dari-hasil-lab-fiktif >, diakses tanggal 12 Juni 2012.

Anggara, UU ITE merupakan ancaman bagi bloger indonesia, <http://anggara.org/2008/03/26/uu-informasi-dan-transaksi-elektronik-adalah-ancaman-serius-bagi-bolger-indonesia/>, diakses tanggal 1 Juni 2012