KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN CYBERCRIME

TESIS

Disusun dalam Rangka Memenuhi Persyaratan
Program Magister Ilmu Hukum

OLEH :

IRENE PUTRIE, SH
NIM. B4A000276

DOSEN PEMBIMBING:
PROF. DR. BARDA NAWAWI ARIEF, SH

PROGRAM PASCA SARJANA
MAGISTER ILMU HUKUM
UNIVERSITAS DIPONEGORO

KEBIJAKAN HUKUM PIDANA DALAM PENANGGULANGAN CYBERCRIME

Disusun Oleh:

IRENE PUTRIE, SH
NIM. B4A000276

Dipertahankan Dihadapan Dewan Penguji
Pada Tanggal:

Tesis Ini Telah Diterima
Sebagai Persyaratan Untuk Memperoleh Gelar
Magister Ilmu Hukum

PEMBIMBING

PROF. DR. BARDA NAWAWI ARIEF, SH
NIP. 130.350.519

Mengetahui
Ketua Program
Magister Ilmu Hukum

PROF. DR. BARDA NAWAWI ARIEF, SH
NIP. 130.350.519

ABSTRAK

Teknologi komputer yang berkembang pesat telah mempengaruhi seluruh aspek kehidupan manusia. Dalam perkembangannya teknologi komputer telah menghasilkan teknologi Internet dimana tercipta *cyberspace,* sebuah ruang yang menembus batas negara. Sisi positif perkembangannya juga diikuti dengan sisi negatif yang memungkinkan munculnya kejahatan di Internet yang dikenal dengan *cybercrime.*

Belum diaturnya masalah *cybercrime* tertentu secara khusus di Indonesia, menyebabkan timbulnya masalah dalam menerapkan ketentuan-ketentuan hukum pidana positif yang ada.. Beberapa ketentuan hukum positif yang dapat diterapkan terhadap *cyubercrime* adalah KUHP, UU No. 36 Tahun 1999 tentang Telekomunikasi, UU No. 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak sehat, UU No. 32 Tahun 2002 tentang Penyiaran, UU No.15 Tahun 2002 tentang Tindak Pidana Pencucian Uang. Khusus untuk hukum acara dalam hal memudahkan pembuktian, maka dapat digunakan UU No. 8 Tahun 1997 tentang Dokumen Perusahaan, UU No 20 Tahun 2001 tentang Perubahan Atas UU No 31 Tahun 1999 tentang Tindak Pidana Korupsi dan UU No.15 Tahun 2002 tentang Tindak Pidana Pencucian Uang. Dalam menerapkan hukum pidana positif tidak boleh dilakukan analogi tetapi dapat dilakukan dengan menggunakan metode penafsiran ekstensif.

Mengingat *cybercrime* merupakan kejahatan yang berdimensi baru dan mempunyai karakteristik yang unik yaitu kejahatan yang dilakukan/terjadi di jaringan sistem komputer yang sedang *online* (internet), maka perlu dilakukan kebijakan formulasi untuk tindak pidana *cybercrime.* Hal ini karena terhadap beberapa bentuk *cybercrime* tidak dapat diterapkan hukum positif.

Dalam membuat suatu kebijakan formulasi untuk tindak pidana diruang siber *(cyberspace),* perlu dilakukan harmonisai secara eksternal yakni dengan memperhatikan instrumen internasional, melakukan perbandingan dengan negara lain dan melakukan harmonisasi internal yakni dengan memperhatikan hukum positif yang ada.

Kata kunci : *cybercrime,* kriminalisasi, jurisdiksi

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas berkat rahmat dan hidayahNya penulis dapat menyelesaikan tugas akhir dibidang Studi Ilmu Hukum dan Sistem Peradilan Pidana. Program Magister Ilmu Hukum Universitas Diponegoro Semarang yang berjudul "KEBIJAKAN HUKUM PIDANA DALAM MENANGGULANGI CYBERCRIME".

Dalam kesempatan ini penulis ingin mengucapkan terima kasih yang dalam kepada :

1. Prof. Dr. Barda Nawawi Arief, SH. Selaku pembimbing dalam penulisan tesis ini dan sebagai ketua Program Magister Ilmu Hukum (S2) Universitas Diponegoro untuk bantuan tak terhingga bagi kelancaran program kerja sama Kejaksaan RI dan UNDIP;
2. Para Guru besar dan dosen yang telah memberikan ilmunya selama penulis menempuh pendidikan S2 di Universitas Diponegoro;
3. Kepala Kejaksaan Tinggi Jawa Tengah, para asisten dan staf bagian pembinaan;
4. Staf tata usaha pada Program Magister Ilmu Hukum Universitas Diponegoro;
5. Rekan-rekan mahasiswa Kajian Sistem Peradilan Pidana, Program Pasca Sarjana Universitas Diponegoro;
6. Rekan-rekan kelas khusus Kejaksaan angkatan 2001 untuk kebersamaan dan dorongannya;

7. Penghuni Erlangga Barat VII/10 A Semarang, untuk sayang dan perhatiannya;
8. Mama Desni Animas dan Papa Asril. S untuk cinta yang tak pernah padam, juga untuk uni Ivonne Estherlie, abang dan ponakanku Imam & Ogif serta adikku Ronny Utama;
9. Bang Ical terkasih untuk semangat, dorongan dan doanya serta untuk Sutan Farrel Habibie, anakku tersayang.

Pada kesempatan ini penulis menyadari bahwa tulisan ini masih jauh dari sempurna, karena itu penulis menerima segala bentuk kritik dan saran yang membangun untuk kesempurnaan tesis ini.

Akhirnya penulis berharap agar tulisan ini meskipun sedikit, tetapi dapat bermanfaat bagi perkembangan hukun Indonesia.

Semarang, Maret 2004

IRENE PUTRIE, SH.

DAFTAR ISI

		Halaman
HALAMAN JUDUL		i
HALAMAN PENGESAHAN		ii
HALAMAN PERSEMBAHAN		iii
HALAMAN MOTTO		iv
ABSTRACT		v
ABSTRAK		vi
KATA PENGANTAR		vii
DAFTAR ISI		ix
BAB I.	PENDAHULUAN	1
	A. Latar Belakang Masalah	1
	B. Perumusan Permasalahan	8
	C. Tujuan Penelitian	8
	D. Kontribusi Penelitian	9
	E. Kerangka Konseptual	10
	F. Metode Penelitian	16
	1. Metode Pendekatan	16
	2. Sampel Penelitian	17
	3. Jenis dan Sumber Data	18
	4. Teknik Pengumpulan Data	20
	5. Metode Analisis Data	21
	G. Sistematika Penulisan	21

BAB II. TINJAUAN PUSTAKA 23

A. KEBIJAKAN HUKUM PIDANA 23

1. Landasan Pemahaman tentang Kebijakan Hukum Pidana 23

2. Upaya Penanggulangan Kejahatan dengan Hukum Pidana 27

B. *CYBERCRIME* 31

1. Perkembangan Teknologi Komputer dan *Cyber* 31

2. Perkembangan *Cybercrime* (Kejahatan Siber) 46

3. Jurisdiksi 55

BAB III. HASIL PENELITIAN DAN PEMBAHASAN 62

A. PENANGGULANGAN CYBERCRIME DENGAN HUKUM POSITIF 62

1. Asas Legalitas dan Metode Interpretasi 65

a. Azas Legalitas 65

b. Metode Interpretasi 72

2. Kebijakan Hukum Pidana dalam Peraturan Perundang-undangan untuk menanggulangi *Cybercrime* 74

a. Dalam KUHP 78

b. Di luar KUHP 88

1) Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan 88

2) Undang-undang Nomor 5 tahun 1999 tentang larangan Praktek Monopoli dan Persaingan Usaha tidak sehat 91

3) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi 96
4) Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-Undang Nomor 31 ahun 1999 tentang Pemberantasan Tindak Pidana Korupsi 106
5) Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang 108
6) Undang-Undang Nomor 32 tahun 2002 tentang Penyiaran 109
3. Contoh Kasus Cybercrime dan Penyelesaiannya 114
a. Kasus Domain Name Mustika Ratu 114
b. Kasus *Hacking* atas nama Wendy Setiawan 120
c. Kasus *Carding* atas nama Agusta Kurniawan 125
B. KEBIJAKAN HUKUM PIDANA UNTUK CYBERCRIME DI MASA YANG AKAN DATANG 129
1. Kriminalisasi 136
a. Perbandingan dengan Negara Lain 138
1) Singapura 141
2) Australia 144
3) Amerika Serikat 149
a. Dalam Rancangan Undang-Undang 151
1) Konsep KUHP 151
2) RUU Informasi dan Transaksi elektronik 152
2. Penalisasi 160
a. Perbandingan dengan Negara Lain 166
b. Dalam Rancangan Undang-Undang 167
3. Jurisdiksi 173

BAB IV. PENUTUP 181
A. Kesimpulan 181
B. Saran 184

DAFTAR PUSTAKA

BAB I

PENDAHULUAN

A. Latar Belakang

Dalam kehidupannya manusia tidak dapat melepaskan diri dari teknologi beserta kemajuannya. Manusia selalu menciptakan teknologi untuk keperluan hidupnya sehari-hari. Teknologi yang diciptakan oleh manusia berkembang seiring dengan meningkatnya berbagai kebutuhan manusia dan mempengaruhi evolusi peradaban manusia. Bahkan manusia juga memadukan teknologi yang ada untuk menciptakan teknologi lainnya.

Penemuan-penemuan di bidang keilmuan telah mengakibatkan perubahan dalam cara pandang, sistem nilai di masyarakat, perubahan kebiasaan dan juga perubahan dalam sistem hukum. Perubahan-perubahan ini suka atau tidak suka, mau atau tidak mau dihadapi oleh manusia dan memberikan bentuk baru dalam perjalanan sejarah peradaban manusia.

Kemajuan teknologi informasi sekarang dan kemungkinannya di masa yang akan datang tidak lepas dari dorongan yang dilakukan oleh perkembangan teknologi komunikasi dan teknologi komputer, sedangkan

teknologi komputer dan komunikasi didorong oleh teknologi mikro-elektronika, material dan perangkat lunak. Kimia, fisika, biologi dan matematika mendasari ini semua.[1] Perpaduan teknologi komunikasi dan komputer melahirkan internet yang menjadi tulang punggung teknologi informasi.

Perkembangan internet sendiri tidak bisa dilepaskan dari perkembangan *hardware* komputer pada tahun 1945-1960 yang menghasilkan komputer dengan ukuran besar dan pada tahun 1977 ditemukan konsep *personal computer* oleh Steve Woznick dan Steve Jobs dari *Silicon Valley* yang memungkinkan pemakaian komputer secara perorangan. Perkembangan *hardware* juga diikuti dengan perkembangan *software.* Perkembangan internet dimulai dengan peluncuran pesawat *Sputnik* milik Uni Sovyet yang kemudian diikuti oleh Amerika Serikat dengan membuat proyek peluncuran pesawat luar angkasa dan pengembangan internet pada tahun 1960-an. Pada awal perkembangannya internet digunakan untuk kepentingan militer Amerika Serikat.

---

[1] Samaun Samadikun, *Pengaruh Perpaduan Teknologi Komputer,Telekomunikasi dan Informasi,* Kompas, 28 Juni 2000.

Setelah Perang Dingin *(Cold War)* internet tidak lagi digunakan hanya untuk kepentingan militer dan pemerintah, namun fungsinya menjadi lebih luas sebagai media yang dapat membawa perubahan dalam kehidupan manusia. Internet digunakan oleh pelaku bisnis, ilmuwan, politikus, untuk transaksi perdagangan dan sebagainya. Pemanfaatan teknologi ini telah mendorong pertumbuhan bisnis yang pesat karena berbagai informasi dapat disajikan dengan canggih dan mudah diperoleh. Melalui hubungan jarak jauh dengan memanfaatkan teknologi telekomunikasi, pendidikan dapat dilakukan bahkan juga untuk propaganda politik.

Kehadiran internet telah membuka cakrawala baru dalam kehidupan manusia. Internet merupakan sebuah ruang informasi dan komunikasi yang menjanjikan, menembus batas-batas antar negara dan mempercepat penyebaran dan pertukaran ilmu dan gagasan di kalangan ilmuwan dan cendikiawan diseluruh dunia. Internet membawa kita pada ruang atau dunia baru yang tercipta yang dinamakan *cyberspace.*[2]

Istilah *cyberspace* pertama kali digunakan oleh William Gibson dalam novel fiksi ilmiahnya yang berjudul *Neuromancer.*[3] *Cyberspace*

---

[2] Agus Raharjo, *Cybercrime: Upaya Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Citra Aditya Bakti, Bandung, 2002, hal. 4.

[3] Jeff Zaleski, *Spiritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia,* Mizan, Bandung, 1999, hal. 9.

menampilkan realitas, namun bukan realitas yang nyata sebagaimana bisa dilihat dan diraba, melainkan realitas virtual *(virtual reality)*, sebuah dunia yang tanpa batas *(borderless world)*, dunia maya. Dalam *cyberspace* tidak lagi dikenal batas negara, hilangnya batas dimensi ruang, waktu dan tempat. Para penghuninya bisa berhubungan di mana saja dan kapan saja.

Cyberspace membawa manusia kepada sebuah dunia yang sangat berbeda dengan berbagai realitas baru yang sebelumnya tidak pernah dijumpai. Realitas ini dirasakan oleh hampir seluruh negara-negara di dunia.

Disamping berbagai hal positif yang ditimbulkan dari realitas dunia maya, perkembangannya yang pesat juga menimbulkan sisi gelap (sisi negatif) yakni dalam bentuk kejahatan dan pelanggaran yang kemudian memunculkan istilah *cybercrime* dan merupakan perkembangan lebih lanjut dari *computercrime.* Dunia maya *(cyberspace)* ternyata rentan terhadap perilaku kriminal. Sebagai contoh adalah praktik-praktik implantasi virus yang mencederai komputer di seluruh dunia, bank dan lembaga keuangan telah kehilangan uang dalam jumlah besar. Negara maju seperti Amerika Serikat dan Inggris mengungkapkan bahwa data tentang keamanan nasional telah dibobol dan di *download* oleh orang-

orang yang tidak berkepentingan. Tindak pidana lain juga dapat dilakukan melalui media internet seperti pornografi anak, penyerangan terhadap privacy seseorang, perdagangan barang illegal, atau hadirnya situs-situs yang meresahkan masyarakat.

Keresahan-keresahan ini memunculkan keinginan untuk adanya pengaturan dan jaminan kepastian hukum di *cyberspace*. Hukum dirasa perlu dalam mengantisipasi hilangnya batas dimensi ruang, waktu dan tempat, agar internet benar-benar bermanfaat.

Perkembangan *Cybercrime* yang juga pesat seiring pesatnya perkembangan *cyberworld* mendapat perhatian yang besar. Ini terlihat dengan dijadikannya masalah *cybercrime* sebagai salah satu topik yang dibahas pada Kongres PBB mengenai *The Prevention of Crime and The Treatment of Offender* ke-8 tahun 1990 di Havana, Cuba dan Kongres ke 10 di Wina. Kongres PBB ke-8 memandang perlu dilakukan usaha-usaha penanggulangan kejahatan yang berkaitan dengan komputer *(computer related crimes)*. Kongres PBB ke-10 menjadikan *cybercrime* sebagai topik bahasan tersendiri dengan judul *crimes related to computer network*.

Council of Europe mempunyai *Convention on Cybercrime* yang terbuka untuk ditandatangani mulai tanggal 23 Nopember 2001 di Budapest. Substansi konvensi mencakup area yang luas, bahkan mengandung kebijakan kriminal *(criminal policy)* yang bertujuan untuk melindungi kepentingan masyarakat dari *cybercrime* baik melalui undang-undang maupun melalui kerjasama internasional.

Perkembangan internet di Indonesia juga cukup pesat, meskipun bila dibandingkan dengan negara-negara yang telah maju penggunaan internet di Indonesia masih jauh ketinggalan. Dewasa ini dapat disaksikan di berbagai kota dan daerah banyak tersedia tempat penyewaan internet (warung internet) untuk umum.

Akses yang bebas dapat dilakukan oleh siapapun, kapanpun dan dimanapun serta tanpa sensor. Bagaimanapun juga informasi tersebut tidak selalu positif. Informasi yang ada di *cyberspace* tidak mensyaratkan profesionalisme apalagi tanggung jawab terhadap isi sebagaimana media massa, sehingga informasi yang beredarpun tidak seluruhnya dapat dipertanggungjawabkan isinya.[4]

---

[4] Al Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Penerbitan Universitas Atmajaya, Jogyakarta, 1999, hal 3.

Perkembangan penggunaan dan pemanfaatan internet perlu segera menjadi perhatian agar tidak seperti hutan belantara yang tidak mempunyai peraturan hukum. Jika terjadi *cybercrime,* maka seharusnya ada peraturan yang dapat mengantisipasinya, mengingat *cybercrime* mempunyai sisi yang kompleks. Akibatnya juga membahayakan bagi perekonomian, nilai-nilai yang fundamental seperti moral, etika dan sebagainya, bahkan juga berdampak secara politis.

Berdasarkan uraian di atas maka dalam hal penanggulangan *cybercrime* diperlukan adanya kebijakan hukum pidana *(penal policy).* Kebijakan ini dapat mengarah pada dua hal. Pertama, kebijakan aplikatif yaitu bagaimana mengoperasionalisasikan peraturan perundang-undangan yang berlaku saat ini. Kedua, kebijakan formulatif atau kebijakan untuk melakukan pembaharuan hukum pidana *(penal law reform),* yaitu kebijakan merumuskan peraturan perundang-undangan yang tepat untuk menanggulangi *cybercrime* pada masa datang.

Untuk memahami lebih dalam masalah ini, perlu dilakukan penelitan yang mendalam sehingga diharapkan dapat memberi gambaran yang jelas dalam menentukan kebijakan hukum pidana dalam menanggulangi *cybercrime.* Pada akhirnya kebijakan tersebut mampu mendukung penyelenggaraan pembangunan untuk mencapai tujuan nasional.

B. Perumusan Permasalahan

Cybercrime merupakan permasalahan yang aktual sehingga perlu mendapat pemecahan melalui kebijakan hukum pidana yang serius. Bertolak dari latar belakang di atas, maka permasalahan pokok yang ingin dibahas adalah bagaimana kebijakan hukum pidana dalam menanggulangi *cybercrime.*

Berdasarkan permasalahan pokok tersebut, maka permasalahan yang akan diteliti dapat dirumuskan sebagai berikut:

1. Bagaimana kebijakan hukum pidana saat ini dalam penanggulangan *cybercrime*?
2. Bagaimana kebijakan hukum pidana dalam penanggulangan *cybercrime* di masa datang ?

C. Tujuan Penelitian

Penelitian ini bertujuan untuk memberikan gambaran serta pemahaman tentang bagaimana konsep kebijakan hukum pidana dalam penanggulangan *cybercrime.* Dari permasalahan pokok di atas, maka tujuan penelitian ini adalah:

1. Untuk mengetahui dan memahami kebijakan hukum pidana dalam penanggulangan *cybercrime* pada saat ini dan keterbatasan yang dimiliki oleh hukum positif.

2. Untuk memberi gambaran bagaimana sebaiknya kebijakan hukum pidana dalam menanggulangi *cybercrime*.

D. Kontribusi Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi berupa:

1. Kontribusi Teoritis

   Penelitian ini diharapkan dapat menambah pengetahuan mengenai *cybercrime* dan memberikan sumbangan pemikiran bagi pengembangan teori hukum (khususnya hukum pidana) di era teknologi informasi.

2. Kontribusi Praktis

   Penelitian ini secara praktis memberikan informasi tentang *cybercrime*. Bagi para pengambil kebijakan atau pembuat undang-undang termasuk penegak hukum, penelitian ini diharapkan dapat dipergunakan sebagai sumbangan pemikiran mengenai hal-hal yang berkaitan dengan *cybercrime* karena hukum selalu dituntut untuk dapat mengikuti perkembangan.

E. Kerangka Konseptual

Hukum memiliki keterikatan yang sangat luas dengan berbagai bidang ilmu, bahkan penguasaan ilmu hukum saja belum dapat memecahkan masalah yang ada dalam masyarakat yang terus menerus mengalami perkembangan. Perkembangan berbagai disiplin ilmu juga mempengaruhi perkembangan hukum itu sendiri.

Perkembangan teknologi juga membawa dampak dalam perkembangan hukum pidana. Tidak mudah untuk menetapkan suatu perbuatan sebagai suatu tindak pidana, artinya ada beberapa proses yang harus dilalui. Selain kajian yang mendalam mengenai perbuatan itu dari sudut kriminologi, maka harus dipertimbangkan pula beberapa hal yang perlu diperhatikan, yaitu tujuan hukum pidana itu sendiri, penetapan perbuatan yang tidak dikehendaki, perbandingan antara sarana dan hasil dan kemampuan badan penegak hukum.[5]

Menurut Barda Nawawi Arief,[6] istilah kebijakan diambil dari istilah *policy* (Inggris) atau *politiek* (Belanda). Bertolak dari kedua istilah asing ini, maka istilah "kebijakan hukum pidana" dapat pula disebut dengan istilah "politik hukum pidana". Istilah politik hukum

---

[5] Sudarto, *Hukum dan Hukum Pidana,* Alumni, Bandung, 1986, hal. 32

[6] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung, 2002, hal. 24

pidana dikenal dengan istilah lain *"penal policy", "criminal law policy"* atau *"strafrechtspolitiek".*

Pengertian kebijakan atau politik hukum pidana menurut Sudarto adalah:[7]

1. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat.
2. Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan.

Menurut A. Mulder, *Strafrechspolitiek* ialah garis kebijakan untuk menentukan:[8]

1. seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu diubah atau diperbaharui;
2. apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana;
3. cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.

(Strafrechts politiek is de beleidslijn om te bepalen :

- *in welk opzicht de bestaande strafbepalingen herzien dienen te worden;*

---

[7] Sudarto, *Op cit,* hal. 25.
[8] Barda Nawawi Arief, *Op cit,* hal. 25-26.

- *wat gedaan kan worden om strafrechtelijk gedrad te voorkomen;*
- *hoe de opsporing, vervolging, berechting en tenuitvoerlegging van straffen dient te verlopen).*

Kebijakan hukum pidana berkaitan dengan proses penegakan hukum (pdana) secara menyeluruh. Oleh sebab itu kebijakan hukum pidana diarahkan pada konkretisasi/operasionalisasi/fungsionalisasi hukum pidana material (substansial), hukum pidana formal (hukum acara pidana) dan hukum pelaksanaan pidana. Al Wisnubroto mengungkapkan bahwa kebijakan hukum pidana dapat dikaitkan dengan tindakan:[9]

1. bagaimana upaya pemerintah untuk menanggulangi kejahatan dengan hukum pidana;
2. bagaimana merumuskan hukum pidana agar sesuai dengan kondisi masyarakat;
3. bagaimana kebijakan pemerintah untuk mengatur masyarakat dengan hukum pidana;
4. bagaimana menggunakan hukum pidana untuk mengatur masyarakat dalam rangka mencapai tujuan yang lebih besar.

Masalah sentral dalam kebijakan hukum pidana adalah masalah penentan perbuatan apa yang seharusnya dijadikan tindak pidana dan sanksi apa yang sebaiknya digunakan atau dikenakan pada si pelanggar. Hal ini berarti bahwa kebijakan hukum pidana berkaitan dengan masalah

---

[9] Al. Wisnubroto, *Op cit*, hal 12.

kriminalisasi dan penalisasi, karena itu penanganannya harus berorientasi pada kebijakan *(policy oriented approach).*

Bassiouni, sebagaimana dikutip oleh Barda Nawawi Arief, mengemukakan bahwa :

> Tujuan-tujuan yang ingin dicapai oleh pidana pada umumnya terwujud dalam kepentingan-kepentingan sosial yang mengandung nilai-nilai tertentu yang perlu dilindungi yaitu: pemeliharaan tertib masyarakat; perlindungan warga masyarakat dari kejahatan, kerugian atau bahaya-bahaya yang tak dapat dibenarkan yang dilakukan oleh orang lain; memasyarakatkan kembali (resosialisasi) para pelanggar hukum; dan memelihara atau mempertahankan integritas pandangan-pandangan dasar tertentu mengenai keadilan sosial, martabat kemanusiaan dan keadilan individu.[10]

Dengan demikian, Bassiouni berpendapat bahwa dalam melakukan kebijakan hukum pidana diperlukan pendekatan yang berorientasi pada kebijakan *(policy oriented approach)* yang lebih bersifat pragmatis dan rasional, dan juga pendekatan yang berorientasi pada nilai *(value judgment approach).*

---

[10] Barda Nawawi Arief, *Op cit* , hal. 35-36.

Selanjutnya mengenai *cybercrime,* sampai saat ini boleh dikatakan belum ada definisi yang seragam baik nasional maupun global. Istilah lain yang juga digunakan untuk menunjuk kejahatan di dunia maya *(cyberspace)* antara lain adalah *computer related crimes.* Dari 2 (dua) dokumen Kongres PBB terlihat himbauan agar negara anggota menggunakan sarana "penal" (baik hukum pidana materiel maupun hukum acara pidana) sebagai salah satu upaya untuk menanggulangi *"Cyber Crime" (CC)* atau *"Computer Related Crimes" (CRC).*[11]

Kongres PBB X/2000 mengakui, bahwa ada beberapa kesulitan untuk menanggulangi *Cybercrime* dengan sarana penal, antara lain:[12]

a. Perbuatan jahat yang dilakukan berada di lingkungan elektronik. Oleh karena itu penanggulangan *cybercrime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di negara yang bersangkutan;
b. *Cybercrime* melampaui batas-batas negara, sedangkan upaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah teritorial negaranya sendiri;
c. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (negara) yang belum mengkriminalisasikan *Cybercrime.* Terjadinya *data havens* (negara tempat berlindung/singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.

---

[11] Barda Nawawi Arief, *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan,* Citra Aditya Bakti, Bandung, 2001, hal. 249.
[12] *Ibid.* hal. 250-251.

Berkaitan dengan hal tersebut di atas, Muladi mengatakan :

Pengaturan *cybercrime* sangat penting, karena baik *"actual victim"* maupun *"potential victim"*nya sangat luas. Jangkauannya sangat luas dan heterogen dengan kualitas dan persepsi yang berbeda, substansinya beragam meliputi segala aspek kehidupan baik yang bersifat positif maupun negatif, bersifat lintas negara *(transborder)*, penyebarannya cepat dan berlipat ganda dan informasi muatannya ada yang masih berupa konsep, issue, data, fakta, gagasan yang bisa bersifat obyektif dan bisa pula bersifat subyektif. Ada yang bersifat mengajak dan tidak jarang bersifat provokatif. Kepentingan yang sangat terkait bisa kepentingan negara, kepentingan umum maupun kepentingan kelompok atau pribadi.[13]

Aktivititas di dunia maya (internet) tidak bisa dilepaskan dari manusia dan akibat hukumnya terhadap manusia yang ada di dalam kehidupan nyata *(real life/physical world)* sehingga muncul pemikiran mengenai perlunya aturan hukum untuk mengatur aktivitas tersebut. Internet memiliki karakteristik yang berbeda dengan dunia nyata sehingga muncul pro dan kontra mengenai bisa tidaknya hukum tradisional/konvensional mengatur aktivitas tersebut atau perlu tidaknya aktivitas di internet diatur oleh hukum. Permasalahan sebenarnya bukan sebatas pada eksistensi hukum tradisional dalam mengatur aktivitas di internet, melainkan mempertanyakan eksistensi sistem hukum tradisional dalam mengatur aktivitas di internet.[14]

---

[13] Muladi, *Kebijakan Kriminal Terhadap Cybercrime*, Majalah Media Hukum Vol. I No.3 tgl 23-8-2003, hal. 2-3.

[14] Atip Latifulhayat, *Cyberlaw dan Urgensinya bagi Indonesia*, Makalah pada Seminar tentang Cyber Law, Yayasan Cipta Bangsa, bandung, 29 Juli 2000, hal. 3

Di Indonesia, pengaturan masalah *cybercrime* masih mempergunakan KUHP. Namun, ancaman hukuman dalam KUHP terhadap *cybercrime* tidak berimbang apabila dibandingkan dengan dampak negatif yang ditimbulkan. Sementara itu, dalam undang-undang di luar KUHP, seperti Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, pengaturan terhadap *cybercrime* juga masih sumir.

Berdasarkan hal tersebut di atas, maka usaha mewujudkan undang-undang yang mengatur mengenai kegiatan di*cyberspace* atau *cyberlaw* memang diperlukan keberadaannya saat ini.

F. Metode Penelitian

1. Metode Pendekatan

Penelitian ini menggunakan metode pendekatan yuridis normatif sebagai pendekatan utama, karena yang menjadi pusat perhatian utama dalam penelitian ini adalah kebijakan legislatif dalam masalah *cybercrime*.

Pendekatan terhadap hukum dengan menggunakan metode normatif dilakukan dengan cara mengidentifikasikan dan mengkonsepsikan hukum sebagai norma kaidah, peraturan perundang-undangan yang berlaku pada suatu negara tertentu yang

berdaulat. Penelitian terhadap hukum dengan pendekatan demikian merupakan penelitian hukum yang normatif atau penelitian hukum yang doktrinal.[15]

Disamping itu juga dilakukan pendekatan yuridis komparatif yang bertujuan untuk mengadakan perbandingan dengan negara-negara lain yang sudah mempunyai peraturan perundang-undangan tentang *cybercrime*, untuk mencari kesempurnaan pembuatan perundang-undangan di Indonesia. Dalam hal ini, perbandingan hukum penting untuk lebih mempertajam dan mengarahkan proses peneitian.[16]

2. **Sampel Penelitian**

Penelitian dilakukan dengan mengambil contoh-contoh kasus *cybercrime* yang ada dan mengungkapkannya. Kasus bisa di dapatkan dari kota-kota besar yang selama ini merupakan tempat atau lokasi pusat perkembangan internet seperti Yogyakarta, Bandung, Jakarta, Semarang.

---

[15] Ronny Hanitijo Soemitro, *Perbandingan Antara Penelitian Hukum Normatif dan Penelitian Hukum Empiris*, Masalah-Masalah Hukum, UNDIP Nomor 9, Semarang, 1991, hal. 4.
[16] Soerjono Soekanto, *Perbandingan Hukum*, Alumni, Bandung, 1979.

Pemilihan sampel atau nara sumber penelitian dilakukan secara *purposive sampling*, sehingga sampel sampel atau nara sumber dalam penelitian ini dapat ditentukan antara lain sebagai berikut :

a. Putusan-putusan Pengadilan Negeri/Pengadilan Tinggi/ Mahkamah Agung yang berkaitan dengan *cybercrime.*
b. Pasal-pasal dalam KUHP, RUU KUHP 2000, RUU Teknologi Informasi.
c. Para ahli hukum yang memiliki perhatian terhadap *cybercrime* untuk mengetahui kebijakan yang sebaiknya.

3. Jenis dan Sumber Data

Sebagaimana uraian di atas, bahwa penelitian ini merupakan penelitian normatif, yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder[17], maka jenis data penelitian ini meliputi data sekunder. Penggunaan data sekunder terutama akan disajikan pada data sekunder yang bersifat publik, baik yang berupa arsip maupun data resmi pada instansi-instansi pemerintah.[18]

---

[17] Soerjono Soekanto dan Sri Mamuji,, *Penelitian Hukum Normatif*, Rajawali Pers, Jakarta, 1985, hal. 5.
[18] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Universitas Indonesia, Jakarta, 1986, hal. 12.

Sumber data dari data sekunder dalam penelitian ini meliputi :

a. Bahan hukum primer, yaitu bahan-bahan hukum yang mempunyai kekuatan mengikat, antara lain :[19]
   - Norma dasar Pancasila
   - Peraturan dasar; Batang tubuh Undang Undang Dasar 1945.
   - Ketetapan-Ketetapan MPR
   - Perundang-undangan yang berlaku di Indonesia, antara lain Kitab Undang-Undang Hukum Pidana (KUHP), dan beberapa undang-undang yang di dalamnya mencantumkan pidana penjara minimum khusus.
b. Bahan hukum sekunder, yaitu bahan-bahan yang erat hubungannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer , antara lain :[20]
   - Konsep Rancangan Kitab Undang-Undang Hukum Pidana (KUHP)
   - Hasil-hasil karya ilmiah (makalah, tulisan di majalah hukum)
   - Hasil-hasil penelitian.
   - Pendapat-pendapat dari para ahli hukum pidana.

---

[19] Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, *Op. Cit.*, hal. 11.
[20] *Ibid*, hal..12.

4. Teknik Pengumpulan Data

Mengingat penelitian ini memusatkan perhatian pada data sekunder, maka pengumpulan data terutama ditempuh dengan melakukan penelitian kepustakaan dan studi dokumen.

Studi tersebut sangat berguna dalam membantu penelitian ilmiah untuk memperoleh pengetahuan yang dekat dengan gejala yang dipelajari, dengan memberikan pengertian penyusunan persoalan yang tepat, mempertajam perasaan untuk menilai, mambuat analisis dan membuka kesempatan memperluas pengalaman ilmiah. .[21]

Studi dokemen sebagai sarana pengumpul data lebih diutamakan diajukan kepada dokumen pemerintah yang termasuk kategori dokumen yanglebih dapat dipercaya daripada dokumen-dokumen lain.[22]

---

[21] Koentjaraningrat, *Metode-Metode Penelitian Masyarakat*, Gramedia, Jakarta, 1991, hal. 65.

[22] Sartono Kartodirjo, *Metode Penyusunan Bahan Dokumen*, dalam : *Metode Penelitian Masyarakat*, Koentjoroningrat, LIPI , Jakarta, 1973, hal, 65.

5. Metode Analisa Data

Analisa data adalah proses mengorganisasikan dan mengurutkan data ke dalam pola, kategori dan satuan uraian dasar sehingga dapat ditemukan tema dan dapat dirumuskan hipotesis kerja seperti yang disarankan oleh data.

Dalam penelitian ini, data yang diperoleh disajikan secara kuantitatif, kualitatif dengan menggunakan analisis deskriptif, yaitu dengan mendeskripsikan data yang telah diperoleh ke dalam bentuk penjelasan-penjelasan. Artinya probem yang ada dianalisis dan dipecahkan berdasarkan teori dan peraturan yang ada, serta dilengkapi analisis historis dan komparatif.

G. Sistematika Penulisan

Sistematika penulisan tesis ini terdiri dari 4 (empat) bab. Tiap-tiap bab membahas materi yang saling berkaitan dengan tema utamanya. Bab satu merupakan Pendahuluan yang terdiri dari Sub Bab A. Latar Belakang Permasalahan, Sub Bab B. Perumusan Permasalahan, Sub Bab C. Tujuan Penelitian, Sub Bab D. Kontribusi Penelitian, Sub Bab E. Kerangka Teori, Sub Bab F. Metode penelitian dan Sub Bab G. Sistematika penulisan.

Bab kedua berupa Tinjauan Pustaka yang terdiri dari Sub Bab A. mengenai Kebijakan Hukum Pidana dan Sub Bab B. mengenai masalah *cybercrime.*

Bab ketiga merupakan hasil penelitian dan pembahasan atas permasalahan yang diteliti.

Bab keempat merupakan bab penutup yang berisi kesimpulan dan saran. Diharapkan bab ini dapat memberikan kesimpulan penelitian yang dapat digunakan sebagai sarana mengembangkan hukum pidana.

BAB II

TINJAUAN PUSTAKA

A. KEBIJAKAN HUKUM PIDANA

1. Landasan Pemahaman tentang Kebijakan Hukum Pidana

Kemajuan teknologi informasi telah menjadikan perkembangan masyarakat yang begitu pesat. Kompleksitas permasalahan yang dihadapi oleh masyarakat dan penegak hukum dalam menanggulangi kejahatan modern perlu diimbangi pula dengan pembenahan sistem hukum pidana secara menyeluruh yang meliputi pembangunan struktur, Substansi dan kultur. Kebijakan hukum pidana (penal policy) menduduki peranan yang strategis dalam pengembangan hukum pidana modern.

Istilah kebijakan dalam hal ini diambil dari bahasa Inggris *"policy"* atau dalam bahasa Belanda *"politiek". Dalam Black"s Law Dictionary,* disebutkan *bahwa policy merupakan :*

"The general principles by which a goverment is guided in its management of public affairs, ...or principles and standard regarded by the legislature or by the courts as being of fundamental concern to the state and the whole of society in measures .....this term, as applied to a low, ordinance, or rule of law, denotes its general

purpose or tendency considered as directed to the welfare or prosperity of the state community".[23]

Politik hukum *(law policy/rehtspolitiek)* dapat diartikan sebagai berikut:[24]

a. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat.
b. Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang di cita-citakan.

Dengan demikian kebijakan hukum pidana *(penal policy/criminal law policy/strafrechtspolitiek)* dapat didefinisikan sebagai "usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang.[25]

Adressat hukum pidana adalah mengatur perbuatan warga masyarakat, namun bila dilihat dari aspek kebijakan hukumnya atau *penal policy* juga mengatur perbuatan penguasa aparat penegak hukum yang dalam hal ini dimaksudkan terhadap kewenangan atau kekuasaan dari penguasa tersebut. Menurut Peter, pembatasan dan pengawasan

---

[23] Henry Campbell Black, *Black's Law Dictionary,* seventh Edition, St. Paulminn West Publishing, C.O, 1999, hal. 1178
[24] Sudarto, *Op cit*, hal 159
[25] Sudarto, *Hukum Pidana dan Perkembangan Masyarakat,* Sinar Baru, Bandung, 1983, hal. 109

atau pengendalian kekuasaan negara merupakan dimensi yuridis yang sesungguhnya dari hukum pidana, tugas yuridis dari hukum pidana bukanlah "mengatur masyarakat" tetapi "mengatur penguasa" *("the limitations of, and control over, the powers of the State constitute the real juridical law dimension of criminal law; The juridical task of criminal law is not policing society but policing the police").*[26]

Kebijakan hukum pidana pada hakikatnya mengandung kebijakan mengatur dan membatasi kekuasaan, baik kekuasaan atau kewenangan warga masyarakat pada umumnya maupunkekuasaan atau kewenangan penguasa / penegak hukum.

Kebijakan hukum pidana mempunyai ruang lingkup yang luas karena merupakan serangkaian proses yang melalui tahap-tahap konkretisasi/operasionalisasi/ fungsionalisasi hukum pidana yang terdiri dari :

a. kebijakan formulatif/legislatif yaitu tahap perumusan /penyusunan hukum pidana;
b. kebijakan aplikatif/yudikatif yaitu tahap penerapan hukum pidana

[26] Barda Nawawi Arief, *Beberapa Aspek Kebijakan dan Pengembangan Hukum Pidana,* Citra Aditya Bakti. Bandung, 1998, hal. 29

c. kebijakan administratif/eksekutif yaitu tahap pelaksanaan hukum pidana;

Dari ketiga tahap kebijakan hukum pidana itu terkandung di dalamnya tiga kekuasaan/kewenangan, yaitu kekuasaan legislatif dalam menetapkan atau merumuskan perbuatan apa yang dapat dipidana dan sanksi apa yang dapat dikenakan. Pembaharuan hukum pidana lebih banyak berkaitan dengan tahap formulatif. Kekuasaan lainnya adalah di bidang yudikatif dalam menerapkan hukum pidana dan kekuasaan eksekutif dalam melaksanakan hukum pidana.

Kebijakan hukum pidana tidak dapat dipisahkan dari sistem hukum pidana yang integral. Menurut Marc Ancel, setiap masyarakat yang terorganisir memiliki sistem hukum pidana yang terdiri dari peraturan-peraturan hukum pidana beserta sanksinya, suatu prosedur hukum pidana dan suatu mekanisme pelaksanaan pidana.[27] Kemudian A. Mulder menyatakan bahwa kebijakan hukum pidana ialah garis kebijakan untuk menentukan:[28]

a. seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui;

---

[27] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op cit*, hal 28-29
[28] *Ibid*, hal. 29

b. apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana;

c. cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.

(Strafrechtpolitiek is de beleidslijn om te bepalen: in welk opzich de bestaande strafbepalingen herzien dienan te worden; wat gedaan kan worden op strafrechtelijk gedrad te voorkomen; hoe de opsporing, berechting en tenuitvoerlegging van straffen dient te verlopen).

2. Upaya Penanggulangan Kejahatan dengan Hukum Pidana

Kebijakan hukum pidana bukanlah merupakan suatu kebijakan yang berdiri sendiri. Kebijakan hukum pidana merupakan bagian dari upaya untuk menanggulangi kejahatan dalam raangka menyejahterakan masyarakat. Tindakan untuk mengatur masyarakat dengan sarana hukum pidana terkait erat dengan berbagai kebijakan dalam suatu proses kebijakan sosial yang mengacu pad atujuan yang lebih luas.

Upaya menanggulangi kejahatan dengan tujuan utama perlindungan masyarakat untuk mencapai kesejahteraan masyarakat secara garis besar dapat dibagi dalam dua jalur yaitu jalur penal dan

non-penal. Upaya menanggulangi kejahatan dengan pemberian sanksi pidana atau penal merupakan uapaya yang telah lama dan tertua yang pernah ditempuh dalam kehidupan manusia. Menurut GP. Hoefnagels, upaya penanggulangan kejahatan dapat ditempuh dengan:[29]

a. Penerapan hukum pidana *(criminal law application);*
b. Pencegahan tanpa pidana *(prevention without punishment);*
c. Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui mass media *(influencing views of society on crime and punishment/ mass media).*

Untuk kategori pertama dikelompokkan ke dalam upaya penanggulangan kejahatan lewat jalur penal, sedangkan kedua dan ketiga termasuk uapaya penanggulangan kejahatan melalui jalur non-penal. Sudarto mengemukakan:[30]

"Apabila hukum pidana hendak dilibatkan dalam usaha mengatasi segi negatif dari perkembangan masyarakat/modernisasi (penanggulangan kejahatan), hendaknya dilihat dalam keseluruhan politik kriminal atau *social defence planning* dan ini pun harus merupakan bagian integral dari rencana pembangunan nasional".

Kebijakan hukum pidana merupakan salah satu alternatif dari kebijakan kriminal *(criminal policy).* Upaya melalui jalur penal

---

[29] Barda Nawawi Arief, *Upaya Non-Penal dalam Kebijakan Penanggulangan Kejahatan,* Bahan Seminar Kriminologi IV 16-18 September 1991, hal. 1
[30] Sudarto, *Hukum dan Hukum Pidana, Op cit,* hal. 38

merupakan upaya repressif yang dalam pelaksanaannya mengandung keterbatasan sehingga perlu diimbangi dengan pendekatan non-penal yang cenderung merupakan upaya preventif. Dengan demikian jika dilihat dari sudut politik kriminal secara makro dan global maka upaya non-penal menduduki posisi kunci dan strategis dari keseluruhan upaya politik kriminal.[31] Hal ini tidaklah berarti bahwa upaya penal tidak penting, namun upaya penal merupakan sarana yang sangat vital dalam proses penegakan hukum *(law enforcement)* dalam menanggulangi kejahatan. Dalam Seminar Kriminologi ke-3 tahun 1976, salah satu kesimpulannya adalah:

"Hukum pidana hendaknya dipertahankan sebagai salah satu sarana untuk *social defence* dalam arti melindungi masyarakat terhadap kejahatan dengan memperbaiki atau memulihkan kembali *(rehabilitatie)* si-pembuat tanpa mengurangi keseimbangan kepentingan perorangan (pembuat) dan masyarakat".[32]

Kebijakan kriminal yang dilakukan melalui jalur penal maupun melalui jalur non-penal adalah sarana untuk melindungi masyarakat terhadap kejahatan *(social defence)* yang merupakan bagian integral dari kebijakan sosial *(social policy)* dan bersama-sama kebijakan untuk menyejahterakan masyarakat *(social welfare policy)*, dengan

---

[31] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op cit,* hal. 49
[32] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana,* Alumni, Bandung, 1998, hal. 92

tujuan akhir yang lebih luas yaitu: perlindungan masyarakat untuk menyejahterakan masyarakat.

Upaya penanggulangan kejahatan perlu ditempuh dengan pendekatan kebijakan secara terpadu (integral), dimana terdapat keterpaduan antara kebijakan kriminal dengan kebijakan sosial juga penanggulangan dengan sarana penal dan non penal.

Selanjutnya kebijakan hukum pidana berkaitan dengan masalah kriminaliasi yaitu perbuatan apa yang akan dijadikan tindak pidana dan penalisasi, yaitu sanksi apa yang sebaiknya dikenakan kepada si pelanggar. Kriminaliasai dan penalisasi menjadi masalah sentral, yang penanganannya diperlukan pendekatan yang berorientasi pada kebijakan (*policy oriented approach*). Kriminaliasi (*criminalization*) mencakup ruang lingkup perbuatan melawan hukum (*actus reus*), pertangungjawaban pidana (*mens rea*) maupun sanksi yang dapat dijatuhkan, baik berupa pidana (punihsment) maupun tindakan (*treatment*). Kriminalisasi harus dilakukan secara hati-hati, jangan sampai menimbulkan kesan represif yang melanggar prinsip untimatum rmidum (ultima ratio principle) dan menjadi bumerang dalam kehidupan sosial berupa kriminalisasi yang berlebihan (over criminalization), yang justru mengurangi wibwa hukum. Kriminalisai

dalam hukum pidana materiil akan diikuti oleh langkah-langkah dogmatis dalam hukum pidana formil untuk kepentingan penyidikan dan penuntutan.[33]

B. *CYBERCRIME*

1. Perkembangan teknologi Komputer dan Siber (Cyber)

Alat yang digunakan untuk memudahkan hitungan ditemukan empat abad sebelum Masehi di Babylonia dan disebutdengan *abacus*. Berkat sistem hitungan desimal yang diperkenalkan oleh budaya Arab pada abad delapan dan sembilan, maka perhitungan matematika dapat dipermudah.

Pada tahun 1614, John Napler menemukan sistem logaritma yang memudahkan perkalian dan pembagian, penambahan dan pengurangan. Selanjutnya pada tahun 1623, Wilhelm Schickard, Guru Besar dari Jerman menemukan kalkulator mekanis, yang mampu menghitung sampai dengan enam digit. Alat tersebut kemudian disempurnakan oleh Blaise Pascal pada tahun 1642 sehingga mampu delapan digit. Sedangkan Joseph-Marie Jacquard menemukan mesin otomatis yang dikontrol dengan *punch-cards*. Sementara itu Charles Babbage dari

---

[33] Muladi, *Kebijakan Kriminal terhadap Cybercrime*, *Op cit*, hal. 1.

Inggris mengkonsepkan apa yang disebut dengan *Difference Engine* pada tahun 1820 dan 1821 yang di desain untuk tabel astronomi, yang disusul dengan temuannya yang lain berupa *analitikal engine*, yaitu komputer mekanik yang mampu memecahkan masalah matematika dengan menggunakan tunch cards. Tahun 1833, Agusta Dabiron bertemu dengan Babbage yang kemudian menemukan dasar-dasar komputer programming dan analisis.[34]

Perkembangan selanjutnya adalah dengan dimulainya zaman komputer elektronik yaitu dengan ditemukannya kalkulator yang dapat diprogram oleh Konrad Zuse, seorang insinyur Jerman. Pada akhir tahun 1943 telah dioperasikan komputer Kolosus yang menggunakan kode Breaking. Disusul ENIAC (*Electronic Numerical Integrator Analizer and Computer*) di Universitas Pennsylvania pada tahun 1945. Kemudian pada tahun 1947, ditemukannya transistor oleh *Bell Telephone Laboratories* yang disusul dengan UNIVAC dan EDVAC masing-masing pada tahun 1951 dan 1952.[35]

---

[34] Heru Supraptomo, *Kejahatan Komputer dan Cyber serta Antisipasi Pengaturan dan Pencegahnnya di Indonesia*, Makalah pada Seminar Cyber Law : Antisipasi Hukum terhadap Transaksi Bisnis melalui Cyber Network, Medan, 30 Januari 2001, hal. 3.

[35] *Ibid.*

Komputer mini mulai diperkenalkan sejalan dengan penemuan *integrated circuit* oleh *Texas Instrumen and Fairchild Semiconductor*. Tahun 1968 Doug Engelboart memperkenalkan *word processor*. Sementara itu, antara Fairchild Semi Conductor dengan Intel berlomba mamproduksi chip yang makin besar kapasitasnya yang akhirnya menjadi *Micro Processor*.[36]

Pada tahun 1977, ditemukan Konsep *Personal Computer* oleh Steve Woznick dan Steve Jobs dari Sillicon Valley yang memungkinkan penggunaan komputer secara perorangan. Jonathan A. Titus juga mendesaian personal mini computer yang kemudian menjadi populer. Kemudian Paul Alllen dan Bill Gates membangun BASIC untuk Altair 8800 dan sejak itu lahir *Microsoft* yang kemudian menjadi perusahaan raksasa.

Perkembangan komputer selanjutnya bersamaan dengan perkembangan teknologi informasi yang menghasilkan *Computer Network*, yaitu konsep yang menghubungkan sejumlah besar pengguna terhadap suatu *single computer* melalui *remote terminal*. Konsep tersebut dibangun oleh *Massachuset Institute of Technology* (MIT) pada tahun 1950-an dan permulaaan tahun 1960-an.

---

[36] *Ibid*. hal. 4.

J.C.R. Licklider dari MIT pada bulan Agustus 1962 menulis dalam sebuah memo bahwa interaksi sosial dapat dilakukan dengan melalui sebuah jaringan komputer. Dalam memo tersebut diuraikan *Galactic Network*-nya. Dia memiliki visi sebuah jaringan komputer global yang saling berhubungan dimana setiap orang dapat mengakses data dan program secara cepat dari tempat manapun. Konsep ini sesuai dengan internet yang ada sekarang. Licklider merupakan pimpinan pertama riset program komputer dari proyek DARPA (*Defence Research Project Agency*) yang dimulai bulan Oktober 1962. selama di DARPA dia bekerja sama dengan Ivan Sutherland, Bob Tylor dan seorang peneliti MIT, Lawrence G. Roberts.[37]

Leonard Kleinrock di MIT mempublikasikan tulisannya berjudul :" *The first paper on packet switching theory*" dalam bulan Juli 1961 dan "*The first book on the subject*" di tahun 1964. Kleinlack dan Roberts dalam Teori Kelayakan Komunikasi mempergunakan sistem paket data daripada hanya mempergunakan sebuah rangkaian elektronik. Teori ini merupakan cikal bakal adanya jaringan komputer. Langkah penting lainnya adalah membuat komputer dapat berkomunikasi secara bersama-sama. Untuk membuktikan hal ini,

[37] http:/www.inet.co.th/cyberclub/indonesia/internet/sekilas_internet.html

pada tahun a965, Roberts bekerja sama dengan Thomas Merril, menghubungkan komputer TX-2 yang berada di Massachuset dengan komputer Q-32 yang berada di California dengan mempergunakan sebuah saluran dalam diall-up berkecepatan rendah. Hal inilah yang merupakan sebuah jaringan komputer pertama yang luas dan pernah dibuat dalam skala kecil.

Dalam bulan Agustus 1968, setelah Roberts dan penyandang dana proyek DARPA merevisi semua struktur dan spesifikasi ARPANET (*Advance Research Project Agency*), maka sebuah RFQ dirilis DARPA untuk pengembangan salah satu komponen kunci dengan paket pensaklarannya yang disebut *Interface Massage Processors* (IMP's). RFQ dikerjakan oleh Bolt Beranek and Newman (BBN) yang dipimpin oleh Frank Heart. Desain utama ARPANET dikerjakan oleh Bob Kahn. Topologi dan ekonomi jaringan didesain oleh Roberts bersama Howard Frank dan tim dari *Network Analysis Corporation.* Pengukuran jaringan dilakukan oleh tim pimpinan Kleinrock di UCLA.

Komputer banyak yang dihubungkan ke ARPANET pada tahun-tahun berikutnya dan tim bekerja melengkapi fungsi *Host-to-Host Protocol* dan software jaringan komputer lainnya. Di bulan Desember 1970, *The Network Working Group* (NWG) bekerja di bawah

pimpinan S. Croker menyelesaikan inisial ARPANET *Host-to-Host Protocol* yang disebut *Network Conrol Protocol* (NCP). ARPANET secara lengkap mempergunakan NCP selama periode 1971-1972 dan para pengguna jaringan komputer akhirnya dapat melakukan pengambangan aplikasinya.

Dalam bulan Oktober 1972, Kahn mendemontrasikan ARPANET ke masyarakat di *International Computer Communication Conference* (ICCC). Dalam demo ini diperkenalkan inisial *"hot" application, electronil mail (e-mail).* Roy Tomlison dari BBN membuat program penulisan e-mail, pengiriman dan pembaca pesan e-mail pertama. E-mail menjadi terkenal dan digunakan tanda @ yang berati at (di/pada). Pengembangan utilitynya dilakukan oleh Roberts dengan program *e-mail utility* pertama ke dalam daftar pemilihan untuk pembacaan, file, meneruskan (*forward*) dan memberikan jawaban sebuah pesan. E-mail kemudian menjadi aplikasi yang paling banyak dipergunakan dlaam jarigan komputer selama beberapa dekade.

Perkembangan internet dipicu oleh peluncuran pesawat *Sputnik* milik Uni Soviet dan diikuti oleh Amerika Serikat dengan membuat proyek peluncuran pesawat luar angkasa dan pengembangan internet

pada tahun 1960. pada waktu itu internet masih dipergunakan untuk kepentingan militer dan negara.

Pengembangan dan evaluasi teknologi internet, khususnya dalam penemuan dan sejarahnya, dapat dibagi dalam empat aspek, yaitu :[38]

a. Adanya aspek evolusi teknologi yang dimuali dari riset packet switching (pensaklaran) ARPANET (berikut teknologi perlengkapannya) yang saat itu dilakukan riset lanjutan untuk mengembangkan wawasan terhadap infrastruktur komunikasi data yang meliputi beberapa dimensi seperti skala, performance/kehandalan dan fungsi tingkat tinggi.
b. Adanya aspek pelaksanaan dan pengelolaan sebuah infrastruktur yang globaal dan kompleks.
c. Adanya aspek sosial yang dihasilkan dalam sebuah komunitas masyarakat besar yang terdiri dari para internauts yang bekerja sama membuat dan mengembangkan teknologi ini secara kontiyu.
d. Adanya aspek komersial yang dihasilkan dalam sebuah perubahaм ekstrim namun efektif dari sebuah penilaian yang mengakibatkan terbentuknya sebuah infrastruktur informasi yang besar dan berguna.

---

[38] *Ibid.*

Ide arsitektur jaringan komputer yang terbuka pertama kali diperkenalkan oleh Bob Kahn di DARPA pada tahun 1972. pekerjaan ini pada awalnya murni merupakan bagian pekerjaan program paket radio. Namun pada akhirnya program ini merupakan program terpisah dan disebut "*internetting*". Kata kunci untuk membuat sistem paket radio bekerja adalah *reabilitas protocol end-to-end* yang dapat memelihara secara efektif komunikasi meskipun dalam kondisi jumming dan adanya interfernsi radio lainnya ataupun gejala blockout intermiten seperti yang biasa terjadi pada komunikasi di dalam sebuah terowongan. Kahn pertama kali mengambangkan protokol lokal hanya untuk paket radio. Akhirnya dia kembali menggunakan NCP kerena sulit menemukan kecocokan dengan sistem operator komputer yang lain.

Kahn kemudian mengembagkan protokol yang dapat bekerja dengan baik yang disebut *Transmission Control Protocol/Internet Protocol* (TCP/IP) dan lebih menyerupai protokol komunikasi. Pada tahun 1982, TCP/IP ditetapkan sebagai standar ARPANET. Jumlah network host yang pada tahun 1987 berjumlah 10.000, pada tahun

1989 menjadi 100.0000, perkembangan yang luar biasa, inilah yang disbut era siber.[39]

Domain Name System (DNS) diperkenalkan pada tahun 1984 dan kemudian tanggung jawab pengaturannya diserahkan pada *Information Science Institute* (ISI). Registrasi pertama dari *Domain Name System* (DNS) adalah simbol .com.

Dari segi penulisannya, internet memiliki 2 arti, yaitu :[40]

a. internet

Jaringan internet (huruf "i" kecil sebagai huruf awal) adalah merupakan jaringan komputer yang mana komputer-komputer terhubung dapat berkomunikasi walaupun perangkat keras dan perangkat lunaknya berlainan (seringkali disebut juga *internet working*);

b. Internet

Jaringan internet (huruf "I" besar sebagai huruf awal) adalah sekumpulan jaringan (*networks of networks*) yang terdiri dari jutaan komputer yang dapat berkomunikasi datu sama lain dengan menggunakan suatu aturan kominukasi jaringan komputer

---

39 of the Nerds" A History of Computer

40 Fransisca Haryani Candra, *Internet : Information Superhighway,* Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi melalui Media Komputer bagi Dosen PTS Kopertis Wilayah VI, Semarang, hal. 1-2.

(protokol) yang sama. Protokol yang digunakan tersebut adalah TCP/IP (*Transmission Control Protocol/Internet Protocol*)

The Federal Networking Council (FNC) memberikan definisi mengenai internet dalam resolusinya tanggal 24 Okober 1995. definisi yang diberikan adalah sebagai berikut :

Internet refers to the global information system that :

a. *Is logically linked together by a globally system unique address space based in the Internet Protocol (IP) or its subsequent extensions/followons*
b. *Is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extension/follow-ons, and/or other IP-compatible protocols, and*
c. *Provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastucture described here in.*[41]

Di indonesia internet berkembang dan menjamur sekitar tahun 1995. Pada awalnya internet masuk ke Indonesia melalui jaringan akademis dan pusat riset, sehingga hanya golongan akademis dan peneliti yang dapat memanfaatkannya. Itupun masih terbatas pada fasilitas e-mail saja.[42]

Kemudian layanan internet mulai terbuka untuk umum. Indo internet berdiri sebagai Penyelia Jasa Internet (PJI) atau *Internet Service Provider* (ISP) pertama di Indonesia. PJI Lainnya kemudian

---

41 of the Nerds" A History of Computer

42 http://www.hukumonline.com/artikel_detail.asp?id=5212

bermunculan seperti Indosat, Radnet, Idola, CBN, Wasantara Net, Meganet dan Telkomnet.

Internet telah membuka dunia baru dimana setiap orang bisa masuk tanpa ada batas untuk komunikasi dan informasi. Pemanfaatan teknologinya juga mendorong pertumbuhan bisnis, pendidikan termasuk juga pengaruh negatifnya. Dunia baru yang tercipta dari internet ini disebut *cyberspace.*

Cyberspace merupakan tempat pengguna internet menjelajahi dunia informasi global. Istilah *cyberspace* yang pertama kali digunakan William Gibson dalam fiksi ilmiahnya *Neoromancer.* Namun dalam konteks internet, John Perry Barlow mengklaim sebagai pengguna pertama.[43]

Bruce Sterling memberikan definisi tentang pengertian *cyberspace* :[44]

> Cyberspace is the "place" where a telephone conversation appears to occur. Not your desk. Not inside the other person's phone, in some other city. The pace between the phone. The indefinite place out there, where two of you, two human beings, actually meet and communication.

---

[43] Jeff Sallesky, *Spiritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia, Op cit,* hal. 9.
[44] http://www.lysator.liu.se/etexts/hacker/

Cyberspace mnampilkan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat melainkan realitas virtual (virtual reality), dunia yang tanpa batas. Inilah yang disebut borderless world, karena memang dalam cyberspace tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu dan tempat.[45]

Lebih lanjut Bruce Sterling mengungkapkan :

Although it is not exactly "real", "cyberspace" is a genuine place. Things happen that have very genuine consequences. This places is not "real" but it is serious, it is earnest. Ten of thousands of people have dedicated their lives to it, the public services of public communication by wire and electronic.[46]

Cyberspace memberikan dunia alternatif yang berbeda dari dunia realitas. Jagad raya *cyberspace* telah membawa masyarakat dalam berbagai sisi realitas baru yang tidak pernah terbayangkan sebelumnya, yang penuh dengan harapan, kesenangan, kemudahan dan pengembangan seperti teleshopping, *teleconference, teledildonic, virtual cafe, virtual architecture, virtual museum, cybersex, cyberparty, cyberorgasm.*[47]

Sementara itu, software yang dipakai dalam internet juga mengalami perkembangan dengan diperkenalkannya Gopher oleh Paul

---

[45] Onno W. Purbo, *Perkembangan Teknoogi Informasi dan Internet di Indonesia*, Kompas 28 Juni 2000.
[46] http://www.lysator.liu.se/etexts/hacker/
[47] Yasraf Amir Piliang dalam Mark Slouka, *Ruang yang Hilang, Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan*, Mizan, Bandung, 1999, hal 14-15.

Lidner dan Mark P. Mc Cathill dari University of Minnesota tahun 1991. Gopher merupakan sistem penampilan dan pengaksesan informasi di Internet yang disusun secara hierarkhis dan terstruktur sehingga mempermudah pemakai untuk mencari dan mendapatkan informasi yang diinginkannya. Gopher merupakan dasar pengembangan sistem *World Wide Web*.

Pada tahun itu juga, *World Wide Web* (WWW) juga diperkenalkan oleh CERN yang dipimpin oleh Tim Berners-Lee sebagai pengembangnya. Lalu lintas yang terjadi di NSFNET pada tahun 1991 itu mencapai 1 triliun bytes/tahun dan 10 billion packet/bulan.

Pada bulan Januari 1992, dibentuk *Internet Society* (ISOC) sebagai reaksi dari meledaknya pengguna internet. Ide pembentukan ini setelah melalui diskusi dalam pertemuan *Internet Activities Board* (IAB) dan *Internet Engineering Task Force* (IETF) di tahun 1991. pertemuan tahunan ISOC pertama berlangsung di Kobe Jepang.[48]

Di eropa, pada waktu yang bersamaan dibentuk RIPE *Network Coordination interNIC* yang menyediakan pelayanan untuk *directory and database* (AT&T), *registration services and Information*

[48] http://www.isoc.org/internet/history/iefthis.html

services. Pada tahun ini pemerintah Amerika membuka on-line untuk umum, yang diikuti oleh negara-negara lain pada tahun berikutnya.

Domain Name System (DNS) yang pada awalnya dapat diperoleh secara gratis dalam perkembangannya menjadi tidak gratis lagi. Biaya DNS yang semula disubsidi oleh NFS, mulai tanggal 14 September 1996 ditentukan biaya tahunan 50 dollar, sedangkan NFS tetap membayar domain.edu dan sementara domain yang berbasis.gov.[49]

Hardware dan software internet terus mengalami perkambangan, bahkan akan terus berlangsung dan digunakan untuk berbagai keperluan seperti yang diungkapkan Vinton Cerf :

It seems likely that the internet will continue to be the environment of choice for the deployment of new prorocols and for the linking of divers systems in the academic, goverment, and bussines sectors for the remainders of this decade and well inti the next.[50]

Selanjutnya teknologi yang digunakan dalam berinternet adalah teknologu jaringan komputer yakni hubungan antara satu komputer dengan komputer lain atau beberapa komputer lain. Beberapa komputer dapat dihubungkan satu dengan lainnya melalui sambungan

---

[49] Agus Raharjo, *Cybercrime, Upaya Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002, hal. 56.

[50] http://www.isoc.org/internet/history/v.cerf.html

telephone atau melalui jaringan komputer lokal (*local area network*) dan dapat juga melalui jaringan komputer luas (*wide area network*).

Jika ingin berinternet, maka orang harus melengkapi komputernya dengan berbagai perangkat yang diperlukan antara lain telpon, modem (*modulator-demodulator*) sebagai perangkat linak komunikasi. Komputer yang diperlukan untuk dapat mengakses ke dalam jaringan komputer (internet) adalah komputer PC/XT dengan kapasitas minimal 268, 1 Mbyte dan 40 Mbyte harddisk. Komputer dengan kapasitas yang semakin besar akan lebih baik dalam melakukan akses.

Akses dilakukan dengan menghubungi nomor yang telah ditentukan ke *Internet Service Provider* (ISP). ISP merupakan suatu organisasi atau perusahaan yang memberikan jasa hubungan internet bagi para pengguna komputer dengan menarik sejumlah biaya. ISP sering hanya disebut dengan *Provider* saja.

Di samping menggunakan alat komunikasi dengan kabel telpon, ISP juga menyediakan sarana yang membuat akses ke internet lebih cepat tanpa memerlukan kabel telpon, yakni dengan menggunakan saluran *terestrial*, melalui satelit atau juga melalui gelombang radio.

2. Perkembangan *Cybercrime* (Kejahatan Siber)

Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, dimana kejahatan tersebut telah muncul sejak permulaan jaman dan akan berlangsung terus di masa yang akan datang.

Kejahatan telah diterima sebagai suatu fakta yang merugikan, baik pada masyarakat yang paling sederhana (primitif), maupun pada masyaeakat modern. Kerugian yang ditimbulkan itu dapat berupa kerugian dalam arti materiil maupun moril. Kerugian materiil berupa timbulnya korban kejahatan dan rusak atau musnahnya harat benda serta meningkatnya biaya yang harus dikeluarkan bagi penanggulangannya. Kerugian moral berupa berkurang aau hilangnya kepercayaan masyarakat terhadap pelaksanaan penegakan hukum yang dilakukan oleh aparat hukum.[51]

P.J. Fitzgerald mengemukakan bahwa kejahatan itu adalah sesuatu yang relatif, tidak terlepas dari perbedaan waktu dan sudut pandang massyarakat. ("*admitted bay different societes at different times take different views about what conduct is right or wrong;*

[51] Romli Atmasasmita, *Kapita Selekta Kriminologi*, Asmico, Bandung, 1982, hal. 8.

wether a crime is thought wrong in it self or only legally will depend on the moral code current society")[52]

Kejahatan yang terus berkembang tidak hanya pada masyarakat yang sudah maju namun juga pada masyarakat yang sedang berkembang. Kejahatan tidak hanya terjadi di dunia nyata (*real world*), akan tetapi juga terjadi di dunia maya (*virtual/cyber*).

Apabila mengikuti kasus-kasus kejahatan komputer dan *cybercrime* yang telah terjadi dan jika hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka ternyata bahwa dari segi hukum, kejahatan komputer dan siber bukanlah kejahatan yang sederhana.[53]

Sampai saat ini, belum disepakati definisi yang jelas mengenai *cybercrime*, demikian juga dengan istilah yang dipergunakan. Selain *cybercrime* juga ada yang menggunakan istilah *computer crimes* atau *computer-related crimes*. Singapura dalam undang-undangnya menggunakan *Computer Misuse*, sedangkan Malaysia secara tegas menggunakan istilah *Computer Crimes*. *Background Paper* untuk Lokakarya pada Kongres PBB X/2000 menggunakan istilah *Cyber*

---

[52] P.J. Fitzgerald, *Criminal Law Punishment*, Clarendon Press, Oxford, 1962, hal. 6.
[53] David I. Bainbridge, *Komputer dan Hukum*, terjemahan dari "*Computer and the Law*", Cet. I, PT Sinar Grafika, Jakarta, 1003, hal. 161.

Crime. Dalam dokumen tersebut dijelaskan bahwa *Cybercrime* dapat dibagi dalam dua kategori, yaitu *cybercrime* dalam arti sempit (*in a narrow sense*) disebut *computer crime* dan *cybercrime* dalam arti luas (*in a boder sense*) yang disebut dengan *computer-related crimes*.[54] Dalam dokumen itu dijelaskan :

a. *Cybercrime in a narrow sense (computer crime)*
   Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;
b. *Cybercrime in a broder sense (computer-related crime)*
   Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by menas of a computer system or network.

OECD membuat definisi kerja (working definiton) tentang Computer Abuse, yaitu :[55]

"Computer Abuse (use in the same fashion as "computer rea=lated crimes") is considered as any illegal, unerthical or unauthorized behaviour relating to the automatic processing anf the transmission of data".

---

[54] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Penanggulangan Kejahatan, Op cit*, hal. 249.
[55] Muladi, *Kebijakan Kriminal terhadap Cybercrime, Op.Cit.*, hal. 4.

Information Technology Association of Canada (ITAC) pada "*International Information Industry Congress (ICC) 2000 Millenium Congress*" di Quebec pada tanggal 19 September 2000 menyatakan bahwa :

"*Cybercrime is a real and growing threat to economic and social development eround the world, information technology touchs every aspect of human lifr and so can electronically enabled crime.*"[56]

Kepolisian Inggris memberikan definisi sebagai berikut :[57]

Cybercrime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Bentuk-bentuk kejahatan tersebut dapat berupa spionase informasi, pencurian data, pemalsuan credit card, penyebaran virus komputer, pornografi anak, penyebaran e-mail bermasalah, hingga kampanye SARA, terorieme, ekstrimisme di Internet.

Cybercrime dapat diartikan juga sebagai penyalahgunaan internet, yaitu sesuatu yang bermaslahat dan mutlak dibutuhkan oleh masyarakat sehingga harus ada, tetapi disalahgunakan untuk merusak kehidupan masyarakat di luar tujuan yang diciptakannya.[58]

---

[56] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Penanggulangan Kejahatan*, Op.Cit, hal. 244.
[57] Ade Maman Suherman, *Aspek Hukum dalam Ekonomi Global*, Ghalia Indonesia, Jakarta, 2002, hal. 168.
[58] http://www.pikiran-rakyat.com/prcetak/062001/15/0802.htm

Convention of Cybercrime oleh Councial of Europe menyebutkan bentuk-bentuk *Cybercrime*, yaitu :[59]

a. *Offences against the confidentially, integrity and availability of computer anda data systems. (tittle 1)*
   1) *Illegal access (Article 2)*
   2) *Illegal interception (Article 3)*
   3) *Data interference (Article 4)*
   4) *System Interference (Article 5)*
   5) *Misuse related offences (Article 6)*
b. *Computer related offences (Tittle 2)*
   1) *Computer related forgery (Article 7)*
   2) *Computer related fraud (Article 8)*
c. *Content related offences (Tittle 3)*
   Offences related to child pornography
d. *Offences related to infringements of copy right and related right*

Sementara itu dalam *Tenth UN Congress on The Prevention of Crime and the Treatment of Offenders* yang diselenggarakan di Wina

[59] Council of Europe, Convention of Cybercrime-Budapest 23.IX.2001, European Treaties Series No. 185.

pada tanggal 10-17 April 2000, menyebutkan bahwa : "*...the confidentially, integrity or availabillity offences include* :[60]

a. *Unauthorizied acces, meaning acces without right to a computer system or network by infringing security measures;*
b. *Damage to computer data or computer programs, meaning the erasure, corruption, deterioration or supression of computer data or computer programs without right;*
c. *Computer sabotage, meaning the input, alteration, erasure or suppression of computer, or interference with computer system, with the intent to hinder the function of a computer or a telecommunication system;*
d. *Unauthorized interception, meaning the interception, made without authorization and by technical means of communication to, from and within a computer system or network;*
e. *Computer espionage, meaning the acquaisition, disclosure, transfer or use of a commercial secret without authorization or legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an illegal adventage for themselves or a third person.*

Heru Supraptomo memberikan bentuk-bentuk kejahatan siber/komputer :[61]

a. Penipuan komputer (*Computer Fraud*) yang mencakup :

   1) Bentuk dan jenis penipuan adalah berupa pencucian uang atau harta benda dengan menggunakan sarana komputer/siber dengan melawan hukum, ialah dalam bentuk penipuan data dan penipuan program, yang secara terinci adalah :

---

[60] *Tenth UN Congress on The Prevention Crime and The Treatments of Offenders*, A/CONF.187.10, hal.5
[61] Heru Supartomo, *Op.Cit.*, hal, 5-6.

a) Memasukkan instruksi yang tidak sah, ialah dilakukan oleh seorang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya transfer);

b) Mengubah data input yang dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum (misalnya memasukkan data gaji pegawai melebihi yang seharusnya);

c) Merusak data, ialah dilakukan seseorang untuk merusak print out atau output dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan itikad tidak baik;

d) Penggunaan komputer untuk sarana melakukan perbuatan pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan;

2) Perbuatan pidana penipuan yang sesungguhnya dapat termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan diri dari kewajiban (misalnya pajak) atau untuk memperoleh sesuatu yanb bukan hal/miliknya melalui sarana komputer;

3) Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses komputer mentransfer rekening orang lain ke rekenignya sendiri, sehingga merugikan orang lain;

4) Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang bersama-sama untuk melakukan penipuan dengan sarana komputer;

5) Pencurian, ialah dengan sengaja mengambil dengan melawan hukum, hak atau milik orang lain dengan maksud untuk dimilikinya sendiri.

b. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri;

c. *Hacking*, ialah melakukan akses terhadap sistem komputer tanpa seijin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan kompouter yang dapat mengancam berbagai kepentingan;

d. Perbuatan pidana komunikasi ialah *hacking* yang dapat membobol sistem on-line komputer yang menggunakan sistem komunikasi;

e. Perbuatan pidana perusakan komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian. Termasuk dalam golongan perbuatan ini adalah berupa penambahan atau perubahan program, informasi, media sehingga merusak sistem, demikian pula sengaja menyebarkan virus yang dapat merusak program dan sistem komputer atau pemerasan dengan menggunakan sarana komputer/telekomunikasi;

f. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk emndapatkan keuntungan melalui perdagangan.

Jenis perbuatan pidana tersebut pada dasarnya dapat terjadi jika komputer dihubungkan dengan teknologi telekomunikasi dan informasi, sehingga menjadi kejahatan siber, terutama dengan berkembangnya teknlogi internet. Dengan demikian, *cybercrime* (kejahatan internet) merupakan kejahatan yang terjadi dalam jaringan komputer (*cyberspace*).

3. Jurisdiksi

Menurut Kamus Besar Bahasa Indonesia, pengertian "jurisdiksi" adalah :[62]

a. Kekuasaan mengabdi lingkungan kuasa kehakiman; peradilan
b. Lingkungan hak dan kewajiban serta tanggung jawab di suatu wilayah atau lingkungan tertentu; kekuasaan hukum.

Black's Law Dictionary memberikan definisi tentang jurisdiksi (*jurisdiction*) adalah :[63]

a. *The word is a term of large and comprehensive import and embraces over kind of judicial action;*
b. *It is the authority by which courts and judicial officers take cognizance of anf decide cases;*
c. *The legal right by which judge exercise their authority;*
d. *It exists when courts has cognizance of class of cases involved, proper parties are present, anp point to be decided is within power of court;*
e. *Power and authority of court to hear anf detemine a judicial proceeding;*
f. *The right of power of a court to adjudicate concerning the subject matter ia a given case.*

Masalah jurisdiksi dalam hukum pidana terkait dengan persoalan berlakunya hukum di suatu wilayah/negara yang berdaulat. Terdapat azas-azas yang membatasi berlakunya hukum pidana tersebut, yakni

---

[62] Departemen Pendidikan dan Kebudayaan, *Kamus Besar Bahasa Indonesia*, Cet.II, Balai Pustaka, Jakarta, 1997, hal. 1134.
[63] Henry Campbel Black, *Black's Law Dictionary, Op.Cit.* pg. 766.

berdasarkan lokasi/tempat (*locus delicti*) dan berdasarkan waktu (*tempus delicti*).

Berdasarkan lokasi dan tempat, ada beberapa asas yang digunakan, antara lain :[64]

a. Azas Teritorial
b. Azas Personal atau Azas Nasional Aktif
c. Azas Perlindungan atau Azas Nasional Pasif
d. Azas Universal

Ruang lingkup jurisdiksi berkenaan dengan penetapan dan pelaksanaan pengawasan terhadap setiap peristiwa, setiap benda dan setiap orang yang dimiliki oleh negara, ada 3, yaitu :[65]

a. Jurisdiksi untuk menetapkan ketentuan pidana (*jurisdiction to prescribe atau legislative jurisdiction atau perspective jurisdiction*).

   Negara, khususnya badan legislatif lebih leluasa dalam melaksanakan *jurisdiction to prescribe* sebab kewenangan untuk menetapkan itu membuat ketentuan hukum tidak dibatasi oleh kekuasaan negara lain. Sebagi organ negara yang berdaulat, badan

---

[64] Sudarto, *Hukum Pidana I*, Cet. II, Yayasan Sudarto, Semarang, 1990, hal. 32.
[65] Tien S. Saifullah, *Cyberlaw Suatu Pengantar : Yurisdiksi sebagai Upaya Hukum dalam Kegiatan Cyberspace*, ELIPS II, Jakarta, 2002, hal. 97.

legislatif punya wewenang penuh untuk mengatur apa saja dalam ketentuan hukum yang dibuatnya, termasuk dalam ketentuan pidananya.

b. Jurisdiksi untuk menetapkan atau melaksanakan ketentuan yang telah ditetapkan oleh badan legislatif (*executive jurisdiction*)

Negara tidak bebas untuk melaksanakan jurisdiksinya sebab harus berhadapan dengan kekuasaan negara lain. Pembatasan yang berlaku dalam hukum internasional adalah bahwa suatu negara tidak boleh melakukan kegiatan yang melanggar kedaulatan negara lain, maka dalam melaksanakan kewajibannya berdasarkan executive jurisdiction, suatu organ negara, baik Kepolisian maupun Kejaksaan tidak dapat dengan bebeas melakukan penelitian dan pemeriksaan di dalam wilayah negara lain. Dalam hal ini, kerja sama antar negara amat dibutuhkan sehingga tujuan untuk mendapatkan bukti-bukti dan keterangan-keterangan, tanpa melanggar prinsip yang berlaku dalam hukum internasional.

c. Jurisdiksi untuk memaksakan ketentuan yang telah dilaksanakan oleh badan eksekutif atau yang telah diputuskan oleh badan peradilan (*enforcement jurisdiction atau jurisdiction to adjudicate*).

Negara tidak boleh memaksakan putusan pengadilan tetrhadap orang yang melakukan tindak pidana yang berada di wilayah jurisdiksi negara lain.

Masaki Hamono mengemukakan tiga kategori jurisdiksi yang didasarkan pada prinsip-prinsip tradisional, yaitu : yurisdiksi legislatif (*legislative juurisdiction atau jurisdiction to prescribe*), jurisdiksi judisial (*judicial jurisdiction atau jurisdiction to adjudicate*) dan jurisdiksi eksekutif (*executive jurisdiction atau jurisdiction to enforce*).[66]

Persoalan jurisdiksi di dunia cyber (*cyberspace*) menjadi hal yang urgent dalam penegakan hukum untuk *cybercrime*, karena keterbatasan jurisdiksi berdasarkan prinsip-prinsip tradisional/konvensional. Beberapa sarjana memberikan pendapat tentang jurisdiksi di dunia cirtual/cyber (*cyberjurisdiction*).

Masaki Hamono membedakan pengertian *cyberjurisdiction* dari sudut pandang dunia *cyber/virtual* dan dari sudut hukum. Dari sudut dunia virtual, cyberspace sering diartikan sebagai "kekuasaan sistem operator dan para pengguna (users) untuk menetapkan aturan dan

---

[66] Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, RajaGrafindo Persada, Jakarta, 2002, hal. 275.

melaksanakannya pada suatu masyarakat di ruang *cyber/virtual*". Dari sudut hukum, *cyberjurisdiction* atau *jurisdiction in cyberspace* adalah "kekuasaan fisik pemerintah dan kewenangan pengadilan terhadap pengguna internet atau terhadap aktivitas mereka di ruang *cyber*" (*physical goverment's power and court's authority over Net users or their activity in cyberspace*).[67]

Darrel Menthe menyebutkan suatu wilayah teritorial yang menggunakan hukum internasional dan disebutnya *international space* (ruang internasional); saat ini ada tiga macam ruang internasional yaitu ; antartica, angkasa luar dan lautan luas. Dalam dunia *cyber*, jurisdiksi mengesampingkan masalah konsep untuk pengadilan domestik dan pengadilan asing yang serupa. Tidak seperti jurisdiksi tradisional yang melibatkan dua atau tiga jurisdiksi yang bertentangan satu sama lain, maka hukum yang dapat diterapkan terhadap *homepage* adalah hukum secara keseluruhan.[68]

Menthe membedakan tiga jenis jurisdiksi yang diakui secara internasional, yaitu : *jurisdiction to prescribe, jurisdiction to*

---

[67] *Ibid*, hal. 276.
[68] Darrel Menthe, *Jurisdicion in A Cyberspace : A Theory of International Spaces*, tersedia pada http://www.mttlr.org/vlogfour/menthe.html.

adjudicate dan *jurisdiction to enforce*. Pendapat Menthe ini sama dengan pendapat Masaki Hamano.

Sedangkan untuk jurisdiksi di internet, Menthe mengemukakan teori bahwa selama berinteraksi di dunia *cyber*, ada dua hal utama, yaitu memberikan informasi ke dalam dunia *cyber* dan mengambil informasi keluar dari dunia *cyber*. Pihak yang memasukkan informasi ke dalam suatu lokasi dalam *cyberspace* disebut *uploader*, sedangkan pihak-pihak yang mengakses/mengambil informasi di *cyberspace* disebut *downloader*. Darel Menthe menyebut teori ini dengan "*The Theory of Uploader and The Downloader*."[69]

Masalah jurisdiksi *cyber* pada hakikatnya berkaitan dengan masalah kekuasaan atau kewenangan, yaitu siapa yang berkuasa/berwenang mengatur dunia internet. Mengenai masalah ini, David R. Johnson dan David G. Prost dalam artikelnya yang berjudul "*And How Should The Internet be Governed?*" mengemukakan 4 model yang bersaing, yaitu : (1) pelaksanaan kontrol dilakukan oleh badan-badan pengadilan yang saat ini ada; (2) penguasa nasional melakkan kesepakatan internasional mengenai *the government of cyberspace*; (3) pembentukan suatu organisasi internasional baru yang

[69] *Ibid.*

secara khusus menangani maslah-masalah di dunia internet; dan (4) pemerintahan/pengaturan sendiri (*self governance*) oleh para pengguna internet.[70]

Menurut Barda Nawawi Arief, sistem hukum dan jurisdiksi memang mempunyai keterbatasan karena tidaklah mudah menjangkau pelaku tindak pidana di ruang *cyber* yang tidak terbatas. Namun tidak berarti aktivitas di ruang *cyber* dibiarkan bebas tanpa hukum. Ruang *cyber* merupakan juga bagian atau perluasan dari lingkungan (*environment*) dan lingkungan hidup (*life environment*) yang perlu dipelihara dan dijaga kualitasnya. Jadi merupakan juga suatu kepentingan hukum yang dilindungi. Oleh karena itu, jurisdiksi legislatif (*jurisdiction to prescribe*) tetap dapat dan harus difungsikan untuk menanggulangi *cybercrime* yang merupakan dimensi baru dari *enviromental crime*.[71]

---

[70] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Penanggulangan Kejahatan, Op.Cit.*, hal. 277.
[71] *Ibid*, hal. 279.

BAB III

HASIL PENELITIAN & ANALISA

A. PENANGGULANGAN CYBERCRIME DENGAN HUKUM POSITIF

Teknologi mengalami perkembangan yang sangat pesat, namun tidak demikian halnya dengan hukum. Perangkat hukum yang ada terkadang dirasa belum mampu untuk mengakomodasi perkembangan teknologi khususnya teknologi tingkat tinggi *(hitech)* seperti teknolgi informasi. Perkembangan teknologi mempunyai dua sisi yang berbeda. Disatu sisi sangat berperan dan bermanfaat dalam kemajuan zaman dan di sisi lain menimbulkan sisi gelap yaitu kejahatan yang juga berkembang sebagai dampak kemajuan teknologi informasi.

Kejahatan yang muncul berdimensi baru dengan menggunakan teknologi tinggi dan dapat mempengaruhi berbagai aspek seperti ekonomi, politik, budaya, sosial, pendidikan dan sebagainya. Kunarto menyebutkan ciri-ciri kejahatan tersebut adalah :[72]

[72] Suyitno & E.Brata Mandala, *Strategi dan Teknik Penyidikan terhadap Kejahatan Telematika,* Makalah pada Seminar Strategi Penanggulangan Kejahatan dalam Bidang Telematika, Universitas Semarang, 23 Juli 2002, hal. 1.

- Kejahatan yang belum dikenal, belum pernah terjadi dan baru sekali ini terjadi. Berarti tidak tercakup dalam KUHP bahkan mungkin belum tertuang dalam undang-undang yang ada di Indonesia.
- Kejahatan konvensional yang dalam melaksanakannya memerlukan peralatan dengan menggunakan teknologi baru;
- Kejahatan yang dilakukan dengan memanfaatkan celah-celah hukum yang ada. Dengan kata lain, perbuatan kejahatan yang tidak terjangkau oleh hukum.

Salah satu usaha penanggulangan kejahatan ialah menggunakan hukum pidana. Namun usaha inipun masih terus dipersoalkan. Perbedaan mengenai peranan pidana dalam menghadapi masalah kejahatan ini, menurut Inkeri Anttila sudah berlangsung beratus-ratus tahun dan menurut Herbert L. Packer, usaha pengendalian perbuatan anti sosial dengan menggunakan pidana pada seseorang yang bersalah melanggar peraturan pidana, merupakan suatu problem sosial yang mempunyai dimensi hukum yang penting.[73]

---

[73] Barda Nawawi Arief, *Kebijakan Legislatif dalam Menanggulangi Kejahatan dengan Pidana Penjara*, Badan Penerbit UNDIP, Semarang, 2000, hal. 16.

Herbert L. Packer dalam bukunya *The Limits of Criminal Sanction* membicarakan masalah pidana dengan segala keterbatasannya dan akhirnya menyimpulkan sebagai berikut:[74]

1. Sanksi pidana sangatlah diperlukan, kita tidak dapat hidup, sekarang maupun di masa yang akan datang, tanpa pidana.
   (The criminal sanction is indispensable, we could not, now or in the foreseable future, get along without it).
2. Sanksi pidana merupakan alat atau sarana terbaik yang tersedia, yang kita miliki untuk menghadapi kejahatan-kejahatan atau bahaya besar dan segera serta untuk menghadapi ancaman-ancaman dari bahaya.
   (The criminal sanction is the best available device we have for dealing with gross and immediate harms and threats of harm).
3. Sanksi pidana suatu ketika merupakan "penjamin yang utama atau terbaik" dan suatu ketika merupakan "pengancam yang utama" dari kebebasan manusia. Ia merupakan penjamin apabila digunakan secara hemat, cermat dan secara manusiawi; ia merupakan pengancam, apabila digunakan secara sembarangan dan secara paksa.
   (The criminal sanction is at once prime guarantor and prime threatener of human freedom. Used providently and humanely, it is guarantor; used indiscriminately and coercively, it is threatener)

Keterbatasan yang dimiliki oleh hukum positif tidak berarti membiarkan kejahatan tersebut terus berkembang. Hukum positif yang ada perlu diberdayakan dalam rangka menanggulangi kejahatan di dunia virtual *(cyberspace)* disamping diperlukan juga upaya pemerintah untuk membentuk peraturan-peraturan baru yang lebih khusus yang mampu mengantisipasi kejahatan tersebut.

---

[74] Muladi dan Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana, Op cit,* hal. 155.

Dalam menanggulangi kejahatan berdimensi baru dengan hukum positif yang ada tidak boleh mengenyampingkan asas dasar dari hukum pidana. Asas yang dimaksud disini adalah asas legalitas. Hal ini bertujuan untuk menjamin adanya kepastian hukum dan perlindungan bagi warga masyarakat agar undang-undang merupakan suatu *lex certa* (undang-undang yang dapat dipercaya).

Disamping itu agar tetap dalam koridor hukum dalam memberdayakan hukum positif yang ada, maka upaya yang dapat ditempuh adalah dengan menggunakan interpretasi. Hal ini untuk mencegah agar tidak terjadi kekosongan hukum, dengan demikian kejahatan yang terus berkembang bisa dicegah dan juga memberikan perlindungan kepada masyarakat.

1. Asas Legalitas dan Metode Interpretasi

a. Azas Legalitas

Asas legalitas merupakan asas dasar/fundamental yang mencerminkan ciri hukum pidana. Azas Legalitas *(Principle of Legality)* merupakan azas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan. Dalam bahasa Latin dikenal dengan

Nullum delictum noella poena sine praevia lege.[75] Ucapan ini pertama kali dikemukakan oleh Paul Johann Anselm von Feurbach (1775-1833), seorang sarjana hukum pidana Jerman dalam bukunya *"Lehrbuch des Peinlichen Recht"*.

Menurut Van Bemmelen, Aturan Legalitas memunculkan tiga peraturan lain : [76]

1) Setiap penggunaan pidana hanya dapat dilakukan berdasarkan hukum pidana *(nulla poena sine lege),*
2) Penggunaan pidana hanya mungkin dilakukan jika terjadi perbuatan yang diancam dengan pidana oleh Undang-undang *(nulla poena sine crimen),*
3) Perbuatan yang diancam dengan pidana menurut Undang-undang membawa akibat hukum bahwa pidana yang diancamkan oleh Undang-undang dijatuhkan *(nullum crimen sine poena legali).*

Sedangkan Menurut Moeljatno, asas Legalitas mengandung 3 (tiga) pengertian:[77]

1) Tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan undang-undang;
2) Untuk menentukan adanya perbuatan tidak boleh digunakan analogi (kiyas)
3) Aturan-aturan hukum pidana tidak berlaku surut.

---

[75] Moeljatno, *Asas-asas Hukum Pidana* Cet. VI, ,Rineka Cipta, Jakarta, 2000, hal 23.
[76] Van Bemmelen, *Hukum Pidana 1*, Terjemahan, Binacipta, Bandung, 1987, hal. 51.
[77] Moeljatno, *Asas-Asas Hukum Pidana, Op cit,* hal.25.

Nico Kejzer dalam Al. Wisnubroto mengemukakan bahwa asas legalitas tersebut pada dasarnya mengandung aspek-aspek sebagai berikut:[78]

1) Tidak dapat dipidana kecuali berdasarkan ketentuan pidana menurut undang-undang.
2) Tidak ada penerapan undang-undang hukum pidana analogis/qiyas
3) Tidak dapat dipidana hanya berdasarkan kebiasaan
4) Tidak ada kekuatan surut dari ketentuan pidana
5) Tidak ada pidana lain kecuali yang ditentukan oleh undang-undang.
6) Tidak boleh ada perumusan delik yang kurang jelas.
7) Penjatuhan pidana hanya diperbolehkan menurut cara yang ditetapkan undang-undang

Asas legalitas dimaksudkan untuk menjamin adanya kepastian hukum. Ini berarti memberikan perlindungan kepada masyarakat dari penyalahgunaan kekuasaan atau kesewenang-wenangan penguasa.

Di Indonesia asas ini terlihat dalam KUHP. Pasal 1 ayat (1) mengaturnya dengan rumusan: "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada sebelum perbuatan dilakukan".[79]

---

[78] Al. Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,Op cit,* hal. 60.

[79] Moeljatno, *KUHP,*Bumi Aksara, Jakarta, 1999.

Oemar Seno Adji mengatakan asas legalitas *(principles of legality)* yang menyatakan bahwa suatu perbuatan tidak dapat dipidana apabila tidak berdasarkan ketentuan hukum yang ada, melarang analogi, dan tidak dapat diperlakukan surut *(retroaktif)*, dipandang sebagai *palladium* dari kepastian hukum dan terdapat dalam semua KUHP sebagai suatu persamaan, suatu identitas dalam asas hukum pidana.[80]

Cesare Beccaria dalam bukunya *"Dei Delitti e Delle Pene"* tahun 1764, mengatakan bahwa hanya Undang-undang yang boleh menentukan pidana terhadap setiap tindak pidana, dan bahwa hak untuk membuat Undang-undang pidana harus berada di tangan pembuat Undang-undang, yang karena perjanjian masyarakat mewakili seluruh masyarakat.[81] Ada 8 (delapan) prinsip dikemukakan Beccaria dalam bukunya tersebut yang menjadi landasan bagaimana hukum pidana, hukum acara pidana dan proses penghukuman dilakukan. Kedelapan prinsip itu adalah:[82]

---

[80] Oemar Seno Adji, dalam Andi Hamzah, ***KUHP Malaysia***, Ghalia Indonesia, Jakarta, 1987, hal. 9.
[81] Van Bemmelen, *Opcit*, hal. 50.
[82] Eva Achjani Zulfa, *Studi tentang Asas Legalitas dalam Perundang-undangan Indonesia* dalam Jurnal Penelitian FHUI Vol 2 No.2, Badan Penerbit FHUI, 2001, hal. 74.

1) Perlunya dibentuk suatu masyarakat berdasarkan prinsip *social contract;*
2) Sumber hukum adalah undang-undang dan bukan hakim. Penjatuhan hukuman oleh hakim harus berdasarkan semata-mata karena undang-undang;
3) Tugas dari seorang hakim hanyalah menentukan kesalahan seseorang;
4) Menghukum adalah merupakan hak negara dan hak itu diperlukan untuk melindungi masyarakat dari keserakahan individu;
5) Harus dibuat suatu skala perbandingan antara kejahatan dan penghukuman;
6) Motif manusia pada dasarnya didasarkan pada keuntungan dan kerugian;
7) Dalam menentukan besarnya kerugian yang ditimbulkan oleh suatu kejahatan maka yang menjadi dasar penentuan hukuman adalah perbuatannya bukan niatnya;
8) Prinsip dari hukum pidana adalah pada sanksinya yang positif.

Pentingnya landasan legalitas juga karena legalitas merupakan salah satu faktor untuk adanya keadilan, seperti dikatakan G. Peter Hoefnagels:[83]

Saya setuju dengan pandangan bahwa efektivitas merupakan prasyarat untuk keabsahan dan bahkan merupakan unsur yang patut diperhitungkan dalam hal pemidanaan, tetapi efektifitas itu sendiri bukanlah jaminan untuk adanya keadilan. Pidana dibatasi tidak hanya oleh efektivitas dan kegunaan, tetapi terutama dibatasi oleh legalitas. *(I agree with the view that effectiveness is a prerequisite for lawfulness and even an element to be taken into account in sentencing, effectiveness alone is no guarantee of justice. Punishment in criminal law is limited not only by effectiveness and purposefulness, but above all by legality).*

[83] Barda Nawawi Arief, *Kebijakan Legislatif dalam Menanggulangi Kejahatan dengan Pidana Penjara, Op cit,* hal. 3.

Disamping itu Legalitas sangat penting mengingat pengaruh tradisi hukum *civil law* yang telah mengakar kuat dalam sistem hukum pidana nasional di Indonesia, sehingga pengaruh dari sistem hukum yang berkembang di Eropa Kontinental akan tetap dominan. Hal ini kemudian terlihat dengan kembali diadopsinya asas ini pada Rancangan KUHP tahun 2000 Pasal 1 ayat (1), yang berbunyi : Tiada seorangpun dapat dipidana atau dikenakan tindakan, kecuali perbuatan yang dilakukan telah ditetapkan sebagai tindak pidana dalam peraturan perundang-undangan yang berlaku pada saat perbuatan itu dilakukan.

Dalam hukum positif dan perkembangannya di Indonesia (dalam UUDS 1950, UU No. 1 Drt 1951 tentang Susunan Pengadilan Negeri dan UU No. 14 Tahun 1970 jo UU No. 35 Tahun 1999 tentang Pokok-Pokok Kekuasaan Hukum dan Konsep KUHP Baru), asas legalitas tidak semata-mata diartikan sebagai *"nullum delictum sine lege"*, tetapi juga sebagai *"nullum delictum sine ius"* atau tidak semata-mata dilihat sebagai asas legalitas formal tetapi juga legalitas materiel. [84] Sebagai contoh dapat dilihat dalam Rancangan KUHP pada Pasal 1 ayat (3) yang menyebutkan, Ketentuan sebagaimana dimaksud dalam ayat (1) tidak mengurangi berlakunya hukum yang hidup atau hukum adat yang

[84] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana,* Citra Aditya Bakti, Bandung, 2003, hal. 10.

menentukan bahwa menurut adat setempat seseorang patut dipidana walaupun perbuatan tersebut tidak diatur dalam peraturan perundang-undangan.

Perkembangan/perubahan yang sangat cepat dan sulit diantisipasi dari *cybercrime* merupakan tantangan cukup besar bagi berlakunya asas *"lex certa"*, karena dunia maya *(cyberspace)* bukan dunia real/realita/nyata/ pasti.[85]

Penyelesaian suatu kasus sangat erat kaitannya dengan asas legalitas. Jika belum ada undang-undang yang melarang suatu perbuatan maka orang yang melakukannya tidak dapat dihukum. Namun dilain pihak jika ada suatu kasus yang menyinggung rasa keadilan masyarakat, maka hakim harus menerima perkara yang diserahkan kepadanya dan tidak boleh menolaknya dengan alasan bahwa belum ada hukum yang mengaturnya. Oleh karena itu untuk mengatasinya agar tidak terdapat kekosongan hukum, hakim harus melakukan penemuan hukum atau dengan cara melakukan interpretasi atau penafsiran hukum. Dalam hal kejahatan *cybercrime* bisa dilakukan penafsiran agar kejahatan tersebut bisa diselesaikan.

---

[85] *Ibid*, hal. 11.

b. **Metode Interpretasi**

Perkembangan teknologi yang pesat diiringi pula dengan sisi negatifnya yaitu perkembangan kejahatan. Hukum sering tertinggal dibanding dengan teknologi. Untuk menyelesaikan kasus-kasus yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet, maka hakim dapat melakukan penafsiran hukum.

Dalam ilmu hukum dikenal beberapa jenis penafsiran:[86]

1) Penafsiran *Gramatikal* berdasarkan uraian pada bahasanya, susunan kata atau bunyi dari sebuah ketentuan perundang-undangan;
2) Penafsiran *Sistematikal* melihat dari keseluruhan perundang-undangan karena terjadinya suatu undnag-undang selalu berkaitan dan berhubungan dengan undang-undang lainnya;
3) Penafsiran *Teologis* atau *sosiologis*, penafsiran yang berdasarkan makna undang-undang itu ditetapkan berdasarkan tujuan kemasyarakatan;
4) Penafisiran *Historis*, dasarnya adalah dengan meneliti sejarah terjadinya;
5) Penafsiran *Komparatif* dengan jalan memperbandingkan hukum;
6) Penafsiran *Futuristis*, adalah invensi hukum yang bersifat antisipasi.
7) Penafsiran *Restriktif* dan *Ekstensif*. Restriktif adalah penjelasan atau penafsiran yang bersifat membatasi sedangkan penafsiran ekstensif dilampaui batas-batas yang diterapkan oleh interpretasi gramatikal.

---

[86] Sudikno Mertokusumo, *Mengenal Hukum (Suatu Pengantar)*, Liberty, Yogyakarta, 1996, hal. 142.

Apabila dikaitkan antara asas legalitas dan metode interpretasi, maka hal penting adalah tidak diterapkannya metode analogi (*qiyas*). Meskipun mengenai kedua hal ini terdapat perbedaan diantara para sarjana.

Moeljatno memberi batas antara penafsiran ekstensif dan analogi. Dalam tafsiran ekstensif tetap berpegang pada aturan yang ada. Ada perkataan yang diberi arti menurut makna yang hidup dalam masyarakat sekarang. Dalam menggunakan analogi, perbuatan yang menjadi soal itu tidak bisa dimasukkan dalam aturan yang ada, berpegang pada ratio.[87] Pendapat Moeljatno ini diikuti oleh Roeslan Saleh dan dikatakannya bahwa analogi bertentangan dengan asas legalitas.[88]

Menurut Sudarto, analogi artinya memperluas berlakunya suatu peraturan dengan mengabstraksikannya menjadi aturan hukum yang menjadi dasar dari peraturan itu *(ratio legis)* dan kemudian menerapkan aturan yang bersifat umum ini kepada perbuatan konkrit yang tidak diatur dalam undang-undang.[89]

---

[87] Moeljatno, *Asas-Asas Hukum Pidana, op-cit,* hal. 28-29.
[88] Roeslan Saleh, *Perbuatan Pidana dan Pertanggungjawaban Pidana,* Aksara Baru, Jakarta, 1983, hal. 43.
[89] Sudarto, *Hukum Pidana I, Op cit* , hal. 23.

Munculnya berbagai kejahatan baru berkaitan dengan internet *(cybercrime)* yang belum diatur secara tegas, maka apabila akan diterapkan peraturan yang ada hendaknya tidak boleh lepas dari asas legalitas. Penafsiran secara analogi bagaimanapun juga tidak diperbolehkan. Namun penafsiran ekstensif diperbolehkan. Agar tidak terjadi penafsiran analogi, maka diperlukan kebijakan hukum pidana yang diarahkan pada pembaharuan perundang-undangan hukum pidana.

2. Kebijakan Hukum Pidana dalam Peraturan Perundang-undangan untuk menanggulangi *Cybercrime*

Seperti dikemukakan pada Bab sebelumnya bahwa belum ada definisi yang seragam tentang *cybercrime*. Perbedaan mendasar dari kejahatan komputer dan kejahatan siber adalah dalam kejahatan siber *(cybercrime)* merupakan perpaduan dari teknologi komputer dan teknologi telekomunikasi yang menghasilkan internet. *Cybercrime* itu sendiri merupakan kejahatan yang terjadi di jaringan internet.

Menurut Muladi, hal yang menarik dari *cybercrime* adalah motivasi dilakukannya perbuatan tersebut. Pelaku *cybercrime* tidak semata-mata karena uang, melainkan adanya suatu tantangan *(challenge)*, yang dipikirkan oleh mereka bukanlah apa yang akan diperoleh dari perbuatan

tersebut (materi) melainkan bagaimana mengakali *(outsmart)* suatu sistem komputer dan menikmati hasil perbuatannya.[90]

Komputer dapat mempermudah suatu bentuk kejahatan yang kuno *(old fashioned)* seperti perbuatan penipuan ataupun perbuatan curang.[91] Penipuan atau perbuatan curang tersebut tentunya dilakukan dengan cara-cara yang baru dan rumit sehingga sulit untuk dilakukan penyelidikan dan penyidikan seperti tindak pidana biasa, karena dalan *cyberspace* sulit untuk diketahui secara pasti dimana sebenarnya suatu peristiwa pidana itu terjadi. Namun demikian harus ada suatu usaha untuk menjaring pelaku kejahatan tersebut.

Hal menarik dari suatu kejahatan komputer adalah rumitnya kejahatan itu dilakukan, kecuali oleh mereka yang memiliki pengetahuan tentang komputer. Belum lagi persoalan dapat atau tidaknya seseorang yang melakukan tindak pidana tersebut dipidana. Menurut Mardjono Reksodiputro dalam Edmon Makarim, kejahatan komputer bukan merupakan kejahatan baru dan masih terjangkau oleh KUHP yang berlaku di negara Indonesia.[92] Manipulasi data komputer sangat sulit untuk

---

[90] Muladi, *Kebijakan Kriminal Terhadap Cybercrime, Op cit*, hal. 4.
[91] David I Bainbridge, *Computer and The Law, Loc cit,*
[92] Edmon Makarim, *Kompilasi Hukum Telematika,* Raja Grafindo Persada, Jakarta, 2003, hal. 390.

ditelusuri, juga sulit untuk mengetahui secara pasti orang yang melakukan penyalahgunaan komputer tersebut.

Karakteristik internet yang tidak lagi mengenal batas wilayah negara *(borderless)* menyebabkan penerapan ketentuan hukum juga menjadi lintas batas wilayah. Sebagai contoh adalah kejahatan *hacking (cracking)* yang dapat dilakukan di berbagai tempat seperti warnet (warung internet), rumah, kantor dan tempat lain. *Hacking* dilakukan di suatu negara dan sistem yang dihacking berada di negara lain. Hal inilah yang menjadikan seolah-olah peraturan pidana tidak bisa efektif dan berakibat tidak dapat ditindaknya pelaku *cybercrime.*

Muladi menyatakan, *cybercrime* merupakan istilah umum yang pengertiannya mencakup berbagai tindak pidana yang diketemukan dalam KUHP atau perundang-undangan pidana lain yang menggunakan teknologi komputer sebagai suatu komponen sentral. Dengan demikian *cybercrime* bisa berupa: tindakan sengaja merusak properti, masuk tanpa ijin, pencurian hak milik intelektual, perbuatan cabul, pemalsuan, pornografi anak, pencurian dan beberapa tindak pidana lainnya.[93] Dengan demikian

---

[93] Muladi, ***Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia,*** Habibie Center, Jakarta 2002, hal. 203.

terhadap tindak pidana dalam dunia maya dapat dikenakan beberapa ketentuan hukum pidana.

Masalah sentral dalam hukum pidana yang dalam penganalisaannya tidak dapat dilepaskan dari konsepsi integral antara kebijakan pembangunan nasional adalah masalah penentuan:[94]

a. perbuatan apa yang seharusnya dijadikan tindak pidana;
b. sanksi apa yang sebaiknya digunakan atau dikenakan kepada sipelanggar.

Penggunaan hukum pidana dalam menanggulangi *cybercrime* dapat dilihat melalui perumusan tindak pidana, dan sanksi pidana. *Cybercrime* merupakan kejahatan yang erat kaitannya dengan konvergensi antara teknologi komputer, telekomunikasi bahkan juga media massa.

Sekalipun saat ini Indonesia belum ada ketentuan yang secara khusus memuat ketentuan mengenai *cybercrime*, namun masalah-masalah yang timbul dengan dunia *cyber* tetap harus diselesaikan oleh aparat penegak hukum, khususnya hakim.

Belum diaturnya masalah *cybercrime* tertentu secara khusus, menyebabkan timbulnya masalah dalam menerapkan ketentuan-ketentuan hukum pidana positif yang ada. Penerapan ketentuan-ketentuan hukum

---

[94] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op cit*, hal. 29.

positif yang ada tidaklah sesederhana penerapan hukum konvensional/di dunia biasa. Hal ini karena karakteristik *cybercrime* bersifat khas, sehingga tidak mudah untuk menafsirkan rumusan ketentuan perundang-undangan hukum pidana yang ada untuk diterapkan terhadap bentuk-bentuk *cybercrime* tertentu secara tepat. Namun demikian terdapat beberapa ketentuan hukum positif yang dapat diterapkan dengan keberanian untuk melakukan terobosan dengan metode interprestasi.

Berikut akan diuraikan peraturan perundang-undangan yang dapat digunakan untuk menjangkau tindak pidana di dunia *cyber (cybercrime)*.

a. **Kitab Undang-undang Hukum Pidana (KUHP)**

Kitab Undang-undang Hukum Pidana (KUHP) yang berlaku sekarang ini berasal dari *Wetboek van Strafrecht voor Nederlandsch Indie* (WvSNI) yang merupakan peninggalan Belanda dan mulai berlaku di negeri Belanda sejak tahun 1918 berdasarkan asas konkordansi *(concordantie beginsel)* dengan berbagai perubahan untuk disesuaikan dengan keadaan di Indonesia (Hindia Belanda) saat itu.

Sebagai sumber hukum pidana disamping sumber-sumber lainnya, KUHP menduduki posisi yang amat penting. Hal ini karena KUHP memuat asas-asas hukum pidana yang dapat dilihat pada Buku Kesatu mengenai Aturan Umum.

Sejak diberlakukannyam, KUHP telah mengalami perubahan dan penambahan. Hal ini dilakukan untuk menghadapi permasalahan-permasalahan yang muncul seiring dengan berkembangnya masyarakat, pengetahuan dan teknologi yang menyertainya. Perubahan itu antara lain: Pemberatan ancaman pidana untuk Pasal-pasal 188, 359 dan 360 yang dianggap terlalu ringan (UU NO. 1 Tahun 1960), perubahan terhadap jumlah denda yang disesuaikan dengan perubahan nilai mata uang (UU No. 18/Prp/1960), tentang penertiban perjudian (UU No. 7 Tahun 1974); penambahan ketentuan mengenai kejahatan penerbangan (UU No. 4 Tahun 1976), perubahan yang berkaitan dengan kejahatan terhadap keamanan negara (UU No.27 Tahun 1999).

Jurisprudensi juga berperan dalam mengembangkan ilmu hukum pidana disamping perubahan dan penambahan KUHP. Sebagai contoh dengan dimasukkannya listrik ke dalam pengertian barang atau benda dalam pengertian Pasal 362 melalui putusan Hoge Raad Nederland Tahun 1921 yang lebih dikenal dengan *electriciteit arrest*.

Hakim Agung Soeharto mengemukan jurisprudensi penting dalam penanganan kasus *cybercrime* adalah putusan Mahkamah Agung

terhadap kasus transfer dana illegal terhadap dana dari Bank BNI.[95] Jurisprudensi dimaksud adalah perkara atas nama Seno Adjie dan Rudy Demsi Nomor: 363/K/Pid/1984 tanggal 25 Juni 1984. Perkara ini menjerat Seno Adjie dan Rudy Demsi atas tindak pidana korupsi atau pencurian dan perusakan dokumen milik negara karena telah mentransfer dana milik PT. Bank BNI secara tidak sah melalui komputer. Kasusnya terjadi di Amerika Serikat. Bersama Rudy Demsi, pada saat itu Seno Adjie secara tidak sah atau melawan hukum telah memindahkan atau mentransfer uang milik Bank BNI sebesar lebih dari US $18 juta. Selanjutnya uang tersebut dimasukkan ke dalam beberapa rekening pribadi Seno dan Rudy di Panama. Kegiatan transfer dana illegal tersebut dilakukan di sebuah kamar hotel di New York dengan menggunakan perangkat komputer dan sebuah modem untuk menghubungkan komputer tersebut dengan jaringan komputer Bank BNI. Perangkat komputer yang digunakan adalah sebuah komputer pribadi bermerk Apple IIC dan Smart Modem 1200. Melalui Putusan Kasasi Mahkamah Agung (MA) Nomor: 1852 K/Pid/1988 tanggal 21 Desember 1988, MA mempertimbangkan

---

[95] http://www.hukumonline.com: *"Hukum Positif Masih Bisa Tangani Kasus Kejahatan Komputer"*, 10 Januari 2004. Lihat juga Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta 1987, dan Al. Wisnubroto, *Op cit*, hal. 131-148.

teknologi komputer/internet sebagai media atau alat yang digunakan untuk melakukan kejahatan pencurian uang. Akhirnya pengadilan menghukum pelaku tindak pidana penyalahgunaan komputer sebagai telah melakukan tindak pidana korupsi atau pun pencurian.

Selanjutnya akan dibahas pasal-pasal dalam KUHP yang bisa digunakan untuk menjerat pelaku tindak pida *cyber*.

1) Ketentuan yang Berkaitan dengan Pembocoran Rahasia

KUHP mengatur delik mengenai pembocoran rahasia, yaitu Pasal 112 tentang pembocoran rahasia negara, Pasal 113 dan Pasal 114 tentang pembocoran rahasia pertahanan dan keamanan negara.

Selain itu KUHP juga mengatur tentang pembocoran rahasia yang menyangkut profesi atau jabatan seseorang (Pasal 322), pembocoran rahasia perusahaan (Pasal 323), dan pembocoran rahasia dalam situasi tertentu (Pasal 431).

Karena dalam rumusan pasal-pasal tersebut tidak disebutkan data komputer atau informasi yang dihasilkan oleh komputer, maka penerapan hukum dilakukan dengan cara interprestasi ekstensif, yaitu dengan memperluas pengertian benda-benda dalam rumusan pasal-pasal tersebut sehingga meliputi pula informasi yang dihasilkan komputer. Disamping itu perlu dibuktikan sampainya

data atau informasi yang dirahasiakan di tangan pihak-pihak yang tidak berwenang.[96]

Jika data komputer yang dibocorkan tersebut berkaitan dengan rahasia profesi, misalnya pengacara, psikolog atau dokter yang mebocorkan rahasia klien atau pasiennya yang disimpan dalam media komputer, maka kiranya ketentuan Pasal 322 KUHP dapat diterapkan. Apalagi ketentuan pasal ini tidak menentukan bentuk media yang memuat data rahasia, sehingga tidak perlu adanya penafsiran tentang data komputer.[97]

2) Ketentuan yang Berkaitan dengan Perbuatan Memasuki atau Melintasi Wilayah Orang Lain Tanpa Hak

KUHP mengatur mengenai perbuatan memasuki atau melintasi wilayah tanpa hak. Ini dapat dilihat dalam ketentuan Pasal 167 (yaitu tanpa hak memasuki rumah, ruangan atau pekarangan tertutup yang ditempati orang lain), dan Pasal 551 (tanpa hak melintasi tanah orang lain).

Rumusan pasal-pasal tersebut menentukan wilayah yang tidak boleh dimasuki atau dilintasi merupakan wilayah fisik (rumah, ruangan atau pekarangan). Dalam perkembangannya sistem jaringan komputer telah menjadi lingkungan non fisik yang ekslusif, dalam arti tidak semua orang dapat/boleh memasuki jaringan

---

[96] Al. Wisnubroto, ***Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer***, *Op cit*, hal. 74.

[97] *Ibid*, hal. 75.

komputer tersebut. Jika terjadi perbuatan memasuki/mengakses jaringan komputer, padahal pemilik/penanggung jawab telah melarang (dikenal dengan *hacking*), maka terhadap pelaku *hacking (hacker)* dapat diterapkan ketentuan Pasal 167 dan Pasal 551 KUHP.

3) Ketentuan yang Berkaitan dengan Perbuatan Pemalsuan

Delik pemalsuan dalam KUHP dimaksudkan sebagai pemalsuan surat. Surat atau data ditulis atau dicetak di atas media kertas yang dapat dipakai sebagai alat bukti secara tertulis. Dengan hadirnya teknologi komputer, sistem penyimpanan konvensional tersebut dialihkan ke dalam media elektronis seperti disket, *tape storage, disk storage, compact disk, hard disk, USB* dan lain-lain.

Dengan hadirnya teknologi komputer telah lahir Kejahatan pemalsuan bentuk baru yang menurut istilah Yusuf Randi disebut *Data Didling*, yaitu kejahatan yang berupa perbuatan mengubah data valid/sah dengan cara melawan hukum yaitu dengan mengubah input data maupun output data dengan memakai sarana komputer.[98]

Terhadap perbuatan ini ketentuan Pasal 263 sampai 276 KUHP mengenai pemasuan surat dapat diterapkan. Dengan adanya

---

[98] Al. Wisnubroto, *Ibid*, hal. 79.

perkembangan tehnologi, maka pengertian surat tida dapat lagi hanya merupakan tulisan tangan/cetakan dalam media kertas. Apalagi dengan maraknya penggunaan *e mail* (*electronic mail*) dalam jaringan komputer (internet) ataupun dunia perbankan yang hanya menggunakan sinyal elektronis dalam melakukan transaksinya. Tentunya diperlukan penafsiran ekstensif untuk mengatasi masalah ketertinggalan hukum pidana dalam merespon cepatnya perkembangan kehidupan masyarakat.

4) Ketentuan yang Berkaitan dengan Perbuatan Pencurian

Delik pencurian diatur dalam Pasal 362 KUHP, sedang variasinya diatur dalam Pasal 363 (pencurian dengan pemberatan), Pasal 364 (pencurian ringan), Pasal 365 (pencurian yang disertai dengan kekerasan/ancaman kekerasan) dan Pasal 367 (pencurian di lingkungan keluarga).

Dalam penerapan ketentuan Pasal 362 di dunia *cyber*, masalah yang timbul adalah interprestasi terhadap dua unsur Pasal 362 tersebut. Pertama terhadap unsur *mengambil*, perbuatan *mengambil* ini termasuk *melepaskan kekuasaan atas benda itu dari pemiliknya dengan maksud untuk memiliki, sehingga perbuatan*

mengkopi data atau program komputer yang dilakukan dengan sengaja tanpa izin dari pemiliknya dapat dikategorikan mengambil sebagaimana dimaksud dalam Pasal 362 KUHP.

Kedua, unsur *barang* atau *benda*, pada *cybercrime* pengertian barang sesuatu/benda adalah termasuk data atau program yang tersimpan dalam media komputer. Hal ini serupa pada penerapan Pasal ini terhadap pencurian listrik *(arrest electriciteit, HR* Nederland 21 Mei 1921), bahwa yang termasuk benda juga benda tidak berwujud (listrik).

5) Ketentuan yang Berkaitan dengan Perbuatan Penggelapan

KUHP mengatur delik penggelapan dalam Pasal 372, sedang variasinya diatur dalam Pasal 373 KUHP (penggelapan ringan), Pasal 374 (penggelapan yang dilakukan atas hubungan kerja), Pasal 375 (penggelapan dengan pemberatan), Pasal 376 (penggelapan di lingkungan keluarga).

Unsur dari Pasal 372 yang memerlukan perhatian adalah unsur *barang yang ada dalam kekuasaannya bukan karena kejahatan,* unsur inilah yang membedakan dengan unsur pencurian. *Cybercrime* dapat juga dilakukan oleh pihak-pihak yang berada dibelakang atau

disekitar lingkungan peralatan komputer, misalnya *programmer, operator, system analyst*, dan sebagainya. Apabila orang-orang ini melakukan perbuatan mengambil (mengaku sebagai miliknya) data komputer yang memang dikuasakan padanya, maka dapat berlaku ketentuan Pasal 372 KUHP, atau Pasal 374 bila dilakukan dalam hubungan kerja.

6) Ketentuan yang Berkaitan dengan Perbuatan Penipuan

Delik penipuan *(bedrog)* diatur dalam Pasal 378 KUHP, sedang variasinya diatur Pasal 379 sampai 395 KUHP. Pasal 378 berbunyi:

> Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat *(hoegnigheid)* palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan dengan pidana penjara paling lama empat tahun.

Perbuatan *memakai nama palsu atau martabat (hoegnigheid) palsu, dengan tipu muslihat ataupun rangkaian kebohongan* merupakan perbuatan yang luas dan dapat dilakukan dalam berbagai bentuk teknisnya. Oleh karena itu perbuatan seperti ini dapat dilakukan di dunia *cyber*, Marak terjadi adalah kasus *carding* dimana pelaku menggunakan nama palsu dan alamat palsu untuk

mendapatkan keuntungan bagi dirinya sendiri. Untuk itu dapat diterapkan ketentuan Pasal 378 KUHP dan variannya.

7) Ketentuan yang Berkaitan dengan Perbuatan Penghancuran atau Perusakan Barang

Penghancuran barang atau perusakan barang diatur dalam Pasal 406 KUHP, dan variasinya diatur dalam Pasal 407 sampai 412 KUHP.

Unsur-unsur yang harus dicermati dalam penerapan Pasal 406 terhadap *cybercrime* adalah unsur *menghancur, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu.*

Pengertian *menghancur, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu,* dapat diartikan sebagai perbuatan yang terhadap suatu data elektronis/program yang tersimpan dalam media komputer/jaringan komputer. Dalam istilah *cyber* dikenal *cracking,* yaitu memasuki jaringan/sistem data secara ilegal kemudian merusak atau menghancurkan data sistem/jaringan tersebut. Atau perbuatan implantasi virus komputer yang tersebar secara otomatis dalam jaringan komputer yang dapat merusak data atau progaram komputer. Terhadap

perbuatan-perbuatan inilah dapat diterapkan ketentuan Pasal 406 KUHP.

8) Ketentuan yang berkaitan dengan pornografi

Berkaitan dengan pornografi maka dapat dikenakan ketentuan Pasal 282 dan 283 KUHP, yaitu menyerbar luaskan gambar, uraian atau informasi lainnya yang melanggar kesusilaan atau bersifat porno. Apalagi dengan maraknya situs-situs porno dalam internet *(cybersex).* Atau perbuatan pornografi terhadap anak, kemudian delik yang dilakukan dengan membuka situs internet.

b. Di Luar KUHP

1) Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

Berkaitan dengan tindak pidana di internet *(cybercrime),* maka hal penting yang dapat dilihat dari undang-undang ini adalah masalah alat bukti. Berbeda dengan KUHAP, dalam undang-undang ini sudah diakui bentuk alat-alat bukti yang lain.

Hal penting yang dapat dilihat dengan diundangkannya UU No. 8 Tahun 1997 tentang Dokumen Perusahaan adalah pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media

lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan, seperti: Compact Disk-Read Only Memory/CD-ROM dan Write-Once-Read-Many/WORM), yang diatur dalam Pasal 15 ayat (1) Undang-undang tersebut sebagai alat bukti yang sah.

Catatan elektronik menjadi hal yang *urgent* dalam *cybercrime*, karena dengan dapat dijadikannya sebagai alat bukti yang sah maka catatan lektronik akan sangat bermanfaat dalam proses persidangan. Catatan lektronik tersebut dapat dijadikan alat bukti seperti *log book* milik Internet Service Provider (ISP) ataupun *web servers* yang mencatat seluruh *internet traffic* ataupun transaksi yang terjadi.

Berkaitan dengan *cybercrime,* dan pengaturan hukumnya, hal ini menjadi penting sebagai cara untuk pembuktian *(documentary evidence).* Bukti tersebut dapat berupa *criminal evidence* atau *civil evidence.* Hal ini seperti yang sudah diatur di Inggris dengan Criminal Evidence Act Tahun 1965 dan Civil Evidence Act Tahun

1968, sedangkan di Amerika Serikat berupa izin *Supreme Court* bahwa *computer print-out* dapat dijadikan sebagai alat bukti.[99]

Hal lain berkaitan dengan *cybercrime* yaitu dalam Penjelasan Umum Undang-Undang tentang Dokumen Perusahaan dijelaskan:

"Ketentuan mengenai pelaksanaan penyimpanan, pemindahan, perusakan dan penyerahan dokumen yang diatur dengan undang-undang ini tidak dimaksudkan menghilangkan fungsi dokumen bersangkutan sebagai alat bukti atau kepentingan hukum lainnya. Oleh karena itu Undang-undang dan ketentuan peraturan perundang-undangan lainnya yang berkaitan dengan pelaksanaan Pasal 6 Kitab Undang-undang Hukum Dagang *(Wetboek van Koophandel voor Indonesie,* Staatsblad 1947: 23), misalnya Pasal 396, Pasal 397, Pasal 398 dan Pasal 399, Kitab Undang-undang Hukum Pidana tetap berlaku sepanjang belum diganti atau tidak bertentangan dengan Undang-undang ini".

Pasal-pasal KUHP yang disebut dalam Penjelasan Umum Undang-undang tentang Dokumen Perusahaan menyangkut tentang pelaksanaan lebih lanjut dari undang-undang tersebut khususnya mengenai Tata Cara Penyerahan dan Pemusnahan Dokumen Perusahaan diatur dalam PP No. 89 Tahun 1999 tanggal 13 Oktober 1999. Sedangkan tentang Tata Cara Pengalihan Dokumen Perusahaan Perusahaan dalam Microfilm maupun media lainnya dan

---

[99] Heru Supraptomo, *Kejahatan Komputer dan Siber serta Antisipasi Pengaturan dan Pencegahannya di Indonesia, Op cit*, hal. 18.

Legalisasi diatur dalam PP No. 88 Tahun 1999 tanggal 13 Oktober 1999.

2) Undang-undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat

Teknologi komputer yang berkembang pesat pada gilirannya menghasilkan teknologi internet. Internet tidak hanya sebagai media komunikasi namun dalam perkembangannya juga bisa dijadikan sebagai sarana bisnis yang menjanjikan. Dari sini muncullah apa yang lebih dikenal dengan sebutan *e-commerce* atau perdagangan secara elektronik. Banyak keuntungan bisa diraih dengan perluasan pasar yang merambah dunia *cyber,* tetapi di sisi lain juga menimbulkan perilaku buruk dalam praktek berusaha di *cyberspace.*

Tindakan untuk monopoli pasar dan/atau persaingan usaha tidak sehat dalam bentuk konvensional/biasa juga dapat terjadi di *cyberspace,* antara lain:[100]

a) *Vertical Integration* yang dilakukan oleh para pihak, dimana pihak yang menyelenggarakan sistem ternyata sebenarnya adalah pelaku usaha yang berlaku dalam satu kelompok saja;

[100] Edmon Makarim. *Kompilasi Hukum Telematika, Op cit,* hal. 579.

b) Keberadaan B2b *market place* yang mungkin akan mendiskriminasikan para pelaku usaha, karena sangat tergantung kepada kewenangan sistem yang diselenggarakan oleh *market provider;*
c) Pengambilan nama domain oleh kompetitor yang berindikasikan kepada penggunaan ataupun penguasaan suatu merk oleh kompetitor.

Untuk masalah nama domain ini kejahatan yang terjadi dikenal dengan istilah *cybersquatting, cyberparasite, cyberhijacking. Cybersquatting* (yang melakukannya disebut *cybersquatter)* adalah tindakan penyerobotan nama domain, dimana ada pihak yang membeli nama domain dari suatu organisasi atau tokoh kemudian dijual dengan harga yang tinggi. *Cyberparasite/cyberhijacking* adalah tindakan mendaftarkan nama domain dari suatu merk terkenal.[101]

Pendaftaran nama domain menggunakan prinsip *first come first served,* berbeda dengan pendaftaran merk yang tidak menggunakan prinsip tersebut. Kejahatan nama domain ini menjadi marak karena ulah *cybersquatter* yang ingin mendapatkan keuntungan atau bisa juga dari pihak yang melakukan persaingan tidak sehat *(unfair competition).* Di Indonesia sendiri sudah

[101] http://www.hukumonline.com: *"Domain Name"*, 10 Januari 2004

terdapat kasus nama domain yang dalam tesis ini dibahas tersendiri.

Sifat nama domain yang unik mengakibatkan fenomena ini seolah tidak dapat dijerat secara hukum. Sebagai identitas, harusnya kepemilikan nama domain ini mendapat perlindungan hukum. Namun sampai saat ini belum ada pengaturan yang tegas mengenai pengambilan hak nama domain dalam peraturan perundang-undangan di Indonesia.

Undang-Undang Nomor 5 Tahun 1999 mempunyai dua jalur kebijakan kriminal yaitu jalur Penal dan jalur Non-Penal. Jalur penal dengan adanya ketentuan pidana sedangkan jalur non-penal dengan adanya komisi Pengawas Persaingan Usaha.

Ketentuan pidana dalam UU tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat terdapat pada Pasal 48 dan Pasal 49. Rumusannya adalah sebagai berikut :

- Pasal 48
  (1) Pelanggaran terhadap ketentuan Pasal 4, Pasal 9 sampai dengan Pasal 14, Pasal 16 sampai dengan Pasal 19, Pasal 25, Pasal 27 dan Pasal 28 diancam dengan pidana denda serendah-rendahnya Rp 25.000.000.0000,- (duapuluh lima milyar rupiah) dan setinggi-tingginya Rp 100.000.000 (seratus milyar rupiah), atau pidana kurungan pengganti denda selama-lamanya 6 (enam) bulan;

(2) Pelanggaran terhadap ketentuan Pasal 5 sampai dengan Pasal 8, Pasal 15, Pasal 20 sampai dengan Pasal 24, dan Pasal 26 Undang-undang ini dengan pidana denda serendah-rendahnya Rp 5.000.000.000,- (lima milyar rupiah) dan setinggi-tingginya Rp 25.000.000.000,- (duapuluh lima milyar rupiah) atau pidana kurungan pengganti denda selama-lamanya 5(lima) bulan;
(3) Pelanggaran terhadap ketentuan Pasal 41 Undang-undang ini diancam pidana denda serendah-rendahnya Rp 1.000.000.000 (satu milyar rupiah) dan setinggi-tingginya Rp 5.000.000.000 (lima milyah rupiah), atau pidana kurungan pengganti denda selama-lamanya 3 (tiga) bulan.

➢ Pasal 49
Dengan menunjuk ketentuan Pasal 10 Kitab Undang-Undang Hukum Pidana, terhadap pidana sebagaimana diatur dalam Pasal 48 dapat dijatuhkan pidana tambahan berupa:
- Pencabutan izin usaha; atau
- Larangan kepada pelaku usaha yang telah terbukti melakukan pelanggaran terhadap undang-undang ini untuk menduduki jabatan direksi atau komisaris sekurang-kurangnya 2 (dua) tahun dan selama-lamanya 5 (lima) tahun;
- Penghentian kegiatan atau tindakan tertentu yang menyebabkan timbulnya kerugian pada pihak lain.

Undang-undang ini tidak menyebutkan kualifikasi deliknya apakah termasuk kejahatan atau pelanggaran. Ancaman pidana dalam undang-undang ini hanya menggunakan pidana denda dan menggunakan ancaman pidana minimal khusus. Hal ini merupakan penyimpangan dari KUHP.

Kemudian dari sisi ancaman pidana, dengan dialternatifkannya pidana denda yang tinggi (miliaran rupiah) dengan kurungan pengganti denda yang hanya berkisar antara 3-6 bulan, maka dikhawatirkan apabila denda tidak akan dibayar oleh terpidana, , akan berlaku Pasal 30 KUHP (yaitu apabila denda tidak dibayar, hanya akan terkena pidana kurungan pengganti 6 bulan atau maksimal 8 bulan apabila ada pemberatan).

Dari hal tersebut, akan timbul kecenderungan dari terpidana untuk tidak membayar denda tersebut dan hanya akan memilih pidana kurungan pengganti denda yang maksimum lamanya hanya 6 bulan. Dengan demikian, sanksi pidana tersebut akan menjadi tidak efektif dalam pelaksanaannya.

Disamping ketentuan pidana, undang-undang ini juga memuat sanksi berupa tindakan administrasi yang terdapat pada Pasal 47. Rumusannya adalah :

- Pasal 47
  (1) Komisi berwenang menjatuhkan sanksi berupa tindakan administratif terhadap pelaku usaha yang melanggar ketentuan undang-undang ini.
  (2) Tindakan administratif sebagaimana dimaksud dalam ayat (1) dapat berupa :
      - Penetapan pembatalan perjanjian sebagaimana dimaksud dalam pasal 4 sampai dengan Pasal 13, Pasal 15 dan Pasal 16; dan/atau

- Perintah kepada pelaku usaha untuk menghentikan integrasi vertikal sebagaimana dimaksud dalam Pasal 14; dan/atau
- Perintah kepada pelaku usaha untuk menghentikan kegiatan yang terbukti menimbulkan praktek monopoli dan atau menyebabkan persaingan usaha tidak sehat dan atau merugikan masyarakat; dan/atau
- Perintah kepada pelaku usaha untuk menghentikan penyalahgunaan posisi dominan; dan/atau
- Penetapan pembatalan atas penggabungan atau peleburan badan usaha dan penetapan pembayaran ganti rugi; dan/atau
- Pengenaan denda serendah-rendahnya Rp 1.000.000.000 (satu milyar rupiah) dan setinggi-tingginya Rp 25.000.000.000,- (dua puluh lima milyar rupiah)

Hal yang cukup janggal adalah tindakan administratif tersebut tidak diancamkan ke dalam sistem pertanggung jawaban pidana untuk korporasi.

3) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-undang Telekomunikasi disusun dengan pertimbangan antara lain bahwa pengaruh globalisasi dan perkembangan teknologi komunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi.

Sementara itu di dalam Penjelasan Umum Undang-undnag tersebut dinyatakan bahwa salah satu alasan dikeluarkannya Undnag-undang Telekomunikasi adalah:

"Sebagai Negara yang aktif dalam membina hubungan antara Negara dan dasar kepentingan nasional, keikutsertaan Indonesia dalam berbagai kesepakatan multilateral menimbulkan berbagai konsekuensi yang harus dihadapi dan diikuti. Sejak penandatanganan Genaral Agreement on Trade and Services (GATS) di Marrakesh, Maroko, pada tanggal 15 April 1994, yang telah diratifikasi dengan Undang-undang No. 7 Tahun 1994, penyelenggaraan telekomunikasi nasional menjadi bagian yang tidak terpisahkan dari sistem perdagangan global".

Pasal 1 angka 1 UU No. 36 Tahun 1999 memberikan definisi tentang telekomunikasi. Telekomunikasi adalah setiap pemancaran, pengiriman dan/atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio atau sistem elektromagnetik lainnya.

Internet merupakan salah satu bentuk media komunikasi elektronik yang terdiri dari komputer dan dilengkapi dengan perlengkapan tertentu sehingga memungkinkan untuk melakukan komunikasi dengan berbagai pihak di *cyberspace.*

Ketentuan pidana dalam UU tentang Telekomunikasi terdapat pada Pasal 47 sampai Pasal 57. Rumusannya adalah sebagai berikut:

- Pasal 47
  Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,- (enamratus juta rupiah).

- Pasal 48
  Penyelenggara jaringan telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 19 dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau denda paling banyak Rp 100.000.000,- (seratus juta rupiah).

- Pasal 49
  Penyelenggara telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 20, dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 200.000.000,- (duaratus juta rupiah).

- Pasal 50
  Barangsiapa yang melanggar ketentuan sebagaimana diamksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,- (enamratus juta rupiah).

- Pasal 51
  Penyelenggara telekomunikasi khusus yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 29 ayat (1) atau Pasal 29 ayat (2), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 400.000.000,- (empatratus juta rupiah).

- Pasal 52
  Barangsiapa memperdagangkan, membuat, merakit, memasukkan atau menggunakan perangkat telekomunikasi di wilayah Negara Republik Indonesia yang tidak sesuai dengan persyaratan teknis

sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau denda paling banyak Rp 100.000.000,- (seratus juta rupiah).

- Pasal 53
  (1) Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 33 ayat (1) atau Pasal 33 ayat (2), dipidana dengan pidana penjara paling lama 4 (empat) tahun tahun dan/atau denda paling banyak Rp 400.000.000,- (empatratus juta rupiah).
  (2) Apabila tindak pidana sebagaimana dimaksud pada ayat (1) mengakibatkan matinya seseorang, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun.

- Pasal 54
  Barangsisapa yang melanggar ketentuan sebagaimana dimaksud dalam pasal 35 ayat (2) atau Pasal 36 ayat (2), dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 200.000.000,- (duaratus juta rupiah).

- Pasal 55
  Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 38, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,- (enamratus juta rupiah).

- Pasal 56
  Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun.

- Pasal 57
  Penyelenggara jasa telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1), dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 200.000.000,- (duaratus juta rupiah)

Tindak pidana pada pasal-pasal tersebut di atas pada intinya adalah:

(a) Pasal 47 : penyelenggaraan telekomunikasi tanpa izin (Pelanggaran Pasal 11 ayat (1));

(b) Pasal 48 : penyelanggaraan jaringan telekomunikasi wajib menjamin kebebasan pengguna lainnya (Pelanggaran Pasal 19);

(c) Pasal 49 : penyelenggara telekomunikasi wajib memberikan prioritas untuk pengiriman, penyaluran dan penyampaian informasi penting yang menyangkut keamanan negara, bencana alam, marabahaya dan atau wabah penyakit (Pelanggaran Pasal 20);

(d) Pasal 50 : melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi (pelanggaran Pasal 21);

(e) Pasal 51 : penyambungan telekomunikasi khusus ke jaringan lain (Pelanggaran Pasal 29 ayat (1) atau Pasal 29 ayat (2));

(f) Pasal 52 : kewajiban produsen memperhatikan persyaratan teknis dan izin sesuai ketentuan jika memperdagangkan, membuat, merakit perangkat telekomunikasi yang dimasukkan

ke wilayah Negara Republik Indonesia (Pelanggaran Pasal 33 ayat (1) dan ayat (2));

(g) Pasal 53 : keharusan mendapat izin dari Pemerintah bagi penguasa spektrum frekuensi radio dan orbit satelit dan tidak saling mengganggu (Pelanggaran Pasal 33 ayat (1) dan ayat (2));

(h) Pasal 54 : larangan penggunaan spektrum frekuensi radio bagi kapal berbendara asing yang berada di wilayah perairan indonesia dan pesawat udara sipil asing dari dan ke wilayah udara Indonesia (Pelanggaran pasal 53 ayat (2) atau pasal 36 ayat (2)) ;

(i) Pasal 54 : larangan melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi (Pelanggaran Pasal 38);

(j) Pasal 56 : larangan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi (Pelanggaran pasal 40);

(k) Pasal 57 : pelanggaran untuk merahasiakan informasi yang dikirim atau diterima oleh pelanggan kecuali untuk proses peradilan pidana yang diminta secara tertulis oleh Jaksa Agung, Kapolri dan penyidik tertentu.

Pada Pasal 59 disebutkan bahwa perbuatan-perbuatan yang disebutkan dalam Pasal 47 sampai dengan Pasal 57 merupakan "kejahatan".

Jika dikaitkan dengan kejahatan-kejahatan di internet yang marak terjadi seperti *hacking (cracking), carding* atau bentuk-bentuk kejahatan lain yang disebutkan dalam *Convention on Cybercrime* di Budapest tahun 2001, maka undang-undang telekomunikasi masih terlalu sumir dan tidak tegas menyebutnya. Sehingga sulit diterapkan dan dikenakan terhadap pelakunya.

Beberapa pasal yang bisa dikenakan seperti Pasal 21 untuk tindak pidana kesusilaan (bisa dalam bentuk pornografi, pornografi anak), agitasi atau tindakan menghasut lainnya. Namun pasal ini tidak ada dalam ketentuan pidananya. Ini berarti pelanggaran terhadap Pasal 21 tidak dikenakan sanksi apapun, padahal ini merupakan salah satu tanggung jawab dari penyelenggara telekomunikasi.

Pasal lain yaitu Pasal 55 merupakan pelanggaran terhadap Pasal 38 undang-undang tentang Telekomunikasi. Hal ini sama dengan yang diatur dalam *Convention on Cybercrime* . yakni Tindak Pidana yang Berkaitan dengan Kerahasiaan, Integritas dan Keberadaan Data dan Sistem Komputer (*offences Againts the*

Confidentiality, Integrity and Availability of Computer Data and System). Kemudian Pasal 56 jika dikaitkan dengan *Convention on Cybercrime*, maka perbuatan yang diatur sama dengan Pasal 55 yaitu termasuk dalam Tindak Pidana yang Berkaitan dengan Kerahasiaan, Integritas dan Keberadaan Sistem Komputer *(Offences againts the confidentiality, Integrity and Availability of computer Data and Systems*). Penjelasan Pasal 40 menyatakan bahwa :

"....Penyadapan adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapat informasi dengan cara tidak sah...."

Namun pasal ini tidak secara tegas menyebutkan untuk kegiatan di Internet.

Hal menarik lainnya seiring dengan perkembangan teknologi telekomunikasi yang digabungkan dengan teknologi komputer khususnya internet adalah *Voice Over Internet Protocol (VOIP).* VOIP juga dikenal dengan *Internet Protocol Telephony.* Di beberapa negara sudah ada pengaturan mengenai penyelenggaraan dan penggunaan VOIP seperti Canada, Singapura dan Cina. Di Indonesia VOIP dimasukkan dalam bentuk penyelenggaraan telekomunikasi khusus, namun tidak disebutkan secara tegas dalam

UU tentang Telekomunikasi. Ini dapat dilihat dalam Peraturan Pemerintah Nomor 52 Tahun 2000, Lembaran Negara No. 107 tentang Penyelenggaraan Telekomunikasi Indonesia, yang dapat dimasukkan dalam jasa multimedia.

Secara sederhana VOIP dapat didefinisikan sebagai suatu sistem yang menggunakan jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol internet.[102]

Kejahatan akan terjadi ketika ada penyelenggara telekomunikasi khusus yang menggunakan teknologi VOIP tetapi tidak mendapat izin dari pemerintah sesuai Undang-undang Telekomunikasi pada Pasal 11. Kegiatan penyediaan VOIP dilakukan karena dianggap tidak ada aturan khusus yang tidak membolehkannya.

Satu-satunya kasus yang terjadi adalah penjualan *Calling Card* yang menggunakan *Voice Over Internet Protocol* sebagai penyedia jasa telekomunikasi di Bandung. Namun dalam perjalanannya kasus ini juga tidak jelas, karena tersangka AT yang ditahan di

---

[102] Edmon Makarim, *Kompilasi Hukum Telematika, Op cit,* hal. 116.

Polwitabes Bandung sudah dilepaskan begitu saja. Padahal waktu kejadiannya adalah tanggal 11 September 2000 dimana UU tentang Telekomunikasi sudah berlaku efektif.[103]

Hal yang dapat dilihat adalah kurangnya keinginan aparat penegak hukum untuk dapat melaksanakan perundang-undangan yang telah berlaku efektif.

Selanjutnya sistem perumusan sanksi pidana dalam Undang-undang Telekomunikasi adalah "alternatif-kumulatif", Pengecualiaan terdapat pada pasal 53 ayat (2) dengan Pidana Tunggal yaitu penjara.

Jenis sanksi pidana yang diterapkan dalam Undang-undang ini yaitu:

a) Pidana penjara

b) Pidana denda

c) Pidana tambahan

Selain pidana penjara dan denda, maka bentuk pidana tambahan dalam undang-undang ini berupa "Tindakan" yang diatur dalam Pasal 58 yang merupakan sanksi pidana administratif.

---

[103] *Ibid.* hal 135-136.

Disebutkan bahwa alat dan perangkat telekomunikasi yang digunakan dalam tindak pidana sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 52 atau Pasal 56 dirampas untuk negara dan/atau dimusnahkan sesuai dengan peraturan perundang-undangan yang berlaku.

4) **Undang-undang No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi**

Pasal 26A Undang-Undang Nomor 20 Tahun 2001 menyatakan bahwa alat bukti yang sah adalah petunjuk, khusus untuk tindak pidana korupsi selain yang dimaksud pada Pasal 184 ayat (2) KUHAP, juga dapat berupa:

(a) Alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu;

(b) Dokumen yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan yang terekan secara elektronil yang

berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, angka, tanda atau perforasi yang memiliki makna

Dalam Penjelasan Umum paragraf ketiga dikemukakan:

"Ketentuan perluasan mengenai sumber perolehan yang alat bukti yang sah yang berupa petunjuk, dirumuskan bahwa mengenai "petunjuk" selain diperoleh dari keterangan saksi, surat, dan keterangan terdakwa, juga diperoleh dari alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu tetapi tidak terbatas pada data penghubung elektronik *(electronic data interchange),* surat elektronik *(e-mail),* telegram, teleks dan faksimili, dan dari dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna".

Selanjutnya dalam Penjelasan Pasal Demi Pasal, pada Pasal 26A huruf a dijelaskan bahwa yang dimaksud dengan "disimpan secara elektronik" misalnya data yang disimpan dalam mikto film, *compact Disk Read Only Memory* (CD-ROM) atau *Write Once Read Many* (WORM). Sedangkan yang dimaksud dengan "alat optik atau yang serupa dengan itu" adalah tidak terbatas pada data penghubung elektronik *(elctronic data interchange),* surat elektronik *(e-mail),* telegram, teleks dan faksimili.

5) Undang- Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Dalam Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang, Pasal 38 menegaskan bahwa alat bukti pemeriksaan tindak pidana pencucian uang dapat berupa:

a) Alat bukti sebagaimana dimaksud dalam Kitab Undang-Undang Hukum Acara Pidana

b) Alat bukti lain berupa informasi yang diucapkan, dikirim, diterima atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan

c) Dokumen yang berupa data, rekaman atau informasi yang dapat dilihat, dibaca dan atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang diatas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada:

(1) Tulisan, suara atau gambar;

(2) Peta, rancanagan, foto atau sejenisnya

(3) Huruf, tanda, angka simbol atau perforasi yang memiliki makna atau dapat dipahami oleh orang lain yang mampu membacanya atau memahaminya.

6) Undang-Undang Nomor 32 tahun 2002 tentang Penyiaran

Informasi dapat disebarluaskan melalui berbagai media seperti radio, televisi, media cetak dan media informasi lainnya. Internet merupakan salah satu bentuk media informasi yang dapat digunakan sebagai sarana untuk menyebarkan informasi. Bahkan dalam perkembangan lebih lanjut, media internet yang semula merupakan media yang efektif untuk kebebasan berekspresi dijadikan juga sebagai sarana provokasi, penyebaran fitnah atau kabar bohong, penipuan, propaganda yang menyesatkan masyarakat, agitasi dan bentuk lainnya. Internet merupakan media informasi yang bersifat terbuka. Penyebaran informasi dari media ini dapat dilakukan dengan cepat dan luas, dengan demikian kejahatan juga mudah terjadi melalui internet dan dapat menimbulkan bahaya sosial yang bersifat global.

Pasal 13 Undang-Undang No. 32 tahun 2002 menyebutkan jasa penyiaran terdiri dari jasa penyiaran radio dan jasa

penyiaran televisi. Jasa penyiaran tersebut diselenggarakan oleh: Lembaga Penyiaran Publik, Lembaga Penyiaran Swasta, Lembaga Penyiaran Komunitas dan Lembaga Penyiaran Berlangganan.

Perumusan tindak pidana dalam undang-undang terdapat pada Bab X Pasal 57 sampai dengan Pasal 59 dengan rumusan:

- Pasal 57
  Dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 1.000.000.000,- (satu milyar rupiah) untuk penyiaran radio dan dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 1.000.000.000,- (satu milyar rupiah) untuk penyiaran televisi, setiap orang yang:
  a) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 17 ayat (3);
  b) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 18 ayat (2);
  c) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 30 ayat (1);
  d) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 36 ayat (5);
  e) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 36 ayat (6);

- Pasal 58
  Dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 500.000.000,- (limaratus juta rupiah) untuk penyiaran radio dan di pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 500.000.000,- (limaratus juta rupiah) untuk penyiaran televisi, setiap orang yang:
  a) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 18 ayat (1);
  b) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 33 ayat (1);

c) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 34 ayat (4);
d) Melanggar ketentuan sebagaimana dimaksud dalam Pasal 46 ayat (3);

➢ Pasal 59
Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 46 ayat (10) dipidana dengan pidana denda paling banyak Rp 2.000.000.000,- (dua milyar rupiah)

Berdasarkan Pasal-pasal di atas, tindak pidananya adalah sebagai berikut:

a) Pasal 57
- lembaga penyiaran swasta tidak memberikan kesempatan kepada karyawan untuk memiliki saham perusahaan dan memberikan bagi laba perusahaan,
- tidak ada pembatasan kepemilikan silang baik langsung maupun tidak langsung bagi lembaga penyiaran swasta yang menyelenggarakan jasa televisis, radio, media cetak dan jasa penyiaran lainnya
- mendirikan lembaga penyiaran asing di Indonesia
- isi siaran yang bersifat memfitnah, menghasut, menyesatkan, berbohong, menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang lainnya, juga mempertentangkan suku, agama, ras dan antar golongan
- isi siaran berisi memperolokkan, merendahkan, melecehkan dan atau mengabaikan nilai-nilai agama, mertabat manusia Indonesia atau merusak hubungan internasional

b) Pasal 58

- Pemusatan kepemilikan dan penguasaan lembaga penyiaran swasta oleh satu orang atau satu badan hukum, baik di satu wilayah siaran maupun di beberapa wilayah siaran,
- Lembaga penyiaran belum atau tidak memperoleh izin penyelenggaraan penyiaran
- Pemindahtangan izin penyelenggaraan penyiaran kepada pihak lain
- Siaran iklan niaga yang bersifat: promosi yang dihubungkan dengan ajaran suatu agama, ideologi, kelompok dan atau pribadi, yang menyinggung perasaan dan atau merendahkan martabat agama lain, pribadi dan atau kelompok lain; promosi minuman keras atau sejenisnya dan bahan atau zar adiktif; promosi rokok yang memperagakan wujud rokok; hal lain yang bertentangan dengan kesusilaan masyarakat dan nilai-nilai agama; serta eksploitasi anak di bawah umur 18 (delapan belas) tahun

c) Pasal 59

Larangan pembelian waktu siaran lembaga penyiaran oleh siapapun untuk kepentingan apapun kecuali untuk siaran iklan.

Perumusan pertanggungjawaban pidana bersifat *strict liability*. Ada atau tidaknya pertanggungjawaban secara hukum yang dapat dilimpahkan secara tertulis pada masing-masing bidang, tidak dirumuskan secara tegas. Disamping itu Pemimpin Umum

bertanggung jawab secara hukum karena bertanggung jawab secara umum.

Undang-undang Penyiaran ini tidak mengatur secara tegas mengenai pertanggungjawaban korporasi. Pertanggungjawban korporasi dilihat dari Anggaran Dasar korporasi tersebut.

Selanjutnya dalam pemidanaan terhadap korporasi juga tidak diatur secara tegas. Dalam Pasal 14 ayat (1) dan pasal 16 ayat (1) disebutkan bahwa lembaga penyiaran berbentuk badan hukum. Dengan demikian seyogyanya ada pengaturan yang tegas mengenai ancaman pidana serta sanksi pidana terhadap korporasi.

Dalam hal perumusan jenis sanksi pidana *(strafsoort)*, undang-undang penyiaran menggunakan pidana penjara dan pidana denda. Jika korporasi dikenakan pidana denda dan tidak dibayar, maka tidak diatur secara jelas ketentuannya.

Untuk perumusan lamanya pidana *(strafmaat)*, undang-undang penyiaran mengatur secara maksimum khusus. Pidana dapat dikenakan kepada individu (manusia) maupun badan hukum.

Pedoman pemidanaan *(strafmodus)* dalam undang-undang ini tidak dicantumkan. Ini dapat dilihat seperti pedoman pemidanaan

untuk pidana penjara bagi korporasi juga pidana denda yang tidak dibayar oleh korporasi.

3. Contoh Kasus Cybercrime dan Penyelesaiannya

a. Kasus Domain Name Mustika Ratu[104]

Dalam perkembangannya nama domain tidak hanya sekedar alamat di Internet karena nama domain bisa merupakan nama produk, merk dagang, slogan, jasa pelayanan, nama tempat, nama keluarga dan lain-lain. Hal inilah yang membuat nama domain menjadi sangat penting karena internet bisa menjadi sarana promosi dan juga untuk kepentingan bisnis lainnya.

Berbagai pihak terus mempermasalahkan nama domain yang berhubungan dengan merk dagang, produk maupun nama perusahaan. Pendaftaran nama domain menganut prinsip *first come first served* yang berarti siapapun yang pertama mendaftar maka dialah pemilik nama tersebut. Sedangkan untuk pendaftaran merk menggunakan prinsip *first come to file.*

Salah satu contoh kasus tentang Domain terjadi di "Mustika Ratu". Berikut di bawah ini adalah penjabarannya.

---

[104] Pengadilan Negeri Jakarta Pusat, Kejaksaan Negeri Jakarta Pusat, http://www.hukumonline.com.

1) **Kasus Posisi**

Kasus nama domain Mustika Ratu berawal dari tindakan Tjandra Sugiono (terdakwa) yang mendaftarkan nama domain **mustika-ratu.com** dengan menggunakan Network Solution Inc. (NSI) di Amerika Serikat pada bulan Oktober 1999. Tjandra Sugiono adalah mantan General Manager International Marketing PT. Martina Berto dan menggunakan alamat Jalan Cisadane 3 Pav. Jakarta Pusat, JA 10330 untuk pendaftaran nama domain tersebut.

Akibat penggunaan nama domain mustika-ratu.com tersebut, PT. Mustika Ratu tidak dapat melakukan sebagian transaksi dengan calon mitra usaha yang berada di luar negeri. Hal ini karena mereka tidak dapat menemukan informasi mengenai Mustika Ratu di *website* (situs) tersebut. Isi *website* mustika-ratu.com justru menampilkan produk-produk Belia dan Sari Ayu yang notabene adalah pesaing dari Mustika Ratu untuk produk kosmetik.

2) **Dakwaan Jaksa Penuntut Umum**

Atas perbuatannya tersebut terdakwa didakwa melanggar Pasal 382 bis KUHP (Dakwaan Kesatu) yaitu perbuatan curang *(bedrog)* dalam perdagangan, dengan ancaman hukuman maksimal 1 (satu) tahun 4 (empat) bulan. Dalam dakwaan kedua terdakwa didakwa melanggar Pasal 48 ayat (1) jo Pasal 19 huruf b Undang-undang Nomor 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat, dengan ancaman hukuman pidana denda serendah-rendahnya Rp 25 milyar dan setinggi-tingginya Rp 100 milyar atau pidana kurungan pengganti denda selama-lamanya 6 (enam) bulan. Pasal 19 ini melarang pelaku usaha melakukan satu atau beberapa kegiatan, baik sendiri maupun bersama pelaku usaha lain, yang dapat mengakibatkan terjadinya praktek monopoli dan atau persaingan usaha tidak sehat berupa: menolak dan atau menghalangi pelaku usaha tertentu untuk melakukan kegiatan usaha yang sama pada pasar yang bersangkutan; atau mematikan usaha pesaingnya di pasar bersangkutan sehingga dapat mengakibatkan terjadinya praktek monopoli dan atau persaingan usaha tidak sehat.

3) Putusan Pengadilan Negeri

Pengadilan Negeri Jakarta Pusat dalam Putusan No. 1075/Pid.B/2001/ PN/JKT.PST tanggal 11 Desember 2001 memutuskan bahwa perbuatan yang didakwakan tidak terbukti dengan pertimbangan pada pokoknya:

a) Terdakwa tidak melakukan penipuan karena domain name didaftarkan di suatu badan resmi dan terdakwa telah menyatakan identitasnya secara jelas;

b) Terdakwa belum sempat menarik keuntungan atau merugikan PT. Mustika Ratu;

c) Terdakwa bukan karyawan PT. Martina Berto

d) Berkaitan dengan dakwaan kedua, perbuatan terdakwa dilakukan sebelum UU No. 5 Tahun 1999 berlaku, sehingga UU tersebut tidak dapat diterapkan.

4) Putusan Mahkamah Agung

Jaksa kemudian mengajukan Kasasi ke Mahkamah Agung dan dalam Putusannya No. Reg: 1082.K/Pid/2002 tanggal 24 Januari 2002 memutuskan bahwa dakwaan kesatu terbukti, sementara dakwaan kedua tidak terbukti dengan pertimbangan:

"…. akibat perbuatan terdakwa tersebut telah menipu untuk mengelirukan orang banyak atau seseorang tertentu yaitu Abdul Rahman Al Zohaifi di Arab Saudi dan Medical Supplier di Malaysia karena ketika memasuki website pada internet mustika-ratu.com yang isinya menunjukkan produk-produk Belia yang merupakan produk perusahaan Sari Ayu. Bahwa dengan perbuatan terdakwa tersebut maka pengguna internet yang mengakses domain name mustika-ratu.com yang terdaftar atas nama terdakwa selaku GM Marketing International PT. Martina Bertho akan dituntun dan diarahkan kepada *website* dengan nama **belia-online.com** dengan cara menyatakan mereka adalah Mustika Ratu, hal mana akan mengakibatkan PT. Mustika Ratu Tbk, yang merupakan pesaing dari PT. Martina Bertho mengalami kerugian setidak-tidaknya dapat menimbulkan kerugian bagi PT. Mustika Ratu Tbk, karena tidak dapat melakukan atau mengurangi transaksi dagang dengan calon mitra usaha yang berada di luar negeri dan dilain pihak dapat menarik keuntungan bagi PT. Martina Bertho".

Pasal 382 bis KUHP yang menjadi dasar Putusan Kasasi MA mempunyai unsur-unsur sebagai berikut:

- Terdakwa harus melakukan suatu perbuatan menipu;
- Perbuatan itu mengelirukan orang banyak atau seseorang tertentu;
- Perbuatan itu dilakukan untuk menarik suatu keuntungan dalam perdagangan atau persahaan sendiri atau orang lain;
- Perbuatan itu dapat menimbulkan kerugian bagi saingannya;
- Saingan tersebut adalah saingan terdakwa sendiri atau yang dibela oleh terdakwa

Pada akhirnya, Mahkamah Agung menjatuhkan putusan berupa pidana penjara selama 4 (empat) bulan kepada Tjandra Sugiono.

Hal menarik dari kasus ini adalah kasus ini merupakan kasus domain name pertama yang dibawa ke pengadilan. Kejahatan yang berkaitan dengan nama domain ini ada beberapa bentuk, antara lain *cybersquatting, cyberparasite, cyberhijacking.*

Indonesia sampai saat ini belum memiliki perangkat hukum pengaturan masalah *domain name, Domain Name* merupakan salah satu elemen penting dalam interaksi di dunia maya. *Domain name* akan sangat berperan dalam memberikan informasi sekaligus kejelasan identitas kepada publik.

Sebenarnya untuk kasus ini dapat diterapkan Undang-Undang tentang Larangan Praktek Monopoli dan Persaingan Tidak Sehat. Namun undang-undang ini juga tidak menyebutkan secara tegas tentang pengaturan nama domain di internet. Disamping itu dalam kasus ini, saat kejahatan ini dilakukan undang-undang tersebut belum berlaku, sehingga yang digunakan hakim dalam pengambilan keputusan berdasarkan KUHP.

b. **Kasus *Hacking* atas nama Wendy Setiawan**[105]

Kasus *Hacking* ini dilakukan seorang *hacker* asal Indonesia dan masih berusia 15 tahun. Akibat perbuatannya National University of Singapore (NUS) harus mengeluarkan SGD $15.000 (setara Rp 75 juta dengan kurs 1 SGD = Rp 5.000) untuk memperbaiki sistem komputer mereka yang rusak ditambah harus mengerahkan 20 teknisi komputer handal.

1) Kasus Posisi

Peristiwa tindak kejahatan yang dilakukan Wendy mulai terdeteksi pada kasus NUS. Pada tanggal 2 Juni 2000, Kho Beng Teck, *Senior Network Specialist* di Data storage Institute (DSI), lembaga dibawah NUS yang berlokasi di DSI Building 5 Engineering Drive 1- mengeluhkan adanya kerusakan cukup serius pada sistem komputernya. Ternyata hal serupa juga dialami oleh MTL instrument Pte.Ltd yang berlokasi di KA Centre, 150 Kampong Ampat #05-01 Singapura. Mereka berkesimpulan bahwa gangguan tersebut akibat kejahilan seseorang.

[105] http://www.its-oke.net/_disraker/000000db.htm; Indonesian Observer, 26 Juli 2001

Menerima keluhan tersebut, kepolisian Singapore divisi Computer Crime segera melakukan investigasi. Gangguan itu kemudian diketahui dikerjakan oleh orang yang tidak berizin dengan memasuki Domain Name Services (DNS) dengan kode *minnie.dsi.nis.edu.sg* milik DSI. Dari sana seseorang berhasil mengakses melauli *telnet session* denga kode *tns00333,signet.cm.sg.* Pihak SingNet's (Perusahaan telekomunikasi Singapura) mencatat, kode tersebut adalah *user id* milik *Wendy* yang dimonitoring pada tanggal 2 Juni 2000 dari pukul 16.47 hingga pukul 20.14 waktu setempat ketika pelaku menghubungkan dengan internet melalui jaringan SingNet.

Polisi Singapura kemudian melakukan penggerebekan terhadap Wendy yang ternyata memang sedang mengutak-atik komputer dan diakses ke program komputer milik orang lain. Wendi dibawa ke kantor polisi dengan barang bukti berupa sebuah komputer dan ia mengakui perbuatannya.

Wendy sendiri pernah belajar di Australia. Pemegang paspor Indonesia No. G941974 ini tiba di Singapura pada Mei 2000 untuk melanjutkan pendidikan. Ketika ditangkap, Wendy tercatat sebagai pelajar dari Asher Success Centre, sebuah sekolah swasta di

Singapura. Wendy mengaku kepada polisi bahwa ia pernah belajar di Australia dari 12 mei 1999 sampai 15 April 2000. Di negara Kangguru tersebut Wendy tertarik belajar *hack computer system* dan tertarik mempelajari lebih dalam operasi Linux. Wendy mencoba mengembangkan pengetahuannya dengan menyerang jaringan komputer melalui pertukaran informasi sesama temannya yang ia kenal malalui Internet Relay Chat (IRC).

2) Dakwaan Jaksa Penuntut Umum

Deputy Public Prasecutar (Jaksa Penuntut Umum) Singapura, David chew, mendakwa Wendy telah melanggar pasal 3 (1) tentang masuk sistem komputer milik orang lain tanpa izin dan Pasal 5 (1) *chapter* 50A tentang perusakan sistem komputer milik orang lain. Pasal-pasal tersebut dapat menjerat Wendy dengan hukuman lima tahun atau denda SGD $10.000.

Laporan polisi yang khusus menangani bidang komputer menyebutkan, Wendy sebelum tertangkap telah melakukan empat kali penyusupan (dalam surat dakwaan disebut pencerobohan) tempat orang lain. Namun dalam persidangan yang digelar Pengadilan Singapura, Hakim Mark Tay Swee Keng akan melanjutkan sidang untuk lima tuduhan sedangkan tuduhan lainnya

masuk kedalam kategori *Taken into consideration* (dipertimbangkan tanpa adanya hukuman).

Wendy yang dianggap manusia jenius oleh sebagian warga Singapura mengatakan di depan hakim bahwa sistem komputer di NUS lemah pertahanannya karena itu ia mencoba melindunginya dari pihak lain yang berusaha merusak sistemnya. Wendy juga menyampaikan permintaan maafnya kepada pihak NUS yang telah dirugikan akibat perbuatannya. Namun permintaan maafnya ditolak pihak NUS dengan alasan kerugian yang diderita NUS mencapai puluhan ribu dolar serta kerugian lainnya yakni terlambatnya aktivitas perguruan tinggi nasional Singapura tersebut.

Wendy akhirnya dijerat dengan *Cyberlaw* Singapura karena perbuatannya dianggap memenuhi unsur melawan hukum seperti yang diatur dalam Pasal 3 *Computer Misuse Act* tentang *Unauthorized Access of Computer Material.*

Dipaparkannya kasus ini karena dalam Kasus hacking yang dilakukan oleh Wendy Setiawan ini kental dengan unsur internasionalnya. Ini dapat dilihat dari kewarganegaraannya yaitu Indonesia. Perbuatan *(locus delicti)* ada di dua tempat yaitu

Singapura dan Australia. Akibat perbuatannya dirasakan oleh Singapura.

Australia juga meminta Wendy Setiawan untuk dapat disidangkan di negaranya dan Indonesia sebenarnya juga mempunyai kewenangan untuk mengadili. Akan tetapi persoalannya adalah Indonesia belum mempunyai aturan mengenai *hacking* (termasuk dalam *Illegal interception).* Apalagi mengingat perbuatan yang dilakukan terdakwa bukan untuk mencari keuntungan melainkan untuk mencoba keahliannya dalam bidang *hacking computer.*

Fenomena *Hacking* yang dalam melakukan kegiatannya tanpa keinginan untuk mencari keuntungan bagi pelaku ini banyak terjadi. Berbagai laporan dan berita dari berbagai instansi dan perusahaan mengeluhkan hal ini. Namun Indonesia belum mempunyai aturan mengenai hal ini. Padahal kerusakan yang ditimbulkannya sangat merugikan instansi atau perusahaan yang di *hacking.*

c. Kasus *Carding* atas nama Adhenico Agusta Kurniawan[106]

Merupakan kasus yang ditangani di wilayah hukum Jawa Tengah dengan tersangka pelaku tindak pidana adalah Adhenico Kurniawan yang berusia 23 tahun dan merupakan mahasiswa sebuah perguruan tinggi swasta di Semarang.

1) Kasus Posisi

Pada hari Rabu 3 Nopember 2000, polisi menyita barang kiriman yang dipesan melalui internet senilai USD 11.996,00. Barang-barang tersebut disita saat terdakwa mengambil kiriman dari jasa pengiriman Federal Express (FEDEX) berupa empat unit computer merk Palm IIIC yang belum beredar di Indonesia.

Pemesanan yang dilakukan terdakwa melalui e-mail adhe_28@www.yahoo.com dengan menggunakan kartu kredit master card atas nama Dario Anzani yang beralamat di 6 Lamington Drive Galdstone QLD Australia. Nomor Kartu kredit tersebut 5313 5520 0003 9280, diperoleh terdakwa melalui Internet Relay Chart (IRC) yaitu *Chatting* di *cyberspace*.

Transaksi yang dilakukan melalui internet ini setelah terlebih dahulu masuk dengan cara tidak sah atau berhasil memecahkan

---

[106] Jaksa pada Kejaksaan Tinggi Jawa Tengah; Pengadilan Negeri Semarang

kode *(password)* dan masuk ke situs Greywolf Computer Services milik Mark Bunner yang beralamat di 80 Liberty Avenue, Weirton, WV 26062-2124 USA.

2) Dakwaan JPU

Jaksa Penuntut Umum mendakwa dengan Dakwaan Alternatif yaitu Pada dakwaan kesatu primair melanggar Pasal 363 ayat (1) ke 5 KUHP, yaitu pencurian yang dilkukan dengan merusak atau mrmakai anak kunci palsu, perintah palsu atau pakaian jabatan palsu dengan ancaman hukuman maksimal 7 (tujuh) tahun. Dakwaan Subsidiair Pasal 362 KUHP tentang pencurian dengan ancaman hukuman maksimal 5 (lima tahun). Dakwaan kedua Pasal 378 KUHP tentang Penggelapan dengan ancaman hukuman 4 (empat) tahun.

Dalam dakwaannya tersebut, Jaksa tidak menyebutkan secara detail bagaimana bisa terdakwa mendapatkan nomor kartu kredit atas nama Dario Anzani yang berdomisili di singapura. Fakta ini terdapat dipemeriksaan persidangan. Cara terdakwa dapat melakukan pemesanan yang berarti berhasil memecahkan kode rahasia *(personal Identification)* dari pemilik kartu kredit juga tidak disebutkan secara detail dalam dakwaan Jaksa. Padahal dalam kejahatan di *cyberspace* hal ini penting untuk dibahas.

3) **Putusan Pengadilan Negeri**

Hakim dalam menjatuhkan putusan terhadap kasus ini berdasarkan Pasal 362 KUHP tentang pencurian yang didakwakan Jaksa dalam Dakwaan Kesatu Subsidiair. Hal ini dengan pertimbangan bahwa terdakwa menggunakan nama dan alamatnya sendiri dalam pengiriman barang dan tidak menggunakan nama atau alamat palsu.

Hukuman yang dijatuhkan adalah 6 (enam) bulan dengan masa percobaan 2 (dua) tahun, sama dengan tuntutan jaksa. Hal ini dengan pertimbangan bahwa terdakwa masih muda dan megakui perbuatannya.

Putusan yang dijatuhkan oleh hakim tersebut terasa sangat ringan., karena terdakwa tidak menjalani penjara karena dikenakan hukuman percobaan. Padahal kejahatan *carding* ini informasinya diperoleh melalui Interpol. Negara Indonesia merupakan negara yang disorot karena lemahnya penanggulangan kejahatan di dunia *cyber.*

Dalam skala lebih luas menurut survey internasional, Indonesia menduduki peringkat kedua setelah Ukraina untuk pembobolan kartu kredit.[107]

Beberapa kasus lain dengan modus yang hampir sama juga terjadi di berbagai kota di Indonesia seperti Bandung, Jakarta, Jogyakarta, Medan dan kota besas lainnya. Salah satu kasus *carding* yang disidangkan di Pengadilan Yogyakarata, pelakunya dijerat dengan Pasal 378 (tentang Penggelapan). Hal ini karena terdakwa menggunakan nama dan identitas palsu kepada pihak tempat pemesanan.

Pada umumnya pelaku kejahatan ini adalah mahasiswa yang belajar komputer secara otodidak. Bahkan menurut dara yang diberikan Satuan fiskal, Moneter dan Devisa Polda Metro Jaya, AKBP Dharma Pongrekun, Yogyakarta dan Bandung menduduki peringkat teratas kejahatan *carding*.[108] Kasus Carding atau pembobolan kartu kredit belum banyak yang berhasil disidangkan karena keterbatasan pihak kepolisian dalam menjerat dan mencari alat bukti untuk kasus-kasus ini.

---

[107] Majalah Gatra, *Menjepit Ulah Pembobol Kartu Kreditt,No. 43 Tahun IX*, Jakarta, 2003, hal 26
[108] *Ibid*, hal. 27

B. KEBIJAKAN HUKUM PIDANA UNTUK CYBERCRIME DI MASA YANG AKAN DATANG

Materi hukum komputer dalam pembahasan literatur secara umum meliputi hak milik intelektual/*intellectual property right* (yang menyangkut paten, *Copyright*, rahasia dagang), kontrak komputer *(hardware, software, personnel, services, sales and lease),* perbuatan hukum dibidang komputer *(komputer tort),* kejahatan komputer *(computer crime),* kebebasan dan informasi rahasia *(privacy and confidential information)* dan bukti komputer *(Computer and evidence).*[109] *Cybercrime* merupakan tindak pidana yang dilakukan dengan memanfaatkan teknologi informasi. Secara teknis tindak pidana tersebut dapat dibedakan menjadi *offline crime, semi offline crime, cybercrime.*[110] Masing-masing memiliki karakteristik tersendiri, namun perbedaan utama diantara ketiganya adalah keterhubungan dengan jaringan komputer (Internet). *Cybercrime* merupakan perkembangan lebih lanjut dari kejahatan atau tindak pidana dengan memanfaatkan teknologi komputer yang terhubung dalam jaringan yang sedang *on-line.*

---

[109] Collin Tapper, *Computer Law*, Longman, London & New York, Second Edition,1982.
[110] http://www.hukumonline/Cybercrime, Last update 9 Januari 2003.

Barda Nawawi Arief mengatakan bahwa *cyber crime* merupakan satu sisi gelap dari kemajuan tehnologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.Beberapa sebutan diberikan kepda jenis kejahatan baru ini seperti *cyber space/virtual space offence*, dimensi baru dari *hi-tech crime*, dimensi baru dari *transnasional crime*, dan dimensi baru dari *white collar crime*.[111]

Kemudian dikatakan oleh Muladi :

> *Cybercrime* pada hakekatnya merupakan sisi negatif dari teknologi komputer, dalam arti ternyata ia juga rentan terhadap perilaku kriminal. Sebagai contoh adalah praktek-praktek implantasi virus yang dapat mencederai virus di seluruh dunia. Beberapa virus hanya bersifat mengganggu, tetapi jenis virus lain dapat menimbulkan kerusakan yang signifikan terhadap data, program dan *hardware*. Bank-bank dan berbagai lembaga keuangan telah kehilangan uang dalam jumlah besar. Ada yang melaporkan perbuatan tersebut tetapi adapula yang merahasiakannya dengan alasan reputasi. Beberapa kejadian di negara maju, data tentang keamanan nasional dan rahasia dagang perusahaan secara melawan hukum telah di *download* oleh orang-orang yang tidak bertangunggungjawab dan dijual kepada dinas intelijen asing. Yang sangat dirugikan juga para pemilik hak atas kekayaan intelektual yang karyanya diakses tanpa membayar royalti. Belum lagi berbagai tindak pidana lain, melalui berbagai sarana teknologi canggih para pelakunya dapat menghindarkan diri dari penuntutan dan melakukannya dari negara-negara yang belum memiliki hukum yang mengatur *cyberlaw* atau *cybercrime*.[112]

---

[111] *Barda* Nawawi Arief, ***Sari Kuliah Perbandingan Hukum Pidana***, *Op cit*, hal. 252.
[112] Muladi, ***Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia***, *Op cit*, hal. 203.

Selain yang sudah dikemukakan pada bab sebelumnya mengenai bentuk-bentuk dan kategori-kategori *cybercrime*, juga dapat dikemukakan pendapat lain mengenai kategori *cybercrime*. Nazura Abdul Manap membedakan 3 kategori *cyber crime*, yaitu :[113]

1. *Cyber crime against property, meliputi theft* (berupa *theft of information, theft of property dan theft of service), fraud/cheating, forgery,* dan *mischief.*
2. *Cyber crimes against persons,* meliputi *pornography, cyber harassment, cyber stalking* dan *cyber trespass,* yang meliputi *Spam e-mail, hacking a web page dan breaking into personal computer.*
3. *Cyber terrorism*

Chaeruddin Ismael menyebutkan beberapa jenis kejahatan di dunia *cyber* antara lain:[114]

1. Pemalsuan *(counterfeiting)*
   Dengan segala kecanggihannya teknologi komputer telah menciptakan suatu revolusi dalam hal pemalsuan. Teknologi baru ini tidak saja telah memperluas lingkup operasi pemalsuan tetapi juga telah membuat semakin sulitnya aparat penegak hukum untuk mendeteksinya
2. Pornografi dan perdagangan sex.
   Keleluasaan dan kebebasan jaringan *computer system* pada Internet pada gilirannya juga menyebabkan pornografi anak merajalela. Situs-situs porno berkembang dengan marak, dan situs pornografi dalam bentuk gambar dan teks menjadi suatu yang bebas dan terbuka
3. *Transnational Gambling*
   Judi Internet juga mmepermudah terselenggaranya perjudian transnasional. Disamping perjudian tersebut, sering terjadi penipuan karena operator judi suka menipu. Masalah ini sangat sulit dilacak karena

---

[113] Nazura Abdul Manap, dalam Agus Raharjo, ***op cit***, hal. 228.
[114] Chaeruddin Ismael, *Cybercrime: Kejahatan Maya, Kerugian Nyata,dalam Jurnal Studi Kepolisian Edisi 056,* PTIK, Jakarta, 2003, hal 8-10

akan menyangkut jurisdiksi kalau opeartor judi berada di negara lain, dan lain-lain;

4. Pencurian dan penggunaan account Internet milik orang lain
   Salah satu kesulitan dari *Internet Service Provider* (ISP) adalah adanya *account* pelanggan yang dicuri dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, pencurian *account* cukup dengan menangkap *user id* dan *password* saja.
5. Membajak situs web
   Salah satu kegiatan yang sering dilakukan *cracker* adalah mengubah halaman web, yang terkenal dengan istilah *deface.* Pembajakan ini dapat dilakukan dengan mengeksploitasi lubang keamanan
6. *Probing* dan *port scanning*
   Salah satu langkah yang dilakukan *cracker* sebelum masuk ke server yang ditargetkan adalah dengan cara melakukan pengintaian untuk melihat pelayanan apa saja yang tersedia di server target.
7. Kejahatan dengan penyebaran virus
   Pada umumnya virus yang disebarkan dalan jaringan Internet dilakukan melalui e-mail. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal itu. Virus kemudian dikirimkan ke tempat lain melalui emailnya. Contohnya adalah penyebaran virus Melissa, I Love You dan SirCam
8. *Dos attack*
   Merupakan serangan yang bertujuan untuk melumpuhkan target *(hang, crash)i* sehingga sebuah server tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan ataupun pemalsuan data, akan tetapi hilangnya layanan maka target tidak dapat memberikan layanan apapun kepada konsumen, sehingga menimbulkan ketugian finansial.
9. Kejahatan yang berhubungan dengan nama domain.

Pengaturan hukum mengenai *cybercrime* yang disebut *cyberlaw* juga berbeda-beda di setiap negara. *Cyberlaw* sendiri meliputi ruang lingkup yang sangat luas, seperti dikatakan Agus Raharjo dengan mengutip Jonathan Rosenoer,[115] meliputi :

1. *Copyright*, meliputi *exclusive rights, subject matter of copyright, formalities, infringement, sources of risk, world wide web sites, hypertext links, graphical elements, e-mail, postings, ciminal liability, fair use, first amandement,* dan *software rental.*
2. *Trademark.*
3. *Defamation* (fitnah atau pencemaran nama baik).
4. *Privacy*, meliputi *common law privacy, constitution law, anonymity* (keadaan anonim pada jaringan internet) dan *technology expanding privacy rights* (pengembangan hak privasi dengan teknologi).
5. *Duty of care*, meliputi :
   a. *negligence* (tindakan yang dilakukan di luar kebiasaan, tetapi dibenarkan oleh hukum sebagai upaya perlindungan dari risiko kekerasan yang tidak perlu).
   b. *Negligent misstatement* (tindakan yang dilakukan pihak penyedia jasa informasi di internet dengan memberikan informasi yang tidak akurat).
   c. *Equipment malfunctions* (kerusakan teknis dari peralatan, dimana ketidaksiapan untuk mengantisipasi kerusakan teknis tersebut akan menimbulkan tanggung jawab atas *negligence*).
   d. *Economic loss may not be recoverable* (kerugian yang secara ekonomis tidak tergantikan).
   e. *Contractual limitations of liability* (tanggung jawab keterbatasan kontrak).
6. *Criminal liability*, meliputi *computer fraud and abuse act, wire fraud, electronic communications privacy act, extortion and threats, exports, sexual exploitation of children, obsence and indecent telephone calls, copyright, stalking.*
7. *Procedural Issues*, meliputi *Jurisdiction, venue dan conflict of law.*

---

[115] Agus *Raharjo*, *Op cit*, hal. 216.

8. *Electronic contract and digital signature, meliputi electronic agreement enforceable, public key encryption and digital signature.*

Tim Pengkajian *Cyberlaw* UNPAD mengkategorikan cyberlaw dari aspek hukum publik dan hukum privat, sebagai berikut :[116]

1. Aspek hukum publik :
   a. Jurisdiksi dan kompetensi Badan Peradilan serta aspek pembuktiannya,
   b. Etika kegiatan dalam *cyberspace,*
   c. Perlindungan konsumen,
   d. Anti monopoli,
   e. Persaingan sehat,
   f. Perpajakan,
   g. Regulatory body,
   h. Perlindungan *electronic database,*
   i. ***Cybercrime.***
2. Aspek hukum privat :
   a. Intellectual *property rights,*
   b. *E*-commerce,
   c. Kontrak dalam internet (cybercontract),
   d. Privacy,
   e. Domain name
   f. Asuransi.

Beberapa bentuk kejahatan di dunia *cyber* memang bisa diatasi dengan menggunakan hukum positif yang ada. Disisi lain berbagai aspek atau bentuk kejahatan lain yang terjadi, secara tegas Indonesia belum memiliki perangkat hukum yamg mengatur masalah *cybercrime.* Seperti pengaturan masalah *domain name, Domain Name* merupakan salah satu elemen penting dalam interaksi di dunia maya. Domain name akan sangat berperan dalam

---

[116] *Ibid.* hal. 221.

memberikan informasi sekaligus kejelasan identitas kepada publik. Demikian juga dengan pengaturan konten internet, dimana internet merupakan *open resources* (sumber yang terbuka) yang dapat diakses oleh siapapun. Pdahal negara-negara yang demokratis sudah memiliki perangkat hukujm berkaitan dengan konten internet.

Pembaharuan hukum pidana pada hakikatnya mengandung makna, suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana sesuai dengan nilai-nilai sentral sosio-politik, sosio filosofik dan sosio kultural masyarakat Indonesia yang melandasi kebijakan sosial, kebijakan kriminal dan kebijakan penegakan hukum di Indonesia.[117]

Dengan demikian penentuan kebijakan hukum pidana untuk menanggulangi *cybercrime* (kejahatan dunia maya) harus melalui pendekatan yang berorientasi pada nilai *(value oriented approach).*

Ronny Nitibaskara mengemukakan bahwa kejahatan siber *(cyber)* berbeda dengan kejahatan-kejahatan lain yang tidak menggunakan jaringan komputer yang terkait dalam sistem yang membentuk *cyberspace.* Kejahatan siber dalam lingkup hukum pidana termasuk dalam tindak pidana khusus yang membutuhkan pengaturan khusus diluar KUHP dengan ciri-cirinya:[118]

---

[117] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op cit,* hal 27-28

[118] Ronny Nitibaskara, *Ketika Kejahatan Berdaulat,Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi,* Peradaban, Jakarta, 2001, hal 69

1. *Non Violence* (tanpa kekerasan)
2. Sedikit melibatkan kontak fisik *(minimize of physical contact)*
3. Menggunakan peralatan *(equipment)* dan teknologi
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika global)

1. Kriminalisasi

Hukum pidana merupakan salah satu sarana kebijakan kriminal untuk menanggulangi *cybercrime*. Dalam kebijakan hukum pidana maka akan bersentuhan dengan persoalan kriminalisasi *(criminalization)* baik itu perbuatan yang melawan hukum *(actus reus)*, pertanggungjawaban pidana *(mens rea)*, maupun sanksi yang dijatuhkan berupa pidana *(punishment)* maupun tindakan *(treatment)*.

Kriminalisasi harus memenuhi pelbagai syarat antara lain bahwa perbuatan tersebut benar-benar menampakkan korban *(victimizing)* baik aktual maupun potensial, kemudian konsistensi penerapan asas *ultimum remedium*, dukungan publik yang kuat, bersifat komprehensif dan tidak bersifat ad-hoc.[119]

---

[119] Muladi, *Kebijkan Kriminal terhadap Cybercrime, Op cit,* hal 2.

Sudarto berpendapat bahwa dalam menghadapi masalah sentral perbuatan apa yang seharusnya dijadikan tindak pidana, sering disebut masalah kriminalisasi, harus diperhatikan hal-hal yang pada intinya sebagai berikut:[120]

a. Penggunaan hukum pidana harus memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil dan makmur yang merata materiil dan spiritual berdasarkan Pancasila; sehubungan dengan ini maka (penggunaan) hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan pengugeran terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat.
b. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan "perbuatan yang tidak dikehendaki", yaitu perbuatan yang mendatangkan kerugian (materiak dan atau spiritual) atas warga masyarakat;
c. Penggunaan hukum pidana harus pula memperhitungkan prinsip "biaya dan hasil" *(cost and benefit principle)*
d. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum, yaitu jangan sampai ada kelampauan beban tugas *(overbelasting)*

Demikian pula menurut Bassiouni, keputusan untuk melakukan kriminalisasi dan dekriminalisasi harus didasarkan pada faktor-faktor, kebijakan tertentu yang mempertimbangkan bermacam-macam faktor, termasuk[121]

a. Keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil yang ingin dicapai;

---

[120] Barda Nawawi Arief, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara, Op cit*, hal. 35
[121] *Ibid*, hal. 37

b. Analisa biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;
c. Penilaian atau penaksiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas-prioritas lainnya dalam pengalokasian sumber daya manusia;
d. Pengaruh sosial dari kriminalisasi dan dekriminalisasi yang berkenaan dengan atau dipandang dari pengaruh-pengaruhnya yang sekunder.

a. **Perbandingan dengan Negara Lain**

Berbagai bentuk kejahatan siber *(cybercrime)* yang terus meningkat di Indonesia dapat ditanggulangi dengan menggunakan hukum positif yang menggunakan metode interpretasi. Namun dalam berbagai hal ditemui adanya kendala-kendala dan kelemahan. Untuk adanya kepastian hukum diperlukan kebijakan legislatif dalam mewujudkan peraturan hukum pidana yang mampu menjangkau kompleksitas *cybercrime* secara tepat.

Disamping perlunya diadakan kajian terhadap hukum-hukum positif, maka diperlukan juga kajian untuk mengadakan pembaharuan hukum pidana untuk mengantisipasi perkembangan *cybercrime* di masa yang akan datang. Hal ini bukanlah mudah mengingat sulitnya merumuskan tindak pidana agar bisa mengikuti perkembangan zaman dan berbagai persoalan lainnya.

Sifatnya yang lintas negara telah menjadikan kejahatan di internet tidak saja merupakan persoalan nasional, namun sudah menjadi persoalan internasional. Hal ini terlihat dari rekomendasi yang dikeluarkan oleh PBB melalui Kongresnya atau juga *Council of Europe*. Penanggulangan *cybercrime* menjadi persoalan negara-negara di dunia. Pengaturannya juga berbeda-beda di setiap negara.

Negara-negara di Eropa Kontinental yang menganut tradisi hukum *civil law* sudah pasti menempatkan peraturan perundang-undangan (hukum tertulis) sebagai sumber hukum yang paling utama. Hal ini tentu saja berbeda dengan negara-negara *Anglo Saxon* yang menganut tradisi hukum *Common Law*, cenderung menitikberatkan pembentukan hukum melalui kasus-kasus konkret *(law in cases)*. Negara-negara tersebut menempatkan putusan hakim sebagai sumber hukum yang utama bagi pertimbangan terhadap kasus-kasus berikutnya. Namun demikian dewasa ini ada kecenderungan yang umum, baik pada tradisi hukum kontinental maupun *anglo saxis*, makin pentingnya peraturan perundang-undangan.[122]

---

[122] Bagir Manan dalam Al. Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, *Op cit*, hal 205

Disamping karena perbedaan tradisi hukum yang melandasi sistem hukum suatu negara, keanekaragaman pengaturan di berbagai negara juga dikarenakan perbedaan pendekatan dalam menyelesaikan kasus. Secara umum terdapat tiga cara penyelesaian dalam menilai ukuran-ukuran isinya yaitu:[123]

1) *Property Approach.* Penyalahgunaan komputer disini dilihat sebagai suatu bagian dari delik terhadap harta kekayaan *(Property),* Dengan demikian isi inti dari catatan-catatan komputer tersenut diterjemahkan menurut nilai finansialnya. Disamping itu kepentingan-kepentingan yang dikaitkan penggunaan sistem komputer dimasukkan ke dalam pengertian *property.* Perlu diketahui bahwa pendekatan ini merupakan yang tertuan dan paling banyak dilakukan.
2) *Forgery Approach.* Disini penyalahgunaan komputer dilihat terutama sebagai bagian dari delik-delik pemalsuan, dimana integritas dari keterangan-keterangan catatan komputer merupakan hal yang terutama harus diperhatikan dalam suatu penyelesaian.
3) *Information Approach.* Merupakan penyelesaian yang teruttama diarahkan pada sifat dipercayainya isi dan arti dan arti dari catatan-catatan komputer.

Kajian perbandingan hukum (Yuridis Komparatif) dilakukan untuk mengetahui bagaimana baiknya pengaturan hukum ke depan dalam masalah *cybercrime* terutama berkaitan dengan model pengaturan, kriminalisasi dan sanksi pidana. Berikut ini akan diberikan beberapa peraturan di negara lain. Tidak semua yang sudah mempunyai aturan

---

[123] *Ibid*, hal. 206

mengenai *cybercrime* diungkapkan. Hal ini karena keterbatasan penulis. Mengingat rumitnya penentuan tindak pidana, maka akan dikemukan tindak pidana yang diatur oleh beberapa negara.

1) Singapura

Singapura telah mempunyai perangkat hukum yang berkaitan dengan *cybercrime*. Disebut dengan ***The Computer Misuse Act*** Tahun 1993, terdapat 4 tipe utama tindak pidana yang terdapat pada *Section* (Bab) 3 sampai dengan *Section* 7, intinya sebagai berikut :

a) *Hacking,* yang mengakibatkan suatu komputer menghasilkan suatu fungsi dengan maksud untuk menjamin akses tanpa hak terhadap suatu program atau data yang disimpan di suatu komputer.

b) *Unauthorized Access*, dengan maksud untuk melakukan atau memudahkan pelaksanaan suatu kejahatan yang berkaitan dengan harta kekayaan, penipuan, ketidakjujuran atau perbuatan yang mengakibatkan kerugian/kerusakan jasmaniah;

c) Modifikasi secara sengaja dan tidak sah muatan/kandungan/isi suatu komputer (data, program perangkat lunak komputer dan *database,* dengan cara misalnya memasukkan virus kedalam komputer.

d) Menggunakan *(using)* atau memintas *(intercepting)* suatu pelayanan komputer tanpa hak; seperti mencuri pelayanan komputer atau waktu *(theft of a computer service or time).*

e) Membantu atau mencoba melakukan perbuatan di atas.

Di Singapura tidak hanya tindak pidana terhadap komputer yang dilakukan di Singapura yang dapat dipidana, tetapi juga yang dilakukan dari luar Singapura dapat dipidana dan terhadap tindak pidana yang ditujukan terhadap komputer luar negeri.

Tahun 1998 *The Computer Misuse Act* di amandemen *(The Computer Misuse (Amandement Act 1998),* dengan pemberatan pidana dan dimasukkannya 2 (dua) tindak pidana baru yaitu :

a) Mengganggu atau menggunakan komputer secara tidak sah mengungkap *access code* atau dengan sarana lain guna memperoleh keuntungan atau tujuan yang tidak sah.

b) Membuka/mengungkap *passsword, access code* atau dengan cara lain memperoleh akses terhadap program atau data yang disimpan di suatu komputer. Dalam hal ini pemikiran sampai pada *confidentiality law;*

c) Tindak Pidana yang melanggar *protected computers* untuk kepentingan pertahanan, keamanan, hubungan internasional, eksistensi dan identitas rahasia tentang sumber informasi dalam rangka penegakan hukum pidana, pengetahuan tentang infrastruktur komunikasi, perbankan dan pelayanan keuangan dan keamanan pulik.

Singapura juga menerapkan aturan yang tegas tentang internet yakni dengan memblokir situs yang tidak disukai oleh Pemerintah seperti situs pornografi dengan menggunakan *proxy server.*[124]

---

[124] Edmon Makarim, *Kompilasi Hukum Telematika ,Op cit,* hal 119.

2) Australia

Australia yang dikenal baik dalam pengaturan media informasi, mengambil kebijakan tegas bagi informasi illegal yang disebarkan melalui internet. *Commonwealth Legislation* dan parlemen negara bagian memberlakukan rezinm sensor terhadap konten Internet di Australia. Sejak 1 Januari 2000, *Commonwealth Legislation* dam parlemen negara bagian memberlakukan regulasi tentang *Internet Content Host* (ICHs) dan *Internet Service Providers* (ISPs), dimana dalam aturan ini, Negara Federal memaksakan agar ICH dan ISP peduli terhadap konten internet yang berada dalam kekuasaan mereka. Ini artinya ICP dan ISP harus memastikan bahwa anak-anak terlindungi dari informasi yang bertentangan dengan hukum. Badan yang diberi wewenang untuk menjalankan tugas ini adalah *The Australian Broadcasting Authority* (ABA) di bawah *The Broadcasting Services Act Amandements.*

Dalam pengaturan tindak pidana di dunia *cyber (cybercrime),* Australia juga telah mengamandemen perundang-undangannya pada tahun 2001 dengan sebutan *Cybercrime Act 2001, An Act to amend the law relating to computer offences, and for other purposes.* Turut pula diamandemen peraturan dan organisasi yang berkaitan dengan

kejahatan computer atau *cybercrime.* Seperti amandemen terhadap *Australian Security Intelligence Organisation Act 1979.* The *Telecommunications (Interception) Act 1979 Telecommunications Act 1997.* Dalam Undang-undang ini diberikan definisi-definisi yang berkaitan dengan kegiatan di internet dan juga berbagai istilah dalam komputer.

Undang-undang ini membedakan secara garis besar dua bentuk kejahatan komputer yaitu *Serious computer offences* dan bentuk lain kejahatan komputer. *Serious computer offences* diatur pada *Division 477* dan terbagi lagi dalam 3 (tiga) bentuk. Berikut akan diuraikan kejahatan dimaksud:

Division 477—Serious computer offences
477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

(1) Intention to commit a serious Commonwealth, State or Territory offence

A person is guilty of an offence if:the person causes:

(a) any unauthorised access to data held in a computer; or any unauthorised modification of data held in a computer; or any unauthorised impairment of electroniccommunication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a telecommunications service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of a serious offence against a law of the Commonwealth, a State

or a Territory (whether by that person or another person) by the access, modification or impairment..

(2) Intention to commit a serious Commonwealth offence
A person is guilty of an offence if:
(a) the person causes: any unauthorised access to data held in a computer; or any unauthorised modification of data held in a computer; or any unauthorised impairment of electronic communication to or from a computer; and
(b) the person knows the access, modification or impairment is unauthorised; and
(c) the person intends to commit, or facilitate the commission of a serious offence against a law of the Commonwealth (whether by that person or another person) by the access, modification or impairment.

477.2 Unauthorised modification of data to cause impairment
A person is guilty of an offence if:
(a) the person causes any unauthorised modification of data held in a computer; and
(b) the person knows the modification is unauthorised; and
(c) the person is reckless as to whether the modification impairs or will impair: access to that or any other data held in any computer; or the reliability, security or operation, of any such data; and
(d) one or more of the following applies: the data that is modified is held in a Commonwealth computer; the data that is modified is held on behalf of the Commonwealth in a computer; the modification of the data is caused by means of a telecommunications service; the modification of the data is caused by means of a Commonwealth computer; the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer; the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer; the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a telecommunications service.

477.3 Unauthorised impairment of electronic communication

A person is guilty of an offence if:

a. *the person causes any unauthorised impairment of electronic communication to or from a computer; and*
b. *the person knows that the impairment is unauthorised; and*
c. *one or both of the following applies: the electronic communication is sent to or from the computer by means of a telecommunications service; the electronic communication is sent to or from a Commonwealth computer.*

Division 478—Other computer offences

478.1 Unauthorised access to, or modification of, restricted data

A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modificationof, restricted data; and
(b) the person intends to cause the access or modification; and
(c) (c) the person knows that the access or modification isunauthorised; and
(d) one or more of the following applies: the restricted data is held in a Commonwealth computer; the restricted data is held on behalf of the Commonwealth;

478.2 Unauthorised impairment of data held on a computer disk etc.

A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on: a computer disk; or a credit card; or another device used to store data by electronic means; and
(b) the person intends to cause the impairment; and
(c) the person knows that the impairment is unauthorised; and
(d) the computer disk, credit card or other device is owned or leased by a Commonwealth entity.

478.3 Possession or control of data with intent to commit a computer offence

A person is guilty of an offence if:

(a) the person has possession or control of data; and
(b) the person has that possession or control with the intention that the data be used, by the person or another person, in: committing an offence against Division 477; or facilitating the commission of such an offence.

Ancaman hukuman untuk kejahatan yang disebut di atas adalah pidana penjara 3 (tiga) tahun.

478.4 Producing, supplying or obtaining data with intent to commit a computer offence
A person is guilty of an offence if:
(a) the person produces, supplies or obtains data; and
(b) the person does so with the intention that the data be used, by the person or another person, in: committing an offence against Division 477; or facilitating the commission of such an offence.

Ancaman hukuman untuk kejahatan yang disebut di atas adalah pidana penjara 3 (tiga) tahun.

Dari ketentuan dalam *Cybercrime Act 2001 di Australia tersebut, terkesan bahwa pengaturan tentang tindak pidana siber diatur secara rinci, sebagaimana diatur dalam* UU *Cybercrime* di Singapura. Meskipun terdapat perbedaan tentang kualifikasi *cybercrime* antara undang-undang di kedua negara tersebut, akan tetapi pada dasarnya *cybercrime* terbagi atas 2 jenis, yaitu "*cybercrime murni*" dan "*tindak pidana lain yang berkaitan dengan cybercrime*".

3) Amerika Serikat

Di Amerika Serikat terdapat berbagai perundang-undangan yang mengatur *cybercrime* dalam kaitannya dengan internet, antara lain :[125]

a) *Access Device Fraud Act of 1984,*
b) *Computer Fraud and Abuse Act of 1986,*
c) *Wire Fraud Statute of 1952,*
d) *Criminal Infringement of a Copyright (Copyright Act of 1976),*
e) *Counterfeit Trademark (The Trademark Counterfeit Act of 1984),*
f) *Mail Fraud,*
g) *Conspiracy to Defraud the US Government,*
h) *False statements,*
i) *Identity Theft and Assumption Deterrence Act of 1998,*
j) *The Racketeer Influenced and Corrupt Organization Act,*
k) *Wire and Electronic Communications Interception of Oral Communication,*
l) *Unlawful Access to Stored Communications,*
m) *Transportation of Stolen Goods, Securities, Money,*
n) *Trafficking in counterfeit Goods and Services,*
o) *Extortion and Threats,*
p) *Transportation of Obscene Matters for Sale or Distribution,*
q) *Communication Decency Act of 1996.*

Dari berbagai peraturan di atas terlihat bahwa di Amerika Serikat tiap kejahatan diatur dalam suatu peraturan khusus. Pengkriminalisasian langsung dijadikan dalam peraturan perundang-undangan. Hal tersebut mungkin disebabkan perkembangan ilmu pengetahuan dan teknologi

[125] Muladi, ***Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia, Op cit,*** hal. 204-205.

diAmerika Serikat yang sudah sangat maju, yang di sisi lain memicu tindak pidana - tindak pidana yang baru atau canggih bermunculan secara cepat, sehingga diperlukan aturan-aturan yang secepat mungkin diwujudkan untuk menanggulanginya.

Hal yang perlu dicatat adalah, apabila kriminalisasi dilakukan tanpa suatu evaluasi mengenai mengenai pengaruhnya terhadap keseluruhan sistem, maka akan timbul :

a) Krisis kelebihan kriminalisasi (*the crisis of over criminalization*)

b) Krisis kelampauan batas dari hukum pidana (*the crisis of overreach of the criminal law*).[126]

---

[126] Lihat Pendapat Bassiouni dalam Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana, Op cit,* hal. 33.

b. Dalam Rancangan Perundang-Undangan

1) Rancangan Undang-Undang KUHP 2000

Upaya kriminalisasi dapat ditempuh melalui Undang-Undang yang umum dalam hal ini di Indonesia adalah RUU KUHP dan Undang-undang yang secara khusus mengatur masalah *cyber crime*. Diupayakan juga dengan memperluas pengertian-pengertian yang terdapat dalam Rancangan KUHP, yaitu :

a) Dalam Buku I (Ketentuan Umum) dibuat Ketentuan Umum tentang :

- Pengertian barang (Pasal 174) yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon/telekomunikasi/jasa komputer,
- Pengertian anak kunci (Pasal 178) yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu magnetik, signal yang telah diprogram untuk membuka sesuatu,
- Pengertian surat (Pasal 188) termasuk data tertulis/tersimpan dalam disket, pita magnetik, media penyimpan komputer atau penyimpan data elektornik lainnya,
- Pengertian ruang (Pasal 189) termasuk bentangan atau terminal computer yang dapat diakses dengan cara-cara tertentu,
- Pengertian masuk (Pasal 190) termasuk mengakses komputer atau masuk ke dalam sistem computer,
- Pengertian jaringan telepon (Pasal 191) termasuk jaringan komputer atau sistem komunikasi komputer.

b) Dalam Buku II (Tindak Pidana) :

- Menyadap pembicaraan di ruangan tertutup dengan alat Bantu teknis (Pasal 263),
- Memasang alat Bantu teknis untuk tujuan mendengar/merekam pembicaraan (Pasal 264),

- Merekam (memiliki/menyiarkan) gambar dengan alat Bantu teknis di ruangan tidak untuk umum (Pasal 266),
- Merusak/membuat tidak dapat dipakai bangunan untuk sarana/ prasarana pelayaran umum (antara lain: bangunan sarana telekomunikasi/komunikasi lewat satelit/komunikasi jarak jauh) (Pasal 546)
- Pencucian uang (money laundering) -Pasal 641-642.

2) **Rancangan Undang-Undang Informasi dan Transaksi Elektronik**

Mengantisipasi perkembangan teknologi yang demikian pesat yang telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk hukum baru. Disamping itu juga menjadi pertimbangan dibuatnya Rancangan Undang-undang tentang Informasi dan Transaksi Elektronik adalah kegiatan pemanfaatan teknologi informasi perlu terus dikembangkan tanpa mengenyampingkan persatuan dan kesatuan nasional dan penegakan hukum secara adil, sehingga pelanggaran-pelanggaran yang berkaitan dengan pemanfaatan teknologi informasi dapat dihindari melalui penerapan keseragaman asas dan peraturan perundang-undangan.

Rancangan Undang-Undang Tentang dan Transaksi Elektronik, mencoba mengkriminalisasikan beberapa tindak pidana *cyber* secara khusus. Hal ini diatur pada Bab V-Bab VII Pasal 24 sampai dengan Pasal 36. Hal-hal yang dirumuskan dalam RUU tersebut adalah :

a) Pasal 24 tentang kesempatan terhadap perubahan informasi di internet melalui agen elektronik

b) Pasal 26 ayat (1) tentang hak kepemilikan nama domain; dan ayat (2) tentang penggunaan nama domain yang bertentangan dengan hak kekayaan intelektual orang lain dan rinsip persaingan sehat. Dalam *convention on cybercrime* tindak pidana ini seperti ini termasuk dalam *infringement of copy right*

c) Pasal 28 tentang penggunaan informasi yang menyangkut data pribadi harus izin pemilik data

d) Pasal 29 ayat (1) tentang penggunaan dan atau mengakses komputer melampaui wewenang. Tindak pidana pada ayat (1) diperberat ancaman pidananya apabila mengakses informasi rahasia milik pemerintah (ayat (2)), dan mengakibatkan gangguan terhadap pertahanan negara dan hubungan internasional (ayat (3). Dalam Konvensi *Cybercrime* ayat (1) termasuk *data interference* dan ayat (2) serta (3) tindak pidananya termasuk *illegal access;*

e) Pasal 30 tentang perbuatan secara melawan hukum yang menyebabkan transimisi, informasi, kode atau perintah, komputer dan atau sistem elektronik yang dilindungi negara menjadi rusak. Dalam konvensi *cybercrime* tindak pidana ini termasuk *system interference.*

f) Pasal 31 tentang perbuatan mengakses komputer untuk memperoleh informasi yang dilindungi negara secara melawan hukum. Dalam konvensi . Dalam konvensi *cybercrime* termasuk dalam *illegal access;*

g) Pasal 32 ayat (1) tentang perbuatan mengakses komputer atau sistem milik pemerintah secara melawan hukum; ayat (2) tentang perbuatan yang mengakibatkan rusaknya sistem elektronik yang dilindungi masyarakat;dan ayat (3) tentang perbuatan yang mengakibatkan gangguan terhadap sistem elektronik yang digunkan pemerintah. Dalam konvensi untuk ayat (1) termasuk *illegal access;* ayat (2) dan (3) termasuk *system interference.*

h) Pasal 33 ayat (1) tentang perbuatan mengakses komputer atau sistem elektronik milik lembaga keuangan/perbankan/penerbit kartu kredit untuk memperolah keuntungan; dan ayat (2) tentang perbuatan menggunakan atau mengkases kartu kredit milik orang lain secara melawan hukum. Dalam konvensi ini termasuk dalam *computer related offenses* , lebih spesifik termasuk *computer related fraud.*

i) Pasal 35 tentang perbuatan menerobos sitem secara melawan hokum. Dalam konvensi termasuk *illegal interception*

j) Pasal 36 tentang perbuatan merusak komputer yang dilindungi Negara dalam wilayah jurisdiksi Indonesia secara melawqm hokum. Dalam Konvensi disebut *System interference*

Sebelum adanya Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik (RUU ITE) ini, maka terdapat RUU tentang Pemanfaatan Teknologi Informasi (RUU PTI). Jika dilihat dari bentuk *cybercrime* yang diatur dalam *Convention on Cybercrime* , maka tindak pidana yang diatur dalam RUU ITE adalah tindak pidana yang berkaitan dengan *Illegal access* dan *illegal interception.* Beberapa tindak pidana yang dimuat dalam RUU PTI tidak lagi terdapat dalam RUU ITE, misalnya masalah tindak pidana kesusilaan, pornografi, pornografi anak. RUU ITE hanya secara khusus mengenai *cybercrime.* Berbeda dengan RUU PTI yang merupakan *umbrella act* dimana masih dimungkinkan pengaturan yang lebih khusus lagi.

RUU PTI mengatur lebih lengkap bila dibandingkan dengan RUU ITE, jika acuannya dilihat dari *Convention on Cybercrime,* antara lain:

a) Pasal 35 tentang penggunaan *domain name* yang bertentangan dengan hak atas kekayaan intelektual milik orang lain. Dalam RUU

ITE melanggar Pasal 50 ayat (1). Dalam konvensi hal ini masuk dengan *infringement of copyright.*

b) Pasal 36 tentang akses data komputer/media elektronik lainnya secara melawan hukum. Dalam RUU ITE diatur pada Pasal 48, Pasal 51. Dalam *convention on cybercrime* disebut *illegal access.*

c) Pasal 37 ayat (1) mengenai perbuatan menahan atau mengintersepsi pengiriman data melalui komputer/media elektronik lainnya secara melawan hukum; ayat (2) mengenai perbuatan mengintersepsi secara melawan hukum pengiriman data melalui komputer/media elektronik yang menghambat komunikasi dalam sistem komputer/jaringan komputer/sistem komunikasi lainnya. Dalam RUU ITE ini diatur pada Pasal 51. Dalam *Convention on Cybercrime disebut illegal interception* (ayat (1)) dan *system interference* (ayat (2));

d) Pasal 38 ayat (1) tentang memasukkan, mengubah, menambah, menghapus atau merusak data komputer/program komputer/ data elektronik lainnya secara melawan hukum. Ayat (2) tentang pemberatan ancaman pidananya apabila mengakibatkan kerugian ekonomi bagi orang lain; dan ayat (3) mengakibatkan terganggunya

fungsi sistem komputer atau sistem media elektronik lainnya. Dalam RUU ITE diatur pada Pasal 51 dan 52. Dalam Convention *on Cybercrime* termasuk dalam *system interference.* dan *data interference*

e) Pasal 39 mengenai penggunaan kartu kredit/alat pembayaran elektronik lainnya milik orang lain secara melawan hukum dalam transaksi elektronik. RUU ITE diatur pada Pasal 52. Dalam *convention on Cybercrime* termasuk *computer related fraud.*

f) Pasal 40 ayat (1) tentang membuat, menyediakan, mengirimkan, mendistribusikan data, tulisan, gambar, rekaman yang isinya melanggar kesusilaam dengan menggunakan komputer/media elektronik lainnya. Ancaman pidana diperberat pada ayat (2) bila objeknya anak. RUU ITE tidak lagi mengatur masalah ini dan dalam *convention on cybercrime* termasuk *child pornoghraphy.*

Dari uraian di atas terlihat bahwa dalam Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik, masalah kriminalisasi dilakukan secara limitatif yakni hanya menerapkan ketentuan tertentu untuk pengaturan *cybercrime.* Bahkan jika dibandingkan dengan RUU Pemanfaatan Teknologi Informasi, RUU

ITE mengatur lebih sempit lagi. Kebijakan formulasi yang limitatif akan menimbulkan kesulitan mengingat kejahatan di dunia *cyber (cybercrime)* mencakup aspek yang sangat luas.

Dari uraian di atas, maka penggunaan pendekatan kebijakan untuk menentukan tindak pidana yang berkaitan dengan dunia virtual *(Cybercrime)*, perlu memperhatikan:

a. perkembangan teknologi informasi memberikan pengaruh yang besar terhadap kemajuan bangsa, terlebih dalam era globalisasi. Perumusan tindak pidana hendaknya dilakukan secara selektif yakni perbuatan mana bertentangan dengan nilai-nilai masyarakat, mendatangkan korban dan benar-benar merugikan.
b. Dalam membuat peraturan perlu diperhatikan *cost and benefit.*
c. Pengaruh sosial bagi masyarakat untuk pengkriminalisasian suatu perbuatan.

Menurut Barda Nawawi Arief kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/merumuskan/memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi/legislasi itu disusun dalam satu

kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu.[127]

Harmonisasi dilakukan secara eksternal melalui instrumen hukum internasional yang sudah disepakati dan harmonisasi secara internal melalui tindak pidana yang sudah diatur dalam hukum positif yang ada.

Berkaitan dengan hal tersebut, maka kebijakan kriminalisasi terhadap *cybercrime* seyogyanya diwujudkan dalam sebuah "undang-undang payung" atau *umbrella act*. Hal tersebut disebabkan untuk mencegah timbulnya perundang-undangan dalam jumlah besar yang mengatur tentang *cybercrime*, yang berpotensi saling tumpah tindih dalam pengaturan terhadap *cybercrime*.

Di samping itu, dengan adanya *umbrella act*, dapat dihindari *over-criminalization* dan *the crisis of overreach of the criminal law* yang dapat menimbulkan kerancuan dalam usaha pengendalian kejahatan.

---

[127] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op cit*, hal. 259-260

2. Penalisasi

Kecenderungan berkembangnya bentuk dan dimensi kejahatan tentulah memerlukan penanganan, yang salah satu cara penanggulangannya adalah dengan sarana penal atau sanksi pidana.

Sanksi pidana merupakan salah satu masalah sentral dalam hukum pidana, karena itu menjadi hal yang penting untuk dikaji bagaimana bentuk pidana yang tepat dalam menanggulangi *cybercrime.*

Masalah penalisasi atau pemidanaan sendiri merupakan bagian masalah yang sangat penting dari suatu kebijakan pemidanaan *(sentencing policy)* yang menurut Herbert L. Packer merupakan salah satu masalah kontroversial saat ini dalam hukum pidana.[128] Masalah kriminalisasi dan penalisasi atau pidana dan pemidanaan, merupakan masalah yang selalu memerlukan peninjauan kembali, mengingat sifatnya yang melekat *(inherent)* dengan sifat dan hakekat kejahatan itu sendiri yang selalu mengalami perubahan dan perkembangan. Kemudian berubah dan berkembangnya kejahatan selalu diikuti berubah dan berkembangnya pidana itu sendiri. Dalam hal ini S. Balakrishnan mengatakan:[129]

---

[128] Muladi dan Barda Nawawi Arief, ***Teori-Teori Kebijakan Hukum Pidana, Op cit,*** hal. 174.

[129] Barda Nawawi Arief, ***Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara,*** ***Op cit,*** hal. 48.

"Hukum pidana sedang berubah dan memang seharusnya memerlukan perubahan sesuai perubahan masyarakat. Perubahan ini tidak hanya mengenai perbuatan apa yang merupakan atau dinyatakan sebagai kejahatan, tetapi juga mengenai apa yang seharusnya dijadikan pidana untuk suatu kejahatan, karena gagasan-gagasan mengenai pidana juga telah berubah sesuai dengan perubahan-perubahan itu sendiri, terutama mengenai pandangan hidup tentang moral dan kemasyarakatan".

Penetapan jenis-jenis ancaman pidana di dalam hukum pidana, merupakan suatu bagian dari keseluruhan kebijakan kriminal. Hal ini dipandang penting karena disamping untuk menyediakan seperangkat sarana penanggulangan tindak pidana yang dapat dipergunakan hakim, sekaligus untuk membatasi kewenangannya dalam penggunaan sarana pidana lain, selain jenis-jenis pidana yang telah disediakan.

Kebijakan menetapkan jenis sanksi pidana apa yang dianggap paling baik untuk mencapai tujuan, setidak-tidaknya mendekati tujuan, tidak dapat dilepaskan dari persoalan pemilihan berbagai alternatif. Masalah pemilihan berbagai alternatif untuk memperoleh pidana mana yang dianggap paling baik, paling tepat atau paling efektif merupakan masalah yang tidak mudah. Hal ini sejalan dengan apa yang dikatakan oleh Fitzgerald[130], bahwa *the problem of selecting the appropriate sentence is not one which can be solved by normal legal techniques. In fact, it is not the typical sort of legal problem.*

---

[130] Muladi dan Barda Nawawi Arief, ***Teori-teori Kebijakan Hukum Pidana, Op cit***, hal. 98.

Penetapan jenis pidana oleh pembuat undang-undang antara lain dimaksudkan untuk menyediakan seperangkat sarana bagi penegak hukum dalam rangka menaggulangi kejahatan. Di samping itu dimaksudkan pula untuk membatasi penegak hukum dalam menggunakan sarana berupa pidana yang telah ditetapkan itu. Mereka tidak boleh menggunakan sarana pidana yang tidak lebih dulu ditetapkan oleh pembuat undang-undang. Dengan demikian jenis pidana yang dipilih dan ditetapkan oleh pembuat undang-undang mengikat dan membatasi penegak hukum lainnya.

Apabila seperangkat sanksi pidana yang telah ditetapkan merupakan hasil pilihan yang kurang tepat atau sudah tidak sesuai lagi dengan perkembangan kriminalitas, maka adalah wajar apabila penanggulangan perkembangan kriminalitas agak terganggu.

Sebelum ditetapkannya sanksi pidana apa yang tepat serta berat ringannya, maka terlebih dahulu harus ditetapkan tujuannya. Tanpa lebih dulu penetapan tujuan dengan baik, tidak dapat dibicarakan mengenai sarana yang rasional dari politik kriminal.

Barda Nawawi Arief mengatakan, bahwa pidana yang akan ditetapkan adalah pidana yang diharapkan dapat menunjang tercapainya tujuan. Efektivitas pidana harus diukur berdasarkan tujuan atau hasil yang ingin dicapai.[131]

Selanjutnya Barda Nawawi Arief berpendapat, *banyaknya tujuan-tujuan pidana berinduk pada satu tujuan* yaitu *Perlindungan masyarakat untuk mencapai kesejahteraan masyarakat.* Tujuan ini merupakan tujuan umum, yang merupakan induk dari keseluruhan pendapat atau teori-teori mengenai tujuan pidana. Dengan kata lain, keseluruhan pendapat atau teori-teori mengenai tujuan pidana hanya merupakan perincian atau pengindetifikasian dari tujuan umum ini.[132]

Identifikasi beberapa aspek atau bentuk-bentuk perlindungan masyarakat untuk mencapai kesejahteraan melahirkan tujuan :[133]

a. Perlindungan masyarakat terhadap perbuatan anti sosial yang merugikan dan membahayakan masyarakat, tujuannya adalah penanggulangan kejahatan, atau dipakai istilah penindasan kejahatan *(repression of crime)*, pengurangan kejahatan *(reduction of crime)*, pencegahan kejahatan *(prevention of crime)*, pengendalian kejahatan *(control of crime)*.
b. Perlindungan masyarakat terhadap sifat berbahayanya (orang) si pelaku, tujuannya adalah untuk memperbaiki si pelaku. Juga dipakai istilah

---

[131] Muladi dan Barda Nawawi Arief, ***Teori-Teori Kebijakan Hukum Pidana, Op cit***, hal. 101.
[132] Barda Nawawi Arief, ***Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara, Op cit***, hal. 85.
[133] *Ibid*, hal. 85-94.

rehabilitasi, reformasi, *treatment of offenders*, reedukasi, readaptasi sosial, resosialisasi, pemasyarakatan dan pembebasan.

c. Perlindungan masyarakat terhadap penyalahgunaan kekuasaan dalam menggunakan sanksi pidana atau reaksi terhadap pelanggar pidana, tujuannya adalah untuk mengatur atau membatasi kesewenangan penguasa maupun warga masyarakat pada umumnya, atau dalam istilah lain *policing the police,* dan tujuan melindungi pelanggar dari pembalasan yang sewenang-wenang atau pembalasan tidak resmi *(unofficial retaliation).*
d. Aspek lain dari perlindungan masyarakat adalah mempertahankan keseimbangan atau keselarasan berbagai kepentingan dan nilai yang terganggu oleh kejahatan, sehingga tujuannya adalah untuk memelihara atau memulihkan keseimbangan masyarakat. Tujuan keempat ini merupakan induk dari teori retributif.

Tujuan perlindungan masyarakat di atas mengandung dua aspek pokok:[134]

a. Perlindungan masyarakat terhadap tindak pidana,
   Aspek pokok yang pertama meliputi tujuan-tujuan:
   - mencegah, mengurangi atau mengendalikan tindak pidana,
   - memulihkan keseimbangan masyarakat yang pewujudannya sering dikemukakan dalam berbagai ungkapan, antara lain : menyelesaikan konflik, mendatangkan rasa aman, memperbaiki kerugian atau kerusakan yang timbul, menghilangkan noda-noda yang timbul, memperkuat nilai-nilai hidup dalam masyarakat.

b. Perlindungan masyarakat terhadap individu atau pelaku tindak pidana,
   Aspek pokok yang kedua bertujuan memperbaiki si pelaku yang sering dikemukakan dalam berbagai ungkapan seperti : melakukan rehabiitasi dan memasyarakatkan kembali si pelaku, membebaskan si pelaku, mempengaruhi tingkah laku si pelaku untuk tertib atau patuh pada hukum, melindungi si pelaku dari pengenaan sanksi atau pembalasan yang sewenang-wenang luar hukum Aspek pokok kedua ini dapat disebut individualisasi pidana.

---

[134] *ibid*

Mengingat persoalan penalisasi bukanlah hal yang mudah karena itu dalam penetapan kebijakannya perlu juga dilakukan perbandingan dan juga kjian terhadap rancangan perundang-undangan

a) Perbandingan dengan Negara Lain

Australia menggunakan ancaman pidana tunggal yakni pidana penjara untuk kejahatan *cyber crime.* Lamanya tergantung dari tindak pidananya dan beragam mulai dari 2 (dua) hingga 10 (sepuluh) tahun. Dapat dikemukakan pidana yang diterapkan dalam *Cybercrime Acts 2001 An Act to amend the law relating to computer offences, and for other purposes:*

- ✓ *Division 477—Serious computer offences*
  - *477.1* Unauthorised *access, modification or impairment with intent to commit a serious offence*

  Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara minimal 5 (lima) tahun.
  - *477.2 Unauthorised modification of data to cause impairment*

  Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara 10 (sepuluh) tahun.
  - *477.3 Unauthorised impairment of electronic communication*

  Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara 10 (sepuluh) tahun.

- ✓ *Division 478—Other computer offences*
  - *478.1 Unauthorised access to, or modification of, restricted data*

Dari tujuan penjatuhan pidana lahirlah teori-teori sebagai dasar pembenaran yang secara tradisional dikenal tiga golongan utama yaitu:

a. Teori Absolut atau teori pembalasan *(retributive/vergeldings theorien)*
   Menurut teori ini pidana dijatuhkan semata-mata karena orang telah melakukan suatu kejahatan atau tindak pidana *(quia peccatum est)*.[135]
b. Teori Relatif atau teori tujuan *(utilitarian/doeltheorien)*
   Menurut teori ini memidana bukanlah untuk memuaskan tuntutan absolut dari keadilan. Pidana bukanlah sekedar untuk melakukan pembalasan kepada orang yang melakukan tindak pidana, tetapi mempunyai tujuan-tujuan tertentu yang sangat bermanfaat. Karena itu teori ini sering disebut teori tujuan. Pidana dijatuhkan bukan *quia peccatum est* (karena orang membuat kejahatan), melainkan *ne peccetur* (supaya orang jangan melakukan kejahatan).

Ruslan Saleh dalam bukunya "*Suatu Reorientasi dalam hukum pidana*", mengemukakan bahwa pada hakekatnya ada dua poros yang menentukan garis-garis hukum pidana, yaitu:[136]

- Segi prevensi, yaitu bahwa hukum pidana adalah hukum sanksi, suatu upaya untuk dapat mempertahankan kelestarian hidup bersama dengan melakukan pencegahan kejahatan.
- Segi pembalasan, yaitu bahwa hukum pidana sekaligus pula penentuan hukum, merupakan koreksi dari dan reaksi atas sesuatu yang bersifat melawan hokum

---

[135] Muladi dan Barda Nawawi Arief, ***Teori-teori Kebijakan Hukum Pidana, Op cit***, hal. 10.
[136] *Ibid*, hal. 22.

Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara 2 (dua) tahun.

- *478.2 Unauthorised impairment of data held on a computer disk etc.*

  Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara 2 (dua) tahun.

- *478.3 Possession or control of data with intent to commit a computer offence*

  Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara 3 (tiga) tahun.

- *478.4 Producing, supplying or obtaining data with intent to commit a computer offence*

  Ancaman hukuman untuk kejahatan-kejahatan dalam *Section* ini adalah pidana penjara 3 (tiga) tahun.

b) Dalam Rancangan Perundang-Undangan

1) RUU KUHP 2000

Rancangan KUHP telah merumuskan tujuan dan pedoman pemidanaan. Menurut Barda Nawawi Arief perumusan ini bertolak dari pokok-pokok pikiran :[137]

- mengenai pedoman pemidanaan konsep memuat beberapa pedoman pemidanaan, yaitu:
  - yang bersifat umum, untuk memberikan pengarahan kepada hakim mengenai hal-hal apa yang sepatutnya

[137] Barda Nawawi Arief, ***Bunga Rampai Kebijakan Hukum Pidana, Op cit***, hal. 152-153.

dipertimbangkan dalam menjatuhkan pidana ;

- yang bersifat khusus, untuk memberikan pengarahan pada hakim dalam memilih atau menjatuhkan jenis-jenis pidana tertentu;

➢ pedoman bagi hakim dalam menerapkan sistem perumusan ancaman pidana yang digunakan dalam perumusan delik.[138]

Pasal 50 Rancangan KUHP 1999-2000 ditetapkan masalah Tujuan pemidanaan, yaitu:

(1) Pemidanaan bertujuan:
   a. mencegah dilakukannya tindak pidana dengan menegakkan norma hukum demi pengayoman masyarakat;
   b. memasyarakatkan terpidana dengan mengadakan pembinaan sehingga menjadi orang yang baik dan berguna ;
   c. menyelesaikan konflik yang ditimbulkan oleh tindak pidana, memulihkan keseimbangan, dan mendatangkan rasa damai dalam masyarakat ; dan
   d. membebaskan rasa bersalah pada terpidana.

(2) Pemidanaan tidak dimaksudkan untuk menderitakan dan merendahkan martabat manusia.

Jenis Pidana dalam Rancangan KUHP terdapat pada Pasal 60 yaitu;

(1) Pidana pokok terdiri dari:
   a. pidana penjara
   b. pidana tutupan
   c. pidana pengawasan
   d. pidana denda
   e. pidana kerja sosial

[138] *Ibid*, hal. 154.

(2) Urutan Pidana sebagaimana ayat (1) menentukan berat ringannya pidana

Pasal 61 menyatakan bahwa pidana mati merupakan pidana yang bersifat khusus dan selalu diancam secara alternatif.

Pasal 62 terdapat jenis pidana lainnya yaitu Pidana Tambahan yang terdiri atas:

a. Pencabutan hak-hak tertentu
b. Perampasan barang tertentu dan atau tagihan
c. Pengumuman putusan hakim
d. Pembayaran ganti kerugian
e. Pemenuhan kewajiban adat

Selanjutnya pada Penjelasan Pasal 60 dinyatakan bahwa:

"Ketentuan dalam Pasal 60 memuat jenis-jenis pidana yang dapat dijatuhkan oleh hakim. Ancaman pidana terhadap tindak pidana yang dirumuskan dalam Buku kedua hanya meliputi jenis pidana penjara, pidana denda dan atau pidana mati. Pidana tutupan dan pidana pengawasan pada dasarnya merupakan suatu cara pelaksanaan pidana sebagai alternatif dari pidana penjara. Sedangkan pidana kerja sosial merupakan jenis pidana baru yang di perlbagai negara sudah dilaksanakan secara luas. Pencantuman jenis pidana ini merupakan konsekuensi diterimanya hukum pidana yang bersifat *"Daad daderstrafrecht"* yang sejauh mungkin berusaha untuk mengembangkan alternatif pidana kemerdekaaan. Melalui penjatuhan jenis pidana ini terpidana dapat dibebaskan dari rasa bersalah dan masyarakat dapat berperan secara aktif untuk memasyarakatkan terpidana dengan melalui hal-hal yang bermanfaat".

Beberapa tindak pidana di internet yang bisa dimasukkan dalam RUU KUHP Buku Kedua dan ancaman hukumannya adalah:

- Menyadap pembicaraan di ruangan tertutup dengan alat Bantu teknis ancamannya paling lama 1 (satu) tahun atau denda paling banyak kategori III (Pasal 263),
- Memasang alat Bantu teknis untuk tujuan mendengar/merekam pembicaraan; ancamannya paling lama 1 (satu) tahun atau denda paling banyak kategori III (Pasal 264),
- Merekam (memiliki/menyiarkan) gambar dengan alat Bantu teknis di ruangan tidak untuk umum; ancamannya paling lama 1 (satu) tahun atau denda paling banyak kategori III (Pasal 266),
- Merusak/membuat tidak dapat dipakai bangunan untuk sarana/ prasarana pelayaran umum (antara lain: bangunan sarana telekomunikasi/komunikasi lewat satelit/komunikasi jarak jauh); ancamannya paling lama 5 (lima) tahun atau denda paling banyak kategori IV (Pasal 546,
- Pencucian uang (money laundering) -Pasal 641; ancaman hukumannya pidana penjara paling lama 20 (dua puluh) tahun dan paling singkat 5 (lima) tahun dan denda paling banyak Kategori VI; dan Pasal 642 ancaman hukumannya paling lama 10 (sepuluh) tahun dan denda paling banyak Kategori V

Dengan demikian untuk tindak pidana yang dijatuhkan terhadap *cybercrime* pidana yang dapat dijatuhkan adalah seperti yang dicantumkan dalam Buku Kesatu Rancangan KUHP. Beberapa kejahatan-kejahatan *cyber* pada dasarnya merupakan kejahatan konvensional yang sudah tercantum dalam konsep, seperti diterangkan sebelumnya, kecuali untuk beberapa kejahatan khusus yang dirumuskan dalam undang-undang khusus diluar KUHP maka

ancaman pidananya sesuai dengan undang-undnag khusus tersebut. Namun mengingat tradisi hukum di Indonesia yang mengkodifikasi peraturan, maka lebih baik bila pidana yang dijatuhkan dalam undang-undang khusus tersebut juga mengacu kepada konsep yang mengatur secara umum, kecuali memang dibutuhkan penjatuhan pidana yang khusus mengingat kekhususan tindak pidananya

2) RUU Informasi dan Transaksi Elektronik

Ketentuan pidana yang terdapat dalam Rancangan Undang-undang ini terdapat pada Pasal 48 sampai dengan Pasal 52. Rumusannya adalah sebagai berikut:

- Pasal 48
  Barangsiapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 29 ayat (1), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp 1.000.000.000,- (satu milyar rupiah).

- Pasal 49
  Barangsiapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 24, Pasal 28 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) bulan dan atau denda paling banyak Rp 100.000.000,- (seratus juta rupiah).

- Pasal 50
  (1) Barangsiapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 26 ayat (2), dipidana dengan pidana penjara paling lama 6 (enam) bulan dan atau denda paling banyak Rp 100.000.000,- (seratus juta rupiah)

(2) Tindak pidana sebagaimana dimaksud dalam ayat (1) hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana.

- Pasal 51
  Barangsiapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 29 ayat (2), Pasal 29 ayat (3), Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 32 ayat (2), Pasal 32 ayat (3), Pasal 32 ayat (4), Pasal 35 ayat (2), atau Pasal 36, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp 2.000.000.000,- (dua milyar rupiah).

- Pasal 52
  Barangsiapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 33 ayat (1), Pasal 33 ayat (2), Pasal 34, atau Pasal 36, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp 2.000.000.000,- (dua milyar rupiah).

Perumusan jenis pidana pada RUU ITE ini belum mengacu sepenuhnya pada konsep. Jenis pidan yang dijatuhkan yaitu pidana penjara dan pidana denda. Lamanya pidana *(strafmaat)* berkisar antara 6 (enam) bulan hingga 10 (sepuluh) tahun. Sedangkan untuk pidana denda rumusannya tidak mengacu pada konsep. Ada penjatuhan denda dengan sistem maksimum khusus, dan ada penjatutahan dengan sistem minimal khusus dan maksimal khusus. Denda tertinggi adalah Rp 2.000.000.000,- (dua milyar rupiah)

3. Jurisdiksi

Jurisdiksi menjadi hal yang juga penting dan krusial dalam penanganan *cybercrime* (kejahatan internet). Tidak terbatasnya ruang dan waktu menjadikan setiap negara seolah-olah memiliki kewenangan yang sama dalam penanganan kejahatan di dunia maya. Meskipun tidak mudah untuk mengungkapkan kejahatan di dunia maya, namun dibutuhkan keberanian dari aparat penegak hukum untuk melakukan penyelidikan dan penyidikan.

Jurisdiksi menyangkut kewenangan dari pengadilan untuk mengadili. Dalam konteks hukum internasional terdapat beberapa prinsip yang digunakan untuk menegaskan siapa yang mempunyai kewenangan untuk mengadili. Beberapa prinsip yang diterapkan antara lain: prinsip teritorial, personalitas, nasionalitas dan universalitas. Tiap-tiap prinsip memiliki karakter yang berbeda antara satu dengan yang lain. Prinsip teritorial mendasarkan pada wilayah dimana tindak pidana itu terjadi, bisa juga dari tempat munculnya akibat tindak pidana. Pada prinsip personalitas menekankan pada kewarganegaraan dari si pelaku. Misalnya jika pelaku adalah warga negara Indonesia, maka si pelaku bisa disidangkan di Pengadilan Indonesia. Pada prinsip nasionalitas yang ditekankan adalah kepentingan dari negara tempat terjadinya tinya tindak pidana. Prinsip terakhir yaitu prinsip universal yang lebih menekankan pada jenis kejahatan

internasional. Setiap negara yang berkepentingan bisa menerapkan dimana saja, kapan saja, dan bagi siapa saja sepanjang kejahatan tersebut tergolong sebagai kejahatan internasional.

Menurut Barda Nawawi Arief, problem jurisdiksi yang menonjol adalah masalah jurisdiksi judisial (kewenangan mengadili atau menerapkan hukum) dan jurisdiksi eksekutif (kewenangan melaksanakan putusan) daripada masalah jurisdiksi legislatif (kewenangan pembuatan hukum) Dikatakan demikian karena masalah jurisdiksi judisial/adjudikasi dan jurisdiksi eksekutif sangat terkait dengan kedaulatan wilayah dan kedaulatan hukum masing-masing Negara.[139]

Menurut Hikmahanto Juwono dalam konteks hukum internasional, terdapat beberapa prinsip yang digunakan untuk menegaskan siapa yang memiliki kewenangan untuk mengadili. Dikatakannya : [140]

> Ada beberapa prinsip yang diterapkan, antara lain teritorial, personalitas, nasionalitas, dan universal. Masing-masing prinsip memiliki karakter yang berbeda satu sama lain. Misalkan, prinsip teritorial yang mendasarkan pada wilayah di mana tindak pidana itu terjadi. Di samping itu, juga bisa juga dilihat dari munculnya akibat. Kemudian, prinsip personalitas yang lebih menekankan pada kewarganegaan dari si pelaku. Jika pelaku tindak pidana adalah warga negara Indonesia, maka yang bersangkutan bisa disidangkan di pengadilan Indonesia. Di samping prinsip personalitas, juga dikenal prinsip nasionalitas yang lebih menekankan pada kepentingan dari negara tempat di mana terjadinya tindak pidana. Prinsip terakhir yang dikenal dalam hukum

---

[139] Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana, Op cit,* hal. 280.
[140] http://www.Hukumonline.com: "Jurisdiksi", 10 Januari 2004.

internasional adalah prinsip universal yang lebih menekankan pada jenis kejahatan internasional. Setiap negara yang berkepentingan bisa menerapkan di mana saja, kapan saja, dan bagi siapa saja sepanjang kejahatan tersebut tergolong sebagai kejahatan internasional.

Dalam *Convention on Cybercrime,* Budapest 2001 pada *Section 3, Article 22* diatur masalah jurisdiksi, dinyatakan:[141]

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Article 2 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 its national, 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 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*

---

[141] Council of Europe, *European Treaty Series No. 185*, Budapest 23.IX.2001, page 13

Barda Nawawi menerjemahkannya sebagai berikut:[142]

1. Tiap Pihak (negara) akan mengambil langkah-langkah legislatif dan langkah-langkah lain yang dipelukan untuk menetapkan jurisdiksi terhadap setiap tindak pidana yang ditetapkan sesuai dengan Pasal 2-11 Konvensi ini, apabila tindak pidana itu dilakukan:
   a. di dalam wilayah teritorialnya; atau
   b. di atas kapal yang mengibarkan bendera negara ybs; atau
   c. di atas pesawat yang terdaftar menurut hukum negara yang bersangkutan; atau
   d. oleh seseorang dari warga negaranya, apabila tindak pidana itu dapat dipidana menurut hukum pidana di tempat tindak pidana itu dilakukan atauapabila tindak pidana itu dilakukan di luar jurisdiksi teritorial setiap negara
2. Tiap negara berhak untuk tidak menerapkan atau hanya menerapkan aturan jurisdiksi sebagaimana disebut dalam dalam ayat (1)b-ayat (1)d Pasal ini dalam kasus-kasus atau kondisi-kondisi tertentu.
3. Tiap Pihak (negara) akan mengambil langkah-langkah yang diperlukan untuk menetapkan jurisdiksi terhadap tindak pidana yang ditunjuk dalam Pasal 24 ayat (1) Konvensi ini dalam hal tersangka berada di wilayahnya dan negara itu tidak mengekstradisi tersangka itu ke negara lain (semata-mata berdasar alasan kewarganegaraan tersangka), setelah adanya permintaan ekstradisi
4. Konvensi ini tidakmeniadakan jurisdiksi kriminal yang dilaksanakan sesuai dengan hukum domestik (hukum negara yang bersangkutan);
5. Apabila lebih dari satu pihak (negara) menyatakan berhak atas jurisdiksi tindak pidana dalam Konvensi ini, maka para Pihak yang terlibat akan melakukan konsultasi untuk menetapkan jurisdiksi yang paling tepat untuk penuntutan

---

[142] Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana, Op cit*, hal 280-281

Terhadap ketentuan di atas konvensi memberikan penjelasan antara lain sebagai berikut:[143]

1. Ayat (1) sub a di atas didasarkan pada asas teritorialitas. Jurisdiksi teritorial ini dapat berlaku, baik apabila pelaku/penyerang komputer dan korbannya berada di wilayahnya maupun apabila komputer yang diserang berada di wilayahnya, tetapi *si penyerang tidak berada di wilayahnya*. Ayat (1) sub b dan sub c didasarkan pada perluasan asas teritorialitas yang telah diimplementasikan di banyak negara, dan ayat (1) sub d didasarkan pada asas nasionalitas.
2. Ayat (2) membolehkan negara untuk mengajukan keberatan/ persyaratan (reservasi) terhadap ayat (1) sub b, sub c dan sub d, tetapi tidak untuk ayat (1) sub a atau ayat (3) diperlukan untuk menjamin negara yang menolak ekstradisi warga negaranya mempunyai kemampuan hukum hukum untuk melakukan investigasi dan proses menurut hukumnya sendiri.
3. Jurisdiksi dalam ayat (1) tidak bersifat eksekutif. Oleh karena itu, ayat (4) membolehkan para pihak sesuai dengan hukum nasionalnya, untuk menetapkan juga tipe-tipe jurisdiksi yang lain.
4. Konsultasi dalam ayat (5) tidak bersifat absolut, tetapi apabila dipandang tepat. Misalnya suatu negara bisa memandang tidak perlu melakukan konsultasi apabila sudah diketahui bahwa negara lain itu tidak berencana untuk melakukan tindakan atau apabila konsultasi itu dipandang akan mengganggu proses penyelidikan

Rancangan Undang-undang tentang Informasi Elektronik dan Transaksi Elektronik juga mengatur masalah jurisdiksi. Hal ini dapat dilihat dari Pasal 45 dan Pasal 46:

---

[143] *Ibid*, hal 252-253.

- Pasal 45:

  Undang-undang ini berlaku di seluruh wilayah Negara Kesatuan Republik Indonesia dan untuk setiap orang di luar Indonesia yang melakukan tindak pidana sebagaimana diatur dalam undang-undang ini yang akibatnya dirasakan di Indonesia.

- Pasal 46:

  Pengadilan di Indonesia berwenang mengadili setiap tindak pidana di bidang teknologi informasi yang dilakukan oleh setiap orang, baik di Indonesia maupun di luar Indonesia yang akibatnya dirasakan di Indonesia.

Barda Nawawi Arief memberikan catatan tentang rumusan kedua pasal di atas, karena pada prinsipnya mengatur hal yang sama. Oleh karena itu, sebenarnya cukup diatur dalam satu pasal. Hal yang patut dicatatat:[144]

a. Masalah jurisdiksi dalam arti ruang/wilayah berlakunya hukum pidana menurut tempat, sebenarnya sudah diatur secara umum dalam KUHP, yaitu didasarkan pada asas teritorial, asas personal (nasional aktif), asas perlindungan (nasional pasif) dan asas universal. Jadi undang-undang khusus di luar KUHP tidak perlu membuat aturan tersendiri, kecuali untuk mengatur hal khusus yang belum diatur KUHP.
b. Menurut kedua pasal di atas, undang-undang berlaku bagi setiap orang yang melakukan tindak pidana:
   1) di seluruh wilayah Indonesia dan
   2) di luar Indonesia yang akibatnya dirasakan di Indonesia

   Ketentuan b 1 jelas memuat asas teritorialitas dan ketentuan b 2 mengandung asas ekstra teritorial, namun sebenarnya juga juga mengandung asas teritorialitas, karena *"akibat yang dirasakan di Indonesia"* itu pada hakikatnya merupakan tindak pidana yang terjadi di Indonesia juga (misal terjadi kerusakan data/program komputer, terganggunya sistem/fungsi/jaringan komputer atau media elektronik lainnya). Kalau prinsip yang dianut hanya asas

[144] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana, Op cit*, hal. 264.

teritorialitas, sebenarnya tidak perlu dirumuskan karena sudah diatur dalam KUHP (Pasal 2).

Selanjutnya Barda Nawawi Arief menyatakan pendapatnya bahwa lebih aman dan lebih luas jangkauannya apabila rancangan undang-undang ini menegaskan berlakunya asas-asas ruang berlakunya hukum pidana menurut KUHP atau nenurut Pasal 22 Konvensi Cyber Crime di Budapest dengan menambah/memperluas hal-hal yang belum ditegaskan dalam KUHP. Misal dalam KUHP, berlakunya asas personal/nasional aktif dan asas universal hanya untuk delik-delik tertentu, oleh karena itu dapat diperluas juga untuk tindak pidan dalam rancanagan undang-undang ini. Perluasan asas universal ini dimaksudkan untuk melindungi jaringan komunikasi/informasi yang saat ini telah menjadi kepentingan internasional/global. Jadi sebenarnya asas universal ini mengandung di dalamnya asas ubikuitas *(omnipresence;* ada dimana-mana). Perumusan RUU dalam b 2 di atas pun terkesan mengandung asas ubikuitas.[145]

Masalah jurisdiksi berkaitan dengan kecakapan dari suatu forum tertentu untuk mengadili kasus *(adjudicative jurisdiction).* Yurisdiksi dalam *cyberspace* dapat menggunakan teori:[146]

---

[145] *Ibid.* hal. 265-265

[146] Edmon Makarim, *Kompilasi Hukum Telematika, Op cit,* hal 305; Teori ini juga dikemukakan oleh Darel Menthe. lihat Bab II tulisan ini.

a) *The theory of uploader and downloader. Uploader* adalah pemberi informasi dan downloader adalah penerima transaksi elektronik.
b) *The law of the server.*Yurisdiksi ditentukan dengan menggunakan atau memperlakukan*server* dimana *webpages* secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik.
c) *The theory of international spaces,* ada usulan bahwa internet dijadikan ruang tersendiri, menjadi ruang ke empat setelah air, darat, dan udara.

Pengaturan mengenai masalah jurisdiksi merupakan hal penting, dan dalam pembentukan undang-undang khusus mengenai *cybercrime* perlu dipikirkan bentuk jurisdiksi yang mampu menjangkau kejahatan di dunia siber mengingat kejahatan ini punya karakter yang khas dan sifatnya lintas negara (*transborder*). Dengan demikian penerapan asas universal (*asas ubikuitas*) dapat digunakan disamping juga diperlukan kerjasama dengan negara-negara lain.

BAB IV

P E N U T U P

A. KESIMPULAN

1. Pengaturan tentang *cybercrime* belum tercantum secara jelas dan terpadu dalam hukum positif di Indonesia, baik dalam Kitab Undang Undang Hukum Pidana (KUHP), maupun dalam perundang-undangan di luar KUHP. Akan tetapi, terdapat ketentuan dalam KUHP dan dalam perundang-undangan di luar KUHP yang dapat diterapkan terhadap *cybercrime.*

   Penerapan ketentuan hukum positif terhadap *cybercrime* tidak diperbolehkan dilakukan dengan analogi, tetapi dapat dilakukan dengan menggunakan metode penafsiran *ekstensif.*

   Perundang-undangan di luar KUHP yang di dalamnya terdapat ketentuan untuk dapat diterapkan terhadap *cybercrime* tersebut antar lain :

a. Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

b. Undang Undang Nomor 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak sehat.

c. Undang Undang Nomor 32 Tahun 2002 tentang Penyiaran.

d. Undang Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.

e. Undang Undang Nomor 20 Tahun 2001 tentang Perubahan Atas UU No 31 Tahun 1999 tentang Tindak Pidana Korupsi.

f. Undang Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang.

2. Kebijakan hukum terhadap masalah *cybercrime* di masa yang akan datang, seharusnya memperhatikan hal-hal sebagai berikut :

a. Pengaturan mengenai *cybercrime* sebaiknya diwujudjan dalam sebuah "undang undang payung", Hal tersebut disebabkan untuk mencegah timbulnya perundang-undangan dalam jumlah besar yang mengatur tentang *cybercrime*, yang berpotensi saling tumpah tindih dalam pengaturan terhadap *cybercrime*. Di samping itu, dengan adanya *umbrella act*, dapat dihindari *over-criminalization* dan *the*

crisis of overreach of the criminal law yang dapat menimbulkan kerancuan dalam usaha pengendalian kejahatan.

b. Dalam hal perbuatan dan sanksi pidana yang diancamkan, maka kriminalisasi dari perbuatan-perbuatan tertentu seharusnya sesuai dengan aspek-aspek tujuan pemidanaan dan sesuai dengan UUD 1945 dan TAP MPR yang mengatur atau melindungi HAM. Khusus mengenai sanksi pidana, seharusnya dirumuskan dalam bentuk yang cermat, jelas dalam menentukan berat ringannya sanksi, serta disusun dalam suatu pola yang seragam.

c. Dalam membuat suatu kebijakan formulasi untuk tindak pidana diruang siber *(cyberspace),* perlu dilakukan harmonisai secara eksternal yakni dengan memperhatikan instrumen internasional dan melakukan harmonisasi internal yakni dengan memperhatikan hukum positif yang ada.

B. SARAN

1. Dalam menanggulangi kejahatan bedimensi baru dengan hukum positif yang ada tidak boleh mengenyampingkan asas dasar dari hukum pidana yaitu asas legalitas yang bertujuan untuk menjamin adanya kepastian hukum dan perlindungan bagi warga masyarakat agar undang-undang merupakan suatu *lex certa* (undang-undang yang dapat dipercaya).

   Upaya lain yang dapat ditempuh adalah dengan menggunakan interpretasi. Hal ini untuk mencegah agar tidak terjadi kekosongan hukum, dengan demikian kejahatan yang terus berkembang bisa dicegah dan juga memberikan perlindungan kepada masyarakat.

2. Penentuan kebijakan hukum pidana untuk menanggulangi *cybercrime* (kejahatan dunia maya) harus melalui pendekatan yang berorientasi pada nilai *(value oriented approach).*

   Diperlukan juga upaya pemerintah untuk membentuk peraturan-peraturan yang mampu mengantisipasi kejahatan siber *(cybercrime)* tersebut. Perumusan tindak pidana hendaknya dilakukan secara selektif yakni perbuatan mana bertentangan dengan nilai-nilai masyarakat, mendatangkan korban dan benar-benar merugikan.

Dalam masalah jurisdiksi diperlukan adanya antisipasi dalam rancangan maupun konsep yang mengatur mengenai kekhususan dari *cybercrime* sehingga masalah jurisdiksi bukanlah menjadi kendala dalam upaya penegakan hukum di *cyberspace.*

DAFTAR PUSTAKA

A. BUKU

Atmasasmita, Romli, *Kapita Selekta Kriminologi,* Aemico, Bandung, 1986

--------, *Pengantar Hukum Pidana Internasional,* Refika Aditama, Bandung, 2000

Bainbridge, David.I, *Komputer dan Hukum (Computer and The Law),* terjemahan oleh: Prasadi T. Susmaatmadja, Sinar Grafika, Jakarta, 1993.

Bemmelen, J.M van, *Hukum Pidana 1,* Terjemahan, Binacipta, Bandung, 1987

Black, Henry Campbell, *Black's Law Dictionary,* Seventh Edition, St. Paul Minnesota, West Publishing. Co, 1999

BPHN, *Lokakarya Penanggulangan Kejahatan Komputer,* Jakarta, 1991.

Box, Steven, *Power, Crime and Mystification,* London Tavistock Publications Ltd., 1983

Cross, Rupert, *Punishment, Prison and The Public,* Stevens & Sons, London, 1971

Departemen Pendidikan dan Kebudayaan, *Kamus Besar Bahasa Indonesia Cet. II,* Balai Pustaka, Jakarta, 1997.

Faisal, Sanapiah *Penelitian Kualitatif, Dasar-dasar dan Aplikasi,* YA3 Malang, 1980.

--------, *Format-format Penelitian Sosial,* Rajawali Press, Jakarta, 1995.

Fitzgerald, PJ, *Criminal Law and Punishment,* Clarendon Press, Oxford, 1962

Hamzah, Andi, *Hukum Pidana yang Berkaitan dengan Komputer,* Sinar Grafika, Jakarta, 1996.

--------, *Hukum Acara Pidana Indonesia,* Sinar Grafika, Jakarta, 1996

Jacobs, Francis. G, *Criminal Responsibility,* Weidenfield & Nicolson, London, 1971.

Makarim, Edmon, *et al, Kompilasi Hukum Telematika,* Raja Grafindo Persada, Jakarta, 2003

Mertokusumo, Sudikno, *Mengenal Hukum (Suatu Pengantar),* Liberty, Yogyakarta, 1996

Moeljatno, *Asas-asas Hukum Pidana* Cet. VI, ,Rineka Cipta, Jakarta, 2000

Moleong, Lexy J, *Metode Penelitian Kualitatif,* PT. Remaja Rosdakarya Bandung, 1998.

Muladi, *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia,* Habibie Center, Jakarta 2002

--------, *Kapita Selekta Hukum Pidana,* Badan Penerbit UNDIP, Semarang, 1995

Muladi & Barda Nawawi Arief, *Teori-Teori dan Kebijakan Pidana,* Alumni, Bandung, 1998.

Nawawi Arief, Barda, *Perbandingan Hukum Pidana,* Rajawali Pers, Jakarta, 1990.

--------,*Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* Citra Aditya Bakti, Bandung, 1998.

--------, *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan,* Citra Aditya Bakti, Bandung, 2001

--------, *Bunga Rampai Kebijakan Hukum Pidana,* Citra Aditya Bakti, Bandung, 2002.

--------, *Sari Kuliah Perbandingan Hukum Pidana,* Raja Grafindo Persada, Jakarta, 2002

--------, *Kapita Selekta Hukum Pidana,* Citra Aditya Bakti, Bandung, 2003

Nitibaskara, Ronny, *Ketika Kejahatan Berdaulat, Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi,* Peradaban, Jakarta, 2001

Putra Jaya, Nyoman Serikat, *Kapita Selekta Hukum Pidana,* Badan Penerbit UNDIP, Semarang, 2001

Rahardo Stajipto, *Ilmu Hukum,* Citra Aditya Bakti, Bandung, 2000

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

Saifullah, Tien. S, *Cyberlaw Suatu Pengantar: Yurisdiksi Penegakan Hukum dalam Kegiatan Cyberspace,* ELIPS II, Jakarta, 2002

Saleh, Roeslan, *Beberapa Asas-Asas Hukum Pidana dalam Perspektif,* Aksara Baru, Jakarta, 1981.

---------, *Perbuatan Pidana dan Pertanggungjawaban Pidana,* Aksara Baru, Jakarta, 1983

Slouka, Mark, *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan,* Mizan, Bandung, 1999

Sitompul, Asril, *Hukum Internet, Pengenalan Mengenai Masalah Hukum di Cyberspace,* Citra Aditya Bakti, bandung, 2001.

Soekanto, Soerjono *Pengantar Penelitian Hukum,* UI Press Jakarta, Cetakan III.

---------, et al, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat,* Raja Grafindo Persada, 1985

Soemitro, Ronny Hanitijo, *Metodologi Penelitian Hukum dan Juimetri,* Ghalia Indonesia, Jakarta, 1990

Sudarto, *Hukum Pidana dan Perkembangan Masyarakat,* Sinar Baru, Bandung, 1983.

---------, *Hukum dan Hukum Pidana,* Alumni, Bandung, 1986

---------, *Hukum Pidana I, Cet. II,* Yayasan Sudarto, Semarang, 1990

Suherman, Ade Maman, *Aspek Hukum dalam Ekonomi Global,* Ghalia Indonesia, Jakarta, 2002.

Sutopo, Heribertus, *Pengantar Penelitian Kualitatif, Dasar-Dasar Teoritis dan Praktis* Pusat Penelitian UNS Surakarta, 1998.

Tapper, Collin, *Computer Law,* Longman, London & New York, Second Edition,1982

Wisnubroto, Al, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* Penerbitan Universitas Atmajaya, Jogyakarta, 1999.

Zaleski, Jeff, *Spiritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia,* Mizan, Bandung, 1999.

B. ARTIKEL, MAKALAH

Chandra, Fransisca Haryani, *Internet: Information Superhighway,* Makalah pada Penataran Kualitas Dosen di Bidang Pengelolaan Data dan Penyusunan Presentasi melalui Media Komputer bagi Dosen PTS Kopertis Wil VI, Semarang

Harris, Freddy, et al, *Jurnal Hukukm dan Teknologi Universitas Indonesia Edisi I Tahun I,* UI, Jakarta, 2001

Ismael, Chaeruddin *Cybercrime: Kejahatan Maya, Kerugian Nyata,* dalam *Jurnal Studi Kepolisian Edisi 056,* PTIK, Jakarta, 2003

Latifulhayat, Atip *Cyberlaw dan Urgensinya bagi Indonesia,* Makalah pada Seminar tentang Cyber Law, Yayasan Cipta Bangsa, bandung, 29 Juli 2000.

Majalah Gatra, *Menjepit Ulah Pembobol Kartu Kreditt,No. 43 Tahun IX,* Jakarta, 11 September 2003

Mandala, E. Brata, et al, *Strategi dan Teknik Penyidikan terhadap Kejahatan Telematika,* Makalah pada Seminar Strategi Penanggulangan Kejahatan dalam Bidang Telematika, Universitas Semarang, 23 Juli 2002

Menthe, Darrel, *Jurisdiction in A Cyberspace: A Theory of International Spaces,* pada: http://www.mttlr.org/vlogfour/menthe.html

Muladi, *Kebijakan Kriminal Terhadap Cybercrime,* Majalah Media Hukum Volume I No.3 tgl 23-8-2003.

Kompas, Harian, *Virus WORM Slammer Serang Internet,* 13 Januari 2003

Nawawi Arief, Barda, *Upaya Non-Penal dalam Kebijakan Penanggulangan Kejahatan,* Bahan Seminar Kriminologi IV 16-18 Sepetember, 1991

---------, et.al, *Masalah-Masalah Hukum Edisi VIII,* FH UNDIP, Semarang, Januari, 2000

Purbo, Onno. W, *Perkembangan Teknologi Informasi dan Internet di Indonesia,* Kompas, 28 Juni 2000

Samadikun, Samaun, *Pengaruh Perpaduan Teknologi Komputer, Telekomunikasi dan Informasi,* Kompas, 28 Juni 2000.

Suningsih, *Pembuktian Kejahatan dalam bidang Telematika,* Seminar Nasional Strategi Penanggulangan Kejahatan dalam Bidang Telematika, Universitas Semarang, 2003

Supraptomo, Heru, *Kejahatan Komputer dan Siber serta Antisipasi Pengaturan dan Pencegahannya di Indonesia,* Seminar Cyberlaw: Antisipasi Hukum Terhadap Transasksi Bisnis melalui Cybernetwork, Medan, 30 Januari 2001

Sutrisman, *Penanggulangan Kejahatan Telematika dalam Perspektif Operator Telekomunikasi,* Seminar Nasional Strategi Penanggulangan Kejahatan dalam Bidang Telematika, Universitas Semarang, 2003

Suwarso, HM, *Fenomena Kejahatan dan Penanggulangan Kejahatan Telematika,* Seminar Nasional Strategi Penanggulangan Kejahatan dalam Bidang Telematika, Universitas Semarang, 2003

Winston, Kenny, *The Internet Issuesof Jurisdiction and Controversies Surrounding Domain Name,* Citra Adutya Bakti, Bandung, 2002

Zulfa, Eva Achjani, *Studi tentang Asas Legalitas* dalam *Perundang-undangan Indonesia* dalam Jurnal Penelitian FHUI Vol 2 No.2, Badan Penerbit FHUI, 2001

C. DATA ELEKTRONIK

http://www.inet.co.th/cyberclub/toom/Indonesia/internet/sekilas_internet.html

http://www.isoc.org/internet/history/letfthis.html

http://www.isoc.org/internet/history/vcerf.html

http://www.pbs.org/nerds/timeline: "Triumph of The Nerds" A History of Computer

http://www.mttlr.org/vlogfour/menthe.html

http://www.hukumonline.com/artikel_detail.asp?/id=5212

http://www.hukumonline.com: *"Hukum Posistif Masih Bisa Tangani Kasus Kejahatan Komputer"*,

http://www.hukumonline.com: *"Domain Name"*, 10 January 2004

http://www.pikiran-rakyat.com/prcetak/062001/15/08012.html

http://www.lysator.lie.se/etexts/hacker/

D. PERATURAN

Australia, *Cybercrime Act 2001, An Act to amend the law relating to computer offences, and for other purposes.*

Council of Europe, *Convention on Cybercrime*, Budapest, 2001

Council of Europe, *Additional Protocol To The Convention on Cybercrime Concerning The Criminalisation of Acts of A Racist and Xenophobic Nature Committed Through Computer System*, Starsbourg, 2003

Departemen Hukum & Perundang-Undangan, *Rancangan KUHP 1999-2000*

Hamzah, Andi, *KUHP Malaysia*, Ghalia Indonesia, Jakarta, 1987

Moeljatno, *KUHP*, Bumi Aksara, Jakarta, 1999

Rancangan Undang-Undang Informasi Elektronik dan Transaksi Elektronik

Singapura, *The Computer Misuse Act 1993*

Soesilo, R, *KUHP Serta Komentar-Komentarnya Lengkap Pasal DemiPasal*, Politea, Bandung, 1983

Soerodibroto, Soenarto, *KUHP dan KUHAP*, Raja Grafindo Persada, Jakarta, 1994

Undang-Undang Republik Indonesia Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

Undang-Undang Republik Indonesia Nomor 5 tahun 1999 tentang larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat

Undang-Undang Republik Indonesia Nomor 37 Tahun 1999 tentang Telekomunikasi

Undang-Undang Republik Indonesia Nomor Undang-Undang Nomor 15 Tahun 2001 tentang Tindak Pidana Pencucian Uang

Undang-Undang Republik Indonesia Nomor No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

Undang-Undang Republik Indonesia Nomor 32 tahun 2002 tentang Penyiaran

United Nations, *Tenth UN Congress on The Prevention of Crime and The Treatment of Offenders*, A/CONF.187.10