

PENGATURAN *CYBER CRIME* DALAM HUKUM PIDANA INDONESIA

TESIS



Oleh

ERDIANSYAH

No. Mahasiswa : 05912097
BKU : Hukum dan Sistem Peradilan Pidana
Program Studi : Ilmu Hukum

**PROGRAM PASCA SARJANA ILMU HUKUM
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2007**

HALAMAN PERSETUJUAN
PENGATURAN *CYBER CRIME* DALAM
HUKUM PIDANA INDONESIA

TESIS

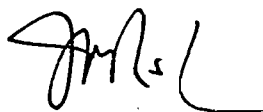
Oleh

ERDIANSYAH

No. Mahasiswa : 05912097
BKU : Hukum dan Sistem Peradilan Pidana
Program Studi : Ilmu Hukum

Telah Disetujui Oleh

Pembimbing I



Dr. Rusli Muhammad, S.H., M.H.

Tanggal 14 April 2007

Pembimbing II



Aroma Elmina Martha, S.H., M.H.

Tanggal 11 April 2007

Mengetahui Direktur
Program Pasca Sarjana Ilmu Hukum



Dr. Ridwan Khairandy, S.H., M.H.

Tanggal 19 April 2007

HALAMAN PANITIA PENGUJI

**PENGATURAN *CYBER CRIME* DALAM
HUKUM PIDANA INDONESIA**

TESIS

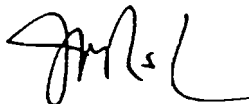
Oleh

ERDIANSYAH

No. Mahasiswa : 05912097
BKU : Hukum dan Sistem Peradilan Pidana
Program Studi : Ilmu Hukum

**Telah Dipertahankan di depan Dewan Penguji
Tanggal 2 Mei 2007 dan dinyatakan Lulus**

Tim Penguji
Ketua



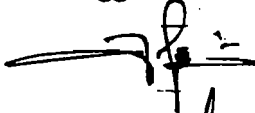
Dr. Rusli Muhammad, S.H., M.H.

Anggota I

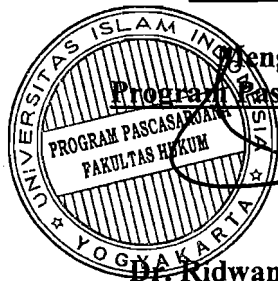


Aroma Elmina Martha, S.H., M.H.

Anggota II



Abdul Kholiq, S.H., M.H.



**Mengetahui Direktur
Program Pasca Sarjana Ilmu Hukum**

Dr. Ridwan Khairandy, S.H., M.H.

ABSTRAK

Kejahatan teknologi informasi atau dikenal dengan istilah *cyber crime* merupakan permasalahan yang harus ditangani secara serius. Hal ini dikarenakan dampak dari kejahatan ini sangat luas dan banyak merugikan perekonomian masyarakat. Apabila tidak ditanggulangi secara dini, maka kejahatan tersebut akan berkembang dan menuntut perhatian yang lebih luas dari aparat hukum dan pembuat UU, agar peluang kerugian yang ditimbulkan oleh *cyber crime* yang tidak semestinya, dibutuhkan perangkat peraturan dan perundangan yang membatasi sekaligus menghukum pelaku karena *cyber crime* apapun bentuknya tergolong tindakan kejahatan yang harus dihukum, pertanyaan yang sering diajukan adalah apakah perundangan Indonesia sudah mengatur masalah tersebut ? Berdasarkan pemahaman ini, maka penulisan tesis ini merumuskan dua rumusan masalah, yakni; *Pertama*, Bagaimanakah pengaturan *cyber crime* dalam hukum pidana positif Indonesia ?, *Kedua*, Bagaimanakah kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*)?

Dari hasil penelitian masalah ada dua hal pokok yang dapat disimpulkan. *Pertama*, *cyber crime* dalam hukum pidana positif Indonesia, apabila diperhatikan telah memiliki pengaturan. Pengaturan itu dapat dilihat pada ketentuan di dalam KUHP, Pasal 112 tentang pembocoran rahasia negara, Pasal 322 tentang membuka rahasia perusahaan, Pasal 282 tentang pornografi, Pasal 362 Pencurian, Pasal 369 tentang pemerasan dan pengancaman, Pasal 378 tentang penipuan, Pasal 372 tentang pengelapan, Pasal 382 bis tentang pelanggaran nama domain, Pasal 406 tentang perusakan, Pasal 506 tentang prostitusi (Pelanggaran Ketertiban Umum). Di samping KUHP beberapa ketentuan perundang-undang diluar KUHP seperti, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Namun demikian, pengaturan *cyber crime* dalam hukum pidana positif Indonesia ada beberapa dari *cyber crime* yang dapat dijerat dengan hukum pidana Indonesia, dan sebagian lagi tidak dikarenakan kejahatan ini relatif baru, oleh karena itu, timbul berbagai permasalahan dalam prakteknya. Misalnya masalah *hacking* karena tidak memenuhi unsur-unsur didalam KUHP, dengan demikian terjadi kekosongan hukum untuk menjangkau kejahatan ini apabila dikaitkan dengan unsur-unsur delik yang diatur dalam KUHP. Bertolak dari hal tersebut maka menurut hemat penulis perlu adanya kebijakan kriminalisasi atau pembaharuan hukum pidana (KUHP).

Kedua, kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*), dimana upaya untuk mengantisipasi atas *cyber crime* ini, telah dilakukan dalam hal ini dituangkan dalam Konsep Rancangan Undang-Undang KUHP yang baru (konsep 2005/2006): Buku I Pasal 158 pengertian "*Anak kunci*", Pasal 165 pengertian "*Barang*", Pasal 186 pengertian "*Masuk*", Pasal 174 pengertian "*Jaringan telepon*", Pasal 203 pengertian "*Pornografi*", Pasal 204 pengertian "*Ruang*", Pasal 207 pengertian "*Surat*." Buku II Pasal 300 tentang Menyadapan

pembicaraan, Pasal 301 Memasang alat bantu teknis, Pasal 373 Penggunaan dan perusakan informasi elektronik, Pasal 374 Pengubahan informasi yang masih dalam proses transaksi, Pasal 376 tanpa hak mengakses komputer dan sistem elektronik, Pasal 377 mengubah dan merusak atau menghilangkan informasi milik pemerintahan, Pasal 378 menggunakan dan mengakses tanpa hak, Pasal 379 Pornografi anak melalui komputer, Pasal 735-736 pencucian uang atau *Money Laundering*, dan juga kebijakan kriminalisasi *cyber crime* ini dengan Rancangan Undang-Undang RUU Informasi dan Transaksi Elektronik dan Tindak Pidana di Bidang Teknologi Informasi.

Saran Penulis, Pertama, segera disahkan Undang-undang yang berkaitan dengan *cyber law* umumnya dan *cyber crime* khususnya. *Kedua*, sebelum adanya aturan khusus tentang *cyber crime*, hakim, aparat penegak hukum lainya harus berani melakukan "*rechtsvinding*" (penemuan hukum). *Ketiga*, Dalam kebijakan kriminalisasi *cyber crime* tersebut perlu mempertimbangkan draft internasional yang telah ditandatangani di Budapest pada tanggal 23 November 2001, (*draft Conventional on Cyber Crime*) yang berkaitan dengan *cyber crime*, mengingat kejahatan ini merupakan "*global crime*" maka perlu adanya suatu asas yang memungkinkan menarik pelaku yang berada di luar wilayah Indonesia yang merugikan Indonesia, dikarenakan yurisdiksi kejahatan ini tidak jelas.

Kata Kunci: Pengaturan - *Cyber Crime* - Hukum Pidana Indonesia

KATA PENGANTAR

Bismillahirramanirrahim

Dengan menadahkan tangan, menundukkan kepala, seraya berdoa mengucapkan puji syukur ke hadirat Tuhan Yang Maha Kuasa, yang senantiasa melimpahkan rahmat dan karuniaNya kepada penulis, sehingga penulis dapat menyelesaikan tesis ini. Tema yang disajikan pada tesis ini adalah:

“Pengaturan Cyber Crime Dalam Hukum Pidana Indonesia”

Tesis ini disusun untuk melengkapi persyaratan dalam memperoleh gelar Magister Hukum pada Program Pasca Sarjana Ilmu Hukum Universitas Islam Yogyakarta.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Bapak Rektor Universitas Islam Yogyakarta.
2. Bapak ***Dr. H. Rusli Muhammad, S.H., M.H.***, Pembimbing I, yang telah memberikan masukan, membimbing, selama penulis mengikuti program dan penulisan tesis.
3. Ibu ***Aroma Elmina Martha, S.H., M.H.***, Pembimbing II, yang telah membimbing penulis dengan penuh kesabaran, kesungguhan dan ketulusan hati.
4. Bapak ***Dr. Ridwan Khairandy, S.H., M.H.***, selaku Direktur Program Pasca Sarjana Ilmu Hukum Universitas Islam Yogyakarta.

5. Ibu *Dekan Fakultas Hukum Universitas Lancang Kuning, Ibu Hj. Hasnati, S.H., M.H.*, yang telah memberikan kesempatan kepada penulis untuk mengikuti pendidikan Pasca Sarjana Ilmu Hukum di Universitas Islam Yogyakarta.
6. Kepada seluruh *Dosen dan Staf* Pasca Sarjana Ilmu Hukum Universitas Islam Yogyakarta.
7. Kepada *Alm. Ayanda M. Soleh, Ibunda Rosani, Mertua, serta saudara-saudaraku*, yang senantiasa mengiringi penulis dengan kasih sayang dan doa, semoga Allah senantiasa memberikan rahmatNya.
8. Kepada *Istriku Eldanis Gusni, S.Hut dan Anakku Vania Gita Salsabilla*, yang penuh pengertian terima kasih atas segalanya, semoga Allah membalas itu semua dengan setimpal.
9. Kepada *Rekan-rekan dan Dosen di Fakultas Hukum Universitas Lancang Kuning Pekanbaru*, serta semua pihak yang tidak mungkin penulis cantumkan satu persatu dalam tesis ini.

Penulis menyadari sepenuhnya bahwa dalam tesis ini masih banyak terdapat kekurangan, untuk itu berbagai saran dan kritik dari semua pihak merupakan masukan yang sangat berguna bagi penulis.

Akhirnya penulis berharap semoga tesis ini dapat berguna bagi semua pihak.

Yogyakarta, April 2007

Penulis

ERDIANSYAH

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PANITIA PENGUJI	iii
ABSTRAK	iv
KATA PENGANTAR	vi
DAFTAR ISI	viii
BAB I PENDAHULUAN	
A. Latar Belakang Masalah	1
B. Rumusan Masalah	9
C. Tujuan Penelitian	10
D. Kerangka Teoritik	10
E. Definisi Operasional	19
F. Metode Penelitian	20
BAB II TINJAUAN UMUM HUKUM PIDANA DI INDONESIA	
A. Pengertian Hukum Pidana	22
B. Asas Legalitas Dalam Konteks Hukum Pidana	26
C. Kebijakan Kriminalisasi dalam Upaya Penanggulangan Kejahatan	28
D. Batas-Batas Berlakunya Perundang-Undangan Hukum Pidana Menurut Waktu dan Tempat	36
E. Pertanggungjawaban Dalam Hukum Pidana	40

BAB III PERKEMBANGAN TEKNOLOGI, KEJAHATAN

DAN HUKUM PIDANA

A. Perkembangan Teknologi dan Kehidupan Manusia	42
B. Teknologi, Kejahatan dan Reaksi Sosial atas Kejahatan	56
C. Hukum Pidana dan Perkembangan Teknologi	65

BAB IV PENGATURAN *CYBER CRIME* DALAM HUKUM

PIDANA INDONESIA

A. Pengaturan <i>Cyber Crime</i> Dalam Hukum Pidana Positif Indonesia	72
B. Kebijakan Kriminalisasi <i>Cyber Crime</i> Dalam Konteks Hukum Pidana Yang Akan Datang (<i>Ius Constituendum</i>)	112

BAB V PENUTUP

A. Kesimpulan	134
B. Saran	136

DAFTAR PUSTAKA

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Proses pembangunan yang selama ini terus menerus dilakukan merupakan salah satu konsekuensi dari eksistensi Indonesia sebagai negara berkembang. Segala bentuk aktivitas pembangunan diharapkan dapat berjalan dalam koridor yang tepat, sehingga tujuan pembangunan yaitu tercapainya masyarakat yang adil dan makmur, material dan spritual dapat segera terwujud.

Proses pembangunan hampir dipastikan akan membawa dampak yang luas pada berbagai aspek kehidupan manusia, karena pembangunan merupakan perubahan terencana dan teratur yang antara lain mencakup aspek-aspek politik, ekonomi, demografi, psikologi, hukum, interlektual maupun teknologi.

Pembangunan di bidang teknologi dewasa ini peradaban manusia dihadirkan dengan adanya fenomena baru yang mampu mengubah hampir setiap aspek kehidupan manusia, yaitu perkembangan teknologi informasi. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat.

Teknologi informasi memegang peran yang penting, baik di masa kini maupun di masa yang akan datang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia.

Setidaknya ada 2 (dua) hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia.

“Menurut Agus Raharjo bahwa teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya. *Kedua*, adalah memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya”.¹

Kemajuan teknologi informasi di samping telah memberikan kemaslahatan terhadap masyarakat dan di sisi lain juga menimbulkan kekhawatiran karena adanya penggunaan yang menyimpang dari tujuan yang sebenarnya. Karena teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulaan zaman sampai sekarang dan masa yang akan datang dan bentuk-bentuk kejahatan yang adapun semakin hari semakin bervariasi.

Kecenderungannya terbukti, bahwa semakin maju dan modern kehidupan masyarakat, maka semakin maju dan modern pula jenis dan modus operandi kejahatan yang terjadi di tengah masyarakat. Kejahatan teknologi informasi atau dikenal dengan istilah *cyber crime* merupakan permasalahan yang harus ditangani secara serius.

Hal ini dikarenakan dampak dari kejahatan ini sangat luas dan banyak merugikan perekonomian masyarakat. Apabila tidak ditanggulangi secara dini, maka kejahatan tersebut akan berkembang dan dampaknya akan sangat fatal bagi kehidupan bermasyarakat.

¹ Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, ctk. Pertama, Citra Aditya Bakti, Bandung, 2002, hlm. 1.

Kendala utama dalam penyelidikan *cyber crime* antara lain *bonderless* baik korbannya maupun tersangkanya, sehingga perangkat hukum konvensional yang ada di Indonesia belum atau tidak dapat menjangkau secara efektif. Oleh karena itu, perlu diwujudkan hukum baru, di mana saat ini dikenal dengan istilah *Cyber Law*.

Di samping itu, untuk mencegah timbulnya *cyber crime* diperlukan juga peralatan *forensik computing* yang tepat guna untuk pembuktian kejahatannya dan hal yang tidak kalah pentingnya lagi perlu juga disiapkan penyidik Polri untuk dididik dan mampu menyidik *cyber crime* serta kerja sama dengan penegak hukum yang ada di luar negeri.

Menurut Mas Wigrantoro Roes Setiyadi bahwa, *cyber crime* secara umum terdiri dari dua kelompok, yaitu:

1. Kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantunya. Dalam kejahatan ini, terjadi peningkatan modus dan operandi dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan teknologi informasi. Dampak dari kejahatan biasa yang telah menggunakan teknologi informasi ternyata cukup serius, terutama bila dilihat dari jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pembobolan rekening, penipuan, pencemaran nama baik, pornografi, perjudian, terorisme, hingga pembelian barang menggunakan kartu kredit curian melalui media internet dapat menelan korban di wilayah hukum negara lain, suatu hal yang jarang terjadi dalam kejahatan konvensional.
2. Kejahatan yang muncul setelah adanya internet, di mana sistem komputer sebagai korbannya. Jenis kejahatan dalam kelompok ini makin bertambah seiring dengan kemajuan teknologi informasi itu sendiri. Salah satu contoh yang termasuk kejahatan kelompok kedua adalah perusakan situs internet, pengiriman virus atau program-program komputer yang tujuannya merusak sistem kerja komputer.²

² Mas Wigrantoro Roes Setiyadi, *Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, GIPI-Indonesia, 2003, hlm. 4.

Perbuatan-perbuatan *cyber crime* dalam beberapa kasus umumnya dilakukan oleh orang dalam (*insider*) atau mereka yang pernah bekerja pada suatu instansi yang mempunyai peralatan komputer, telekomunikasi, dan informasi baik berupa *hardware*, *software* maupun *brainware* dan rasa keingintahuan yang tinggi.

Beberapa contoh kasus *cyber crime* yang pernah terjadi di Indonesia antara lain :³

1. Pembobolan BRI cabang Brigjen Katamso Yogyakarta, 15 September 12 Desember 1982;
2. Pembobolan BNI New York, 31 Desember 1986;
3. Pembobolan BDN cabang Bintaro Jaya, 1988;
4. Pembobolan Bank Danamon Pusat, 1998;
5. Pembobolan Bank Danamon Glodok Plaza, 1990;
6. Pembobolan BRI cabang Jatinegara Timur, 1991;
7. Percobaan pembobolan *Union Bank of Switzerland* di London, 1988;
8. Pembajakan *Mapping Products* Milik *Loxtech, Ltd.* oleh *Thaimapguide.com*;
9. Kasus bobolnya sistem komputer di Mabes Polri pada tahun 1999. Ketika itu, apabila komputer diaktifkan maka yang muncul adalah gambar porno;
10. Kasus BCA, dimana lewat situs www.klikbca.com dirusak oleh seorang *hacker* dengan cara melahirkan lima nama situs "*plesetan*" yang mirip situs aslinya (*typosite*). Akibatnya, bila nasabah BCA menggunakan fasilitas internet tapi salah mengetik nama situsnya (www.klikbca.com) ia akan masuk ke situs tiruan. Si nasabah pun tak bisa bertransaksi,

³ <http://www.mediaindo.co.id/cetak/berita.asp/>, 12 Juli 2006, 10.00

sementara *Personal Identification Number* (PIN) miliknya terekam di situs gadungan tadi;

11. Data Mabes Polri selama tahun 2002 terdapat 23 kasus *cyber crime* di Indonesia, terdiri atas 15 kasus *cyber crime* yang menjadikan teknologi informasi sebagai sarana (misalnya *credit card fraud*, *stock exchange fraud*, *banking fraud*, *child pornography* dan *drug trafficking*) dan 8 kasus *cyber crime* yang menjadikan teknologi informasi sebagai sasaran (misalnya *Denial of Service Attack*, *defacing*, dan *cracking*),
12. Kasus Petrus Pangkur alias Bony Diobok-obok, membobol kartu kredit milik warga AS, yang terjadi pada hari Sabtu, tanggal 3 Maret 2003 pukul 00.30 di Warnet Naganet, jalan Pringgondani nomor 6 Condongcatur, Depok, Sleman, Yogyakarta, ia melakukan pembelian barang melalui internet. Barang-barang yang dibelinya tersebut seperti helm dan sarung tangan merk AGV dengan total harganya sebesar 4 juta. Petrus Pangkur ditangkap sesaat setelah mengambil barang kirimannya dari UPS di sebuah hotel di Yogyakarta.⁴
13. Kasus Deni Firmansyah, merusak jaringan IT KPU dan berhasil menempus *IP tnp.kpu.go.id* yang mengubah hasil perolehan suara dengan cara jumlah perolehan suara dikalikan 10 namun tidak berhasil, kasus ini terjadi di warnet di jalan Kaliurang, Yogyakarta pada hari Jumat dan Sabtu tanggal 16 dan 17 April 2004, kemudian tanggal 22 April 2004, Dani Firmansyah berhasil ditangkap oleh Satuan *Cyber Crime Distreskrimsus* Polda Metro Jaya,⁵
14. Kasus pembobolan situs resmi Presiden RI yang terjadi pada hari Minggu, tanggal 17 Maret 2007 pukul 05.30 Wib, situs resmi Presiden Susilo Bambang Yudhoyono (*www.presidensby.info*). dibobol *hacker*. Halaman utama situs yang dikelola juru bicara Kepresidenan Andi Mallarangeng itu berubah tampilannya menjadi surat tuntutan yang ditujukan kepada SBY. Pengirim surat mengatasnamakan *on behalf underground community dan beralamat di the word where the devils gather*. Komunitas tersebut mengeluarkan tiga tuntutan pertama meminta penurunan harga *bandwidth*, agar masyarakat bisa menikmati internet, kedua, meminta SBY mendukung dan melaksanakan IGOS (*Indonesia Go Open Source*) dan yang ketiga, Menuntut pemberantasan korupsi, kolusi, dan nepotisme (KKN), pornografi dan porno aksi).⁶ dan masih banyak lagi kasus-kasus lainnya.

⁴ Aroma Elmina Martha, "Diktat Hukum Pidana dan Perkembangan Teknologi Informasi", *Pasca Sarjana Ilmu Hukum UII*, Yogyakarta, 2006, hlm. 55.

⁵ <http://students.ukdw.ac.id/-22033149/dani.htm>, 20 Desember 2006. 21.30

⁶ Riau Pos, Senin, 19 Maret 2007, hlm.1.

Di Indonesia, lokasi dari para pelaku *cyber crime* tidak terkonsentrasi hanya pada pusat-pusat bisnis dan ekonomi nasional seperti Jakarta atau Surabaya saja misalnya, namun bahkan juga pada daerah-daerah yang dikenal sebagai pusat-pusat pendidikan seperti Bandung, Yogyakarta, dan Semarang.⁷

“Pakar telematika Roy Suryo bahkan mengatakan bahwa daerah dengan tingkat kejahatan *cyber* tertinggi di Indonesia adalah justru kota Yogyakarta. Sebagai gambaran, apabila di tahun 2002 terdapat sekitar 160 kasus *cyber crime*, maka 60 % dari total seluruh kejahatan tersebut berasal dari kota Yogyakarta.”⁸

Sebagai gambaran tingginya tingkat kejahatan internet dapat pula dilihat pada tabel hasil penelitian dari IFCC pada tahun 2001, *internet Fraud Report, January 1, 2001 – December 31, 2001. National White Collar Crime Center and Federal Bureau of Investigation* berikut ini:⁹

1. Enterprise Security – Survey by: Data Monitor Co. 2001

<i>Virus Attack</i>	70 %
<i>Unauthorized Access</i>	42 %
<i>Data/Stytem Corruption</i>	20 %
<i>Denial of Service Attack</i>	12 %
<i>Payment Fraud</i>	7 %
<i>Data Theft</i>	7 %
<i>Inability to Login</i>	5 %
<i>Others</i>	4 %

2. Persentasi pelaku kejahatan penipuan berdasarkan negara:

Negara	%
Amerika Serikat	87.6
Nigeria	2.7
Kanada	2.5
Romania	0.9
Inggris	0.9

⁷ Aroma Elmina Martha, *Op.cit*, hlm. 18.

⁸ http://www.Tempointeraktif.com/news/2003%5C6%5C24/1,1,25_id.html, Yogyakarta Pusat Kejahatan Informasi/, 25 Juni 2003. 15.00

⁹ Aroma Elmina Martha, *Op.cit*, hlm. 18.

kemajuan teknologi informasi mendorong semakin beragam bentuk *cyber crime* yang terjadi. Hasil survei AC Nielsen menunjukkan, Indonesia menempati posisi keenam terbesar di dunia atau keempat di Asia dalam *Cyber Crime*.¹⁰

Nandang Sutrisno mengutip dari Scoot Chaney menyatakan sebagai berikut :¹¹

“Bahwa kerugian ekonomis akibat dari *cyber crime* ini cukup besar. Laporan yang dilansir oleh *Computer Security Institute Survey* menunjukkan bahwa berdasarkan data dari FBI, jumlah kerugian akibat *cyber crime* pada tahun 1995 mencapai US \$ 2 Milyar. Hasil survey lain menunjukkan bahwa 98.5 % dari 82 responden menyatakan bahwa bisnis mereka telah menjadi korban *cyber crime* 43,3 % darinya mengaku menyatakan bahwa mereka telah menjadi korban lebih 25 kali”

Dengan melihat fenomena serta sejumlah pendapat di atas, tidak dapat dipungkiri bahwa *cyber crime* semakin menuntut perhatian yang lebih luas dari aparat hukum dan pembuat UU, agar peluang kerugian yang ditimbulkan oleh adanya pemanfaatan teknologi informasi yang tidak semestinya, dibutuhkan perangkat peraturan dan perundangan yang membatasi sekaligus menghukum penggunaan teknologi informasi untuk kejahatan, karena *cyber crime* apapun bentuknya tergolong tindakan kejahatan yang harus dihukum, pertanyaan yang sering diajukan adalah apakah perundangan Indonesia sudah mengatur masalah tersebut ?

Namun sampai hari ini belum ada perundangan yang mengatur masalah kriminalitas penggunaan teknologi informasi (*cyber crime*), oleh itu

¹⁰ Mas Wigrantoro R.S., “Sistem Hukum Indonesia Dalam Menghadapi Potensi Kriminalitas di Dunia Cyber”, disampaikan sebagai *Makalah dalam pelatihan Information Security, diselenggarakan oleh STT Telkom Bandung*, 4 April 2002, hlm. 4.

¹¹ Nandang Sutrisno, “Cyber Law: Problem dan Prospek Pengaturan Aktivitas Internet”. Artikel dalam *Jurnal Hukum UII* Yogyakarta, No. 16. hlm. 37.

jika terjadi tindakan kriminal di dunia *cyber* sulit bagi aparat penegak hukum untuk menghukum pelakunya.

Berdasarkan kenyataan tersebut diharapkan ada suatu ketentuan perundang-undangan, dalam hal ini hukum pidana, yang mampu menjangkau perbuatan tersebut. Penyusunan suatu perundang-undangan pidana untuk menanggulangi *cyber crime* tidaklah mudah mengingat terus berkembangnya teknologi informasi, untuk itu suatu kajian melalui kebijakan hukum menjadi relevan dan penting untuk dilakukan.

Pendapat ini diperkuat dari kenyataan bahwa banyak kasus kriminal yang berkaitan dengan dunia *cyber* tidak dapat diselesaikan oleh sistem peradilan dengan tuntas karena aparat menghadapi kesulitan dalam melakukan penyidikan dan mencari pasal-pasal hukum yang dapat digunakan sebagai landasan tuntutan di pengadilan.

Berdasarkan alasan-alasan di atas, maka menarik untuk diteliti pengaturan *cyber crime* dalam konteks hukum positif dan hukum yang akan datang (*ius constituendum*). Untuk maksud demikian penelitian merumuskannya dalam suatu judul penelitian Pengaturan *Cyber Crime* dalam Hukum Pidana Indonesia.

B. Rumusan Masalah

1. Bagaimanakah pengaturan *cyber crime* dalam hukum pidana positif Indonesia ?
2. Bagaimanakah kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*)?

C. Tujuan Penelitian

1. Untuk mengkaji dan mengetahui pengaturan *cyber crime* dalam hukum pidana positif Indonesia.
2. Untuk mengkaji dan mengetahui kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*).

D. Kerangka Teoritik

Hukum pidana yang berlaku di Indonesia sekarang ini ialah hukum pidana yang telah dikodifisir, yaitu sebagian tersebar dari aturan-aturannya telah disusun dalam Kitab Undang-undang (*wetboek*), yang dinamakan Kitab Undang-undang Hukum Pidana, menurut suatu sistem tertentu.¹²

Kitab Undang-undang hukum pidana agar dapat diterapkan secara tepat tidak cukup hanya mencari dan memberikan makna sekedar dari dalam pasal-pasal (*dogmatis*) dan secara politis atau teknis perundang-undangan, akan tetapi sesuatu ketentuan peraturan perundang-undangan hukum pidana itu harus diberikan makna menuju kepada arti kesesuaian dan/atau kemanfaatan dengan perasaan hukum dan keadilan sebagaimana terdapat di dalam asas-asas hukum pidana yang hidup didalam masyarakat.

Dan mengenai definisi hukum pidana ada beberapa rumusan yang dikemukakan oleh pakar hukum diantara lain :

W.L.G Lemaire, merumuskan bahwa:

“Hukum Pidana itu terdiri dari norma-norma yang berisi keharusan-keharusan dan larangan-larangan yang (oleh pembentuk undang-

¹² Moeljatno, *Asas-Asas Hukum Pidana*, ctk. Kelima, Rineka Cipta, Jakarta, 1993, hlm. 16

undang) telah dikaitkan dengan suatu sanksi berupa hukuman, yakni suatu penderitaan yang bersifat Khusus”.¹³

Dalam hubungan ini, rumusan tentang pengertian hukum pidana yang ditunjukan oleh van HATTUM barangkali lebih kontekstual dengan realitas sosial Indonesia. Beliau menyatakan:

“Hukum pidana adalah, suatu keseluruhan dari asas-asas dan peraturan-peraturan yang diikuti oleh negara atau suatu masyarakat hukum umum lainnya, dimana mereka sebagai pemelihara dari ketertiban hukum umum telah melarang dilakukannya tindakan-tindakan yang bersifat melanggar hukum dan telah mengaitkan pelanggaran terhadap peraturan-peraturannya dengan suatu penderitaan yang bersifat khusus berupa hukuman”.¹⁴

Dalam perspektif yang lain yakni tinjauan dari sudut institusi sosial yang memiliki kewenangan untuk merigandakan/membuat hukum pidana, **Simons** mengemukakan bahwa hukum pidana adalah : (a) seluruh perintah dan larangan yang diadakan oleh negara dan yang diancam dengan suatu pidana/nestapa bagi barang siapa yang tidak menaatinya. (b) seluruh aturan yang ditentukan oleh negara yang berisi syarat-syarat untuk menjalankan pidana tersebut¹⁵

Sedangkan menurut Menurut Moeljatno, Ia menyatakan bahwa Hukum Pidana adalah bagian dari keseluruhan hukum yang berlaku di suatu negara yang mengadakan dasar-dasar dan aturan-aturan untuk:

1. Menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan, yang dilarang, dengan disertai ancaman atau sanksi yang berupa pidana tertentu bagi barangsiapa melanggar larangan tersebut.

¹³ P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, ctk. Ketiga, Citra Aditya Bakti, Bandung, 1997, hlm. 2.

¹⁴ *Ibid*

¹⁵ Soeharto, *Hukum Pidana Materil (Unsur Objektif sebagai Dasar Dakwaan)*, ctk. Pertama, Sinar Grafika, Jakarta, 1993, hlm. 4.

2. Menentukan kapan dan dalam hal-hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan.
3. Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.¹⁶

Bagian dari hukum tersebut dibagi dalam dua jenis yaitu hukum publik dan hukum privat, dan hukum pidana digolongkan dalam golongan hukum publik, yaitu mengatur hubungan antara negara dan perseorangan atau mengatur kepentingan umum. Bila definisi tersebut diamati secara saksama, akan diperoleh suatu kesimpulan bahwa sesungguhnya yang dibahas dalam hukum pidana adalah 3 hal, yakni; (1) Perbuatan Pidana, (2) Pertanggungjawaban Pidana, (3) Sanksi Pidana

Di samping itu juga dapat ditemukan berbagai ketentuan yang tercakup dalam hukum pidana, secara sistematis sumber hukum pidana yang terdiri dari :¹⁷

1. Sumber Hukum Pidana Materiil yang terdiri dari :
 - a. Tertulis terdiri dari : (KUHP, Peraturan Pidana di luar KUHP, Yurisprudensi Hukum Pidana
 - b. Tidak Tertulis : Pidana Adat
2. Sumber Hukum Pidana Formil : KUHP, serta berbagai peraturan pelaksanaan yang berhubungan dengan hukum pidana formil (Hukum Acara Pidana).

¹⁶ Moeljatno, *Op.cit*, hlm.1.

¹⁷ Sumarni Prijohutomo, "Buku Ajar Hukum Pidana", *Fakultas Hukum Unilak*, Pekanbaru, 1999, hlm, 3.

Pada awal dibentuknya ketentuan hukum pidana, subyek hukum pidana adalah orang. Namun dalam perkembangannya, subjek hukum pidana tidak saja “*orang*” akan tetapi juga berbagai bentuk badan hukum, walaupun yang dipertanggungjawabkan adalah pengurusnya (*orang*). Karena tujuan diadakannya sanksi pidana hanya bermanfaat bagi orang. Dan tujuan pidana yang berkembang dari dahulu sampai kini telah menjurus ke arah yang lebih rasional.

Tujuan pidana yang paling tua adalah pembalasan (*revenge*) atau tujuan memuaskan pihak yang dendam baik masyarakat sendiri maupun pihak yang dirugikan/menjadi korban kejahatan. Hal ini bersifat *primitif*, tetapi kadang-kadang masih terasa pengaruhnya pada jaman modern ini. Tujuan pidana yang dianggap kuno ialah penghapusan dosa (*expiation*) atau retribusi (*retribution*) yaitu melepaskan pelanggar hukum dari perbuatan jahat atau menciptakan *balances* antara yang hak dan batil.

Tujuan yang berlaku sekarang adalah variasi-variasi dari bentuk-bentuk; penjeraan (*deterrent*), baik ditujukan kepada pelanggar hukum sendiri maupun kepada mereka yang mempunyai potensi menjadi penjahat; perlindungan kepada masyarakat dari perbuatan jahat; perbaikan (*reformasi*) kepada penjahat. Yang tersebut terakhir yang paling modern dan populer dewasa ini. Bukan saja bertujuan memperbaiki kondisi pemenjaraan tetapi yang mencari alternatif lain yang bukan bersifat pidana dalam membina pelanggar hukum.

Selanjutnya dalam hukum pidana Indonesia, asas legalitas diatur dengan jelas dalam KUHP yang berlaku sekarang (*Wetboek van Strafrecht*) maupun dalam Rancangan KUHP (selanjutnya disingkat RKUHP).

Pasal 1 ayat (1) KUHP yang menyatakan bahwa;

“Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada, sebelum perbuatan dilakukan. Bunyi Pasal 1 Ayat (1) KUHP ini, secara rinci, berisi dua hal penting, yaitu: (i) suatu tindak pidana harus dirumuskan terlebih dahulu dalam peraturan perundang-undangan; (ii) peraturan perundang-undangan harus ada sebelum terjadinya tindak pidana (tidak berlaku surut).”¹⁸

Asas legalitas menghendaki bahwa suatu perbuatan dapat dinyatakan sebagai tindak pidana apabila terlebih dahulu ada undang-undang yang menyatakan bahwa perbuatan itu sebagai tindak pidana. Oleh karenanya, asas legalitas melarang penerapan hukum pidana secara surut (*retroaktif*).

Pasal 1 Ayat (1) KUHP inilah yang menjadi landasan penegakan hukum pidana di Indonesia, terutama dalam kaitannya dengan kepastian hukum.¹⁹

“Asas legalitas ini diatur pula dalam Pasal 6 Ayat (1) UU Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman yang menyebutkan bahwa tidak seorang pun dapat dihadapkan di depan pengadilan selain dari pada yang ditentukan oleh undang-undang. Bunyi pasal ini memperkuat kembali kehendak asas legalitas terhadap hukum pidana yang dibuat secara tertulis”.

Terkait dengan asas legalitas, maka lazimnya di dalam hukum pidana hal-hal baru yang akan diatur di dalam hukum pidana dibuat dalam bentuk pembaharuan hukum pidana.

18 Beberapa yuris menerangkan juga bahwa sebenarnya dalam Pasal 1 KUHP tersebut terdapat larangan analogi. Dengan demikian, dalam Pasal 1 KUHP terkandung tiga hal penting dengan memasukkan larangan menggunakan analogi dalam menentukan adanya tindak pidana.

19 www.pemantauperadilan.com. Lihat: Eva Achjani Zulfa, *Ketika Jaman Meninggalkan Hukum*, 01 April 2003, www.pemantauperadilan.com./, 20 Juli 2006. 16.00

“Pembaharuan hukum pidana adalah memperbaharui ketentuan hukum pidana yang berlaku (*sebagai Ius Contitutum*) untuk menghasilkan hukum pidana baru yang lebih baik karena memenuhi syarat keadilan, efektivitas dan kesesuaian dengan situasi pada saat hukum dibuat dan pada saat sesudahnya/mendatang (*ius constituendum*).”²⁰

Pembaharuan hukum pidana (*Penal Reform*) merupakan bagian dari politik/kebijakan hukum pidana,“ ini sering ini dikenal dengan berbagai istilah, antara lain “*penal policy*“, “*criminal law polcy*“, atau “*strafrechtspolitik*“.²¹

“Marc Ancel mendefinisikan politik hukum pidana (*penal policy*) sebagai suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif (terutama hukum pidana) dapat dirumuskan secara baik. Ia merupakan *the rational organization of the control of crime by society* (upaya rasional masyarakat dalam mengontrol/menanggulangi kejahatan).”²²

Dalam rangka menanggulangi kejahatan terhadap berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa sarana pidana (*penal policy*) maupun sarana di luar hukum pidana (*non penal policy*), yang dapat diintegrasikan satu dengan yang lainnya.

“Menurut Sudarto, apabila sarana pidana dipanggil untuk menanggulangi kejahatan, berarti akan dilaksanakan politik hukum pidana, yakni mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang.”²³

Di samping usaha penanggulangan kejahatan, lewat pembuatan undang-undang pidana pada hakekatnya merupakan bagian integral dari usaha

²⁰ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, ctk. Kedua, PT. Citra Aditya Bakti, Bandung, 2002, hlm. 24.

²¹ *Ibid*

²² M. Abdul Kholiq, “Tinjauan Politik Hukum Pidana Tentang RUU APP”, Makalah disampaikan pada *Kuliah Program Pasca Sarjana*, UII, Yogyakarta, 2006, hlm. 4.

²³ Sudarto, *Hukum Pidana dan Perkembangan Masyarakat*, ctk. Pertama. Sinar Baru, Bandung 1983, hlm.109.

kesejahteraan masyarakat (*social welfare*). Oleh karena itu wajar pula apabila dikatakan, bahwa politik hukum pidana juga merupakan bagian integral dari kebijakan sosial (*social policy*).

Social policy dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat sekaligus mencakup perlindungan masyarakat. Jadi di dalam pengertian *social policy*, sekaligus didalamnya tercakup *social welfare policy* dan *social defence policy*.

Maka perbuatan-perbuatan tertentu yang oleh masyarakat atau golongan-golongan masyarakat dianggap sebagai perbuatan pidana perlu dikriminalisasikan menurut, Barda Nawawi Arief:²⁴

“Kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana. Pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal dengan menggunakan sarana hukum pidana, dan oleh karena itu termasuk bagian dari kebijakan hukum pidana”.

Dilihat dari sudut yang luas tersebut, maka dapat ditegaskan bahwa masalah kebijakan hukum pidana pada hakikatnya bukanlah semata-mata pekerjaan teknik perundang-undangan yang dapat dilakukan secara yuridis normatif dan sistematis-dogmatik.

M. Abdul Kholiq, menyatakan sebagai berikut :

“Di samping pendekatan yuridis normatif, kebijakan hukum pidana juga memerlukan pendekatan yuridis faktual yang dapat berupa pendekatan sosiologis, psikologis, historis dan komparatif, bahkan memerlukan pula pendekatan integral dengan kebijakan sosial dengan pembangunan nasional pada umumnya.”²⁵

²⁴ Barda Nawawi Arief, “Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tindak Pidana Mayantara”, Makalah *Seminar Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi*, Semarang, 26 Juli 2001, hlm. 2-3.

²⁵ M. Abdul Kholiq, *Op.cit*, hlm.6

Telah dijelaskan diatas bahwa kriminalisasi merupakan suatu proses penetapan suatu perbuatan yang semula bukan tindak pidana menjadi tindak pidana. Untuk menetapkan suatu perbuatan yang sebelumnya tidak dikategorikan sebagai tindak pidana menjadi perbuatan yang dikategorikan sebagai tindak pidana bukanlah suatu pekerjaan yang mudah.

Proses kriminalisasi berakhir dengan terbentuknya undang-undang yang menetapkan perbuatan yang itu dilarang dan diancam dengan sanksi yang berupa pidana.²⁶

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.²⁷

Hukum pidana mempunyai sifat *ultimum remedium* atau alat terakhir yang berisi pengenaan penderitaan kepada pelaku kejahatan. Sifat hukum pidana ini menyebabkan hukum pidana dinilai sangat kejam sehingga pengenaannya haruslah merupakan upaya terakhir apabila upaya-upaya lain tidak dapat dilakukan untuk memperbaiki pelaku kejahatan. Mengingat sifat kejamnya hukum pidana ini, maka penetapan suatu perbuatan dengan ancaman hukumannya haruslah memperhatikan berbagai aspek kemanusiaan.

²⁶ Sudarto, *Hukum dan Hukum Pidana*, ctk. Pertama, Alumni, Bandung, 1986, hal. 32 dan hal. 151.

²⁷ *Ibid*, hal. 36.

Proses kriminalisasi dalam hal ini tidak boleh dilakukan sembarangan karena hal ini menyangkut harkat, martabat dan hak asasi manusia untuk hidup. Penetapan suatu perbuatan menjadi tindak pidana atau bukan haruslah didasarkan pada pertimbangan yang matang. Penetapan ini harus dijauhkan dari unsur-unsur politis sehingga mereka yang mempunyai kekuasaan tidak dapat mempengaruhi pembuat undang-undang agar perbuatan jahatnya tidak terkena jerat hukum.

Meskipun ada anggapan bahwa undang-undang adalah hasil dari kompromi politis, tetapi sebisa mungkin unsur politis yang merugikan berbagai pihak (terutama mereka yang tidak mempunyai kekuasaan untuk mempengaruhi pembuat undang-undang) dapat ditekan atau diminimalisir.

Penetapan suatu perbuatan menjadi tindak pidana harus pula memperhatikan perbandingan antara sarana dan hasil serta kemampuan aparat penegak hukum.

Apabila sarana yang diperlukan dan kemampuan aparatnya tidak memadai, maka penetapan suatu perbuatan menjadi tindak pidana menjadi tidak berarti karena sarana untuk menegakkannya tidak ada sehingga penetapan itu hanya menjadi macan kertas saja, tidak ada implementasinya dan hanya merupakan pemborosan anggaran negara.

Dari uraian tersebut, maka dapatlah dikatakan bahwa proses kriminalisasi merupakan proses yang tidak hanya bersifat sosial, tetapi juga politis. Pandangan hidup yang ada dan dipelihara oleh masyarakat atau pemegang kekuasaan akan mewarnai hasil kriminalisasi.

Untuk menetapkan suatu perbuatan itu sebagai tindakan kriminal, perlu memperhatikan kriteria umum sebagai berikut:

- 1) Apakah perbuatan itu tidak disukai atau dibenci oleh masyarakat karena merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban;
- 2) Apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya *cost* pembuatan undang-undang, pengawasan dan penegakan hukum, serta beban yang dipikul korban, pelaku dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai;
- 3) Apakah akan makin menambah beban aparat penegak hukum yang tidak seimbang atau nyata-nyata tidak dapat diimbangi oleh kemampuan yang dimilikinya;
- 4) Apakah perbuatan-perbuatan itu menghambat atau menghalangi cita-cita bangsa Indonesia, sehingga merupakan bahaya bagi keseluruhan masyarakat.²⁸

E. Definisi Opsional

Pengaturan adalah suatu cara untuk mengatur kejahatan teknologi informasi atau dikenal dengan istilah *cyber crime* yang dapat berupa aturan yang berlaku saat ini (*ius constitutum*) maupun aturan yang akan diberlakukan di masa yang akan datang (*ius constituendum*)

Cyber Crime adalah istilah yang merujuk pada bentuk-bentuk kejahatan yang terdapat di dunia maya dengan menggunakan sarana teknologi informasi, khususnya internet.

Hukum Pidana Indonesia, dalam hal ini ialah hukum pidana material adalah bagian dari keseluruhan hukum yang berlaku di negara Indonesia yang mengadakan dasar-dasar dan aturan-aturan untuk menentukan: a) Masalah

²⁸ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana... Op. cit*, hal. 36-37.

Perbuatan Pidana, b) Masalah Pertanggungjawaban Pidana, 3) Masalah Sanksi Pidana.²⁹

F. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang dilakukan dalam penelitian ini penelitian hukum normatif.

2. Objek Penelitian

- a) Pengaturan *cyber crime* dalam hukum positif Indonesia
- b) Kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*)

3. Sumber Data

a. Bahan Hukum Primer, yakni data yang diperoleh dari :

- 1) Undang-Undang Dasar 1945
- 2) Kitab Undang-Undang Hukum Pidana
- 3) Undang-Undang Nomor 4 tahun 2004 Tentang Ketentuan-Ketentuan Pokok Kekuasaan Kehakiman
- 4) Undang-Undang Nomor 36 tahun 1992 tentang Telekomunikasi
- 5) Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta
- 6) Undang-Undang Nomor 25 tahun 2003 tentang Pencucian Uang
- 7) Ketentuan *Convention On Cybercrime* 2001 yang terkait dengan Hukum Positif Indonesia
- 8) Peraturan-Peraturan Hukum lainnya

²⁹ P.A.F. Lamintang, *Op.cit*, hlm.1.

- b. Bahan Hukum Sekunder, yakni data yang diperoleh dari bahan-bahan kepustakaan berupa dokumen-dokumen hukum, buku-buku, jurnal, makalah dan lain-lain.
- c. Bahan Hukum Tertier, Bahan Hukum Tertier, data yang diperoleh melalui kamus, ensiklopedi, dan data yang sejenisnya yang berfungsi untuk mendukung data primer dan data sekunder.

4. Metode Pendekatan

Doktriner, Yuridis Normatif, yakni mendekati permasalahan dari aspek norma hukum yang diimplementasikan dalam tataran normatif. Selanjutnya, dilihat fakta-fakta normatif tersebut yang merupakan fakta-fakta hukum.

5. Analisis Data

Deskriptif kualitatif, yaitu menguraikan data-data yang diperoleh berdasarkan dari hasil studi keperpustakaan dan selanjutnya di analisis dengan teori-teori, konsep-konsep yang ada didalam hukum pidana. Kemudian setelah dilakukan analisis ditarik pada suatu kesimpulan.

BAB II

TINJAUAN UMUM HUKUM PIDANA DI INDONESIA

A. Pengertian Hukum Pidana

Istilah "*hukuman*" yang merupakan istilah umum dan konvensional, dapat mempunyai arti yang luas dan beruba-ruba karena istilah itu dapat berkonotasi dengan bidang yang cukup luas.³⁰ Istilah tersebut tidak hanya sering digunakan dalam bidang hukum, tetapi juga dalam istilah sehari-hari di bidang pendidikan, moral, agama dan sebagainya.

Oleh karena "*pidana*" merupakan istilah yang lebih khusus, maka perlu ada pembatasan pengertian atau makna sentral yang dapat menunjukan ciri-ciri atau sifat-sifatnya yang khas, dan masalah pengertian atau definisi hukum pidana sesungguhnya tidak semudah untuk merumuskannya seperti yang disangka orang.

Istilah hukum pidana sebagaimana istilah secara umum, dapat dibedakan arti menurut sudut pandang seseorang dari mana aspek hukum pidana itu diperhatikan. Oleh karena itu wajar apabila dijumpai adanya beragam macam definisi yang berkaitan dengan pengertian hukum pidana yang pernah dikemukakan oleh para ahli dalam khasanah kepustakaan.

Sekedar untuk menyebutkan beberapa contoh, Andi Zainal Abidin misalnya menyatakan bahwa:

³⁰ Muladi, *et.al*, *Teori-teori dan Kebijakan Pidana*, ctk. Ketiga, Alumni, Bandung, 2005. hlm. 2.

“Istilah hukum pidana itu dapat diberikan arti baik secara obyektif maupun secara subjektif. Dalam arti obyektif (sering juga disebut *Ius Poenale*), hukum pidana dapat diartikan sebagai sejumlah peraturan hukum yang mengandung larangan dan perintah atau keharusan yang terhadap pelanggarannya diancam dengan sanksi hukum berupa pidana tertentu bagi barangsiapa yang membuatnya.”

Sedangkan dalam arti subjektif (lazim pula disebut *Ius Puniendi*), hukum pidana itu ialah peraturan hukum yang menetapkan tentang penyidikan, penyidikan lanjutan, penuntutan, penjatuhan dan pelaksanaan pidana.³¹

Senada dengan rumusan diatas, dalam konteks definisi tentang hukum pidana ini **Moeljanto** juga membuat batasan-batasan sebagai berikut :

“Hukum pidana adalah bagian daripada keseluruhan hukum yang berlaku di suatu negara yang mengadakan dasar-dasar dan aturan-aturan untuk: (1) menentukan perbuatan-perbuatan mana yang tidak boleh dilakukan, yang dilarang, dengan disertai ancaman atau sanksi berupa pidana tertentu bagi barangsiapa melanggar larangan tersebut. (2) menentukan kapan dan dalam hal-hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhi pidana sebagaimana yang telah diancamkan, (3) menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.”³²

Dalam perspektif yang lain yakni tinjauan dari sudut institusi sosial yang memiliki kewenangan untuk mengadakan/membuat hukum pidana, **Simons** mengemukakan bahwa hukum pidana adalah : (a) seluruh perintah dan larangan yang diadakan oleh negara dan yang diancam dengan suatu pidana/nestapa bagi barang siapa yang tidak menaatinya. (b) seluruh aturan

³¹ Andi Zainal Abidin, *Asas-asas Hukum Pidana Baigan Pertama*, ctk. Pertama, Alumni, Bandung, 1987, hal 1-2

³² Moeljanto, *Asas-asas Hukum Pidana*, ctk. Keempat, Bina Aksara, Jakarta, 1987, hal 1.

yang ditentukan oleh negara yang berisi syarat-syarat untuk menjalankan pidana tersebut.³³

Khusus dalam konteks Indonesia, definisi yang dikemukakan oleh Simon yang terkesan memberi tekanan (*accent*) kepada negara sebagai satu-satunya pihak yang mengadakan hukum pidana tersebut, tentu kurang realitis. Sebab dalam kenyataan, di Indonesia juga berlaku (hidup) hukum pidana adat yang legitimasi keberadaannya tidak diberikan oleh negara dalam artian Negara Kesatuan Republik Indonesia. Akan tetapi oleh masyarakat hukum adat bersangkutan dengan justifikasi melalui keputusan-keputusan para pemuka adat.

Dalam hubungan ini, rumusan tentang pengertian hukum pidana yang ditunjukkan oleh van HATTUM barangkali lebih kontekstual dengan realitas sosial Indonesia. Beliau menyatakan:

“Hukum pidana adalah suatu keseluruhan dari atas asas-asas dan peraturan-peraturan yang diikuti dan ditetapkan oleh suatu negara atau oleh suatu masyarakat hukum umum lainnya, dimana mereka itu sebagai pemelihara dari ketertiban hukum umum telah melarang dilakukannya tindakan-tindakan yang bersifat melanggar hukum dan telah mengkaitkan pelanggaran terhadap peraturan-peraturannya dengan suatu penderitaan yang bersifat khusus berupa pidana”.³⁴

Rumusan mengenai hukum pidana oleh van Hattum di atas yang cenderung menekankan pada inti hukum pidana positif (yaitu hukum pidana yang sedang berlaku di suatu negara atau wilayah tertentu), apabila diperbandingkan dengan ketiga rumusan yang telah dipaparkan sebelumnya maka dapat dinyatakan bahwa rumusan van Hattum tersebut kurang lengkap.

³³ Soeharto, *Op.cit.* hlm.4.

³⁴ P.A.F. Lamintang, *Op.cit.* hlm. 2.

Sebab hakekat hukum pidana positif itu bukan hanya merupakan suatu keseluruhan dari asas-asas dan peraturan-peraturan yang berkenaan dengan penentuan tentang norma-norma dan sanksi-sanksi saja, melainkan juga berkenaan dengan penentuan mengenai syarat-syarat bagi akibat hukumnya suatu pelanggaran norma (yang bisa disebut sanksi pidana), serta berkenaan dengan ketentuan-ketentuan mengenai penjatuhan dan pelaksanaan dari sanksi pidana itu sendiri.

Berdasarkan pemaparan tentang beberapa definisi hukum pidana seperti telah dicontohkan di atas, secara inti dapat disimpulkan bahwa di dalam istilah hukum pidana, ternyata ruang lingkup pengertiannya mencakup beberapa makna.

Pertama, pengertian hukum pidana adakalanya bermakna hukum pidana material yaitu yang terdiri dari aturan mengenai perbuatan yang terlarang (sering disebut dengan istilah delik/tindak pidana/perbuatan pidana), hal-hal atau syarat yang menjadikan orang dapat dipidana (sering dikenal dengan istilah pertanggungjawaban pidana), dan berisi aturan mengenai ancaman sanksi hukum berupa pidana (sanksi pidana).

Kedua, adakalanya makna istilah hukum pidana itu mencakup pengertian hukum pidana formil yakni yang berisi tentang tata cara atau prosedur penjatuhan sanksi pidana bagi seorang yang diduga telah melanggar hukum pidana material.

Kemudian yang *ketiga*, pengertian hukum pidana juga terkait dengan makna sebagai hukum pelaksanaan pidana yaitu yang berupa ketentuan-

ketentuan mengenai bagaimana suatu sanksi pidana yang telah dijatuhkan terhadap seorang pelanggar hukum pidana material itu harus dilaksanakan.

Sesuai dengan batasan kajian dalam penulisan thesis ini, selanjutnya yang dimasukkan dengan pengertian hukum pidana dalam hal ini ialah hukum pidana material, dimana persoalan-persoalan dasarnya ialah terdiri dari tiga masalah pokok yaitu : (1) masalah tindak pidana, (2) masalah pertanggungjawaban pidana dan (3) masalah sanksi pidana.

Kesimpulan tentang pengertian dan ruang lingkup dari masalah-masalah dasar hukum pidana material tersebut sesuai dengan pandangan Sudarto yang menyatakan bahwa hukum pidana material itu memuat aturan-aturan yang menetapkan dan merumuskan perbuatan-perbuatan yang dapat dipidana, aturan-aturan yang memuat syarat untuk dapat menjatuhkan dan ketentuan mengenai pidana.³⁵

B. Asas Legalitas dalam konteks Hukum Pidana

Asas legalitas tercantum di dalam Pasal 1 Ayat 1 KUHP. Kalau kata-katanya yang asli dalam bahasa latin: "*Nullum delictum nulla poena sine praevia legi poenali*" yang dapat disalin kedalam bahasa Indonesia kata demi kata, maka akan berbunyi:

"Tiada suatu perbuatan (*feit*) yang dapat dipidana selain berdasarkan kekuatan ketentuan perundang-undangan pidana yang mendahuluinya". atau dengan kata lain: "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada, sebelum perbuatan dilakukan".³⁶

³⁵ Sudarto, *Hukum Pidana I*, ctk. Kedua, Penerbit Yayasan Sudarto, UNDIP, Semarang, 1990, hal. 10.

³⁶ Andi Hamzah, *Asas-Asas Hukum Pidana*, ctk. Kedua, Rineka Cipta, Jakarta, 1994. hlm. 39.

Perlu pula diperhatikan bahwa dengan istilah *feit* itu disalin orang juga dengan kata “*peristiwa*”, karena dengan istilah *feit* itu meliputi baik perbuatan yang melanggar sesuatu yang dilarang oleh hukum pidana maupun mengabaikan sesuatu yang dilarang oleh hukum pidana maupun mengabaikan sesuatu yang diharuskan.

Penerapan hukum pidana atau suatu perundang-undangan pidana berkaitan dengan waktu dan tempat perbuatan dilakukan. Berlakunya hukum pidana menurut waktu menyangkut penerapan hukum pidana dari segi lain.

“Menurut Hazewinkel-Suringa, jika suatu perbuatan (*feit*) yang mencocoki rumusan delik yang dilakukan sebelum berlakunya ketentuan yang bersangkutan, maka bukan saja hal itu dapat dituntut tetapi untuk orang yang bersangkutan sama sekali tidak dapat dipidana.”³⁷

Asas legalitas ini menurut Moeljatno mengandung tiga pengertian:³⁸

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

Beberapa yuris menerangkan juga bahwa sebenarnya dalam Pasal 1 Ayat (1) KUHP ini merumuskan secara rinci, berisi dua hal penting, yaitu: (i) suatu tindak pidana harus dirumuskan terlebih dahulu dalam peraturan perundang-undangan; (ii) peraturan perundang-undangan harus ada sebelum terjadinya tindak pidana (tidak berlaku surut”).

³⁷ *Ibid*

³⁸ Moeljatno, *Asas-asas Hukum Pidana*, ctk. Keempat, ... *Op.cit*, hlm. 25.

Asas legalitas melarang penerapan hukum pidana secara surut (*retroaktif*). Pasal 1 Ayat (1) KUHP inilah yang menjadi landasan penegakan hukum pidana di Indonesia, terutama dalam kaitannya dengan kepastian hukum.

Asas legalitas ini diatur pula dalam Pasal 6 Ayat (1) UU Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman yang menyebutkan bahwa tidak seorang pun dapat dihadapkan di depan pengadilan selain daripada yang ditentukan oleh undang-undang. Bunyi pasal ini memperkuat kembali kehendak asas legalitas terhadap hukum pidana yang dibuat secara tertulis.

C. Kebijakan Kriminalisasi dalam Upaya Penanggulangan Kejahatan

Kejahatan merupakan entitas yang selalu lekat dengan dinamika perkembangan peradaban umat manusia. Kejahatan yang oleh Saparinah Sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada tiap bentuk masyarakat; tidak ada masyarakat sepi dari kejahatan.³⁹

Oleh karena itu, upaya penanggulangan kejahatan sesungguhnya merupakan upaya yang terus menerus dan berkesinambungan. Tidak ada, bahkan tidak akan pernah ada upaya yang bersifat final. Dalam hal ini dimaksudkan bahwa setiap upaya penanggulangan kejahatan tidak dapat menjanjikan dengan pasti bahwa kejahatan itu akan terulang atau tidak akan memunculkan kejahatan baru. Namun demikian, upaya itu tetap harus dilakukan lebih menjamin perlindungan dan kesejahteraan masyarakat.

³⁹ Muladi. *et.al.*, *Bunga Rampai Hukum Pidana*, ctk. Pertama, Alumni, Bandung 1992, hlm. 148.

Dengan semakin maju peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, muncul berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cyber crime*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi cita ketertiban masyarakat.

Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab terhadap dampak negatif yang timbul, yang biasa disebut dengan kejahatan. Ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk sejarah yang sudah barang tentu berjalan dalam logika sejarah yang menaunginya, walaupun dalam batas tertentu mempunyai prediktabilitas atas perkembangan masyarakat.

Bertolak dari hal tersebut, maka seiring dengan semakin kompleksnya permasalahan yang dihadapi masyarakat dan penegak hukum, perlu diimbangi dengan pembangunan sistem hukum pidana secara terus menerus. Dengan demikian, dalam persepektif ini, kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana dalam kaitannya dengan perkembangan masyarakat.

Kebijakan hukum pidana dapat didefinisikan sebagai usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang.⁴⁰

A. Mulder mengemukakan bahwa kebijakan hukum pidana ialah garis kebijakan untuk menentukan:

1. Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui;
2. Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana;
3. Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.⁴¹

Dari definisi ini tampak bahwa Mulder memandang hukum pidana sebagai sebuah sistem. Dengan demikian objek kebijakan hukum pidana mencakup hukum pidana dalam arti formil dan materiil. Menurut hemat penulis, definisi ini lebih komprehensif. Sebab dengan objek kebijakan hukum pidana yang terfokus pada hukum pidana materiil akan tidak efektif dalam menghadapi peristiwa hukum konkrit yang dalam hal ini berkaitan erat dengan hukum pidana formil. Ini tampak dalam menyikapi perkembangan teknologi dan masyarakat yang sangat pesat.

Definisi Mulder di atas sesungguhnya bertolak dari pengertian "*sistem hukum pidana*" menurut Marc Ancel, yang menyatakan bahwa tiap masyarakat yang terorganisir memiliki sistem hukum pidana yang terdiri dari

⁴⁰ Al. Wisnusobroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta, 1999, hlm. 11.

⁴¹ *Ibid*, hlm. 12.

peraturan-peraturan hukum pidana dan sanksinya, suatu prosedur hukum pidana dan suatu mekanisme pelaksana pidana.⁴²

“Marc Ancel mengemukakan, *penal policy* (kebijakan hukum pidana) adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak saja kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan.”⁴³

Pada hakekatnya kebijakan untuk membuat peraturan hukum pidana menjadi lebih baik merupakan bagi dari upaya dalam penganggulangan kejahatan. Dengan demikian kebijakan hukum pidana, hakekatnya merupakan bagian dari kebijakan penanggulangan kejahatan (politik kriminal)

Dalam persepektif ini (politik kriminal), kebijakan hukum pidana identik dengan pengertian “*kebijakan penanggulangan kejahatan dengan hukum pidana*”

Oleh karena itu, dengan perkataan yang lain “*kebijakan penanggulangan kejahatan dengan hukum pidana*” bisa disebut dengan kebijakan kriminalisasi, di mana dalam proses ini (*kriminalisasi*) menggunakan sarana pidana. Dari sisi tampak bahwa dalam persepektif kebijakan hukum pidana kriminalisasi merupakan bagian dari kebijakan hukum pidana.

Untuk lebih jelas pengertian kriminalisasi, secara etimologis kriminalisasi berasal dari kata bahasa Inggris *Criminalization*, yang

⁴² Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana...Op.cit*, ctk. Pertama, hlm. 26.

⁴³ *Ibid*, hlm. 21.

mempunyai padanan dalam bahasa Belanda *Criminalisatie*,⁴⁴ dengan kata lain kriminalisasi dalam kepustakaan asing dikenal dengan nama *Criminalization* atau *Criminalisering*.

“Kriminalisasi bukan hanya suatu kata, tetapi juga suatu perbuatan istilah (*terminologi*) dalam hukum pidana materil. Oleh karena itu, dalam pembentukan kaidah hukum pidana, kriminalisasi merupakan suatu objek kajian yang penting ada bermacam pengertian kriminalisasi, yang sekaligus dapat menjelaskan ruang lingkup kriminalisasi.”⁴⁵

Kriminalisasi merupakan tindakan atau penetapan penguasa mengenai perbuatan-perbuatan tertentu yang oleh masyarakat atau golongan-golongan masyarakat dianggap sebagai perbuatan yang bukan dapat dipidana menjadi perbuatan pidana. Atau proses penetapan suatu perbuatan sebagai perbuatan yang dilarang dan diancam dengan pidana bagi barang siapa yang melanggar larangan tersebut.⁴⁶

“Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana. Pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal dengan menggunakan sarana hukum pidana, dan oleh karena itu termasuk bagian dari kebijakan hukum pidana.”⁴⁷

Di Indonesia sesungguhnya proses kriminalisasi sejak Proklamasi Kemerdekaan terus berlangsung sampai sekarang dan tidak akan berhenti. Dengan UU No. 1 Tahun 1946 telah banyak diciptakan tindak pidana-tindak

⁴⁴ Salman Luthan, “Kebijakan Kriminalisasi dalam Reformasi Hukum Pidana”, *Jurnal Hukum*, Fakultas Hukum UII Yogyakarta, No. 11 Vol.6. 1999, hlm. 3.

⁴⁵ *Ibid.*

⁴⁶ Suwondo, *Himpunan Karya Tentang Hukum Pidana*, Yogyakarta : Liberty, hlm. 61.

⁴⁷ Barda Nawawi Arief, “Kebijakan Kriminalisasi dan Masalah Yurisdiksi...*Op.cit*”, Makalah Seminar Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi, Semarang, 26 Juli 2001, hlm. 2-3.

pidana. Penciptaan tindak pidana baru ini merupakan cerminan masyarakat dan negara pada waktu pembuatan undang-undang tersebut.⁴⁸

Suatu perbuatan dijadikan perbuatan pidana (*dikriminalisasikan*) karena alasan-alasan sebagai berikut :⁴⁹

1. Perbuatan itu merugikan masyarakat;
2. Sudah berulang-ulang dilakukan;
3. Ada reaksi sosial atas perbuatan itu.
4. Ada unsur bukti

Berdasarkan keempat parameter ini maka tidak serta merta perbuatan yang merugikan dapat dirumuskan secara formal sebagai perbuatan pidana (tindak pidana).

Sebagaimana telah dijelaskan di atas bahwa kriminalisasi merupakan upaya menjadikan suatu perbuatan menjadi tindak pidana. Proses kriminalisasi ini pada akhirnya akan berujung pada perumusan hukum pidana. Dengan demikian, proses kriminalisasi akan berkaitan erat dengan mekanisme penyelenggaraan hukum pidana.

Maka dalam rangka menanggulangi kejahatan terhadap berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa sarana pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya..

⁴⁸ Sudarto, *Hukum dan Hukum Pidana... Op.cit*, hlm. 32.

⁴⁹ Tb. Rony R. Nitibaskara, "Problem Yuridis Cyber Crime". Kompas Online, dapat dijumpai dalam situs di internet: <http://www.kompas.com/kompas-cetak/007/31/poin/prob04.htm>, 5 Mei 2006.

Apabila sarana pidana dipanggil untuk menanggulangi kejahatan, berarti akan dilaksanakan politik hukum pidana, yakni mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang.⁵⁰

Di samping usaha penanggulangan kejahatan, lewat pembuatan undang-undang pidana pada hakekatnya merupakan bagian integral dari usaha kesejahteraan masyarakat (*social welfare*). Oleh karena itu wajar pula apabila dikatakan, bahwa politik hukum pidana juga merupakan bagian integral dari kebijakan sosial (*social policy*).

Social policy dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat sekaligus mencakup perlindungan masyarakat. Jadi di dalam pengertian *social policy*, sekaligus didalamnya tercakup *social welfare policy* dan *social defence policy*.

Dilihat dari sudut yang luas tersebut, maka dapat ditegaskan bahwa masalah kebijakan hukum pidana pada hakikatnya bukanlah semata-mata pekerjaan teknik perundang-undangan yang dapat dilakukan secara yuridis normatif dan sistematis-dogmatik.

Di samping pendekatan yuridis normatif, kebijakan hukum pidana juga memerlukan pendekatan yuridis faktual yang dapat berupa pendekatan sosiologis, psikologis, historis dan komparatif, bahkan memerlukan pula

⁵⁰ Sudarto, *Hukum Pidana dan Perkembangan Masyarakat*,...*Op.cit*, hlm.109.

pendekatan integral dengan kebijakan sosial dengan pembangunan nasional pada umumnya.

Karena suatu undang-undang (hukum pidana) yang telah dirumuskan dan dilaksanakan, ia akan menggerakkan banyak badan dan orang untuk diterapkan. Ada korp polisi, badan penuntut umum (kejaksaan), pengadilan, lembaga pemasyarakatan, kedokteran (*forensik*) dan lain sebagainya.⁵¹

Hukum pidana sejak dari proses pembentukan sampai penerapannya dalam masyarakat dengan demikian telah menghabiskan biaya yang tidak sedikit. Dan ini harus ditanggung oleh pemerintah yang pada gilirannya menjadi beban masyarakat. Hal ini tampak dalam APBN. Dan ini juga harus dipertimbangkan dalam upaya kriminalisasi.

Maka disini ada beberapa hal yang fundamental harus diperhatikan adalah sebagai berikut:⁵²

1. Tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil makmur secara material dan spiritual berdasarkan Pancasila; sehubungan dengan ini maka penggunaan hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan pengadugeraan terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat.
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan perbuatan yang tidak dikehendaki, tidak disukai atau dibenci oleh warga masyarakat yaitu perbuatan yang merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban. Selain itu harus pula dipertimbangkan sejauh mana perbuatan tersebut bertentangan dengan nilai-nilai fundamental yang berlaku dalam masyarakat.
3. Perhitungan prinsip biaya dan hasil (*cost benefit principle*) dari penggunaan hukum pidana tersebut, yaitu apakah biaya mengkriminalisasi

⁵¹ Sudarto, *Hukum dan Hukum Pidana, ...Op.cit*, hlm. 32.

⁵² Sudarto, *Hukum Pidana dan Perkembangan Masyarakat, ...Op.cit*, hlm. 44-48.

seimbang dengan hasilnya yang akan dicapai, artinya *cost* pembuatan undang-undang, pengawasan dan penegak hukum, serta beban yang dipikul oleh korban dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai.

4. Kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum, yaitu jangan sampai ada kelampauan beban tugas dan keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai.

Selain keempat hal tersebut diatas perlu pula berpedoman pada 6

(enam) asas yang dikemukakan **De Roos**, yaitu⁵³ :

1. Masuk akal nya kerugian yang digambarkan;
2. Adanya toleransi yang didasarkan pada kehormatan atas kebebasan dan tanggungjawab individu;
3. Apakah kepentingan yang dilanggar masih dapat dilindungi dengan cara lain;
4. Ada keseimbangan antara kerugian, toleransi dan pidana yang diancamkan;
5. Apakah kita dapat merumuskan antara kerugian, toleransi dan pidana yang diancamkan;
6. Kemungkinan penegakannya secara praktis dan efektif (serta dampaknya pada prevensi umum)

Sebab bila tidak demikian halnya, maka akan terjadi apa yang dimakan *over criminalization* (kelebihan perbuatan yang dijadikan tindak pidana). Pada gilirannya hal ini akan menimbulkan *inflasi pidana*, sehingga penghargaan terhadap hukum pidana tidak pada semestinya lagi.

D. Batas-Batas Berlakunya Perundang-Undangan Hukum Pidana Menurut

Waktu dan Tempat Terjadinya Perbuatan

Ditaatnya ketentuan berlakunya perundang-undangan hukum pidana yang telah disepakati beberapa negara secara universal, bukanlah merupakan tujuan prinsipiil. Prinsip dasar ketentuan tersebut justru beroreintasi pada

⁵³ Marjono Reksodiputro, "Cyber Crime: Intellectual Property Rights, Ecommerce", *Penataran Nasional Hukum Pidana dan Kriminologi Indonesia (ASPEHUPIKI)* di FH Universitas Surabaya, 13-19 Januari 2002, hlm. hlm.5.

pencegahan terhadap pelaku delik yang karena keadaan maupun dengan cara tertentu terlepas dari sanksi pidana. Dengan kata lain pelaku delik di negara manapun berada harus dapat dikenai sanksi pidana.

Dalam Pasal 1 Ayat 1 KUHP, diadakan aturan-aturan mengenai batas-batas berlakunya perundang-undangan pidana menurut waktu atau saat terjadinya perbuatan. Dalam pasal 2 sampai 9 KUHP sebaliknya diadakan aturan-aturan mengenai batas-batas berlakunya perundang-undangan hukum pidana menurut tempat terjadinya perbuatan.⁵⁴

Tentang berlakunya hukum pidana secara sistematis teoritis dibedakan:⁵⁵

1. Menurut waktu terjadinya delik (*tempus delicti*)
2. Menurut tempat terjadinya delik (*locus delicti*)

1. Menurut waktu terjadinya delik (*tempus delicti*)

Ketentuan tentang *tempus delicti*, berorientasi pada azas legalitas yang menetapkan bahwa suatu delik harus dirumuskan dalam peraturan perundang-undangan dan tidak boleh berlaku surut. Pada prinsipnya segala bentuk perbuatan baru dapat dikategorikan sebagai delik jika sudah ada undang-undang yang menetapkan.

Selain hal tersebut ditetapkan pula bahwa seseorang baru dapat didakwa sebagai pelaku delik apabila perbuatan yang dilakukan sudah terlebih dahulu dirumuskan dalam Undang-undang.

⁵⁴ *Ibid*, hlm. 38.

⁵⁵ Sumarni Priohutomo, *Op.cit*, hlm. 11.

2. Menurut tempat terjadinya delik (*locus delicti*)

Untuk menentukan *locus delicti* pada prinsipnya kita berorientasi pada azas teritorial dan personal tanpa mengabaikan prinsip nasional pasip dan universal.

Ditinjau dari sudut negara, ada dua kemungkinan pendirian, yaitu:⁵⁶

1. Perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi di dalam wilayah negara, baik dilakukan oleh warga negaranya sendiri maupun oleh orang asing (*azas teritorial*).
2. Perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga negara, dimana saja, juga di luar wilayah negara (*azas personal*). Juga dinamakan prinsip nasional yang aktif.

Dalam azas pertama, titik berat diletakkan pada terjadinya perbuatan di dalam wilayah negara. Siapa yang melakukannya, warga negara atau orang asing, tidak menjadi soal. Dengan kata lain aturan hukum pidana suatu negara berlaku bagi semua delik yang terjadi di wilayah hukum negara tersebut, tanpa memperhatikan kewarganegaraan sipelaku.⁵⁷

Hal tersebut didasarkan pada konsep pemikiran bahwa setiap orang yang berada di wilayah suatu negara harus tunduk pada peraturan hukum negara tersebut. Artinya setiap negara harus saling mengakui kedaulatan negara lain. Azas ini terkenal dan banyak pendukungnya karena mengadung pengertian "*pengakuan kedaulatan setiap negara*"

Azas kedua, titik berat diletakkan pada orang yang melakukan perbuatan pidana, tempat terjadinya delik adalah tidak penting. Dengan kata

⁵⁶ Moeljatno, *Asas-asas Hukum Pidana*, ctk. Keempat, ...*Op.cit*, hlm. 38.

⁵⁷ *Loc.cit*

lain perundang-undangan hukum pidana suatu negara berlaku bagi semua delik yang dilakukan oleh warga negara tersebut.

“Seperti, hukum pidana Republik Indonesia berlaku bagi warga negara Indonesia. Tanpa memperhatikan tempat terjadinya delik maupun tempat keberadaan pelaku, warga negara Indonesia yang melakukan delik di Amerika, kemudian melarikan diri ke Australia, yang berlaku tetap hukum pidana Indonesia. Walaupun sukar untuk mendapatkan pengakuan sepenuhnya.”⁵⁸

Azas personal memiliki arti penting sehubungan dengan perlindungan terhadap kepentingan nasional (prinsip nasional pasif) dan prinsip universal (kepentingan internasional). Dengan kata lain bahwa dasar pemikiran azas personal dirasakan arti pentingnya dalam hal suatu delik bagi negara tertentu dianggap bukan delik bagi negara lain. Dengan diterapkan azas tersebut pelaku delik dapat menghindari sanksi pidana.

Dari kedua azas tersebut diatas, Azas teritorial yang pada masa ini lazim dipakai oleh kebanyakan negara-negara, juga Indonesia dan ini sudah sewajarnya. Tiap-tiap orang yang berada dalam wilayah suatu negara harus tunduk kepada peraturan-peraturan negara.

Dalam sistem hukum pidana Indonesia wilayah berlakunya hukum pidana diperluas sampai dengan sarana transportasi Indonesia baik darat, laut maupun udara, walaupun berada di luar wilayah Indonesia. Namun demikian masih terdapat pengecualian yang berlaku berdasarkan azas universal/ketentuan hukum internasional, seperti:⁵⁹

1. Kepala Negara; Asing yang berkunjung ke Indonesia

⁵⁸ Sumarni Priohutomo, *Op.cit*, hlm. 12.

⁵⁹ *Log.cit*

2. Konsul negara asing dan keluarganya; Duta, Atase Pertahanan, Kebudayaan, Wakil Konsultan.
3. Anak buah kapal perang dan tentara; sopir, pengawal
4. Para wakil-wakil Badan Internasional, Utusan PBB, Bank Dunia, IMF, Palang Merah.

E. Pertanggungjawaban Dalam Hukum Pidana

Perbuatan pidana hanya menunjukan kepada dilarang dan diancamnya perbuatan dengan suatu pidana.⁶⁰ Dengan kata lain apabila seseorang melakukan suatu delik, terhadap delik yang dilakukan dapat dipertanggungjawabkan dan tidak ada dasar penghapusan pidana, maka terhadap sipelaku akan dikenakan sanksi yang berupa pidana.

Pertanggungjawaban pidana pada hakekatnya merupakan suatu mekanisme yang dibangun oleh hukum pidana untuk bereaksi terhadap pelanggaran atas suatu tindak pidana.⁶¹

Namun demikian, sebelum kita menerapkan sanksi pidana, hendaknya di ingat bahwa di dalam sistem hukum pidana dikenal suatu adagium bahwa sanksi pidana bersifat "*ultimum remedium*". Hal ini berarti bahwa sanksi pidana baru diterapkan apabila hukum yang lain tidak mampu menjamin ditaatinya ketentuan hukum tersebut, atau dengan istilah lain, bahwa sanksi pidana harus diterapkan sebagai senjata "*pamungkas*".

⁶⁰ Moeljatno, *Asas-asas Hukum Pidana*, ctk. Keempat, ...*Op.cit.*, hlm. 153.

⁶¹ Chairul Huda, "Kesalahan dan Pertanggungjawaban Pidana", *Ringkasan Disertasi Program Doktor*, Fakultas Hukum UI, Jakarta, 2004, hlm. 24.

Bentuk pertanggungjawaban pidana terdiri dari:⁶²

1. Kesegajaan (*dolus*) : Perbuatan secara sadar/dengan kehendak untuk mencapai tujuan tertentu.
2. Kealpaan (*culpa*) : Kesalahan yang disebabkan oleh tindakan kurang hati-hati sehingga menimbulkan akibat negatif.

Dalam menerapkan sanksi perlu kita lihat apakah orang yang melakukan perbuatan kemudian juga dijatuhi pidana, sebagaimana telah diancamkan, ini tergantung dari soal apakah dalam melakukan perbuatan ini dia mempunyai kesalahan. Sebab azas dalam pertanggungjawaban dalam hukum pidana ialah: "*Tiada pidana tanpa kesalahan*" (*Green straf zonder schuld*).⁶³

"Kesalahan adalah dapat dicelanya pembuat tindak pidana, karena dilihat dari segi masyarakat sebenarnya dia dapat berbuat lain jika tidak ingin melakukan perbuatan tersebut. "*dapat dicela*" baik berarti "*dapat dipertanggungjawabkan dalam hukum pidana*" yaitu makna kesalahan dalam hubungannya berfungsi *preventif*, maupun dapat dijatuhi pidana, yaitu makna kesalahan dalam hubungannya dengan fungsi *represif* hukum pidana."⁶⁴

Dengan kata lain kesalahan dalam istilah hukum pidana berarti kemampuan seseorang mempertanggungjawabkan perbuatan yang dilakukannya.

⁶² Sumarni, *Op.cit*, hlm.12.

⁶³ Moeljatno, *Asas-asas Hukum Pidana*, ctk. Keempat,... *Op.cit*, hlm. 153.

⁶⁴ *Ibid*, hlm. 25.

BAB III

PERKEMBANGAN TEKNOLOGI, KEJAHATAN DAN HUKUM PIDANA

A. Perkembangan Teknologi dan Kehidupan Manusia

Perkembangan teknologi sekarang ini amat pesat ibarat sebuah revolusi tengah berlangsung, dan kita berada didalamnya. Pada zaman Yunani, teknologi diartikan sebagai seni memproduksi alat-alat produksi dan menggunakannya. Kemudian, berkembang menjadi penggunaan ilmu pengetahuan sesuai dengan kebutuhan manusia bahkan ada yang menyebutnya sebagai keterampilan saja.⁶⁵

Teknologi juga dapat diartikan sebagai *the know-how of making things*. Juga, dapat diartikan sebagai *the know-how of doing things*, dalam arti kemampuan untuk mengerjakan sesuatu dengan hasil nilai yang tinggi, baik nilai kegunaan maupun nilai jual.⁶⁶

Dengan demikian, maka teknologi bukanlah ilmu pengetahuan dan juga bukan produk. Teknologi adalah penetapan atau aplikasi ilmu pengetahuan untuk memproduksi atau membuat barang dan/atau jasa. Produk tersebut merupakan hasil akhir teknologi, tetapi produk itu sendiri bukanlah teknologi.

⁶⁵ H. Daud Silalahi, *Rencana Undang-Undang Alih Teknologi: Perbandingan Perspektif*, Prisma, No. 4 Th. XVI, April 1987, hlm. 40.

⁶⁶ Agus Suswanto, *Pendidikan, Iptek dan Pembangunan*, Riau Mandiri, 3 Agustus 2005, hlm. 4.

Dari beberapa definisi teknologi tersebut di atas, ada beberapa segi atau aspek yang perlu diperhatikan, yaitu:⁶⁷

1. Teknologi terdiri dari informasi yang mampu mengaplikasikan semua tahapan dari perencanaan, organisasi, dan operasi suatu industri atau perusahaan (komersial) dengan segenap aktivitasnya.
2. Teknologi mempunyai kontribusi untuk membuat setiap tahapan yang mencakup perencanaan, organisasi dan operasi kegiatan suatu industri atau perusahaan; maka teknologi tidak hanya terdiri dari *scientific knowledge*, tetapi juga pengetahuan bisnis atau organisasi.
3. Teknologi bisa berupa teknologi yang berwujud (bertubuh) dan tidak berwujud.

Perkembangan teknologi telah mempengaruhi kehidupan manusia bahkan sampai hal-hal yang bersifat pribadi. Dalam hal perkembangan teknologi, T. Jacob membagi siklus ilmu pengetahuan dan teknologi menjadi 5 (lima) siklus *kondratieff*, yaitu yang berulang-ulang setiap 50 (lima puluh) tahun. Kelima siklus itu adalah:⁶⁸

1. Siklus pertama dimulai dengan revolusi teknologi (1760).
2. Siklus kedua ditandai dengan terbentangnya jaringan kereta api (1848).
3. Siklus ketiga dimulai dengan ban berjalan (1895).
4. Siklus keempat ditandai dengan tenaga atom dan motorisasi masal (1945).
5. Siklus kelima (sekarang) ditandai dengan ciri perkembangan mikroelektronik dan bioteknologi.

Pada tahap awal lembaga teknologi diperlakukan sebagai sesuatu yang statis, tidak berubah oleh keadaan. Pada tahap kedua, lembaga teknologi telah diakui sebagai sesuatu yang berubah atau dinamis, tetapi perubahannya bersifat *independent* dari perubahan masyarakat, atau dengan istilah lain merupakan suatu variabel *exogenous* dalam model masyarakat. Baru pada

⁶⁷ Ridwan Kairandy, "Francise dan Kaitannya Sebagai Sarana Alih Teknologi: Suatu Tinjauan Hukum", *Jurnal Hukum Ius Quia Iustum*, No. 7 Vol. 4, FH UII Yogyakarta, 1997, hlm. 115-116.

⁶⁸ T. Jacob, *Menuju Teknologi Berperikemanusiaan*, ctk. Pertama, Yayasan Obor Indonesia, Jakarta, 1996, hlm. 15.

tahap ketiga lembaga teknologi diperlakukan sebagai variabel yang *endogenous*. Dengan perkataan lain, baru pada tahap ketiga ini diakui bahwa lembaga teknologi berhubungan dengan variabel-variabel sosial-ekonomi lainnya.⁶⁹

Ilmu pengetahuan dan teknologi yang berkembang dalam 62 (enam puluh dua) tahun terakhir ternyata lebih luas dan lebih cepat daripada perkembangan yang dicapai manusia selama 160 (seratus enam puluh) tahun sebelumnya.

Teknologi pada satu sisi membawa kemajuan yang menjanjikan perbaikan umat manusia (pemanfaatannya sebagai tenaga, energi, pengawetan tanaman dan sebagainya), tetapi di sisi lain memungkinkan pemanfaatannya yang dapat memusnahkan peradaban hampir 5 (lima) sampai 6 (enam) kali lipat.

Luas dan kecepatan penemuan di bidang teknologi telah demikian cepatnya sehingga tenggang waktu untuk membahas layak tidaknya suatu temuan baru itu diterapkan pada kehidupan manusia menjadi salah satu persoalan tersendiri. Apa yang layak secara etis dan apa yang tidak layak ditinjau dari segi dampaknya secara kemanusiaan selalu menjadi bahan perbincangan hangat.

Bagaimanapun juga kemajuan teknologi cepat atau lambat akan mempengaruhi kaidah-kaidah kebudayaan kita, lembaga-lembaga sosial budaya kita dan dari segi sosial politik pola-pola pengambilan keputusan

⁶⁹ Ronny Hanitijo Soemitro, "Hukum dan Perkembangan Ilmu Pengetahuan dan Teknologi di dalam Masyarakat", *Pidato Pengukuhan Guru Besar Tetap Fakultas Hukum UNDIP*, Semarang 6 Desember 2004, hlm. 23.

kebijakan pemerintahan negara kita.⁷⁰ Hampir semua negara meyakini bahwa ilmu pengetahuan dan teknologi adalah salah satu faktor yang penting dalam menopang pertumbuhan dan kemajuan negara.

T. Jacob, bahkan mengatakan bahwa:

“Negara yang tidak memiliki dan menguasai ilmu pengetahuan dan teknologi akan tertinggal dari peradaban. Ilmu pengetahuan dan teknologi sekarang diagung-agungkan dan dijadikan sebagai ideologi. Orang cenderung mendewa-dewakan teknologi seakan-akan teknologi adalah suatu azimat, paspor atau tanda masuk satu-satunya menuju kesejahteraan, kemakmuran dan keadilan. Tidak hanya itu, teknologi yang dikembangkan ternyata sangat jelas menimbulkan kultus baru dalam teknologi, yaitu menimbulkan masyarakat yang konsumtif.”⁷¹

Ada juga mitos yang mengundang banyak simpati terhadap teknologi, yaitu memandang teknologi sebagai alat pembebas, sarana demokrasi dan partisipasi serta dapat mewujudkan otonomi manusia. Anggapan ini masih harus dipertanyakan secara kritis sebab teknologi juga bisa bertindak sebagai belenggu bagi kebebasan manusia.

Miftah Wirahadikusumah, mengatakan bahwa :

“Teknologi dapat menjadi alat pembebas manusia apabila manusia memiliki tradisi praksis yang kritis dan mempraktekkan *practical reason*. Pada saat nilai-nilai kemanusiaan dikorup, dikekang dan dimatikan oleh nilai-nilai yang mementingkan “fungsi” dan “*pragmatisme*”, maka teknologi akan menjadi alat perusak dan penindas yang efektif.”⁷²

Teknologi canggih dapat memudahkan pertumbuhan kebebasan manusia hanya karena teknologi canggih dapat mengurangi secara radikal

⁷⁰ Juwono Sudarsono, “Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial-Politik, Masyarakat”, *Jurnal Sosiologi*, No. 3 Vol. 2, FISIP UI-Gramedia, Jakarta, 1992, hlm. 4.

⁷¹ T. Jacob, *Manusia, Ilmu dan Teknologi*, ctk. Kedua, PT Tiara Wacana, Yogyakarta, 1993, hlm. 13.

⁷² Miftah Wirahadikusumah, “Logika dan Gramar Teknologi: Sebuah Tinjauan Psikoanalisis, Masyarakat”: *Jurnal Sosiologi*, No. 5 Vol. 3, FISIP UI-Gramedia, Jakarta, 1992, hlm. 30.

ketidaksesuaian dalam hubungan kita dengan lainnya, yang dibatasi oleh dimensi waktu, tempat dan suasana dan ketegangan yang ditimbulkan oleh ketidaksesuaian ini.

Teknologi canggih memudahkan pertumbuhan kebebasan manusia karena teknologi canggih membuat kita tidak perlu lagi dan tidak harus terus bersandar pada saluran-saluran komunikasi dan transportasi yang tidak menentu.

Masyarakat atau sekelompok kecil orang dapat berinteraksi secara lebih efektif dan harmonis dalam sistem organisasi yang sangat disederhanakan, tetapi ini hanya mungkin terjadi jika organisasi yang menggunakan teknologi canggih mempunyai semua bahan, teknik dan masukan budaya di tempat itu. Dengan mengurangi perbedaan ruang dan pembagian kerja yang ekstrem, pengawasan hierarki atau birokrasi yang terpusat menjadi tidak berguna.⁷³

Di sisi lain, terdapat kekhawatiran terhadap perkembangan teknologi seperti ditulis oleh George Orwell dalam bukunya *Nineteen Eighty-Four*. Dalam bukunya George Orwell mengisahkan betapa kemajuan teknologi telah dipergunakan oleh kekuasaan untuk memasang pengawasan yang amat ketat terhadap semua anggota masyarakat.

Semua kehidupan warga negara diatur dari pusat kekuasaan, yang memonopoli segala peralatan teknologi canggih. Tidak ada lagi warga negara

⁷³ Eliot D. Chappie, *Mengurangi Pita Merah*, dalam Lewis H. Lapham, *Teknologi Canggih dan Kebebasan Manusia*, ctk. Pertama, Yayasan Obor Indonesia, Jakarta, 1989, hlm. 50.

yang berpikir bebas,⁷⁴ karena kehidupan menjadi semakin mekanis dengan realita atau fakta yang sudah dapat ditebak sesuai dengan proses mekanistik itu. Dengan demikian, melakukan kegiatan observasi dan penilaian secara kritis atas teknologi sangat diperlukan oleh suatu masyarakat. Hal ini dilakukan melalui peran agen-agen manusia dan aktor sosial.

Teknologi yang sebenarnya mengandung arti *automotif* dan alat apabila tidak dipahami secara jelas dan tepat maka manusia menjadi budak dan akan didikte oleh teknologi. Sedangkan pandangan kita tentang teknologi menganggap hanya sebagai alat maka kita akan memperlakukan teknologi tersebut sesuai dengan tuntutan (*demand*) dan kebutuhan (*need*) tertentu demi pencapaian nilai-nilai kemanusiaan yang tinggi.

Pilihan strategis tentang pemilihan dan penguasaan teknologi yang lebih proporsional dan tepat akan mengarahkan tindakan manusia menuju ke arah yang dicita-citakan itu. Apabila kita memandang teknologi dari aspek *automotif*, maka kita akan memperlakukan teknologi sebagai sesuatu hal yang dapat menggantikan berbagai fungsi aktivitas motorik, sensorik dan bahkan mampu mewakili sebagian dari fungsi intelektual.⁷⁵

Sikap pandang yang memperlakukan teknologi sebagai pengganti fungsi-fungsi aktivitas manusia inilah yang telah banyak menimbulkan krisis. Krisis tersebut antara lain adalah krisis rasionalitas yang ditimbulkan oleh kekeliruan proyek besar kemanusiaan di abad *Renaissance* yang terjadi di Eropa Barat dan di mana teknologi itu asalnya diciptakan. Kemudian, krisis

⁷⁴ *Ibid*, hal. x

⁷⁵ Miftah Wirahadikusumah, *Op.cit*, hlm. 29.

yang terjadi di Amerika Serikat sebagai tempat di mana teknologi dikembangkan dan berikutnya krisis yang terjadi di Jepang di mana teknologi diproduksi dan dijual di pasar.

Tidak dapat disangkal oleh siapapun bahwa tingkat perkembangan suatu teknologi memerlukan dukungan pranata nilai budaya dan pranata sosial-ekonomi masyarakat di mana teknologi itu ada dan dikembangkan. Upaya teknologi yaitu upaya untuk menciptakan sistem memerlukan pemahaman akan berbagai sistem kehidupan yang telah ada. Hal ini disebabkan sistem ciptaan orang (anggota masyarakat) hanya dapat dibentuk dengan mengubah atau mensintesis struktur sistem yang telah ada.

Saswinadi Sasmojo, bahkan mengatakan bahwa:

“Upaya ilmiah menghasilkan pemahaman akan struktur sistem yang ada, oleh karena itu hasil upaya ilmiah menyediakan basis informasi bagi upaya teknologi. Tingkat kemampuan teknologi suatu masyarakat sangat dipengaruhi oleh intensitas upaya ilmiah yang dilakukan oleh masyarakat tersebut yang pada gilirannya sangat dipengaruhi oleh tata nilai budaya yang dianut. Akan tetapi, perlu dicatat bahwa suatu masyarakat dengan budaya ilmiah tinggi belum tentu kuat dalam berteknologi”.⁷⁶

Pada hakikatnya, teknologi itu mempunyai logika dan *grammarnya* sendiri yang berhubungan secara erat dan menyatu secara integral dengan kosmologi (sistem nilai kepercayaan) dan *world view* suatu masyarakat yang menemukan (*invent*), memproduksi (*inovative, produce*) dan mengembangkan (*develop*) teknologi tersebut.

Kesenjangan, perbedaan, pertentangan atau konflik antara sistem kepercayaan atau kosmologi dan *world view* suatu masyarakat dengan sesuatu

⁷⁶ Saswinadi Sasmojo *et.al*, *Budaya Sains, Teknologi dan Perubahan Masyarakat*, ctk. Pertama, Seri Penerbitan Sains, Teknologi dan Masyarakat, tanpa tahun, hlm. 35-36.

bentuk teknologi tertentu yang terdapat di dalam masyarakat tersebut bisa menyebabkan terjadinya berbagai krisis seperti krisis moral dan krisis nilai sosial-budaya.⁷⁷

Selanjutnya teknologi dan ilmu pengetahuan mempunyai 2 (dua) sisi yang berbeda (*ambiguitas*). Yaitu:

“Pada satu sisi ia telah banyak membantu menyelamatkan, menyehatkan dan memperpanjang usia manusia. Akan tetapi, di sisi lain setiap hari kita mendengar, membaca dan menonton berita mengenai polusi, perusakan lingkungan, pemanasan global, berkurangnya lapisan ozon, hujan asam, penggundulan hutan, perburuan flora dan fauna dan sebagainya. Ilmu pengetahuan dan teknologi yang didewa-dewakan justru membuat manusia makin merasa dirinya dewa sehingga lupa bahwa salah satu tugas dewa adalah justru melestarikan kelangsungan hidup”.⁷⁸

Dari uraian di atas dapat dilihat bahwa eksistensi dan fungsi teknologi harus didukung oleh suatu pranata nilai budaya dan pranata sosial ekonomi tertentu di mana teknologi itu diciptakan. Pranata itu juga termasuk tingkat pengetahuan atau tingkat intelek masyarakat yang sesuai.

Setiap teknologi bisa menjadi misteri dan penuh keajaiban jika tidak dilihat secara kritis. Ia akan menjadi monster atau tuyul-tuyul yang magis dan berkuasa, ia ditakuti sekaligus dikagumi. Lihatlah bangsa Jepang dalam melihat teknologi. Mereka konsisten untuk melakukan *secrutiny* dan *dekonstruksi* terhadap teknologi dalam rangka untuk menguasainya dan memproduksinya, sehingga secara satir ada pemeo yang mengatakan bahwa *technology was invented in Europe and developed in USA, but produced as*

⁷⁷ Miftah Wirahadikusumah, *Op.cit*, hlm. 26-27.

⁷⁸ Juwono Sudarsono, *Op.cit*, hlm. 6.

made in Japan. Pertanyaan ini kurang lebih sama bisa juga dilontarkan di sini: Bagaimana dengan bangsa Indonesia?⁷⁹

Indonesia sendiri saat ini sedang dan akan terus mengembangkan teknologi untuk berbagai keperluan. Hal ini dilakukan untuk menghadapi tantangan yang semakin menantang di masa mendatang terutama dalam bidang industri dan perdagangan. Francois Raillon mengungkapkan dengan baik sekali usaha yang dilakukan Indonesia dalam bidang teknologi ini seperti yang dikatakannya dalam Nasir Tamara.

“... bahwa di Indonesia kesadaran akan kebutuhan teknologi bukanlah hal yang baru. Yang baru hanyalah keinginan memacu pemakaiannya sejalan dengan majunya industrialisasi. Pemakaian teknologi dalam setiap produksi menjadi semakin besar; penguasaan atas prosesnya, adanya kemampuan untuk menyesuaikan serta mengembangkan teknologimenjadikewajiban mendasar”.⁸⁰

Dari uraian tersebut sebenarnya ada 3 (tiga) hal yang ingin dicapai dan pengembangan teknologi itu. *Pertama*, importasi teknologi asing sesuai dengan kebutuhan. *Kedua*, pengembangan teknologi domestik melalui riset dan pengembangan serta menyediakan tenaga ahli (*skill formation*). *Ketiga*, mengubah kesenjangan antara negara maju dengan negara sedang berkembang.⁸¹

Upaya mengembangkan teknologi di Indonesia akan berhasil jika tata nilai budaya yang ada di Indonesia mendukung usaha-usaha tersebut. Setidak-

⁷⁹ Miftah Wirahadikusumah, *Op.cit.*, hlm. 31.

⁸⁰ Francois Raillon, *Indonesia Tahun 2000 (Tantangan Teknologi dan Industri)*, (terjemahan Nasir Tamara), ctk. Pertama, CV Haji Masagung, Jakarta, 1990, hlm. 54.

⁸¹ T. Mulya Lubis, “Alih Teknologi: Antara Harapan dan Kenyataan”, *Prisma*, No. 4 Th. XVI, April 1987, hlm. 11.

tidaknya ada 3 (tiga) ciri penting dari tata nilai budaya yang mendukung kesuburan perkembangan ilmu pengetahuan dan teknologi, yaitu:⁸²

- a. Menghargai dan menghormati upaya pemahaman akan berbagai fenomena kehidupan.
- b. Menghargai upaya pemanfaatan pengetahuan yang dimiliki untuk membentuk sistem-sistem baru.
- c. Memiliki kriteria untuk memilih upaya-upaya ilmiah dan teknologi yang membawa pada terwujudnya tata kehidupan yang lebih baik.
- d. Memiliki kriteria yang memungkinkan terwujudnya hubungan sosial yang lebih terbuka, serta terkendalikannya pertumbuhan institusi yang tidak tanggap terhadap permasalahan lingkungannya.

Dengan dilakukan pengembangan teknologi yang terus-menerus, maka akan timbul penguasaan atas teknologi itu sendiri. Penguasaan teknologi berarti penguasaan atas suatu misteri dan misteri adalah *power*. Arti simbolik dari kekuasaan atau misteri sebagai suatu *power* di zaman dahulu adalah ibarat api.

Pengembangan teknologi di Indonesia betul-betul harus dilakukan dengan memperhatikan berbagai aspek yang dapat ditimbulkan akibat pengembangan itu. Teknologi dan hasil-hasilnya sekarang ini tidak hanya dimanfaatkan untuk kesejahteraan manusia, tetapi sekaligus dapat menghancurkan kehidupan manusia.

Salah satu wujud dari sifat negatif penggunaan teknologi adalah digunakan teknologi dan hasil-hasilnya untuk kejahatan dengan modus operandi yang baru. Kejahatan saiber atau *cybercrime*, penggunaan kartu kredit secara tidak sah, penggandaan pulsa atau menekan jumlah pulsa telepon dan pencucian uang (*money laundering*) melalui internet merupakan beberapa

⁸² Saswinadi Sasmojo, *et.al*, *Op.cit*, hlm. 37.

contoh dari pemanfaatan teknologi untuk kejahatan. Teknologi itu sendiri sebenarnya tidak jahat, bahkan bisa membantu manusia dalam meningkatkan taraf hidup dan mengubah masyarakat.

Sebagai contoh adalah perkembangan teknologi informasi yang telah melipatgandakan kemampuan berkreasi manusia pada batas yang tidak ada toleransinya sama sekali. Percepatan inovasi sekarang dimungkinkan karena terintegrasinya seluruh kemampuan berpikir dan daya imajinasi manusia ke dalam sebuah jaringan Internet.

Jaringan internet menjadi semacam jembatan penghubung telepatis dari semua manusia ke manusia lain, dengan kecepatan cahaya menembus batas waktu dan batas negara. Teknologi informasi sama dengan teknologi lain, hanya di sini informasi merupakan komoditas yang diolah dengan teknologi tersebut. Dalam hal ini teknologi mengandung konotasi memiliki nilai ekonomis.

Budi Rahardjo mengatakan bahwa:

“Teknologi pengolahan informasi ini memang memiliki nilai jual, seperti teknologi *database* dan *security*, semuanya dapat dijual. Bentuk dari teknologi adalah kumpulan pengetahuan (*knowledge*) yang diimplementasikan dalam tumpukan kertas (*stacked of papers*) atau sekarang dalam bentuk CD-ROM. Tumpukan kertas inilah yang didapatkan jika anda membeli sebuah teknologi dalam bentuk *patent* atau bentuk HAKI (*Intellectual Property Rights*) lainnya”.⁸³

⁸³ Budi Rahardjo, “Implikasi Teknologi dan Internet Terhadap Pendidikan, Bisnis dan Pemerintahan, Siakah Indonesia”, Makalah pada *seminar di Riau, dapat dijumpai di* <http://budi.insan.co.id/articies/riau-it.doc>.

Indonesia telah mulai memanfaatkan teknologi informasi ini untuk berbagai keperluan, tetapi ada beberapa kendala yang menyebabkan teknologi informasi belum dapat digunakan seoptimal mungkin, yaitu:⁸⁴

- a. Kurangnya ketersediaan infrastruktur telekomunikasi. Jaringan telepon masih belum tersedia di berbagai tempat di Indonesia. Biaya penggunaan jasa telekomunikasi juga masih mahal. Hal ini dapat diatasi dengan perkembangan telekomunikasi yang semakin canggih dan semakin murah.
- b. Penetrasi komputer (PC) di Indonesia masih rendah, untuk itu perlu dipikirkan akses ke Internet tanpa melalui komputer pribadi di rumah. Penggunaan *Internet devices* lain seperti *Internet TV* diharapkan dapat menolong, sementara itu akses Internet dapat diperlebar jangkauannya melalui fasilitas di kampus, sekolahan dan bahkan melalui warung Internet.
- c. Isi atau *content* yang berbahasa Indonesia masih langka. Hal ini merupakan masalah yang serius sehingga perlu ada upaya atau kegiatan atau inisiatif untuk memperkaya materi yang ditujukan kepada masyarakat Indonesia yang dilakukan secara sadar dan objektif.

Memang ada kekhawatiran munculnya revolusi teknologi informasi di masa mendatang tidak hanya membawa dampak pada teknologi itu sendiri, tetapi juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi dan kehidupan bermasyarakat lainnya.

Jaringan informasi global atau internet saat ini menjadi salah satu sarana untuk melakukan kejahatan. Internet menjadi medium bagi pelaku kejahatan untuk melakukan kejahatan dengan sifatnya yang mondial, internasional dan melampaui batas atau kedaulatan suatu negara. *Cross boundaries countries*, menjadi motif yang menarik bagi para penjahat digital.

⁸⁴ *Ibid*

Kejahatan dan penjahat saat ini menjadi pasangan yang serasi dan kebaikan dan orang baik yang ada dalam masyarakat. Dalam masyarakat modern yang sangat kompleks dan heterogen, perangai antisosial dan kejahatan itu berkembang dengan cepatnya.

Kondisi lingkungan dengan perubahan-perubahan yang cepat, norma-norma dan sanksi sosial yang semakin longgar serta macam-macam subkultur dan kebudayaan asing yang saling berkonflik, semua faktor itu memberikan pengaruh yang mengacau dan memunculkan disorganisasi dalam masyarakatnya. Muncullah banyak kejahatan.⁸⁵

Apa yang berkembang dan dikembangkan oleh teknologi tidak luput dan akan selalu diatur oleh hukum. Perhatian terhadap hukum teknologi itu sendiri saat ini merupakan hal penting sejalan dengan pesatnya perkembangan teknologi yang secara langsung memberi pengaruh terhadap hukum.

Pada kenyataannya, piranti hukum yang ada saat ini tidak dapat secara penuh mengimbangi eksese-eksese yang ditimbulkan akibat pemanfaatan teknologi. Sebagai contoh, perkembangan teknologi informasi akan memberikan pengaruh terhadap bentuk-bentuk perbuatan hukum berdimensi baru.⁸⁶

Sebagian besar teknologi saat ini dikuasai oleh korporasi. Korporasi menggunakan teknologi untuk mencapai tujuan utamanya, yaitu:

⁸⁵ Kartini Kartono, *Patologi Sosial*, ctk. Pertama, CV Rajawali, Jakarta, 1983, hlm. 167-169.

⁸⁶ Bentuk-bentuk perbuatan itu antara lain *joycomputing, hacking, the trojan horse, data leakage, data diddling, to frustrate data communication, software piracy* dan sebagainya. Bentuk kejahatan ini sebelumnya tidak dikenal dalam berbagai sistem hukum sebelum berkembangnya teknologi informasi.

“Mencari keuntungan sebesar-besarnya. Korporasi dilakukan dengan menggunakan usaha manajerial yang baik, koordinasi produksi yang baik serta pemasaran produk yang terarah pula sehingga dalam sebuah korporasi terdapat sejumlah akumulasi modal yang kuat dan menjadi sumber kekayaan utama dalam pengembangan korporasi. Ia menggunakan teknologi yang ada, pengumpulan modal yang kuat. Mereka membangun jaringan dalam skala yang besar”.⁸⁷

Sering kali dalam upayanya untuk memperoleh keuntungan tersebut dilakukan dengan tidak atau kurang memperhatikan dan karenanya merugikan pihak lain seperti lingkungan, konsumen, buruh, masyarakat luas, bahkan negara.⁸⁸ Bentuk tindakan itu berupa penggunaan teknologi dan hasil-hasilnya yang dapat merugikan masyarakat luas. Tindakan mereka disebut dengan nama kejahatan korporasi (*corporate crime*).

Dari uraian di atas terlihat bahwa teknologi selain membawa keuntungan berupa meningkatnya taraf kehidupan manusia, juga mempunyai sisi gelap terutama apabila dipakai untuk tujuan kejahatan. Teknologi itu sendiri sebenarnya tidak jahat, yang membuat teknologi itu tampak jahat adalah pembuat atau pemakainya yang memang mempunyai tujuan untuk melakukan kejahatan.

Jika teknologi informasi memenuhi harapan bisa membawa penggunaannya pada kehidupan, kemakmuran dan kesejahteraan yang lebih tinggi, maka teknologi informasi itu perlu dikembangkan, tetapi jika perkembangannya akan membawa dampak negatif bagi masyarakat atau

⁸⁷ Clinard & Yeager, *Corporate Crime*, The Free Press A Division of Mac Millan Publishing Co. Inc, New York, 1980, hlm. 1.

⁸⁸ I.S. Susanto, “Menciptakan Lingkungan Hidup yang Nyaman”, *Pidato Dies Natalis* UNDIP ke-40, Semarang, 15 Oktober 1997, hlm. 6.

penggunanya, maka lupakan saja teknologi informasi, dan kita akan memetik akibatnya berupa ketertinggalan peradaban.

B. Teknologi, Kejahatan dan Reaksi Sosial atas Kejahatan

Kemajuan teknologi di samping telah memberikan memberikan kemaslahatan terhadap masyarakat di sisi lain juga menimbulkan kekhawatiran karena adanya penggunaan yang menyimpang dari tujuan yang sebenarnya. Dengan kata lain teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahkannya penjahat melakukan kejahatannya.

Teknologi juga memberikan pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran dalam kriminologi yang menitikberatkan pada faktor manusia, baik secara lahir maupun psikologis.

Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulaan zaman sampai sekarang dan masa yang akan datang. Bentuk-bentuk kejahatan yang adapun semakin hari semakin bervariasi.

Suatu hal yang patut untuk diperhatikan adalah bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui untuk menjadi suatu tradisi atau budaya, padahal jika dibandingkan dengan berbagai budaya yang ada, usia kejahatan tentulah lebih tua.

Kejahatan sebenarnya tumbuh dan berkembang dalam masyarakat. tidak ada kejahatan tanpa masyarakat atau seperti ucapan **Lacassagne** bahwa

masyarakat mempunyai penjahat sesuai dengan jasanya.⁸⁹ Betapapun kita mengetahui banyak tentang berbagai faktor kejahatan yang ada dalam masyarakat, namun yang pasti adalah bahwa kejahatan merupakan salah satu bentuk perilaku manusia yang terus mengalami perkembangan sejajar dengan perkembangan masyarakat itu sendiri.

Romli Atmasasmita, bahkan mengatakan bahwa:

“Kejahatan telah diterima sebagai suatu fakta, baik pada masyarakat yang paling sederhana (*primitif*) maupun pada masyarakat yang modern, yang merugikan masyarakat. Kerugian yang ditimbulkan itu dapat berupa kerugian dalam arti materiil maupun moral. Kerugian materiil berupa timbulnya korban kejahatan dan rusak atau musnahnya harta benda serta meningkatnya biaya yang harus dikeluarkan bagi penanggulangannya. Kerugian moral berupa berkurang atau hilangnya kepercayaan masyarakat terhadap pelaksanaan penegakan hukum yang dilakukan oleh aparat penegak hukum.”⁹⁰

Sebenarnya, banyak faktor yang harus dipertimbangkan dalam membicarakan mengenai kejahatan, sehingga menimbulkan berbagai sudut pandang yang berbeda. Kejahatan tidak bisa dibicarakan hanya dengan memfokuskan pada 1 (satu) permasalahan saja yang menjadi sebabnya, karena kejahatan merupakan peristiwa yang mempunyai faktor multi-dimensi yang menjadi penyebabnya dan mempunyai pengertian yang relatif.

Menarik sekali apa yang dikemukakan oleh J.E. Sahetapy dan B. Mardjono Reksodiputro dalam kaitannya dengan kejahatan yang dikaitkan dengan perilaku masyarakat dan ruang serta waktu. Mereka berdua mengatakan:

⁸⁹ Agus Raharjo, *Op.cit*, hlm. 1.

⁹⁰ Romli Atmasasmita, *Kapita Selekta Kriminologi*, ctk. Kedua, Armico, Bandung, 1983, hlm.

“Berbicara mengenai kejahatan dan penjahat, saya berkesimpulan bahwa kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relatif, mengandung variabilitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagian mayoritas atau minoritas masyarakat sebagai suatu perbuatan yang antisosial, suatu perkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu”⁹¹

Di lain kesempatan, J.E. Sahetapy mengemukakan bahwa:

“Persepsi tentang apa itu yang dinamakan kejahatan, tidak dapat tidak ada pasti akan merupakan bahan debat yang kontroversial, seperti apa yang dinamakan cantik atau kecantikan bisa menimbulkan perdebatan atau dikatakan *beauty is in the eye of the beholder*. Jalan yang paling aman untuk mengkaji permasalahan kejahatan dapat ditempuh dengan menghindari diskusi tentang berbagai teori yang masing-masing mempunyai pangkal tolak atau *outlook-nya* serta asumsi yang implikatif sendiri-sendiri”.⁹²

Kejahatan merupakan perbuatan antisosial, tidak hanya terdapat di masyarakat yang sedang berkembang, tetapi ada juga di masyarakat yang sudah maju (dengan peralatan teknologi yang lebih canggih tentu-nya). Kejahatan tidak hanya ada di dunia nyata (*real*), tetapi ia juga ada di dunia maya (*virtual*) dengan bentuk yang berbeda dengan wajah kejahatan yang konvensional karena telah diperhalus sedemikian rupa. Keberadaan suatu kejahatan identik dengan keberadaan manusia itu sendiri meskipun ada kemungkinan bentuk atau tipe kejahatan dari tiap-tiap masyarakat berbeda.

Pemahaman terhadap kejahatan dan sebab-sebab terjadinya suatu kejahatan bukanlah suatu persoalan yang sederhana. Kita tidak bisa mengatakan bahwa seseorang melakukan kejahatan karena dendam, lapar atau khilaf saja, tentu ada faktor lain yang ada di belakang kejadian tersebut.

⁹¹ J.E. Sahetapy dan B. Mardjono Reksodiputro. *Paradoks Dalam Kriminologi*. ctk. Pertama, CV Rajawali, Jakarta, 1983, hlm. 167-168.

⁹² J.E. Sahetapy, *Pisau Analisa Kriminologi*, ctk. Kedua, Armico, Bandung, 1984, hlm. 9.

Berbagai faktor yang ada dalam kehidupan di dunia ini dapat atau berpotensi untuk menimbulkan kejahatan. bahkan perbuatan baik pun dapat memicu seseorang untuk melakukan kejahatan. Kejahatan tidak dapat diprediksi kejadiannya karena ia begitu antik, tidak mempedulikan tempat dan suasana ketika ia hendak muncul dan tidak pula membanding-bandingkan siapa pelaku dan siapa korbannya, tidak mengenal kasta atau status sosial pelaku dan korbannya. Ia begitu misterius ketika belum muncul dan ketika muncul ia menjadi bahan yang menarik untuk dibicarakan, baik di ruang-ruang seminar, lokakarya, penataran bahkan di warung kopi pinggir jalan.

Pembicaraan mengenai kejahatan pada masa lampau sering kali kehilangan maknanya karena melepaskan diri dari konsepsi masyarakat sebagai suatu totalitas,⁹³ yaitu lingkungan sosial tempat berlangsungnya kejahatan. Adapun kejahatan sebagai fenomena sosial selalu merupakan kejahatan di dalam masyarakat sebagai rangkaian dari keseluruhan proses-proses sosial, budaya, politik, ekonomi dan struktur yang ada di dalam masyarakat.

Semua itu merupakan hasil sejarah hubungan antar-manusia dan untuk selanjutnya ikut mempengaruhi hubungan antar-manusia. Dengan demikian, untuk memahami masalah kejahatan perlu diperhatikan keseluruhan proses-

⁹³ Hal ini tampak nyata jika pembicaraan mengenai kejahatan dilakukan dengan menggunakan paradigma kriminologi klasik dan positif. Kedua paradigma itu lebih menitikberatkan pada faktor-faktor yang bersifat fisik dari si pelaku. baik faktor yang bersifat jasmaniah maupun psikologi. Uraian lebih jelas mengenai kedua pemikiran itu dapat dibaca dalam I.S. Susanto, Kriminologi, FH UNDIP, 1995. Kejahatan Korporasi, BP UNDIP, 1995, Romli Atmasasmita, Teon dan Kapita Selektia Kriminologi dan sebagainya serta lihat juga dalam homepage Dian M. DeMelo, *Criminology Theory on the Web*, dapat dijumpai di <http://personal.tmlp.com/ddemelo/crime/classical.html>

proses yang terjadi di dalam masyarakat mengingat pengertian kejahatan bersifat relatif dan jauh dari pengertian absolut.⁹⁴

Membicarakan kejahatan tidak lengkap jika hanya melihat dari segi perbuatannya dan tidaklah disebut kejahatan jika tidak ada korban karena salah satu ciri dari kejahatan adalah adanya korban di samping sifat merugikan dari perbuatan/kejahatan itu dan reaksi sosial atas kejahatan tersebut. Keberadaan korban ini tidak dapat dihindari, tetapi jumlahnya dapat diminimalisir jika orang-orang yang terlibat di dalamnya sudah mengetahui risiko yang akan diterima dan mempersiapkan alat pencegah (dalam hal pokok bahasan ini adalah sistem keamanan yang diperketat/diperkuat).

Kebanyakan korban kurang memperhatikan masalah keamanan ini meskipun mereka menganggap masalah ini sebagai masalah yang penting, bahkan ada yang sama sekali tidak memasang sistem keamanan pada situs yang dikelolanya, seolah-olah mereka percaya bahwa dalam dunia *cyber* ini tidak ada penjahat atau semua *netizen* adalah baik, padahal penjahat dalam jumlah yang besar bergentayangan hampir setiap menit bahkan detik untuk menemukan mangsa yang tepat.

Dengan segala kecerobohan dan kurang hati-hatian yang ada pada pemilik situs, *webmaster* dan *administrator system*, membawa kerugian yang tidak sedikit jumlahnya. Tidak hanya pelayanan situs kepada pengakses yang terganggu, tetapi untuk melakukan *back up* (jika masih ada data yang ada tersedia di lain komputer) memerlukan uang dan waktu yang tidak sedikit.

⁹⁴ I.S. Susanto, "Statistik Kriminal Sebagai Konstruksi Sosial (Penyusunan, Penggunaan dan Penyebarannya, Suatu Studi Kriminologi)", *Ringkasan Disertasi untuk memperoleh Gelar Doktor dalam Ilmu Hukum di UNDIP*, Semarang, 10 Maret 1990, hlm. 1.

Jika kerusakan yang ditimbulkan oleh serangan *cracker* itu sangat vital seperti hilangnya semua data, *log file* dan matinya semua aplikasi dalam sistem komputer, ini merupakan malapetaka yang menunjukkan betapa cerobohnya pemilik, *webmaster* dan *administrator system* dari sistem komputer yang dikelolanya itu.

Cracker dengan aktivitas *hacking-nya* mempunyai sejarah yang panjang, tetapi berdasarkan catatan yang dilakukan oleh Robert H'obbes' Zakon, seorang *Internet Evangelist*, *hacking* yang dilakukan oleh *cracker* pertama kali dilakukan pada tanggal 12 Juni 1995 terhadap *The Spot* dan tanggal 12 Agustus 1995 terhadap *Crackers Movie Page*.⁹⁵

Berdasarkan catatan itu pula, situs pemerintah Indonesia pertama kali mengalami serangan *cracker* pada tahun 1997 sebanyak 5 (lima) kali, yaitu tanggal 19 Januari, 10 Februari, 24 April, 30 Juni dan 30 November. Pada tahun yang sama, situs *NASA* (5 Maret), *UK Conservative Party* (27 April) dan *Spice Girls* (14 November) juga diserang *cracker*.

Sejak serangan yang pertama itu sampai sekarang, korban-korban serangan *cracker* terus berjatuhan. Akan tetapi, hampir sebagian besar tidak terpublikasikan sehingga data yang akurat mengenai berapa jumlah yang telah menderita akibat serangan *cracker* tidak dapat dicatat dan dihitung secara pasti. Indonesia, meskipun dapat dikatakan tertinggal dalam mengikuti dan

⁹⁵ *Hacking* dalam pengertian ini adalah *hacking* yang dilakukan terhadap situs layanan publik, bukan situs penelitian dan juga bukan situs untuk keperluan pendidikan. Lihat dalam Robert H'obbes' Zakon, *loc.cit.* *Hacking* dalam pengertian yang lebih luas telah mulai ada sejak tahun 1961, ketika Laboratorium kecerdasan di MIT memperoleh sebuah POP yang kemudian digunakan oleh mahasiswa MIT untuk melakukan penyusupan-penyusupan. Inilah aksi *hacking* yang pertama, sebagai cikal bakal *cracker-cracker modem*.

menikmati perkembangan teknologi informasi, juga telah menjadi korban *hacking*.

Berikut ini ada beberapa kejadian yang menimpa beberapa situs milik pemerintah dan perusahaan di Indonesia yang telah menjadi korban *cracker* dan dapat diperinci sebagai berikut:

1. Pada tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negeri dan ABRI dijebol oleh *cracker Porto* (Portugis) yang pro-kemerdekaan. Desain depan (*beranda/frontpage*) kedua situs tersebut diganti semua. Aksi yang disebut *East Timor Campaign* menambahkan pada situs yang diserang itu dengan kata-kata antiintegrasi Timor Timur dan antiABRI. Dalam tahun yang sama situs pendidikan yang dalam manifesto *hacker* dilarang untuk disentuh, juga dirusak oleh *cracker*. Situs yang menderita tersebut adalah milik LIPI dan Universitas Airlangga. Selain mereka, situs milik harian *Media Indonesia* juga kena imbas aksi *cracker Porto* itu. Serangan dari *cracker Porto* ini mendapat balasan dari *cracker Indonesia*. Hal ini dilakukan karena menurut mereka *cracker Porto* dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah situs itu milik pemerintah atau bukan, situs bisnis maupun situs pendidikan. *Toxin*, pangkalan Timor-Timur di Internet milik kelompok antiintegrasi dihancurkan dalam serangan balik. Dari semua serangan balik itu, yang paling menghebohkan adalah serangan balik yang tidak saja menghancurkan *homepage* dan sekaligus menghantam salah satu perusahaan penyedia *server* di Irlandia yang bernama **Connect Ireland**, perusahaan yang dikenal sebagai penyedia *server* untuk situs yang beroperasi di bawah *East Timorese Project*, yaitu web yang memperjuangkan kemerdekaan Timor-Timur dari wilayah Indonesia. Serangan balik ini terjadi pada akhir tahun 1999. Menurut keterangan yang diberikan oleh administrator *Connect Ireland*, 18 (delapan belas) serangan dilakukan secara serempak dari seluruh penjuru dunia. Akan tetapi, berdasarkan pengamatan, domain Timor-Timur tersebut *di-hack* dan kemudian ditambahkan *subdomain* yang bernama *need.tp*. Berdasarkan pengamatan yang dilakukan oleh Budi Rahardjo, *need.tp* merupakan sebuah perkataan yang sedang dipopulerkan oleh *Beavis and Butthead* (sebuah acara TV di MTV). Dengan kata lain, *cracker* yang melakukan serangan tersebut kemungkinan penggemar atau paling tidak pernah menonton acara itu. Jadi, kemungkinan dilakukan oleh seseorang dari Amerika Utara.⁹⁶

⁹⁶ Budi Rahardjo, *Op.cit*, hlm. 7.

2. Pada pertengahan tahun 1988, situs milik Pusat Dokumentasi dan Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) yang beralamat di <http://www.pdii.lipi.go.id> di-*hack* oleh orang yang tidak dikenal. Tampilan depan atau *frontpage* PDII LIPI diganti dengan gambar wanita telanjang. Pengelola situs PDII LIPI tidak bisa mendeteksi siapakah yang melakukan penyerangan dan kerusakan terhadap situs yang dikelolanya itu.
3. Tahun 1998, setelah kerusuhan Mei, *cracker* yang diduga berasal dari Cina menghantam situs milik pemerintah. Situs yang tidak beruntung itu adalah situs *web* milik BKKBN (Badan Koordinasi Keluarga Berencana Nasional) yang diserang oleh *cracker* yang menyebut dirinya *Discover*. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan. Tidak hanya merusak situs *web* milik BKKBN, mereka juga mengancam akan merusak situs-situs milik pemerintah Indonesia yang lain.
4. Juni 1999, *cracker* lokal menyerang *homepage* lokal. Kali ini yang menjadi korban adalah *homepage* POLRI. *Frontpage* atau gambar depan dari *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip dengan logo atau gambar PDI-P.
5. Pada Januari 2000, beberapa situs web Indonesia diacak-acak oleh *cracker* yang menamakan dirinya *fabianclone* dan *naisenodni*. Situs yang diserang antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.
6. Pada tanggal 11 Januari 2000, situs penerbitan buku-buku Islam yang beralamat di <http://www.mizan.com> diserang oleh *cracker* yang menamakan dirinya sebagai Hotmilk@www.com. Akibat serangan itu, seorang yang hendak membuka situs Mizan tidak mendapatkan tampilan yang seharusnya, tetapi akan menjumpai pesan yang disampaikan oleh *cracker* dalam bahasa Inggris. Haidar Bagir, pemilik Penerbitan Mizan menduga *cracker* yang menyerang situs miliknya berasal dari Australia.⁹⁷
7. September dan Oktober 2000, seorang *cracker* dengan julukan *Fabian Clone* berhasil menjebol *web* milik Bank Bali. Sebelumnya, Fabian Clone juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking* pada nasabahnya sehingga

⁹⁷ Bunyi pesan tersebut kira-kira seperti ini: "Maaf, sebetulnya kami hanya mencoba sistem keamanan anda, dan ternyata kami dapati bahwa sistem keamanan anda sangat rapuh. Pembuat sistem keamanan anda (dia menggunakan kata makian) ... suatu hari nanti anda harus berhati-hati, atau sewaktu-waktu kami akan kembali dan melakukan kerusakan lebih dari yang sekarang ini. Jadi, tidak usah mencoba mencari tahu siapa saya, cari saya si pembuat sistem keamanan. Ha ... ha... ha ... kami masuk ke *server* dan *website* anda tanpa izin. Hati-hati kawan. Salam dari Hotmilk@www.com. Republika, 16 Januari 2000, hlm. 15.

kerugian yang diderita lebih besar dibandingkan dengan kerugian yang diderita BEJ termasuk terputusnya layanan terhadap nasabah.

8. Pada pertengahan Januari 2001, situs milik PT Ajinomoto Indonesia diserang *cracker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* yang digunakan sebagai katalis dalam proses pembuatan *monosodium glutamate* (bumbu penyedap rasa) yang mengandung lemak babi. Akibat ulah *cracker* pada situs PT Ajinomoto yang beralamat di <http://www.mjk.ajinomoto.co.id>, ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K*. Di samping itu, terdapat juga tampilan tulisan yang berwarna-warni yang muncul silih berganti dengan menggunakan bahasa Jawa yang jika dirangka akan berbunyi "*Ajinomoto You Lied to Us*". Di bawah gambar babi tertulis *Ajinomoto gift. This little pig went to the Ajinomoto* dan pada bagian judul halaman tersebut terdapat *kalimat* "*Ajinomoto: HARAM ... HARAM... HARAM*". Situs ini di-*hack* oleh seorang *cracker* yang bernama boyons dengan alamat e-mail boyons@crackermail.com.
9. Setelah mendapat serangan pada pertengahan tahun 1998, situs RDM LIPI kembali diserang oleh *cracker* yang sekali lagi tidak dapat diidentifikasi karena tidak meninggalkan jejak. Kerusakan yang ditimbulkan tidak seberapa dibandingkan dengan serangan pertama, karena yang diserang adalah bagian yang disediakan untuk buku tamu dan buku saran/kritik. Bagian tersebut sama sekali hilang dari situs atau dengan kata lain dihapus oleh *cracker*. Serangan ini tidak menyebabkan layanan publik PDII LIPI menjadi terhenti.
10. April 2001, situs *web* milik Departemen Agama dan Departemen Perindustrian dan Perdagangan dirusak oleh *cracker*. Situs milik Departemen Perindustrian dan Perdagangan tidak sekadar dirusak, tetapi file-file penting dan *log file*-nya dihapus, sehingga administrator sistemnya tidak bisa mendeteksi siapa yang melakukan penyerangan, lagi pula *cracker* tersebut tidak meninggalkan jejak sehingga menyulitkan penelusuran. Untung saja pihak Departemen Perindustrian dan Perdagangan mempunyai *back up* sehingga kerusakan dapat segera diperbaiki.
11. Pada tanggal 8 Mei 2001, situs resmi Kepolisian Republik Indonesia yang beralamat di <http://www.polri.go.id>, sekitar 10 (sepuluh) menit tidak bisa tampil atau tidak dapat diakses karena mendapat serangan dari *cracker* yang menamakan dirinya Kesatuan Aksi *Cracker* Muslimin Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

12. Pada tanggal 25 Mei 2001, situs Riset Unggulan Terpadu (RUT) yang dikelola oleh LIPI dan beralamat di <http://www.rut.lipi.go.id> diserang oleh *cracker* yang berhasil diidentifikasi. Serangan itu dibuat oleh *Hacking from C.OS of P.P.C at yeah net*. Serangan ini menyebabkan layanan situs RUT macet total untuk beberapa saat karena data-data penting yang tersedia di situ beserta *log file* dan aplikasinya dihapus oleh *cracker*. Korban-korban *cracker* yang tersebut di atas adalah korban *cracker* sampai akhir Mei 2001. Mengingat perkembangan teknologi informasi yang tiap hari terus berubah dan jumlah *hacker*, *cracker* serta *vandal* komputer semakin bertambah dan ketertutupan korban *hacking* terhadap publikasi atau laporan ke polisi, ada kemungkinan jumlahnya akan terus bertambah. Jumlah korban *cracker* yang telah disebutkan tidak mencerminkan korban *hacking* secara keseluruhan karena banyak korban yang tidak berani mengemukakan atau menyatakan kepada publik bahwa situs yang dikelolanya telah menjadi korban *hacking*.
13. Selanjutnya pada hari Minggu, tanggal 17 Maret 2007 pukul 05.30 Wib, situs resmi Presiden Susilo Bambang Yudhoyono (www.presidensby.info) dibobol *hacker*. Halaman utama situs yang dikelola juru bicara Kepresidenan Andi Mallarangeng itu berubah tampilannya menjadi surat tuntutan yang ditujukan kepada SBY. Pengirim surat mengatasnamakan *on behalf underground community* dan beralamat di *the word where the devils gather*. Komunitas tersebut mengeluarkan tiga tuntutan pertama meminta penurunan harga *bandwith*, agar masyarakat bisa menikmati internet, kedua, meminta SBY mendukung dan melaksanakan IGOS (*Indonesia Go Open Source*) dan yang ketiga, Menuntut pemberantasan korupsi, kolusi, dan nepotisme (KKN), pornografi dan porno aksi).⁹⁸

C. Hukum Pidana dan Perkembangan Teknologi

Kejahatan sesungguhnya merupakan sesuatu hal yang tak lepas dari sejarah panjang umat manusia di muka bumi ini. Dan pembicaraan mengenai kriminologi dengan teori-teorinya yang telah berkembang tidak akan berhenti selama masih ada kejahatan di masyarakat. Akan tetapi, pembicaraan itu tidak bisa dilepaskan dari institusi lain karena ada keterkaitan yang sangat erat antara kriminologi dengan institusi itu, yaitu hukum terutama hukum pidana,

⁹⁸ Riau Pos, *Op.cit*, hlm.1.

bahkan sejak kelahirannya kriminologi dan hukum pidana mempunyai hubungan yang sangat erat.

Hukum memiliki keterikatan yang sangat luas dengan berbagai bidang ilmu, bahkan penguasaan ilmu hukum secara tunggal tidak akan dapat memecahkan masalah yang dihadapi masyarakat, sehingga diperlukan pengetahuan lain agar pemahaman terhadap permasalahan menjadi lebih jelas, tajam dan tidak simpangsiur. Dengan berbekal pengetahuan hukum dan pengetahuan sosial lain, seperti sosiologi, psikologi, antropologi, religi, ekonomi, politik dan budaya maka diagnosis mengenai kesulitan-kesulitan yang dihadapi masyarakat dapat lebih cermat dan pemecahannya pun lebih dapat diterima oleh masyarakat.

Mulyana W. Kusuma bahkan mengatakan bahwa:

“Perkembangan kriminologi dari dahulu sampai sekarang tidak bisa dilepaskan dari keberadaan hukum pidana dan sosiologi hukum itu sendiri. Kriminologi, sosiologi dan hukum pidana memiliki lahan kajian yang satu sama lain saling berkaitan, sehingga tidak mengherankan apabila dengan memberdayakan ketiga kajian itu secara integral akan diperoleh pemahaman yang lebih baik dan mendekati kebutuhan senyatanya mengenai realitas kejahatan yang ada di masyarakat”.⁹⁹

Kriminologi, khususnya sebagai pengaruh pemikiran kritis mengarahkan studinya pada proses-proses (kriminalisasi), baik proses pembuatan maupun bekerjanya undang-undang, dapat memberikan sumbangan besar di bidang sistem peradilan pidana khususnya berupa

⁹⁹ Mulyana W. Kusuma, *Realitas Sosial Kejahatan*, Prisma, LP3ES, Jakarta, 1982, hlm. 39.

penelitian tentang penegakan hukum sehingga dapat digunakan untuk memperbaiki bekerjanya aparat penegak hukum.¹⁰⁰

Perkembangan teknologi juga membawa dampak dalam perkembangan hukum pidana. Kajian yang dilakukan oleh kriminologi dapat dijadikan sebagai sarana untuk membangun hukum pidana yang didasarkan pada alasan-alasan logis hasil pemikiran kriminologis. Sampai tahap tertentu pemikiran kriminologis penting untuk perkembangan teori kriminologi dan pada tahap selanjutnya penting untuk ilmu hukum pidana terutama dalam kaitannya dengan persoalan kriminalisasi, dekriminalisasi dan depenalisasi.

Permasalahan kriminalisasi, dekriminalisasi dan depenalisasi adalah bidang kajian hukum pidana yang erat kaitannya dengan kriminologi. Ketiganya tidak bisa dilepaskan dari kriminologi apabila ingin mendapatkan pengetahuan yang luas dan keputusan yang komprehensif mengenai suatu masalah yang hendak dikriminalkan, didekriminalisasi atau didepenalisasi. Tanpa kajian kriminologi hukum pidana sebenarnya bisa melakukan ketiga hal tersebut, tetapi hasil yang dicapai tentunya tidak akan selengkap dan sebaik apabila menggunakan bantuan kriminologi.

Menurut Sudarto bahwa:

“Kriminalisasi merupakan suatu proses penetapan suatu perbuatan yang semula bukan tindak pidana menjadi tindak pidana. Untuk menetapkan suatu perbuatan yang sebelumnya tidak dikategorikan sebagai tindak pidana menjadi perbuatan yang dikategorikan sebagai tindak pidana bukanlah suatu pekerjaan yang mudah. Proses kriminalisasi berakhir dengan terbentuknya undang-undang yang menetapkan perbuatan yang itu dilarang dan diancam dengan sanksi yang berupa pidana”.¹⁰¹

¹⁰⁰ I.S. Susanto, *Kriminologi*, FH UNDIP Semarang, 1995, hlm. 14.

¹⁰¹ Sudarto, *Hukum dan Hukum Pidana*,...*Op.cit*, hlm. 32 dan hlm. 151.

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.¹⁰²

Hukum pidana mempunyai sifat *ultimum remedium* atau alat terakhir yang berisi pengenaan penderitaan kepada pelaku kejahatan. Sifat hukum pidana ini menyebabkan hukum pidana dinilai sangat kejam sehingga pengenaannya haruslah merupakan upaya terakhir apabila upaya-upaya lain tidak dapat dilakukan untuk memperbaiki pelaku kejahatan. Mengingat sifat kejamnya hukum pidana ini, maka penetapan suatu perbuatan dengan ancaman hukumannya haruslah memperhatikan berbagai aspek kemanusiaan. Proses kriminalisasi dalam hal ini tidak boleh dilakukan sembarangan karena hal ini menyangkut harkat, martabat dan hak asasi manusia untuk hidup.

Penetapan suatu perbuatan menjadi tindak pidana atau bukan haruslah didasarkan pada pertimbangan yang matang. Penetapan ini harus dijauhkan dari unsur-unsur politis sehingga mereka yang mempunyai kekuasaan tidak dapat mempengaruhi pembuat undang-undang agar perbuatan jahatnya tidak terkena jerat hukum. Meskipun ada anggapan bahwa undang-undang adalah hasil dari kompromi politis, tetapi sebisa mungkin unsur politis yang

¹⁰² *Ibid*, hlm. 36.

merugikan berbagai pihak (terutama mereka yang tidak mempunyai kekuasaan untuk mempengaruhi pembuat undang-undang) dapat ditekan atau diminimalisir.

Penetapan suatu perbuatan menjadi tindak pidana harus pula memperhatikan perbandingan antara sarana dan hasil serta kemampuan aparat penegak hukum. Apabila sarana yang diperlukan dan kemampuan aparatnya tidak memadai, maka penetapan suatu perbuatan menjadi tindak pidana menjadi tidak berarti karena sarana untuk menegakkannya tidak ada sehingga penetapan itu hanya menjadi macan kertas saja, tidak ada implementasinya dan hanya merupakan pemborosan anggaran negara.

Dari uraian tersebut, maka dapatlah dikatakan bahwa proses kriminalisasi merupakan proses yang tidak hanya bersifat sosial, tetapi juga politis. Pandangan hidup yang ada dan dipelihara oleh masyarakat atau pemegang kekuasaan akan mewarnai hasil kriminalisasi.

Sudarto juga mengatakan bahwa:

“Dekriminalisasi adalah suatu proses penghapusan sama sekali sifat dapat dipidananya suatu perbuatan yang semula merupakan tindak pidana dan juga penghapusan sanksinya berupa pidana. Dalam proses dekriminalisasi ini tidak hanya kualifikasi pidana saja yang dihapuskan,”tetapi juga sifat melawan hukum atau melanggar hukumnya, lebih dari itu adalah penghapusan sanksi negatif itu tidak diganti dengan reaksi sosial lain, baik perdata maupun administrasi”.¹⁰³

Dalam proses dekriminalisasi ini penelitian kriminologi diperlukan untuk menentukan apakah perbuatan itu layak didekriminalisasikan dan bagaimana kemungkinannya di masa yang akan datang. Tidak menutup

¹⁰³ *Ibid*, hal. 32.

kemungkinan perbuatan yang telah didekriminalisasikan di masa mendatang oleh masyarakat dituntut untuk dikriminalisasikan sehingga kajian mengenai manfaat dan kerugian dekriminalisasi haruslah mendapat perhatian.

Suatu proses dekriminalisasi dapat terjadi karena beberapa sebab, seperti misalnya (contoh ini tidak bersifat limitatif):¹⁰⁴

1. Suatu sanksi secara sosiologis merupakan persetujuan (sanksi positif) atau penolakan terhadap pola perilaku tertentu (sanksi negatif). Ada kemungkinan bahwa nilai-nilai masyarakat mengenai sanksi negatif tertentu terhadap perilaku tertentu mengalami perubahan, sehingga perilaku yang terkena sanksi-sanksi tersebut tidak lagi ditolak.
2. Timbulnya keragu-raguan yang sangat kuat akan tujuan yang ingin dicapai dengan penetapan sanksi-sanksi negatif tertentu.
3. Adanya keyakinan yang kuat, bahwa biaya sosial untuk menerapkan sanksi-sanksi negatif tertentu sangat besar.
4. Sangat terbatasnya efektivitas dari sanksi-sanksi negatif tertentu sehingga penerapannya akan menimbulkan kepudaran kewibawaan hukum.

Dalam kaitannya dengan kriminalisasi dan dekriminalisasi ini, Simposium Pembaharuan Hukum Pidana Nasional pada bulan Agustus 1980 dalam salah satu laporannya menyatakan:¹⁰⁵

“Masalah kriminalisasi dan dekriminalisasi atas suatu perbuatan haruslah sesuai dengan politik kriminil yang dianut oleh bangsa Indonesia, yaitu sejauh mana perbuatan tersebut bertentangan atau tidak bertentangan dengan nilai-nilai fundamental yang berlaku dalam masyarakat dan oleh masyarakat dianggap patut atau tidak patut dihukum dalam rangka menyelenggarakan kesejahteraan masyarakat.”

¹⁰⁴ Soerjono Soekanto et.al., *Kriminologi, Suatu Pengantar*, ctk. Pertama. Ghalian Indonesia, Jakarta, 1986. hal. 47-48.

¹⁰⁵ Laporan Simposium Pembaharuan Hukum Pidana Nasional 1980 di Semarang. seperti dikutip oleh Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Hukum Pidana*, BP UNDIP Semarang, 1994. hal. 36.

Khusus mengenai kriteria kriminalisasi dan dekriminalisasi, laporan simposium itu menyatakan untuk menetapkan suatu perbuatan itu sebagai tindakan kriminil, perlu memperhatikan kriteria umum sebagai berikut:

1. Apakah perbuatan itu tidak disukai atau dibenci oleh masyarakat karena merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban;
2. Apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya *cost* pembuatan undang-undang, pengawasan dan penegakan hukum, serta beban yang dipikul korban, pelaku dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai;
3. Apakah akan makin menambah beban aparat penegak hukum yang tidak seimbang atau nyata-nyata tidak dapat diemban oleh kemampuan yang dimilikinya;
4. Apakah perbuatan-perbuatan itu menghambat atau menghalangi cita-cita bangsa Indonesia, sehingga merupakan bahaya bagi keseluruhan masyarakat.¹⁰⁶

Depenalisasi merupakan proses penghapusan ancaman pidana (sehingga ancaman pidananya itu hilang) terhadap perbuatan yang semula merupakan tindak pidana, tetapi masih dimungkinkan adanya penuntutan secara lain.¹⁰⁷ Hal ini dapat dilakukan mengingat sifat hukum pidana sebagai *ultimum remedium*, di mana ancaman pidana yang ada dianggap tidak aspiratif atau terlalu berat, sehingga perlu diganti dengan ancaman pidana lain yang lebih ringan dan manusiawi.

¹⁰⁶ Bandingkan dengan kriteria yang dikemukakan oleh Bassisouni dalam Barda Nawawi Arief, *ibid*, hlm. 36-37.

¹⁰⁷ Sudarto, *Hukum dan Hukum Pidana, ...Op.cit.*, hlm. 151.

BAB IV

PENGATURAN *CYBER CRIME* DALAM HUKUM PIDANA INDONESIA

A. Pengaturan *Cyber Crime* dalam Hukum Pidana Positif Indonesia

Perkembangan teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat.

Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.¹⁰⁸

Pada perkembangannya, dengan ditemukannya komputer sebagai bagian dari kemampuan produk ilmu pengetahuan dan teknologi, terjadilah konvergensi antara teknologi telekomunikasi, media dan komputer. Konvergensi antara teknologi komunikasi, media dan komputer menghasilkan sarana baru yang disebut dengan internet. Internet telah memberikan sesuatu yang sama sekali baru pada umat manusia.

Kecanggihan peralatan tersebut menunjang kebutuhan hidup manusia, bahkan menembus batas-batas apa yang dahulu tidak terbayang akan bisa

¹⁰⁸ Ahmad M. Ramli, *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, ctk. Pertama, Refika Aditama, Bandung, 2004, hlm. 1.

diwujudkan. Sebagai gambaran, ditemukannya alat pemacu jantung yang dikendalikan dari jarak jauh (*computer operation system*), sehingga sangat berguna sebagai pertolongan pertama bagi yang mengalami gangguan jantung sebelum dilarikan ke rumah sakit.¹⁰⁹

Meningkatnya hubungan tiap komponen masyarakat yang berkaitan dengan tuntutan untuk memenuhi kebutuhan hidup seperti transaksi ekonomi antar negara telah melampaui batas-batas wilayah yang selama ini dibatasi oleh rintangan geografis karena ditemukannya internet.¹¹⁰

Abdul Wahid mengatakan bahwa:

“Internet merupakan sekumpulan jaringan komputer yang menghubungkan situs akademik, pemerintah, komersial, organisasi maupun perorangan. Internet menyediakan akses untuk pelayanan telekomunikasi dan sumberdaya informasi untuk jutaan pemakainya yang tersebar di seluruh dunia”.¹¹¹

Menurut Al.Wisnubroto, Internet berasal dari kata *interconnection networking*, yaitu hubungan berbagai komputer dengan berbagai tipe yang membentuk sistem jaringan yang mencakup seluruh dunia (jaringan komputer global) dengan melalui jalur komunikasi seperti telepon atau satelit.¹¹²

Internet yang telah diidefinisikan oleh *The US Supreme Court* sebagai “*International Network of Interconnected Computer*” telah menghadirkan

¹⁰⁹ Aroma Elmina Martha, *Op.cit*, hlm. 4.

¹¹⁰ *Ibid*

¹¹¹ Abdul Wahid, *et.al*, *Kejahatan Mayantara (Cyber Crime)*, ctk. Pertama, Refika Aditama, Bandung, 2005, hlm. 24

¹¹² Al. Wisnubroto, *Op.cit*, hlm. 31.

kemudahan-kemudahan bagi setiap orang, bukan saja untuk berkomunikasi tapi juga melakukan transaksi bisnis kapan saja dan di mana saja.¹¹³

Dengan internet manusia dapat melakukan aktivitas layaknya kehidupan di dunia nyata (*real*). Manusia dapat melakukan berbagai aktivitas di sana seperti *ngobrol*, *kongkow-kongkow*, transaksi bisnis dan lain sebagainya. Internet seakan membentuk suatu realitas baru yang menjadikannya realitas kehidupan manusia terbagi secara dikotomis menjadi *real life* (kehidupan nyata) dan *virtual life* (kehidupan maya).¹¹⁴

Seorang yang ingin membeli barang tak perlu datang ke tempat penjual untuk melihat barang yang akan dibeli atau orang yang gemar *shopping* tak perlu bersusah payah ke mal, tapi cukup di depan komputer yang disambung jaringan internet dengan menekan tuts-tuts pada komputer terlihatlah barang yang diinginkan.

Selanjutnya, bila tertarik dapat dilakukan transaksi dengan memasukan nomor kredit beserta alamat rumah. Langsung barang dikirim. Hal ini tentunya sangat mudah. Aktivitas di dalam internet dapat menjangkau seluruh belahan bumi dengan melampaui batas-batas negara. Sesuatu yang dalam dunia nyata jauh dari harapan kita, dalam dunia maya dapat kita hadirkan di hadapan kita.

Penerapan teknologi internet melalui sarana komputer yang saling terkoneksi dari suatu wilayah dengan wilayah lain menjadi batasan-batasan alam yang selama ini menjadi penghambat komunikasi atau transaksi antar negara seakan menjadi hilang.

¹¹³ Ari Julianto, *Cyber Crime: Sebuah Fenomena di Dunia Maya, dapat dijumpai dalam situs di internet*, <http://www.Theceli.com/dokumen/jurnal/ajo/a002.shtml>.

¹¹⁴ Abdul Wahid, *et.al*, *Op.cit*, hlm. 24.

Layanan internet meliputi komunikasi langsung (*E-mail, Chat*), diskusi (*Usenet, News, E-mail, Milis*), sumberdaya informasi yang terdistribusi (*World wide web, Gopher*), *remote login* dan lalu lintas *life* (*Telnet, FTP*), dan aneka layanan lainnya.¹¹⁵

Di antara layanan yang diberikan internet yang dikenal dan umum dilakukan antara lain :¹¹⁶

1. *E-Commerce*, contoh paling umum dari kegiatan ini adalah aktivitas transaksi perdagangan umum melalui internet. Dengan memanfaatkan *E-Commerce*, para penjual (*merchant*) dapat menjajakan produknya secara lintas negara, hal ini karena sifat internet sendiri yang melintasi batas negara. Transaksi dapat terjadi secara *real time* dimana saja, asal terhubung dengan internet. Umumnya transaksi melalui sarana *E-Commerce* dilakukan melalui sarana suatu situs *web* yang dalam hal ini berlaku sebagai semacam etalase bagi produk yang dijajakan. Dari situs ini pembeli dapat melihat barang yang ingin dibeli, lalu bila tertarik dapat melakukan transaksi dan seterusnya.
2. *E-Banking*, hal ini diartikan sebagai aktivitas perbankan di dunia maya (*virtual*) melalui sarana internet. Layanan ini memungkinkan pihak bank dan nasabah bank dapat melakukan berbagai jenis transaksi perbankan melalui sarana internet, khususnya via *web*. Lewat sarana internet seseorang dapat melakukan pengecekan saldo tabungan, transfer dana antar rekening hingga melakukan pembayaran tagihan dan lain sebagainya.
3. *E-Government*, ini bukan merupakan pemerintahan model baru yang berbasis dunia internet, tapi merupakan pemanfaatan teknologi internet untuk bidang pemerintahan. Pemerintah dalam memberikan layanan publik dapat menggunakan sarana ini. Dengan membuat suatu situs tertentu pemerintah dapat memberikan informasi tentang kebijakan pemerintah mulai regulasi sampai program-program sehingga dapat diketahui publik yang mengaksesnya. Dalam kerangka demokrasi dan untuk mewujudkan *clean government* dan *good governance* ini tentu sangat menarik sekali.
4. *E-Learning*, istilah ini didefinisikan sebagai sekolah di dunia maya (*virtual*). Definisi *e-learning* sendiri sesungguhnya sangat luas, bahkan sebuah portal informasi tentang suatu topik juga dapat tercakup dalam *e-learning* ini. Namun pada prinsipnya istilah ini ditujukan pada usaha

¹¹⁵ *Ibid*, hlm. 25.

¹¹⁶ <http://dhani.singcat.com/internet/modul.php>. 18 Maret 2007.

untuk membuat transformasi proses belajar mengajar di sekolah dalam bentuk digital yang dijumpai oleh teknologi internet.

Kemajuan teknologi yang merupakan hasil budaya manusia di samping membawa dampak positif, dalam arti dapat dimanfaatkan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan.

J.E. Sahetapy telah menyatakan dalam tulisannya, bahwa:

“Kejahatan erat kaitannya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya”.¹¹⁷

Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau komunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cyber crime*. Barda Nawawi Arief menggunakan istilah tindak pidana mayantara untuk menunjukan jenis kejahatan ini.¹¹⁸

Dengan kata lain *cyber crime* merupakan tindak pidana dengan menggunakan teknologi informasi sebagai wahana sasaran. Teknologi informasi yang dimaksud di sini adalah media komputer yang terkoneksi dengan jaringan internet.¹¹⁹

“Secara sederhana, yang dimaksud dengan *cyber crime* adalah setiap tindakan atau perilaku yang melanggar atau melawan hukum, etika atau tanpa kewenangan yang menyangkut pemerosesan data dan/atau

¹¹⁷ Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer*, ctk. Pertama, Lembaga Penerbit Fakultas Hukum Unisba, Malang, 2002, hlm. 21.

¹¹⁸ Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, ctk. Pertama, Citra Aditiya Bakti Bandung, 2003, hlm. 255.

¹¹⁹ Aroma Elmina Martha, *Op.cit*, hlm. 10.

pengiriman data. Umumnya perbuatan tersebut dilakukan dengan melalui perangkat digital dalam suatu dunia maya (*cyber*)”.¹²⁰

Definisi *cyber crime* diatas dapat diartikan sebagai berikut: “*cyber crime*” adalah kejahatan di dunia *cyber* atau dunia *virtual* dengan menggunakan teknologi tinggi. Kejahatan ini juga dapat didefinisikan sebagai kejahatan di mana teknologi informasi merupakan target dari kejahatan atau di mana teknologi informasi dipergunakan sebagai sarana atau alat untuk melakukan kejahatan.

Dengan kata lain kejahatan menggunakan teknologi informasi, teknologi informasi sebagai alat, teknologi informasi sebagai tempat penyimpanan, dan teknologi informasi sebagai target.

Dari definisi diatas, kita bisa mengetahui unsur dari *cyber crime* sebagai berikut.¹²¹

1. Perbuatan yang bertentangan dengan hukum, etika dan tanpa kewenangan.
2. Menggunakan teknologi tinggi atau digital
3. Dengan teknologi informasi sebagai sasaran atau sarana kejahatan
4. Di dunia *cyber*.

Selanjutnya di sini muncul pertanyaan apa perbedaan *cyber crime* dengan *computer crime*? Samakah *cyber crime* dengan *komputer crime* ? seringkali *cyber crime* disamakan dengan *computer crime*, di mana hal ini

¹²⁰ M. Zaenal Arifin *et.al*, “Modus Operandi Cyber Crime di Indonesia Makin Canggih” Artikel dalam Analisis Hukum 2002, Jangan Tunggu Langit Runtuh, Jakarta, *hukumonline.com*, Justika Siar Publika, 2003, hlm. 155.

¹²¹ Aroma Elmina Martha, *Op.cit*, hlm. 11.

muncul apabila kita mengacu kepada sejumlah rumusan mengenai *computer crime* antara lain:¹²²

1. Perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih.
2. Perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan orang lain.
3. Definisi menurut *Encyclopedia of crime and Justice*, yang dimaksud dengan *computer crime* adalah setiap tindakan *ilegal* yang membutuhkan pengetahuan tentang teknologi komputer guna dapat melakukan kejahatan, penyidikan atau penuntutan, sehingga ada dua kategori, yaitu komputer sebagai alat untuk sesuatu kejahatan dan yang kedua adalah komputer sebagai objek dari suatu kejahatan.

Melihat rumusan pengertian maupun unsur di atas, dapat dengan mudah mengetahui bahwa *cyber crime* dan *computer crime* memang memiliki kesamaan, namun sesungguhnya keduanya berbeda. Kesamaan keduanya adalah baik *cyber crime* maupun *computer crime* sama-sama menggunakan teknologi tinggi (komputer dan perangkat pendukungnya) sebagai sarana atau sarana kejahatan, namun dalam *cyber crime* lingkup kejahatannya lebih luas karena sistem komputer yang digunakan sebagai sarana sekaligus terkoneksi dengan sistem jaringan internet (memanfaatkan teknologi telekomunikasi).¹²³

Dalam *computer crime*, kejahatan dilakukan hanya pada lingkup wilayah sempit tanpa menggunakan media internet, misalnya dalam satu perusahaan yang sama. Dalam *cyber crime* yang mempergunakan teknologi informasi dan telekomunikasi itulah maka *cyber crime* menjadi suatu bentuk tindak pidana baru yang bersifat global dan *mobile*, dapat dilakukan dimana

¹²² *Ibid*, hlm. 11.

¹²³ *Ibid*, hlm. 12.

saja tanpa mengenal batas negara sepanjang terjangkau oleh fasilitas internet.¹²⁴

Jadi penggunaan sarana teknologi dengan lingkup global (internet), merupakan perbedaan antara *cyber crime* dengan *computer crime* yang menggunakan jaringan lokal dari teknologi informasi.

Dari paparan tersebut tampak bahwa terhadap *computer crime*, masih dimungkinkan menggunakan regulasi yang bersifat lokal, selain juga yuridiksinya jelas. Sementara itu dalam *cyber crime* sulit ditentukan yuridiksinya. Karena *locus delicti* dari kejahatan tersebut berada dalam dunia maya. Dunia maya ini sifatnya melampaui wilayah teritorial negara.¹²⁵

Dengan demikian dari sudut alat yang digunakan (komputer), maka dalam kaitan antara *cyber crime* dengan *computer crime* dapat disimpulkan bahwa *cyber crime* termasuk bagian dari *computer crime*. Singkatnya *cyber crime* juga bisa disebut sebagai *computer crime*. Dalam perspektif ini bisa dipahami bila *cyber crime* diidentikkan dengan *computer crime*. Tapi dalam perkembangannya identifikasi ini tidak relevan lagi, karena pelaku tidak harus menggunakan komputer sebagai alat dalam aksinya.¹²⁶

Untuk Lebih menjelaskan perbedaan antara *cyber crime* dengan *computer crime* dapat dilihat dari bagan yang dilukiskan oleh Agus Raharjo sebagai berikut:¹²⁷

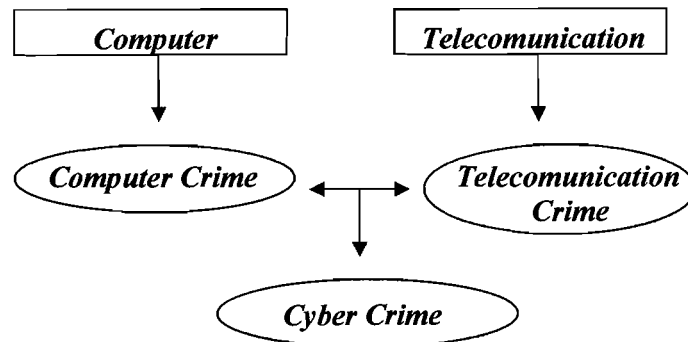
¹²⁴ *Ibid*, hlm. 14.

¹²⁵ Achmad Ali, "Hukum dan Teknologi" *Makalah dalam seri diskusi panel PII*, Bandung, 17 Mei 2003 dapat dijumpai dalam situs di Internet: <http://www.pii.or.id/dunia-ir/di0803no02seminar1.html>.

¹²⁶ <http://www.theceli.com.dokumen/jurnal/ajo/a002.shtml>, 25 Nopember 2006.

¹²⁷ Agus Raharjo, *Op.cit*, hlm. 228.

Perbedaan *Computer Crime* dan *Cyber Crime*



Ade Manan Suherman menyatakan bahwa menurut NCIS Inggris, manifestasi dari tindak kejahatan *cyber crime* muncul dalam berbagai macam atau variasi seperti berikut ini :¹²⁸

1. *Recreational Hackers*

Kejahatan ini dilakukan oleh *netter* tingkat pemula untuk sekedar mencoba kekuranghandalan sistem sekuritas suatu perusahaan.

2. *Crackers atau Criminal Minded Hackers*

Pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, *sabotase*, dan penghancuran data. Sebagai contoh, pada tahun 1994 *Citibank AS* kebobolan senilai 400.000 dolar oleh *cracker* dari Rusia yang akhirnya dijatuhi hukuman penjara selama tiga tahun serta harus mengembalikan sejumlah uang tersebut. Tipe kejahatan ini dapat terjadi dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis

3. *Political Hackers*

Aktivis politis atau lebih populer dengan sebutan *hactivist* melakukan perusakan terhadap ratusan *situs web* untuk mengkampanyekan program-programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendeskriditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan konsisten dalam usaha untuk kampanye anti-Indonesia dalam masalah Timor-Timur yang dipelopori oleh Ramos Horta. Situs *Deplu* sempat mendapat serangan yang diduga keras dari kelompok anti-integrasi.

4. *Denial of Service Attack*

Serangan *denial of service attack* atau *FBI* dikenal dengan istilah "*unprecedented*" tujuannya adalah untuk memacetkan sistem dengan

¹²⁸ Ade Manan Suherman, *Aspek Hukum dalam Ekonomi Global*, ctk. Pertama, Ghalian Indonesia, Jakarta, 2002, hlm. 168-171.

mengganggu akses dari pengguna yang *legitimate*. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs *web* dengan data yang tidak perlu. Pemilik situs *web* menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs *web* memakan waktu yang tidak sedikit

5. *Insiders atau Internal Hackers*

Insider hackers ini bisa dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan. Departemen Perdagangan dan Industri Inggris mengumumkan bahwa pada tahun 1998 perusahaan-perusahaan telah menderita kerugian senilai 1,5 miliar poundsterling

6. *Viruses*

Program pengganggu (*malicious*) dengan penyebaran virus dewasa ini dapat menular melalui aplikasi internet. Sebelumnya, pola penularan virus hanya bisa melalui *floppy disk*. Virus bisa bersembunyi dalam file dan *terdown load oleh user* bahkan bisa menyebar melalui kiriman *e-mail*. Seperti halnya dunia kedokteran, dunia komputer telah menciptakan jurus anti virus, seperti *melissa* 1999 atau *lovebug* 2000, tetapi masih belum bisa berbuat banyak.

7. *Piracy*

Pembajakan *software* merupakan *trend* dewasa ini. Pihak produsen *software* dapat kehilangan *profit* karena karyanya dapat dibajak melalui *down load* dari internet dan dikopi ke dalam CD-ROM yang selanjutnya diperbanyak secara ilegal atau tanpa seizin penciptanya.

8. *Fraud*

Fraud adalah segala jenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya. Contohnya, harga tukar saham yang menyesatkan melalui rumor. Situs lelang fiktif dengan mengeruk uang masuk dari para peserta lelang dan barangnya tidak dikirim bahkan identitas pelakunya tidak dapat dilacak.

9. *Gambling*

Perjudian di dunia *siber* yang berskala global sulit dijerat dengan hukum nasional suatu negara. *Dart* kegiatan *gambling* dapat diputar kembali di negara yang merupakan *tax heaven*, seperti *Cayman Islands* merupakan surga bagi *money laundering*.

10. *Pornography and Pedophilia*

Dunia *cyber* selain mendatangkan berbagai kemudahan dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dunia pornografi yang mengkhawatirkan berbagai kalangan. Melalui *news group*, *chat rooms* mengeksploitasi pornografi anak-anak di bawah umur.

11. *Cyber-Stalking*

Cyber-Stalking adalah segala bentuk kiriman *e-mail* yang tidak dikehendaki oleh *user* atau *junk e-mail* yang sering memadati *folder* serta tidak jarang dengan pemaksaan walaupun *e-mail "sampah"* tidak dikehendaki oleh *user* bahkan tidak jarang secara paksa memperoleh identitas personal secara detail calon para korbannya.

12. *Hate Sites*

Situs ini sering dipergunakan untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para ekstrimis. Penyerangan terhadap lawan atau *opponent* sering mengangkat isu rasial, perang program dan promosi kebijakan atau suatu pandangan.

13. *Criminal Communication*

NCIS telah mendeteksi bahwa internet telah dijadikan sebagai alat yang handal dan modern untuk melakukan komunikasi antar *gangster*, anggota sindikat obat bius, dan komunikasi antar *hooligan* di dunia sepak bola.¹²⁹

Di lain pihak, Ari Julianto Gema menyatakan bahwa dalam beberapa literatur dan praktik kejahatan yang berhubungan dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi (*cyber Crime*) dikelompokkan dalam beberapa bentuk yaitu:¹³⁰

1. *Unauthorized Acces to Computer System and Servis*. Kejahatan ini dilakukan dengan memasuki/menyusuf ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik jaringan komputer yang dimasukinya. Motifnya bisa bermacam-macam, antara lain adalah *sabotase*, pencurian data dsb. Sebagai contoh adalah *website* milik Pemerintah RI dirusak oleh *hacker*.¹³¹
2. *Illegal Contents*. Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh yang termasuk kejahatan jenis ini adalah *pornografi*, *pemuatan berita bohong*, *agitasi termasuk juga delik politik* dapat dimasukkan dalam katagori ini bila menggunakan media ruang siber.
3. *Data Forgery*. Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.

¹²⁹ Republika, *Awas Bandit dan Vandalisme Digital*, 27 Mei 2001, hlm.7.

¹³⁰ <http://www.theceli.com.dokumen/jurnal/ajo/a002.shtml>., 25 Nopember 2006.

¹³¹ Riau Pos, *Op.cit*, 19 Maret 2007.

4. *Cyber Espionage*. Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau dayanya tersimpan dalam suatu sistem yang *computerized*.
5. *Cyber Sabotage and Extortion*. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program tertentu sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Kejahatan ini juga kadang disebut dengan *cyber terrorism*.
6. *Offence Againsts Intellectual Property*. Kejahatan ini ditujukan terhadap HAKI yang dimiliki pihak lain di internet. Sebagai contoh, meniru tampil *web* suatu situs tertentu, penyiaran rahasia dagang yang merupakan rahasia dagang orang lain.
7. *Infringements of Privacy*. Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan secara *computerized*. Yang apabila diketahui orang lain maka dapat merugikan korban secara materiil atau immaterial, seperti nomor PIN ATM, nomor kartu kredit dan sebagainya.

Walaupun kejahatan ini belum begitu diketahui secara umum, namun

The Federal Bureau of Investigation (FBI) dalam laporannya mengatakan bahwa:

“Tindak kejahatan yang dapat dikategorikan sebagai *cyber crime* telah meningkat empat kali lipat sejak tiga tahun belakangan ini, dimana pada tahun 1998 saja telah tercatat lebih dari 480 kasus *cyber crime* terjadi di Amerika Serikat. Hal ini membuat lebih dari 2/3 warga Amerika Serikat memiliki perhatian serius terhadap perkembangan *cyber crime*, sebagaimana hasil polling yang dilakukan EDI, suatu perusahaan Amerika Serikat yang bergerak di bidang TI”.¹³²

Di Indonesia, penyalahgunaan jaringan internet sudah mencapai tingkat yang memprihatinkan. Akibatnya Indonesia dijuluki dunia sebagai

¹³² *Ibid*, hlm. 7.

negara kriminal internet. Kerena itu, tak heran, apabila saat ini pihak luar negeri langsung menolak setiap transaksi di internet dengan menggunakan kartu yang dikeluarkan oleh perbankan Indonesia.¹³³

Pada bulan Januari-September 2002, pihak kepolisian Republik Indonesia telah mengungkap 109 kasus *cyber crime* yang dilakukan oleh 124 tersangka WNI yang melakukan aksinya diberbagai kota di Indonesia.¹³⁴

Di Indonesia, lokasi dari para pelaku *cyber crime* tidak terkonsentrasi hanya pada pusat-pusat bisnis dan ekonomi nasional seperti Jakarta, atau Surabaya saja misalnya, namun bahkan juga pada daerah-daerah yang dikenal sebagai pusat-pusat pendidikan seperti Bandung, Yogyakarta, dan Semarang.

Pakar telematika Roy Suryo bahkan mengatakan bahwa:

“Daerah tingkat kejahatan *cyber crime* tertinggi di Indonesia adalah justru kota Yogyakarta. Sebagai gambaran, apabila di tahun 2002 terdapat sekitar 160 kasus *cyber crime*, maka 60 % dari total seluruh kejahatan tersebut berasal dari kota Yogyakarta.¹³⁵ Kasus tersebut adalah *Credit Card Fraud* (penipuan dengan kartu kredit)”.

Kemudian berdasarkan kasus yang tercatat pada Badan Reserse dan kriminal (Bareskrim) Mabes Polri, terdapat sekitar 20 kasus *cyber crime* selama periode Januari hingga Desember 2006. Penipuan kartu kredit (*carding*) tercatat mendominasi kejahatan tersebut sejak 1998 hingga akhir 2004, kerugian akibat *carding* dilaporkan telah mencapai US\$ 4.543.176,5.¹³⁶

Kemudahan dan kepraktisan yang telah menjadi *brand image* dari aktivitas belanja di Internet nampaknya terancam tidak bisa dinikmati lagi oleh

¹³³ Abdul Wahid, *et.al*, *Kejahatan Mayantara ...Op.cit*, hlm. 26.

¹³⁴ *Ibid*, hlm. 27.

¹³⁵ Aroma Elmina Martha, *Op.cit*, hlm. 15.

¹³⁶ Arief Pitoyo, *Bisnis Indonesia*, Kamis 23 tahun 2006.

para *shopper* mania yang gemar mengubek-ubek “*pasar*” di dunia maya (*cyber*).

Shintia Dian Arwida bahkan mengatakan bahwa:

“*Embargo* atau *blocking* yang dilakukan oleh banyak situs belanja internasional terhadap pengguna internet yang menggunakan nomor *Internet Protocol (IP)* atau kartu kredit asal Indonesia dapat dikatakan sebagai konsekuensi logis dari tindakan sekelompok *netter* asal Indonesia tersebut adalah Amerika Serikat yang mula-mula memprakarsai pemblokiran ini, karena banyak situs belanja *online*-nya yang merasa dirugikan”.¹³⁷

Menurut pihak Amerika, citra Indonesia sedang berada di titik terendah sejak masuknya teknologi ke tanah air. Akibat langkah Amerika tersebut, sejumlah situs transaksi *on-line* negara-negara lain ikut-ikutan melakukan pemblokiran.¹³⁸

Selanjutnya baru-baru ini pada hari Minggu, tanggal 17 Maret 2007 pukul 05.30 Wib, situs resmi Presiden Susilo Bambang Yudhoyono (*www.presidensby.info*). dibobol *hacker*. Halaman utama situs yang dikelola juru bicara Kepresidenan Andi Mallarangeng itu berubah tampilannya menjadi surat tuntutan yang ditujukan kepada SBY.¹³⁹

Pengirim surat mengatasnamakan *on behalf underground community* dan beralamat di *the word where the devils gather*. Komunitas tersebut mengeluarkan tiga tuntutan *pertama*, meminta penurunan harga *bandwith*, agar masyarakat bisa menikmati internet, *kedua*, meminta SBY mendukung dan melaksanakan IGOS (*Indonesia Go Open Source*) dan yang *ketiga*,

¹³⁷ Shintia Dian Arwida, *Tabloit PC Plus*, No.99/III/09 Oktober 2005, dapat dijumpai dalam situs di internet: <http://cybertech.cbn.net.id/detil.asp.kategori=Feature&newsno=14>.

¹³⁸ *Ibid*

¹³⁹ Riau Pos, *Op.ci*, hlm.1.

Menuntut pemberantasan korupsi, kolusi, dan nepotisme (KKN), pornografi dan porno aksi).¹⁴⁰

Menurut Heru Sutadi bahwa secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua, yaitu:

“*Petama*, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Dan *kedua*, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Namun begitu, mengingat teknologi informasi merupakan konvergensi telekomunikasi, komputer dan media, kejahatan jenis ini berkembang menjadi luas lagi”.¹⁴¹

Dalam catatan beberapa literatur dan situs-situs yang mengetengahkan *cyber crime*, berpuluh jenis kejahatan yang berkaitan dengan dunia *cyber*. Yang masuk dalam katagori kejahatan umum yang difasilitasi teknologi informasi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta teorisme.

Kejahatan yang menjadikan sistem dan fasilitas TI (teknologi informasi) sebagai sasaran diantaranya adalah *denial of service attack (Ddos)*, *defacing*, *cracking* ataupun *phreaking*.¹⁴² Oleh karena itu betapa perlunya untuk segera membenahi sektor hukum di bidang ini, termasuk hukum positif yang terkait dengan aktivitas *Cyber*.

Karena hukum adalah gejala dalam kenyataan kemasyarakatan yang majemuk, yang mempunyai banyak aspek, dimensi dan faset. Hukum berakar dan terbentuk dalam proses interaksi berbagai aspek kemasyarakatan (politik, ekonomi, sosial, budaya, teknologi), dibentuk dan ikut membentuk tatanan

¹⁴⁰ *Ibid*, hlm.8.

¹⁴¹ Heru Sutadi, “Cyber Crime, apa yang bisa diperbuat?”. [http://www. Sinarharapan.co.id/berita/0304/05/opi01.html](http://www.Sinarharapan.co.id/berita/0304/05/opi01.html). 23 Desember 2006.

¹⁴² *Ibid*

masyarakat, bentuknya ditentukan oleh masyarakat dengan berbagai sifatnya, namun sekaligus ikut menentukan bentuk dan sifat-sifat masyarakat itu sendiri. Jadi, dalam dinamikanya, hukum itu dikondisikan dan mengondisikan masyarakat.

Karena menyangkut tujuan untuk mewujudkan ketertiban dan keadilan secara konkret dalam masyarakat, maka dalam hukum terkandung baik kecenderungan konservatif (mempertahakan dan memelihara apa yang sudah tercapai) maupun kecenderungan moderenisme (membawa, menganalisis dan mengarahkan perubahan).¹⁴³

Berdasarkan pandang ini, maka dapat dipahami bahwa hukum senantiasa berdialektika dengan aspek non hukum. Sejalan dengan pemahaman ini, tidak menutup kemungkinan juga hukum akan berdialektika dengan perkembangan teknologi.

Dalam posisi yang demikian ada tiga kemungkinan yang akan timbul, yakni, *pertama*, hukum akan dipengaruhi oleh perkembangan teknologi, *kedua*, hukum akan mempengaruhi perkembangan teknologi, dan *ketiga*, hukum dan teknologi akan saling mempengaruhi.

Dalam konteks ini, umumnya fenomena berpengaruhnya perkembangan teknologi terhadap hukum berhubung langsung dengan pemanfaatan teknologi. Permasalahan yang mendasar disini bagaimana sebenarnya kedudukan hukum yang berlaku (hukum positif) terhadap semakin tidak dapat dikendalikannya perkembangan teknologi. Hal ini didasarkan pada

¹⁴³ Moctar Kusumaatmadja, "Fungsi dan Perkembangan Hukum dalam Pembangunan Nasional," *Majalah Padjadjaran*, Jilid III, No. 1, 1970, hlm. 8-11. Dalam Bernard Arief Sidharta, *Refleksi Tentang Struktur Ilmu Hukum*, Bandar Maju, Bandung, 2000, hlm. 116.

kekhawatiran bahwa hukum yang berlaku tidak *andequit* dengan perkembangan teknologi.¹⁴⁴

Kalau melihat kepada perkembangan teknologi, nampak perubahan teknologi sangat berkembang dengan pesat dibanding dengan hukum sendiri yang selalu mengejar. Melalui perkembangan teknologi ini telah menimbulkan perubahan masyarakat, baik dalam konteks cara berperilaku individu maupun masyarakat itu sendiri.

Fenomena ini hendaknya menjadi suatu tantangan bagi kalangan hukum berkaitan dengan model pendekatan hukum yang selama ini dilakukan. Dengan kata lain bahwa perkembangan teknologi ini telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global dimana sekat-sekat negara mulai memudar.

Sistem tata nilai dalam masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral dan kesusilaan.

Melihat fenomena di atas timbul persoalan apakah hukum pidana positif kita dapat menjangkau kejahatan yang terjadi di dunia *cyber* atau dunia maya mengingat teknologi internet yang membentuk relitas *virtual* merupakan sesuatu yang sama sekali baru. Sementara hukum pidana kita (KUHP) adalah buatan masa lalu di mana saat dibuat belum mengenal komputer apalagi internet. Perdebatan terjadi di antara para pakar hukum pidana.

¹⁴⁴ Chairul Huda, "Perkembangan Teknologi dan Tuntutan Reformasi Hukum," *Jurnal Magister Hukum UII*, Vol.2 No. 1, Februari 2000, hlm. 100-101.

Sebagian berpendapat sesungguhnya kejahatan yang berkaitan dengan dunia *cyber*, pada dasarnya adalah sama dengan kejahatan biasa. Pada prinsipnya kejahatan yang berkaitan dengan dunia *cyber* adalah kejahatan konvensional, sama dengan kejahatan yang diatur di dalam KUHP. Sebagai contoh pornografi di dunia *cyber* bisa dijerat dengan pasal kesusilaan, kemudian kejahatan *credit card fraud* dapat dibidik dengan pasal penipuan, demikian seterusnya.

Sementara sebagian yang lain berpendapat bahwa minimal perlu pembaharuan hukum pidana atau yang lebih ekstrim lagi perlu undang-undang atau peraturan tertentu yang berkaitan dengan kejahatan dunia maya (*cyber*). Ini dikarenakan pada kenyataannya, dengan menggunakan instrumen hukum pidana yang telah ada, ternyata kejahatan di dunia *cyber* atau *cyber crime* masih sulit untuk ditanggulangi bahkan cenderung semakin meningkat, kompleks dengan variasi modus operadinya.

Berkaitan dengan hal tersebut Romli Atmasasmita mengatakan:¹⁴⁵

“Semakin berkembangnya dunia komunikasi melalui jasa internet dan semakin bergantungnya transaksi bisnis menggunakan jasa perbankan lewat internet, maka pengaturan *cyber crime* di Indonesia sudah sangat mendesak dibutuhkan”

Permasalahan secara yuridis untuk menjerat pelaku kejahatan ini biasanya berkaitan dengan berbagai persoalan yang berhubungan dengan beberapa karakteristik kejahatan *cyber*, yaitu, *pertama*, siapakah yang berwenang mengatur atau membuat regulasi yang berkaitan dengan kejahatan di internet mengingat kejahatan ini melintasi batas *teritorial* atau *borderless*

¹⁴⁵ <http://www.komputekonline.com/detail.cfm?ID=43>. 27 Januari 2007

territory, atau bahkan bisa dikatakan di luar teritorial negara (*out of the state territory*), yang pada akhirnya berkaitan dengan yurisdiksi mana yang berhak melakukan proses peradilan.

Kedua, berkaitan dengan asas legalitas yang sangat fundamental dalam hukum pidana, apakah kejahatan dalam dunia maya dapat dijerat dengan hukum pidana melalui penafsiran, mengingat kejahatan tersebut merupakan sesuatu yang sama sekali baru. Sementara umumnya hukum pidana hanya menerima penafsiran otentik saja. Di samping berbagai persoalan lain yang berkaitan seperti alat bukti elektronik dan sebagainya sebagai kelanjutannya.

Persoalan tersebut di atas sesungguhnya berkaitan dengan kebijakan hukum pidana (*penal policy*). Marc Ancel mendefinisikan kebijakan hukum pidana (*penal policy*) sebagai sesuatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif (dalam hal ini hukum pidana) dirumuskan secara baik.¹⁴⁶

Sementara itu upaya perumusan hukum pidana secara lebih baik, mencakup di dalamnya kebijakan merubah atau membuat aturan khusus (hukum pidana) yang berkaitan dengan kejahatan dunia *cyber*. Artinya walaupun mungkin secara essensial dapat dianalogikan dengan kejahatan atau tindak pidana yang diatur dalam KUHP, namun menurut pendapat ahli, hukum pidana tidak menerima analogi. Disamping itu, juga karena karakteristik kejahatan tersebut yang berbeda maka dimungkinkan dijadikan tindak pidana

¹⁴⁶ Al. Wisnubroto, *Op.cit*, hlm. 12.

tersendiri dengan aturan tersendiri pula dalam kerangka mewujudkan rumusan hukum pidana yang lebih baik.

Maka selama ini, fenomena kejahatan *cyber crime* masih menjadi perdebatan serius di antara para pakar hukum. Hal ini dikarenakan kejahatan ini merupakan jenis baru dalam dunia kriminal. Sebagian berpendapat bahwa hukum pidana positif (KUHP dan KUHPA) tidak dapat menjangkau kejahatan ini, sementara itu sebagian yang lain berpendapat bahwa hukum pidana positif dapat menjangkau kejahatan ini.

Kalau kita lihat selama ini aparat penegak hukum untuk menjaring *cyber crime* Kitab Undang-undang Hukum Pidana (KUHP) masih dijadikan sebagai dasar hukum untuk menjaring *cyber crime*, khususnya jenis *cyber crime* yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Ketika produk ini dinilai belum cukup memadai untuk menjaring beberapa jenis *cyber crime*.

Maka untuk Indonesia di samping KUHP beberapa instrumen hukum pidana yang dapat digunakan untuk menyelesaikan kejahatan dengan menggunakan sarana teknologi ini dengan mendekati beberapa ketentuan perundang-undang diluar KUHP, juga menggunakan interpretasi hukum.

Oleh itu untuk membahas pengaturan *cyber crime* dalam hukum pidana positif Indonesia, penulis untuk pertama kali akan mengkaji dalam kaitannya dengan unsur-unsur delik yang diatur dalam KUHP. Dalam hal ini penulis akan mengemukakan beberapa jenis dari kejahatan ini yang menurut para ahli disebut sebagai *cyber crime*, mengingat dalam bentuknya *cyber crime* banyak sekali sejenisnya.

Maka di sini penulis akan mengemukakan beberapa pengaturan hukum pidana positif Indonesia yang dapat dipergunakan dalam menghadapi *cyber crime*, yaitu:

1. Pasal 167 Ayat (1), (2), KUHP

Menyusup dan menyadap *password* milik orang lain tanpa izin di Internet (*Hacking*), orang yang melakukan kejahatan ini disebut dengan *hacker*. *Hacking* oleh kongres PBB X di Wina ditetapkan sebagai *first crime*. Ini disebabkan karena kejahatan tersebut merupakan sesuatu yang istimewa karena mempunyai kelebihan tertentu dibanding jenis kejahatan *cyber* lainnya.¹⁴⁷

“Menurut Agus Raharjo bahwa kelebihan kejahatan ini antara lain yaitu, *pertama*, orang yang dapat melakukan kejahatan jenis ini sudah barang tentu dapat melakukan kejahatan *cyber crime* yang lain. *Kedua*, secara teknis imbas dari aktivitas *hacking* kualitas yang dihasilkannya lebih serius jika dibandingkan dengan bentuk-bentuk *cyber crime* yang lain. Untuk menyebarkan gambar porno atau *cyber phornography* tidak perlu memiliki kemampuan *hacking*, cukup kemampuan minimal tentang internet”.¹⁴⁸

Di samping itu, dalam kejahatan *hacking* ini biasanya merupakan aktivitas awal (perbuatan awal) sebelum seseorang melakukan suatu pidana tertentu misalnya, mencari dan menyadap sistem komputer, menyadap *password*. Setelah diperoleh “*kunci masuk*” maka pelaku dapat melakukan tindakan yang merupakan perwujudan dari niat, yang dilakukan dapat berupa memasuki atau melewati sistem, melakukan pencurian (mencuri isi *web site* yang ada di internet, misalnya dalam *website* BCA (www.bca.com) dengan

¹⁴⁷ Agus Raharjo, *Op.cit*, hlm. 200.

¹⁴⁸ *Ibid*, hlm. 201

mencuri nomor *credit card* dsb), pembocoran rahasia negara, pembocoran rahasia perusahaan, perusakan sistem (*cracking*).¹⁴⁹

Hacker secara umum adalah orang yang mengakses suatu sistem komputer dengan suatu cara yang tidak sah atau salah. Perbuatan ini biasanya dilakukan dengan diawali rasa keingintahuan, kekaguman dan terakhir adalah adanya suatu tantangan yang ditujukan terhadap suatu sistem komputer.¹⁵⁰

Pada prakteknya *hacker* dapat dikategorikan ada yang baik dan buruk. Namun terlepas dari hal itu, keduanya tetap melakukan akses secara *illegal* atau dengan kata lain pelaku telah melakukan peyusupan terhadap sistem komputer. *Hacker* dalam melakukan aksinya ada beberapa tahapan yang dilalui yaitu sebagai berikut:¹⁵¹

1. Mencari sistem komputer yang hendak dimasuki;
2. Menyusup dan menyadap *password*;
3. Menjelajahi sistem komputer;
4. Membuat *backdoor* dan menghilangkan jejak.

Dalam dunia nyata, kejahatan ini dapat dianalogikan dengan memasuki suatu wilayah tanpa izin. Dalam KUHP hal ini diatur dalam pasal 167. Selanjutnya apakah kejahatan ini bisa dimasukkan dalam ketentuan pasal tersebut.

Pasal 167 KUHP menyatakan:

- (1) Barangsiapa dengan melawan hak orang lain dengan memaksa ke dalam rumah atau ruangan yang tertutup atau perkarangan, yang

¹⁴⁹ Edmon Makarim, *Kompilasi Hukum Telematika*, ctk. Pertama, Raja Grafindo Persada, Jakarta, 2003, hlm. 405.

¹⁵⁰ *Ibid*, hlm. 401.

¹⁵¹ *Ibid*, hlm. 402.

dipakai oleh orang lain, atau sedang ada di situ dengan tidak ada haknya, tidak dengan segera pergi dari tempat itu atas permintaan orang yang berhak, dihukum penjara selama-lamanya sebulan atau denda sebanyak-banyaknya Rp. 4.500.

- (2) Barang siapa masuk dengan memecah atau memanjat, memakai kunci palsu, perintah palsu atau pakaian dinas palsu, atau barang siapa dengan tidak setuju yang berhak dan lain daripada lantaran keliru, masuk ke tempat yang tersebut tadi dan kedatangan di sana pada waktu malam, dianggap sebagai sudah masuk dengan memaksa.¹⁵²

Untuk mengkatagorikan *hacking* ke dalam delik yang diatur Pasal 167, maka akan diuraikan unsur-unsurnya sebagaimana disebut dalam Ayat (1):

1. Barang siapa dengan melawan hak orang lain;
2. Masuk dengan memaksa;
3. Ke dalam rumah atau ruangan yang tertutup atau perkarangan, yang dipakai oleh orang lain;
4. Atau sedang di situ dengan tidak ada haknya;
5. Tidak segera pergi dari tempat itu;
6. Atas permintaan orang yang berhak atau atas nama orang yang berhak.

Selanjutnya Pasal 167 Ayat (2) unsur-unsurnya sebagai berikut:

1. Barang siapa;
2. Masuk;
3. Dengan memecah atau memanjat, memakai kunci palsu, perintah palsu, atau pakaian dinas palsu;
4. Atau barangsiapa;
5. Dengan tidak setuju yang berhak dan lain daripada lantaran keliru;

¹⁵² R. Soesilo, *KUHP Serta Komentor-komentarnya Lengkap Pasal Demi Pasal*, Politeia, Bogor, 1994, hlm. 143

6. Masuk ke tempat yang tersebut tadi.

Dari unsur delik tersebut dapat diajukan beberapa persoalan. *Pertama*, apakah *website* dalam jaringan komputer (internet) bisa dikategorikan dalam objek yang diatur dalam Pasal 167 tersebut, dalam hal ini dikategorikan rumah. *Kedua* persoalan apakah “*menyadap password*” bisa disamakan dengan “*menggunakan kunci palsu*”.

Berkaitan dengan persoalan tersebut, kalau kita lihat berpegang secara harafiah sesuai dengan bunyi Pasal 167 tersebut maka objek yang dituju adalah “*rumah*” dan ini jelas. R. Soesilo, menyatakan bahwa yang menjadi objek dalam Pasal 167 ialah: rumah, ruangan, atau perkarangan yang tertutup.¹⁵³

Menurut hemat penulis bahwa *website* tidak dapat disamakan dengan objek dari yang diatur Pasal 167 KUHP sebagaimana yang dijelaskan oleh R. Soesilo tersebut. Ini karena alasan, bahwa *website* berada dalam ruang maya yang mempunyai paradigma kehidupan *virtual*, sementara pengertian rumah, ruangan atau perkarangan adalah dalam kehidupan nyata.

Berkaitan dengan objek yang diatur dalam Pasal 167 tersebut tampaknya ada usaha untuk memperluasnya, dalam hal ini tidak hanya sekedar “*ruangan*” dalam arti fisik dalam dunia nyata, tapi lebih luas lagi. Hal ini tampak dalam RUU KUHP tahun 2004, pengertian “*ruang*” Pasal 204, termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu.¹⁵⁴

¹⁵³ *Ibid*, hlm.144.

¹⁵⁴ Elsam, *Rancangan Undang-Undang KUHP* tahun 2004. hlm. 46.

Pada dunia nyata kita dapat menggambarkan bagaimana aktivitas bisa dikategorikan sebagai aktivitas "*memasuki*". Jika dihubungkan dengan kejahatan *hacking* dalam kaitannya dengan ketentuan Pasal 167, maka menjadi sulit untuk digambarkan. Ini dikarenakan dalam *hacking* semuanya serba maya (*virtual*), tidak sebagaimana aktivitas dalam dunia nyata.

KUHP tidak menjelaskan apa yang dimaksud dengan pengertian "*masuk*". Berkaitan dengan perkembangan kejahatan, tampaknya ada usaha untuk menjangkau jenis kejahatan yang berkaitan dengan sistem komputer, dengan memperluas pengertian masuk yang tidak hanya menjangkau pengertian "*masuk*" secara fisik saja.

Hal ini terlihat dalam Buku I (Ketentuan Umum) RUU KUHP 2005 dalam Pasal 186, pengertian "*masuk*" termasuk mengakses komputer atau masuk ke dalam sistem komputer.

Selanjutnya berkaitan dengan sarana yang digunakan untuk masuk. Dalam Pasal 167 (2) tersebut ditentukan "*kunci palsu*". Pasal 100 KUHP menyatakan "*yang masuk sebutan kunci palsu yaitu sekalian perkakas yang gunanya tidak untuk membuka kunci itu*". Berkaitan dengan "*kunci*" ini R. Soesilo, dalam komentarnya menyatakan, yaitu segala macam anak kunci yang tidak dipergunakan oleh orang yang berhak untuk membuka kunci dari suatu barang lemari, rumah, peti dan sebagainya. Termasuk pula anak kunci yang palsu yaitu anak kunci duplikat bila tidak digunakan oleh yang berhak.¹⁵⁵

¹⁵⁵ R. Soesilo, *Op.cit*, hlm. 105.

Melihat dari uraian diatas kalau kita berpegang pada aturan yang tertuang dalam Pasal 1 KUHP (asas legalitas) maka akan terasa muskil untuk mengatakan bahwa *hacking* bisa dijerat dengan Pasal 167 KUHP.

Berkaitan dengan *hacking* ini, Edoman Makarim,¹⁵⁶ menyatakan bahwa terhadap kejahatan ini dapat diterapkan dengan Pasal 22, 40 dan 42 Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi dan juga mengatur kerahasiaan informasi, antara lain:

1. Pasal 22 Undang-undang tersebut menyatakan, setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi:
 - a. Akses ke jaringan telekomunikasi; dan/atau
 - b. Akses ke jasa telekomunikasi; dan/atau
 - c. Akses ke jaringan telekomunikasi khusus.
 Bagi pelanggar ketentuan tersebut diancam pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp. 600 juta.
2. Pasal 40 menyatakan, setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun. Bagi yang melanggar ketentuan tersebut diancam pidana penjara maksimal 15 tahun penjara.
3. Pasal 42 ayat 1, mengatur kewajiban penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya bagi penyelenggara yang melanggar kewajiban tersebut diancam pidana penjara maksimal 2 tahun dan/atau denda maksimal Rp. 200 juta.

Selanjutnya menurut hemat penulis bahwa bila dilihat secara umum, dalam istilah "*internet*" memang mengandung makna telekomunikasi sebagaimana telah dikemukakan, bahwa internet merupakan konvergensi media, komputer, telekomunikasi.

¹⁵⁶ Edoman Makarim, *Op.cit*, hlm. 412.

Dengan demikian maka menurut hemat penulis pasal Undang-undang No. 36 Tahun 1999 tersebut dapat diterapkan terhadap kejahatan *cyber crime* yang termasuk di dalamnya adalah *hacking*.

2. Pasal 406 Ayat (1).

Perusakan *website* di internet, kasus ini dikenal dengan sebutan *Denial Of Service (DoS) Attack*. Kejahatan ini dilakukan dengan menyerang dengan tujuan untuk melumpukan target, misalnya *website BCA online*. Kemudian kasus penyebaran virus di internet yang menyebabkan sistem menjadi *hang*. Bila menggunakan KUHP terhadap kejahatan ini dapat diterapkan Pasal 406 Ayat (1).

Pasal 406 Ayat (1) KUHP yang berkaitan dengan tindakan perusakan, yaitu:

“Barang siapa dengan sengaja dan dengan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah”

Dan Pasal 406 Ayat (1) KUHP tersebut merupakan dasar hukum yang ditujukan (diancamkan) misalnya kepada *hacker*, karena aktivitas *hacker* ini dinilai telah menimbulkan kerusakan atau kerugian yang luar biasa kepada usaha seseorang, kepentingan institusi atau negara. Aparat menilai kalau yang dilakukan oleh *hacker* jelas-jelas mengakibatkan kerugian pada orang lain, salah satunya berupa kerusakan atau menjadikan tidak berfungsinya barang lain. Jika barang ini termasuk *website*, maka *website* inilah yang mengalami kerusakan.

3. Pasal 282 Ayat (1), (2), (3) KUHP

Kejahatan Pornografi di Internet, (*cyberporn/cyber phornography*) juga termasuk dalam *cyber crime*. Kejahatan ini berkaitan dengan pornografi di internet. Dalam hal ini sebagai contoh adalah situs *www.pondok putri. com*, *www. playboy. com* dan banyak lagi situs yang berbau pornografi, ini salah satu problem besar yang dibawa oleh teknologi informasi global melalui jaringan internet.

Seolah-olah sekarang ini, sulit sekali memproteksi jaringan internet dari sebuah pebisnis hiburan yang menjual pornografi. Pasar informasi global sebagian sudah diwarnai oleh berbagai bentuk atau gaya hidup seks bebas.

Seseorang yang mengakses melalui internet dengan asal-asalan misalnya tiba-tiba bisa dikejutkan dengan keluarnya sejumlah gambar yang menampilkan adegan seronok, nudis, dan sek dengan berbagai posenya. Hal ini menunjukkan bahwa masyarakat di era global sekarang ini dengan gampang dapat terkena virus bermoduskan pelecehan nilai-nilai kesusilaan.

Untuk mencegah menjalarnya penggunaan jaringan internet secara melawan hukum, dasar hukum yang digunakan/diterapkan Pasal 282 KUHP yaitu:

- (1) Barangsiapa menyiarkan, mempertontonkan, atau menepelkan dengan terang-terangan suatu tulisan yang diketahui isinya, atau gambar atau barang yang dikenalnya yang melanggar perasaan kesopanan, maupun membuat, membawa masuk, mengirimkan langsung, membawa keluar atau menyediakan tulisan, gambar atau barang itu untuk disiarkan, dipertontonkan atau ditempelkan sehingga kelihatan oleh banyak orang, atau pun dengan terang-terangan diminta atau menunjukkan bahwa tulisan, gambar atau barang itu boleh didapat, dihukum penjara selama lamanya satu tahun empat bulan atau denda sebanyak-banyaknya Rp. 45.000,-.

- (2) Barangsiapa menyiarkan, mempertontonkan atau menempelkan dengan terang-terangan suatu tulisan, gambar atau barang yang melanggar perasaan kesopanan, maupun membawa masuk, mengirimkan terus, membawa keluar, atau menyediakan surat, gambar atau barang itu disiarkan, dipertontonkan atau ditempelkan, sehingga kelihatan oleh orang banyak ataupun dengan terang-terangan atau dengan menyiarkan suatu tulisan menawarkan dengan tidak diminta atau menunjukan, bahwa tulisan, gambar atau barang itu boleh didapat, dihukum penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya Rp. 45.000,- jika ada alasan yang sungguh-sungguh untuk menduga, bahwa tulisan, gambar atau barang itu melanggar kesopanan.
- (3) Jika melakukan kejahatan yang diterangkan dalam ayat pertama dijadikan suatu pencaharian atau kebiasaan, oleh tersangka, dapat dijatuhkan hukuman penjara selama-lamanya dua tahun delapan bulan atau denda sebanyak-banyaknya Rp. 75.000,-¹⁵⁷

Dengan melihat ketentuan tersebut maka pornografi di internet dapat dikenakan dengan Pasal 282 KUHP. Terhadap pornografi di internet yang bertujuan bisnis, misalnya situs "*www.playboy*" dan "*www.pondokputri.com*", dapat diterapkan pasal tersebut 282 ayat 3.

Pada pasal 282 tersebut perbedaanya adalah ayat (1) pelaku harus mengetahui bahwa tulisan dan seterusnya, itu melanggar perasaan kesopanan, sementara dalam ayat (2) tidak perlu mengetahui, sudah cukup apabila padanya ada alasan sungguh-sungguh untuk menduga bahwa tulisan tersebut dan seterusnya, itu melanggar kesopanan.

Secara sepintas lalu unsur yang tersebut dalam Pasal 282 dapat diterapkan pada pornografi di internet. Akan tetapi apabila dikaji lebih jauh ternyata terdapat persoalan yang sangat rumit. Persoalan ini berkaitan dengan ukuran kesopanan dimana setiap daerah dan masyarakat mempunyai ukuran sendiri.

¹⁵⁷ R. Soesilo, *Op.cit*, hlm. 205-206

Sebagai contoh bagaimana apabila situs dalam internet menampilkan pornografi yang akibatnya dirasakan orang Indonesia, sementara situs itu milik “playboy” Amerika. Menurut pendapat penulis hal ini tidak bisa diterapkan Pasal 282, karena dalam pasal tersebut tidak dijelaskan lebih lanjut ukuran kesopanan itu bagaimana. Di mana tempat pelaku atau tempat akibat. Mengingat internet bersifat transnasional atau global, dalam kasus ini KUHP tidak bisa dilakukan.

4. Pasal 378 KUHP

Penipuan dengan kartu kredit (*Credit Card Fraud*) di internet, kejahatan ini seringkali terjadi akhir-akhir ini adalah pencurian identitas atau menggunakan identitas orang lain untuk memenuhi kepentingan sendiri, identitas orang lain digunakan dengan maksud jahat, yakni merugikan orang lain yang dicuri atau dipakai identitasnya.

Pencurian identitas dan *fraud*. Adapun skema pencurian identitas, yaitu memperoleh dan menggunakan data personal orang lain untuk melakukan *fraud* atau penipuan demi kepentingan ekonomis. Sebagai contoh seorang memperoleh nama dan nomor *social security* sejumlah pejabat militer AS dari *website*. Kemudian menggunakan lebih dari seratus nama dan nomor tersebut untuk membuat aplikasi kartu kredit via internet pada *Delaware Bank*.¹⁵⁸ Dalam berita di SCTI bahwa kasus penipuan kartu kredit via internet di Indonesia pada tahun 2005 lebih kurang 400 kasus.¹⁵⁹

¹⁵⁸ Widi Prajo, *Internet Fraud; Suatu Tantangan Bagi Auditor*, tulisan ini dapat dijumpai secara online di internet dalam situs Budi Raharjo, 12 Nopember 2006.

¹⁵⁹ Sumber Data, *Mabes Polri, Berita Buser Siang*, Tanggal 26 Maret 2007.

Selain kasus di atas juga pernah ada kasus yang berkaitan dengan *cyber crime* di Indonesia. Kasus tersebut disidangkan oleh Pengadilan Negeri Sleman Yogyakarta dengan nomor putusan perkara No. 24/Pid.B/2002/PN.SLMN dengan terdakwa Petrus Pangkur (23) alias Bonny Diobok-obok. Kasus tersebut disidangkan oleh majelis hakim yang terdiri dari, Hakim Ketua Cicut Sutiarto, SH, dengan anggota Sarjiman, SH dan Jurpiyandi, SH. Selaku Jaksa Penuntut Umum (JPU) adalah Oemar Dhani, SH.¹⁶⁰

Dalam kasus tersebut terdakwa didakwa melakukan *cyber crime*. Dalam amar putusannya, majelis hakim berkeyakinan bahwa Petrus alias Bonny Diobok-obok, telah membobol kartu kredit milik warga AS. Hasil kejahatannya digunakan untuk membeli barang-barang, seperti helm, dan sarung tangan merk AGV. Total harga barang yang dibelinya mencapai 4 juta.

Kejahatan tersebut diatas kalau melihat kontruksinya dapat dikualifikasikan pada pelanggaran ketentuan Pasal 378 KUHP, yaitu:

“Barangsiapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu, baik dengan akal tipu muslihat, maupun dengan karangan perkataan-perkataan bohong, membujuk orang supaya memberikan sesuatu barang, membuat utang atau menghapuskan piutang, dihukum karena penipuan, dengan hukuman penjara selama-lamanya empat tahun.”

Melihat ketentuan pasal tersebut maka dapat diterapkan apabila sesuai dengan unsur-unsurnya.

¹⁶⁰ Pikiran Rakyat, 31 Agustus 2003.

5. Pasal 112, 322, 323 KUHP

Pembocoran rahasia di internet (*data leakage*), diartikan sebagai pembocoran data rahasia yang dilakukan dengan cara menulis data-data rahasia tersebut ke dalam kode-kode tertentu sehingga data dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggungjawab.

Ketika *website* KPU, yang nota bene mewakili negara dalam menyelenggarakan kegiatan-kegiatan besar seperti Pemilu, dibobol oleh *hacker*, maka kejahatan yang dilakukan oleh *hacker* ini dapat dikategorikan memenuhi unsur *cyber crime*. Karena ada tindakan berupa “*membocorkan rahasia*”, sebagaimana disebut dalam Pasal 112 KUHP berikut:

“Barangsiapa dengan sengaja mengumumkan surat-surat atau benda-benda atau keterangan-keterangan yang diketahuinya bahwa harus dirahasiakan untuk kepentingan negara atau dengan sengaja memberitahukan atau memberikannya kepada negara asing, diancam dengan pidana penjara paling lama tujuh tahun”

Selanjutnya yang berkaitan dengan pembocoran rahasia ini Pasal, 322 dan Pasal 323 KUHP yang intinya, tindak pidana membuka rahasia perusahaan atau berkewajiban menyimpan rahasia profesi atau jabatan.

6. Pasal 362 KUHP

Salah satu bentuk *cyber crime* adalah “*pencurian data*”, pencurian data di internet (*Joycomputing*) artinya sebagaimana perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa izin dan menggunakannya melampaui wewenang yang diberikan, tindakan ini dapat dikategorikan sebagai tindak pidana pencurian. Meski istilah “*pencurian data*” ini

dikategorikan sebagai kejahatan konvensional pada umumnya, yakni pencurian, sebagaimana diatur dalam Pasal 362 KUHP, yang menyebutkan:

“Barangsiapa mengambil barang yang sama sekali atau sebagian kepunyaan orang lain, dengan maksud memilik barang itu dengan melawan hukum, dipidana dengan penjara selama-lamanya lima tahun atau denda sebanyak-banyaknya sembilan ribu rupiah.”

Jadi pengambilan data di komputer dengan cara melawan hukum diinterpretasikan memenuhi salah satu unsur kejahatan pencurian. Kasus ini tergolong sebagai pencurian dengan modus operandi modern, karena menggunakan produk teknologi canggih.

7. Pasal 369 KUHP

Tindakan pemerasan dan pengacaman yang dilakukan melalui media elektronik, ancaman disini pencemaran nama baik dengan lisan maupun tulisan, atau dengan ancaman membuka rahasia, kalau ancaman yang dilakukannya tidak dipenuhi ia akan membuka rahasia kepada publik. Dan kejahatan ini bersifat delik aduan apabila korban tidak mengadu maka perbuatan tersangka maka kejahatan ini tidak bisa dituntut.

Adapun bunyi Pasal 369 Ayat (1) dan (2) KUHP adalah sebagai berikut :

- (1) Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran nama baik dengan lisan maupun tulisan, atau dengan ancaman akan membuka rahasia, memaksa seorang supaya memberikan barang sesuatu yang seluruhnya atau sebahagian kepunyaan orang itu orang lain atau supaya memberi hutang atau menghapuskan piutang, diancam dengan pidana penjara paling lama empat tahun.
- (2) Kejahatan ini tidak dituntut kecuali atas pengaduan orang yang terkena kejahatan.

8. Pasal 372, 374, KUHP

Penggelapan data di internet (*The Trojan Horse*), pasal ini dapat digunakan untuk menjaring pelaku penggelapan data. Pelaku kejahatan ini umumnya orang dalam dari suatu perusahaan yang bergerak di bidang teknologi informasi atau operator sistem suatu perusahaan *server*. Orang dalam, yaitu tentu saja menguasai berbagai bentuk informasi ini kemudian menjual kepada orang lain dengan memanfaatkan fasilitas teknologi komputer. (internet).

Sebagaimana diatur dalam Pasal 372, 374, KUHP, yang menyebutkan:

1. *Pasal 372.* Barangsiapa dengan sengaja dan dengan melawan hukum memiliki barang, yang sama sekali atau sebagian kepunyaan orang lain, dan yang ada padanya bukan karena kejahatan, dipidana karena pengelapan, dengan pidana penjara selama-lamanya empat tahun atau denda sebanyak-banyaknya sembilan puluh rupiah.
2. *Pasal 374.* Penggelapan yang dilakukan oleh orang yang penguasaanya terhadap barang disebabkan karena hubungan kerja ada hubungan kerja atau karena pencariannya atau karena mendapat upah untuk itu diancam dengan pidana penjara paling lama lima tahun.

9. Pasal 382 bis KUHP

“Barangsiapa untuk mendapatkan, melangsungkan atau memperluas debit perdagangan atau perusahaan kepunyaan sendiri atau orang lain, melakukan perbuatan curang untuk menyesatkan khalayak umum atau seorang tertentu, diancam, jika karenanya dapat timbul kerugian bagi konkiren-konkirennya atau konkiren orang lain itu, karena persaingan curang, dengan pidana penjara paling lama satu tahun empat bulan atau denda paling banyak sembilan ratus rupiah.”

Pasal ini dapat diterapkan pada, *Passing off* pelanggaran nama domain di internet yang merugikan orang lain akibat perbuatan curang tersebut. Di

Indonesia kasus ini pernah terjadi antara PT. Mustika Ratu dan Tjandra, pihak yang mendaftarkan nama domain tersebut.

10. Pasal 383 KUHP

“Diancam dengan pidana penjara paling lama satu tahun empat bulan, seorang penjual yang berbuat curang terhadap pembeli:

Ke-1 : Karena seganja menyerahkan barang lainpada yang ditunjuk untuk dibeli.

Ke-2 : Mengenai jenis keadaan atau banyaknya barang yang diserahkan, dengan menggunakan tipu muslihat.

Pasal ini penjual curang kepembeli yang menyakut tentang sertifikasi keandalan (*trust mark*).

11. Pasal 506 KUHP

“Barangsiapa menarik keuntungan dari perbuatan cabul sorang wanita dan menjadikanya sebagai pencaharian, diancam dengan pidana kurungan paling lama satu tahun”

Pasal ini diterapkan terhadap tindak pidana dengan menggunakan sarana teknologi informasi, kasus seperti ini sangat sering sekali terjadi di Indonesia.

Dari uraian tersebut diatas penulis simpulkan ada beberapa kejahatan *cyber crime* yang dijerat dengan KUHP. Hal ini kalau melihat unsur delik yang diatur dalam KUHP. Dengan demikian jangan sampai ada kekosongan hukum dalam menyelesaikan *cyber crime*.

Bertolak dari sini maka diperlukan adanya keberanian hakim untuk menafsirkan undang-undang. Selama ini hakim terkesan kurang “berani” untuk bertindak. Hakim selalu dibayang-bayangi dengan Pasal 1 KUHP. Padahal hakim tidak boleh menolak perkara yang diajukan ke pengadilan dengan alasan tidak ada hukumnya.

Kalau kita kaji sebenarnya sikap hakim tersebut akan kontras dengan ketentuan Pasal 22 AB (*Algemeene Bepalingen Van Wetgeving Voor Indonesia*); pasal ini menyatakan:

“Hakim yang menolak untuk mengadakan keputusan terhadap perkara dengan dalih undang-undang tidak mengaturnya, terdapat kegelapan ketidak lengkapan dalam undang-undang, dapat dituntut karena menolak mengadili perkara”¹⁶¹

Lebih tegas lagi hal tersebut dinyatakan dalam Undang-Undang Nomor 4 Tahun 2004 tentang ketentuan-ketentuan Pokok Kekuasaan kehakiman, dalam Pasal 28 Ayat (1) menyatakan:

“Hakim wajib menggali, mengikuti, dan memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat”

Dari ketentuan tersebut sesungguhnya mendorong bahkan memberikan justifikasi untuk melakukan interpretasi atau penafsiran hukum terhadap ketentuan undang-undang. Bahkan ada ancaman bila menolak dapat dituntut (dihukum). Dalam mengatasi kekosongan hukum, hakim untuk sementara dapat melakukan interpretasi.

Kemudian yang menjadi persoalan selanjutnya adalah berkaitan dengan yurisdiksi, mengingat *cyber crime* ini dalam bahasanya Barda Nawawi Arief adalah merupakan *global crime*, yaitu kejahatan yang tidak jelas yurisdiksinya. Misalnya si A (di Indonesia) menipu lewat internet dengan transaksi *on line* terhadap B melalui situs (*website*-nya milik A) sedangkan B tersebut adalah warga Amerika Serikat dan bertempat di Amerika Serikat, *website* A itu terdaftar pada *server* di ISP Inggris, umpama. Kalau melihat

¹⁶¹ Al. Wisnubroto, *Op.cit*, hlm. 57.

kasus ini maka KUHP sulit diterapkan karena kejahatan ini (*cyber crime*) *locus delicti*-nya tidak jelas.

Maka disini Pasal 3 KUHP menyatakan:¹⁶²

“Ketentuan-ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi tiap orang yang di luar wilayah Indonesia melakukan tindak pidana di dalam kendaraan air atau pesawat udara Indonesia”

Dalam ketentuan tersebut memang memperluas Pasal 2 (*Asas Teritorial*) akan tetapi terbatas jangkauannya. Pasal ini hanya memperlakukan hukum pidana Indonesia terhadap siapa saja yang melakukan tindak pidana dalam kendaraan air (kapal) dan pesawat udara.

Berkaitan dengan kapal tersebut Pasal 95 KUHP menentukan sebagai berikut :

“Yang disebut dengan kapal Indonesia adalah kapal yang mempunyai surat laut atau pas kapal, atau surat izin sebagai penggantinya sementara, menurut aturan umum mengenai surat laut dan pas kapal di Indonesia”.

Dari ketentuan pasal ini tampak ada penyempitan jangkauan hukum pidana, yaitu hanya kapal resmi saja dalam arti secara legal terdaftar.

Selanjutnya dalam Pasal 4 KUHP yaitu :

(1) Ketentuan pidana dalam undang-undang Indonesia berlaku bagi tiap orang yang melakukan di luar Indonesia:

1. Melakukan salah satu kejahatan yang disebut dalam Pasal 104, 106, 107, 108, 111 bis ke-1, 127 dan 131.
2. Suatu kejahatan tentang mata uang, uang kertas negeri atau uang kertas bank atau tentang materai atau merek yang dikeluarkan atau disuruh oleh pemerintah Indonesia.

¹⁶² R. Soesilo, *Op.cit*, hlm. 32.

3. Pemalsuan tentang surat-surat hutang atau sertifikat hutang yang ditanggung Indonesia, daerah atau sebagian daerah, talon-talon, surat hutang sero atau surat-surat bunga hutang yang masuk surat-surat itu, serta surat-surat keterangan ganti surat itu atau dengan sengaja mempergunakan surat palsu atau yang dipalsukan demikian itu seakan-akan surat itu benar dan tidak dipalsukan.
4. Salah satu kejahatan yang disebut dalam Pasal 438, 444 sampai dengan Pasal 446 tentang pembajakan laut dan Pasal 447 tentang penyerahan kendaraan air kepada kekuasaan bajak laut dan Pasal 479 huruf j, m, n dan o tentang kejahatan yang mengancam keselamatan penerbangan sipil.

Ketentuan pada Pasal 4 KUHP tersebut lebih memperluas lagi terhadap tuntutan atas tindak pidana yang telah dilakukan. Dalam pasal ini didapati asas melindungi kepentingan nasional, maupun kepentingan universal, yaitu yang menyatakan dalam poin 2.¹⁶³

Dalam Pasal ini terdapat ketentuan untuk memperluas tuntutan terhadap semua orang yang melakukan tindak pidana di luar Indonesia. Walaupun demikian, dalam ketentuan Pasal 4 KUHP ini hanya memberlakukan terhadap kejahatan tertentu, yaitu yang berkaitan dengan kejahatan terhadap keamanan negara untuk poin satu (1), yaitu Pasal 104, 106, 107, 108, 110, 111 bis ke-1, 127 dan 131 KUHP. Demikian pula dalam poin (1) dan poin (2, 3, 4) mengatur kejahatan tertentu saja.

Pasal 5 KUHP menentukan sebagai berikut :

(1) Ketentuan pidana dalam undang-undang Indonesia berlaku bagi tiap warga Indonesia yang melakukan di luar Indonesia:

1. Melakukan salah satu kejahatan yang disebut dalam BAB I dan II Buku Kedua dan dalam Pasal 160, 161, 240, 279, 450 dan 451.

¹⁶³ Moeljatno, *Asas-asas Hukum Pidana*, ctk. Keempat, ...*Op.cit*, hlm. 43.

2. Suatu perbuatan yang dipandang sebagai kejahatan menurut ketentuan pidana dalam UU Indonesia dan boleh dihukum menurut UU negeri ia berada.

(2) Penuntutan terhadap suatu perbuatan yang dimaksudkan pada ke-2 boleh juga dilakukan, jika tersangka baru menjadi warga negara Indonesia setelah melakukan perbuatan itu.

Dari ketentuan Pasal 5 tersebut tampak bahwa dalam ketentuan tersebut KUHP memperluas berlakunya tuntutan terhadap tindak pidana yang dilakukan oleh “*warga negara*” di luar Indonesia. Ketentuan dalam Pasal 5 tersebut dengan prinsip nasional aktif.¹⁶⁴

Kemudian Pasal 7 KUHP menentukan :

“Aturan pidana dalam perundang-undangan Indonesia berlaku bagi setiap pejabat yang di luar Indonesia melakukan salah satu perbuatan pidana tersebut dalam Bab XXVIII Buku Kedua”

Ketantuan dalam pasal inipun juga terbatas pada subjek hukum (pelaku) yang berstatus sebagai pejabat dan juga terbatas pada perbuatan yang diatur dalam Bab XXVIII Buku Kedua saja.

Pasal 8 KUHP menyatakan:

“Aturan pidana dalam perundang-undangan Indonesia berlaku bagi nahkoda dan penumpang perahu Indonesia, yang di luar Indonesia sekalipun di luar perahu, melakukan salah satu perbuatan pidana tersebut Bab XXIX Buku Kedua, dan Bab IX Buku Ketiga; begitu pula yang tersebut dalam peraturan mengenai surat laut dan pas kapal di Indonesia, maupun dalam *Schepen ordonnantie 1927*”.

Dalam ketentuan pasal ini juga sama, yaitu memperluas tuntutan, akan tetapi juga terbatas pada pelaku tertentu dan juga perbuatan tertentu saja, yaitu yang diatur dalam Bab XXIX Buku Kedua dan Bab IX Buku Ketiga.

¹⁶⁴ *Ibid*, hlm. 46.

Pasal 9 menyatakan: "*Berlakunya Pasal 2, 5, 7 dan 8 dibatasi oleh pengecualian-kecualian yang diakui dalam hukum Internasional*"

Maka dapat disimpulkan bahwa hukum pidana mengenal asas berlakunya hukum pidana berhubung dengan tempat, sebagaimana diatur dalam Pasal 2 sampai 9 KUHP. Asas-asas tersebut ialah:¹⁶⁵

a. Asas Teritorial

Yang dimaksud dengan asas teritorial ini adalah bahwa undang-undang pidana Indonesia berlaku terhadap setiap orang yang melakukan suatu pelanggaran/kejahatan di dalam wilayah Republik Indonesia. Asas ini tertuang dalam KUHP Pasal 2 dan 3.

b. Asas Nasional Aktif

Asas ini mengandung pengertian bahwa undang-undang pidana Indonesia berlaku juga bagi warga negara Indonesia yang berada di luar negeri. Hal ini diatur dalam KUHP Pasal 5 Ayat (1) sub 1.

c. Asas Nasional Pasif

Asas ini mengandung pengertian bahwa undang-undang pidana Indonesia berkuasa juga mengadakan penuntutan terhadap siapapun juga di luar negara Republik Indonesia juga terhadap orang asing di luar RI. Di sini dipentingkan kepentingan hukum suatu negara yang dilanggar seseorang. Yang termasuk perbuatan yang merugikan negara kita ialah memalsukan uang Indonesia, materai, lambang negara Indonesia, cap negara dan lain sebagainya.

d. Asas Universal

Undang-undang pidana Indonesia dapat juga diberlakukan terhadap perbuatan-perbuatan jahat yang bersifat merugikan keselamatan Internasional, yang terjadi dalam daerah tak bertuan.

Dari keseluruhan uraian tersebut dapat disimpulkan bahwa kalau kita melihat unsurnya maka pengaturan *cyber crime* dalam hukum pidana positif

¹⁶⁵ CST. Kansil, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, Balai Pustaka, Jakarta, 1989, hlm. 227-279

ada beberapa dari *cyber crime* yang dapat dijerat dengan hukum pidana Indonesia, dan sebagian lagi tidak dikarenakan kejahatan ini relatif baru.

Namun demikian, apabila melihat ketentuan yang mengatur tentang berlakunya hukum pidana maka sulit sekali. Hal ini dikarenakan *cyber crime* tidak jelas yurisdiksinya atau merupakan *global crime*. Bertolak dari hal tersebut maka menurut hemat penulis perlu adanya kebijakan kriminalisasi atau pembaharuan hukum pidana (KUHP).

B. Kebijakan Kriminalisasi *Cyber Crime* dalam Konteks Hukum Pidana Yang Akan Datang (*Ius Constituendum*)

Kejahatan merupakan entitas yang selalu lekat dengan dinamika perkembangan peradaban umat manusia. Kejahatan yang oleh Saporinah Sadli disebut sebagai perilaku menyimpang, selalu ada dan melekat pada tiap bentuk masyarakat; tidak ada masyarakat sepi dari kejahatan.¹⁶⁶

Di samping itu dengan semakin maju peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, muncul berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya *cyber crime*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi cita ketertiban masyarakat.

Bertolak dari hal tersebut, maka seiring dengan semakin kompleksnya permasalahan yang dihadapi masyarakat dan penegak hukum, perlu diimbangi

¹⁶⁶ Muladi. *et.al.*, *Bunga Rampai Hukum Pidana, ...Op.cit.*, hlm. 148.

dengan pembangunan sistem hukum pidana secara terus menerus. Dengan demikian, dalam persepektif ini, kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana dalam kaitannya dengan perkembangan masyarakat.

Kebijakan hukum pidana dapat didefinisikan sebagai usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang.¹⁶⁷

A. Mulder mengemukakan bahwa kebijakan hukum pidana ialah garis kebijakan untuk menentukan:

1. Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui;
2. Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana;
3. Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.¹⁶⁸

Dari definisi ini tampak bahwa Mulder memandang hukum pidana sebagai sebuah sistem. Dengan demikian objek kebijakan hukum pidana mencakup hukum pidana dalam arti formil dan materiil. Menurut hemat penulis, definisi ini lebih komprehensif. Sebab dengan objek kebijakan hukum pidana yang terfokus pada hukum pidana materiil akan tidak efektif dalam menghadapi peristiwa hukum konkrit yang dalam hal ini berkaitan erat dengan hukum pidana formil. Ini tampak dalam menyikapi perkembangan teknologi dan masyarakat yang sangat pesat.

¹⁶⁷ Al. Winusubroto, *Op.cit*, hlm. 11.

¹⁶⁸ *Ibid*, hlm. 12.

Definisi Mulder di atas sesungguhnya bertolak dari pengertian “*sistem hukum pidana*” menurut Marc Ancel, yang menyatakan bahwa tiap masyarakat yang terorganisir memiliki sistem hukum pidana yang terdiri dari peraturan-peraturan hukum pidana dan sanksinya, suatu prosedur hukum pidana dan suatu mekanisme pelaksana pidana.¹⁶⁹

Marc Ancel mengemukakan, *penal policy* (kebijakan hukum pidana) adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak saja kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan.¹⁷⁰

Pada hakekatnya kebijakan untuk membuat peraturan hukum pidana menjadi lebih baik merupakan bagi dari upaya dalam penggulungan kejahatan. Dengan demikian kebijakan hukum pidana, hakekatnya merupakan bagi dari kebijakan penanggulungan kejahatan (politik kriminal)

Dalam persepektif ini (politik kriminal), kebijakan hukum pidana identik dengan pengertian “*kebijakan penanggulungan kejahatan dengan hukum pidana*”

Oleh karena itu, dengan perkataan yang lain “*kebijakan penanggulungan kejahatan dengan hukum pidana*” bisa disebut dengan kebijakan kriminalisasi, di mana dalam proses ini (*kriminalisasi*) menggunakan sarana pidana. Dari sisi tampak bahwa dalam persepektif

¹⁶⁹ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana...Op.cit*, ctk. Pertama, hlm. 26.

¹⁷⁰ *Ibid*, hlm. 21.

kebijakan hukum pidana kriminalisasi merupakan bagian dari kebijakan hukum pidana.

Untuk lebih jelas pengertian kriminalisasi, secara etimologis kriminalisasi berasal dari kata bahasa Inggris *Criminalization*, yang mempunyai padanan dalam bahasa Belanda *Criminalisatie*,¹⁷¹ dengan kata lain kriminalisasi dalam kepustakaan asing dikenal dengan nama *Criminalization* atau *Criminalisering*.

Kriminalisasi bukan hanya suatu kata, tetapi juga suatu perbuatan istilah (*terminologi*) dalam hukum pidana materil. Oleh karena itu, dalam pembentukan kaidah hukum pidana, kriminalisasi merupakan suatu objek kajian yang penting.

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana menjadi suatu tindak pidana melalui undang-undang. Pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal dengan menggunakan sarana hukum pidana, dan oleh karena itu termasuk bagian dari kebijakan hukum pidana¹⁷².

Di Indonesia sesungguhnya proses kriminalisasi sejak Proklamasi Kemerdekaan terus berlangsung sampai sekarang dan tidak akan berhenti. Dengan UU No. 1 Tahun 1946 telah banyak diciptakan tindak pidana-tindak

¹⁷¹ Salman Luthan, *Op.cit*, hlm. 3.

¹⁷² Barda Nawawi Arief, "*Kebijakan Kriminalisasi dan Masalah Yurisdiksi...Op.cit*", Makalah Seminar Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi, Semarang, 26 Juli 2001, hlm. 2-3.

pidana. Penciptaan tindak pidana baru ini merupakan cerminan masyarakat dan negara pada waktu pembuatan undang-undang tersebut.¹⁷³

Suatu perbuatan dijadikan perbuatan pidana (*dikriminalisasikan*) karena alasan-alasan sebagai berikut :¹⁷⁴

1. Perbuatan itu merugikan masyarakat;
2. Sudah berulang-ulang dilakukan;
3. Ada reaksi sosial atas perbuatan itu.
4. Ada unsur bukti

Berdasarkan keempat parameter ini maka tidak serta merta perbuatan yang merugikan dapat dirumuskan secara formal sebagai perbuatan pidana (tindak pidana).

Sebagaimana telah dijelaskan di atas bahwa kriminalisasi merupakan upaya menjadikan suatu perbuatan menjadi tindak pidana. Proses kriminalisasi ini pada akhirnya akan berujung pada perumusan hukum pidana. Dengan demikian, proses kriminalisasi akan berkaitan erat dengan mekanisme penyelenggaraan hukum pidana.

Maka dalam rangka menanggulangi kejahatan terhadap berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa sarana pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya.

Apabila sarana pidana dipanggil untuk menanggulangi kejahatan, berarti akan dilaksanakan politik hukum pidana, yakni mengadakan pemilihan

¹⁷³ Sudarto, *Hukum dan Hukum Pidana... Op.cit*, hlm. 32.

¹⁷⁴ Tb. Rony R. Nitibaskara, *Op.cit*, 5 Mei 2006.

untuk mencapai hasil perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang.¹⁷⁵

Di samping usaha penanggulangan kejahatan, lewat pembuatan undang-undang pidana pada hakekatnya merupakan bagian integral dari usaha kesejahteraan masyarakat (*social welfare*). Oleh karena itu wajar pula apabila dikatakan, bahwa politik hukum pidana juga merupakan bagian integral dari kebijakan sosial (*social policy*).

Social policy dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat sekaligus mencakup perlindungan masyarakat. Jadi di dalam pengertian *social policy*, sekaligus didalamnya tercakup *social welfare policy* dan *social defence policy*.

Dilihat dari sudut yang luas tersebut, maka dapat ditegaskan bahwa masalah kebijakan hukum pidana pada hakikatnya bukanlah semata-mata pekerjaan teknik perundang-undangan yang dapat dilakukan secara yuridis normatif dan sistematik-dogmatik.

Di samping pendekatan yuridis normatif, kebijakan hukum pidana juga memerlukan pendekatan yuridis faktual yang dapat berupa pendekatan sosiologis, psikologis, historis dan komparatif, bahkan memerlukan pula pendekatan integral dengan kebijakan sosial dengan pembangunan nasional pada umumnya.

¹⁷⁵ Sudarto, *Hukum Pidana dan Perkembangan Masyarakat, ... Op.cit*, hlm.109.

Karena suatu undang-undang (hukum pidana) yang telah dirumuskan dan dilaksanakan, ia akan menggerakkan banyak badan dan orang untuk diterapkan. Ada korp polisi, badan penuntut umum (kejaksaan), pengadilan, lembaga pemasyarakatan, kedokteran (*forensik*) dan lain sebagainya.¹⁷⁶

Hukum pidana sejak dari proses pembentukan sampai penerapannya dalam masyarakat dengan demikian telah menghabiskan biaya yang tidak sedikit. Dan ini harus ditanggung oleh pemerintah yang pada gilirannya menjadi beban masyarakat. Hal ini tampak dalam APBN. Dan ini juga harus dipertimbangkan dalam upaya kriminalisasi.

Maka disini ada beberapa hal yang fundamental harus diperhatikan adalah sebagai berikut:¹⁷⁷

1. Tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil makmur secara material dan spiritual berdasarkan Pancasila; sehubungan dengan ini maka penggunaan hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan pengadugeraan terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman masyarakat.
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan perbuatan yang tidak dikehendaki, tidak disukai atau dibenci oleh warga masyarakat yaitu perbuatan yang merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban. Selain itu harus pula dipertimbangkan sejauh mana perbuatan tersebut bertentangan dengan nilai-nilai fundamental yang berlaku dalam masyarakat.
3. Perhitungan prinsip biaya dan hasil (*cost benefit principle*) dari penggunaan hukum pidana tersebut, yaitu apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya *cost* pembuatan undang-undang, pengawasan dan penegak hukum, serta beban yang dipikul oleh korban dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai.

¹⁷⁶ Sudarto, *Hukum dan Hukum Pidana*, ...*Op.cit*, hlm. 32.

¹⁷⁷ Sudarto, *Hukum Pidana dan Perkembangan Masyarakat*, ...*Op.cit*, hlm. 44-48.

4. Kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum, yaitu jangan sampai ada kelampauan beban tugas dan keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai.

Selain keempat hal tersebut diatas perlu pula berpedoman pada 6 (enam) asas yang dikemukakan **De Roos**, yaitu¹⁷⁸ :

1. Masuk akal nya kerugian yang digambarkan;
2. Adanya toleransi yang didasarkan pada kehormatan atas kebebasan dan tanggungjawab individu;
3. Apakah kepentingan yang dilanggar masih dapat dilindungi dengan cara lain;
4. Ada keseimbangan antara kerugian, toleransi dan pidana yang diancamkan;
5. Apakah kita dapat merumuskan antara kerugian, toleransi dan pidana yang diancamkan;
6. Kemungkinan penegakannya secara praktis dan efektif (serta dampaknya pada prevensi umum)

Sebab bila tidak demikian halnya, maka akan terjadi apa yang dimakan *over criminalization* (kelebihan perbuatan yang dijadikan tindak pidana). Pada gilirannya hal ini akan menimbulkan *inflasi pidana*, sehingga penghargaan terhadap hukum pidana tidak pada semestinya lagi.

Berkaitan dengan kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*), maka pertama-tama yang harus ditentukan terlebih dahulu adalah bentuk pengaturannya. Ada beberapa pilihan dalam mengatur atau pendekatan kriminalisasi *cyber crime*, yakni:¹⁷⁹

1. Diintegrasikan ke dalam kodifikasi (KUHP) dengan cara: menambah, menyisipi atau merubah/memperbarui pasal-pasal dalam KUHP.

¹⁷⁸ Marjono Reksodiputro, *Op.cit*, hlm.5.

¹⁷⁹ Al Wisnubroto, "Cyber Crime Permasalahan dan Penanggulangan dari Aspek Hukum Pidana", *Diskusi Bagian Kepidanaan*, FH UMY, 6 Juli 2000, hlm. 4-6.

- a. Perbaikan Buku I
- b. Penambahan Kejahatan pada Buku II
- c. Konsep KUHP

2. Undang-undang Khusus

Suatu pengaturan secara khusus diperlukan apabila tindak pidana *cyber crime* dianggap sebagai kejahatan kategori baru (*new category of crime*) yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan biasa, dan karena itu perlu diatur secara tersendiri di luar KUHP.

Sedangkan apabila menganggap tindak pidana *cyber crime* sebagai kejahatan biasa (*ordinary crime*) yang dilakukan dengan komputer teknologi tinggi (*high-tech*) dan KUHP dapat dipergunakan untuk menanggulangnya baik melalui amandemen KUHP maupun perubahan KUHP secara menyeluruh.¹⁸⁰

Untuk menentukan pilihan tersebut maka secara konseptual harus mempertimbangkan sistem hukum (pidana) di Indonesia. **Rene David** pernah mengatakan bahwa sistem hukum di Indonesia adalah *mixed system of law*¹⁸¹.

Namun dibidang hukum publik khususnya hukum pidana tradisi hukum kontinental nampak lebih menonjol dalam praktek dan pengembangan ilmu hukum. Oleh sebab itu pengembangan pengaturan mengenai masalah

¹⁸⁰ Marjono Reksodiputra, *Op.cit*, hlm. 2-3.

¹⁸¹ Barda Nawawi Arief, "Beberapa Aspek Pengembangan Ilmu Hukum Pidana: Menyongsong Generasi Baru Hukum Pidana Indonesia", *Naskah Pidato Pengukuhan Guru Besar dalam Ilmu Hukum Pidana*, Universitas Diponegoro Semarang, 15 Juli 1994, hlm. 24.

tindak pidana *cyber crime* lebih tepat apabila menggunakan pendekatan integratif dengan pengaturan dalam KUHP baik melalui amandemen maupun perubahan menyeluruh KUHP.

Dengan demikian setidaknya terdapat tiga hal yang perlu dipertimbangkan dalam mengkriminalisasikan *cyber crime*, yaitu:¹⁸²

- a) Hendaknya dipilih perbuatan-perbuatan yang benar-benar merugikan dan dapat menimbulkan akses serius (prinsip selektif dan limitatif) agar pengaturan perbuatan yang dikategorikan sebagai *cyber crime* tidak bersifat *overcriminalization* sehingga justru akan berdampak *counterproductive* bagi pengembangan teknologi komputer di bidang multimedia atau TI yang sangat dibutuhkan oleh negara Indonesia dalam menghadapi era globalisasi.
- b) Hendaknya dipertimbangkan apakah biaya yang harus dikeluarkan untuk menyusun ketentuan yang mengatur *cyber crime* yang dikategorikan sebagai tindak pidana *cyber crime* yang bersifat rumit dan kompleks, biaya untuk mengawasi dan menegakkan ketentuan tersebut yang memerlukan fasilitas atau sarana teknologi tinggi dan beban yang harus dipikul korban akan berimbang dengan hasil yaitu situasi tertib hukum di dunia *cyber* (*cost and benefit principle*)
- c) Hendaknya dipertimbangkan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum di Indonesia yang nantinya akan dibebani tugas untuk menegakkan ketentuan yang mengatur delik komputer yang dikategorikan sebagai tindak pidana *cyber crime*, sehingga tidak terjadi beban tugas yang bersifat *overbelasting* sehingga banyak peraturan yang dibuat ternyata dalam prakteknya di lapangan tidak dapat ditegakkan.

Kebijakan kriminalisasi terhadap *cyber crime* telah diupayakan dalam Konsep Rancangan Undang-Undang KUHP yang baru (konsep 2005/2006), Rancangan Undang-Undang RUU Informasi dan Transaksi Elektronik dan Tindak Pidana di Bidang Teknologi Informasi.

¹⁸² Al Wisnubroto, *Cyber Crime Permasalahan dan Op... cit*, hlm. 5-6.

Dalam Rancangan Undang-Undang KUHP tersebut mengatur regulasi yang mendukung dalam kebijakan kriminalisasi *cyber crime*. Ini terlihat dalam beberapa ketentuan :

1. Rancangan Undang-Undang KUHP dalam Buku I

- 1) *Pasal 158*. Pengertian "*Anak Kunci*", yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu magnetik, atau signal yang telah diprogram yang dapat digunakan untuk membuka sesuatu oleh orang lain diberi hak untuk itu.
- 2) *Pasal 165*. Pengertian "*Barang*" yang di dalamnya termasuk benda berwujud termasuk air dan uang giral dan benda tidak berwujud termasuk aliran listrik, gas, data dan program komputer, jasa termasuk jasa telepon, jasa telekomunikasi, atau jasa komputer.
- 3) *Pasal 186*. Pengertian "*Masuk*" yang didalamnya termasuk mengakses komputer atau kedalam sistem komputer.
- 4) *Pasal 174*. Pengertian "*Jaringan Telepon*" yang termasuk didalamnya jaringan komputer atau sistem komunikasi komputer.
- 5) *Pasal 203*. Pengertian "*Pornografi*" yang didalamnya termasuk substansi dalam media atau komunikasi yang dibuat untuk menyampaikan gagasan-gagasan yang mengeksploitasi seksual, kecabulan, dan/atau erotika.
- 6) *Pasal 204*. Pengertian "*Ruang*" yang di dalamnya termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu.
- 7) *Pasal 207*, Pengertian "*Surat*" yang di dalamnya termasuk surat yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpanan komputer atau media penyimpan data elektronik lain.

2. Rancangan Undang-Undang KUHP dalam Buku II

- 1) *Pasal 300*. Menyadap pembicaraan yang berlangsung di dalam atau diluar, atau ruangan atau halaman tertutup atau yang berlangsung melalui telepon padahal bukan menjadi peserta pembicaraan tersebut dengan alat bantu teknis;
- 2) *Pasal 301*. Memasang alat bantu teknis untuk tujuan mendengar atau merekam suatu pembicaraan.

- 3) *Pasal 302*. Memiliki barang yang diketahui atau patut diduga memuat hasil pembicaraan yang diperoleh dengan mendengar atau merekam.
- 4) *Pasal 373*. Penggunaan dan Perusakan Informasi Elektronik (setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik).
- 5) *Pasal 374*. Penyelenggara agen elektronik yang tidak menyediakan fitur pada agen elektronik yang dioperasikannya yang memungkinkan penggunaanya melakukan perubahan informasi yang masih dalam proses transaksi.
- 6) *Pasal 376*, Tanpa Hak Mengakses Komputer dan Sistem Elektronik
 - a. Menggunakan, mengakses komputer, dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara dan/atau hubungan dengan subjek hukum internasional;
 - b. Melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah komputer dan/atau sistem elektronik yang dilindungi negara menjadi rusak;
 - c. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan/atau sistem elektronik yang dilindungi oleh negara;
 - d. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik milik pemerintah yang dilindungi secara tanpa hak;
 - e. Menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;
 - f. Menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;
 - g. Mempengaruhi atau mengakibatkan terganggunya komputer dan/atau sistem elektronik yang digunakan oleh pemerintah;
 - h. Menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses (*passwod*) atau informasi yang serupa dengan hal tersebut, yang

dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan komputer dan/atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah;

- i. Melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun; atau
 - j. Melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun.
- 7) *Pasal 377*, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi.

8) *Pasal 378*:

- 1. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari bank sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;
- 2. Menggunakan data atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan;
- 3. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik bank sentral, lembaga perbankan dan/atau lembaga keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, dengan maksud menyalahgunakan, dan/atau untuk mendapatkan keuntungan dari padanya; atau
- 4. Menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik bank sentral, lembaga perbankan dan/atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

9) *Pasal 379*. Pornografi Anak melalui Komputer

Setiap orang yang tanpa hak melakukan tindak pidana yang berkaitan dengan pornografi anak berupa :

- 1) Memproduksi pornografi anak dengan tujuan untuk didistribusikan melalui sistem komputer;
- 2) Menyediakan pornografi anak melalui suatu sistem komputer;
- 3) Mendistribusikan atau mengirimkan pornografi anak melalui sistem komputer;
- 4) Membeli pornografi anak melalui suatu sistem komputer untuk diri sendiri atau orang lain; atau
- 5) Memiliki pornografi anak didalam suatu sistem komputer atau dalam suatu media penyimpanan data komputer;

10). *Pasal 735-736. Pencucian Uang atau Money Laundering.*

2. RUU Informasi dan Transaksi Elektronik

1. *Pasal 30. Setiap orang dilarang:*

- (1) Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan atau sistem elektronik
- (2) Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi
- (3) Menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan melampaui batas wewenangnya, dengan maksud memperoleh informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap Negara dan atau hubungan dengan subjek hukum Internasiol.

2. *Pasal 31. Setiap orang dilarang melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah, komputer dan atau sistem elektronik yang dihubungi negara menjadi rusak.*

3. *Pasal 32. Setiap orang dilarang menggunan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan atau sistem elektronik yang dilindungi oleh negara.*

4. *Pasal 33. Setiap orang dilarang dengan sengaja dan melawan hukum :*

- (1) Menggunakan dan atau mengakses komputer dan atau sistem elektronik milik pemerintah yang dilindungi secara tanpa hak.
- (2) Menggunakan dan atau mengakses tanpa hak atau melampaui wewenangnya komputer dan atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer dan atau sistem elektronik tersebut menjadi rusak
- (3) Menggunakan dan atau mengakses tanpa hak atau melampaui wewenangnya komputer dan atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer dan atau sistem elektronik tersebut menjadi rusak.
- (4) Mempengaruhi atau mengakibatkan terganggunya komputer dan atau sistem elektronik yang digunakan oleh pemerintah.

5. *Pasal 34.* Setiap orang dilarang:

- (1) Menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya.
- (2) Menggunakan dan atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan.

6. *Pasal 35.* Setiap orang dilarang menggunakan dan atau mengakses komputer dan atau sistem elektronik Bank Sentral, lembaga perbankan dan atau lembaga keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, dengan maksud menyalahgunakan, dan atau untuk mendapatkan keuntungan daripadanya

7. *Pasal 36.* Setiap orang dilarang dengan sengaja dan melawan hukum :

- (1) Menyebabkan, memperdagangkan, dan atau memanfaatkan kode akses (*password*) atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik keuangan dan atau perbankan, serta perniagaan didalam dan diluar negeri.
- (2) Menyebarkan, memperdagangkan, dan atau memanfaatkan kode akses (*password*) atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan

tujuan untuk menyalahgunakan komputer dan atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah.

8. *Pasal 37.* Setiap orang dilarang melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun

3. RUU Tindak Pidana di Bidang Teknologi Informasi

1. *Pasal 3.* Setiap orang dilarang:

- (1) Setiap orang dilarang dengan sengaja atau tidak sengaja melakukan akses tanpa hak, secara tidak sah, atau ilegal
- (2) Setiap orang dilarang dengan sengaja atau tidak sengaja melakukan intersepsi tanpa hak, secara atau ilegal.
- (3) Setiap orang dilarang dengan sengaja atau tidak sengaja merusak atau mengganggu data yang tersimpan dalam alat penyimpanan data elektronik yang tersusun sebagai bagian dari sistem komputer
- (4) Setiap orang dilarang dengan sengaja atau tidak sengaja atau tidak sengaja menghilangkan bukti-bukti elektronik yang dapat dijadikan alat bukti sah dipengadilan yang terdapat pada suatu sistem informasi atau sistem komputer.
- (5) Setiap orang dilarang dengan sengaja atau tidak sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer dan internet.
- (6) Setiap orang dilarang dengan sengaja atau tidak sengaja menggunakan teknologi informasi untuk menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi.
- (7) Setiap orang dilarang dengan sengaja atau tidak sengaja menggunakan teknologi informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat-sifat pornografi.
- (8) Setiap orang dilarang dengan sengaja atau tidak sengaja menggunakan teknologi informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.
- (9) Perusahaan penyelenggara akses internet, atau penyelenggara layanan teknologi informasi, baik untuk keperluan komersial maupun keperluan internal perusahaan, diwajibkan memelihara catatan transaksi elektronik, secara periodik, sekurang-kurangnya dua tahun. Kelalaian atau kesengajaan yang dilakukan oleh pengelola sistem komputer yang

berakibat pada tidak tersedianya catatan transaksi elektronik dapat dianggap sebagai pelanggaran terhadap undang-undang ini, terutama jika terjadi tindak kejahatan yang terungkap dan memerlukan catatan transaksi elektronik dari institusi atau organisasi bersangkutan.

2. *Pasal 4.* Barangsiapa menggunakan teknologi informasi dengan maksud untuk memfasilitasi usaha-usaha penghilangan nyawa orang, atau usaha menggulikan pemerintahan yang sah, atau membahayakan keamanan negara dalam bentuk terpisahnya sebagian dari wilayah negara ke tangan musuh, atau sebagai bagian dari kegiatan teror.
3. *Pasal 5.* Barangsiapa melakukan pencurian dengan menggunakan teknologi informasi sehingga memenuhi ketentuan sebagaimana dinyatakan pada pasal 362 KUHP.
4. *Pasal 6.* Barangsiapa masuk ke dalam lingkungan atau sarana fisik sistem informasi tanpa hak atau secara tidak sah menggunakan sandi akses palsu, melakukan pembongkaran atau kerusakan dengan tanpa maksud merugikan pemilik sah.
5. *Pasal 7.* Barangsiapa masuk ke dalam lingkungan dan atau sarana fisik sistem informasi milik instansi pemerintah, militer, perbankan atau instansi strategis lainnya yang ditetapkan dengan Peraturan Pemerintah, tanpa hak atau secara tidak sah dengan menggunakan sandi akses palsu, melakukan pembongkaran atau merusak dengan atau tanpa maksud merugikan instansi dituju.
6. *Pasal 8.*
 - (1) Barangsiapa dengan sengaja atau tidak sengaja terbukti menggunakan teknologi informasi untuk melakukan transaksi elektronik menggunakan identitas palsu, atau identitas milik orang lain.
 - (2) Bila transaksi elektronik pada ayat 1 diatas disertai dengan transaksi ekonomi menggunakan alat pembayaran berupa kartu kredit, atau kartu debit atau lainnya yang bukan miliknya yang sah.
7. *Pasal 9.* Barangsiapa dengan sengaja atau tidak sengaja dan tanpa hak merubah, menghapus, atau menghilangkan sebagian data komputer yang menyebabkan hilangnya keaslian data dan menggunakan data yang tidak asli tersebut untuk keperluan lain yang sah, dikategorikan sebagai tindakan pemalsuan.
8. *Pasal 10.* Barangsiapa dengan sengaja atau tidak sengaja dan tanpa hak menyebabkan kerugian ekonomi pada pihak lain dengan cara

memasukkan, merubah, menghapus, atau menghilangkan sebagian data komputer atau mengganggu mekanisme kerja sistem komputer.

9. *Pasal 11.* Barangsiapa menggunakan teknologi informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat-sifat pornografi sehingga memenuhi ketentuan Pasal 281, 282, 283, KUHP.
10. *Pasal 12.* Barangsiapa dengan sengaja atau tidak sengaja dan tanpa hak menggunakan teknologi informasi untuk menyimpan, memproduksi, menyebarkan, atau menawarkan bahan-bahan atau informasi yang bersifat pornografi dengan menggunakan anak-anak sebagai model atau sasarannya.
11. *Pasal 13.* Barangsiapa dengan sengaja atau tidak sengaja menggunakan teknologi informasi untuk membantu terjadinya percobaan, atau perekrutungan yang menjurus pada kejahatan.
12. *Pasal 14.* Barangsiapa dengan sengaja atau tidak sengaja dan tanpa hak melakukan akses kepada komputer tertentu yang statusnya dilindungi, atau melanggar hak akses yang diberikan kepadanya, dengan maksud untuk mencuri atau memperoleh sesuatu yang tidak menjadi haknya.
13. *Pasal 15.* Barangsiapa menggunakan teknologi informasi untuk melakukan teror sehingga memenuhi ketentuan yang tercantum dalam Undang-Undang Anti Teror.
14. *Pasal 16.* Barangsiapa dengan sengaja atau tidak sengaja melakukan intersepsi tanpa hak, secara tidak sah, atau ilegal.
15. *Pasal 17 :*
 - (1) Barangsiapa dengan sengaja atau tidak sengaja terbukti merusak situs internet milik orang lain sehingga menyebabkan kerugian yang bersifat material.
 - (2) Jika situs internet yang merusak tersebut milik pemerintah, militer atau situs internet lain yang termasuk dilindungi.
16. *Pasal 18.* Barangsiapa tanpa hak melakukan penyadapan terhadap komunikasi data sistem komputer yang berhubungan dalam jaringan komputer lokal maupun global (internet).
17. *Pasal 19.* Barangsiapa memalsukan nomor Internet Protocol untuk berkomunikasi dengan pihak lain yang menimbulkan kerugian material.
18. *Pasal 20.* Barangsiapa dengan sengaja mengacaukan atau membuat sistem komputer tidak dapat berfungsi sebagaimana mestinya dengan cara

merusak data base atau teknologi enkripsi yang ada pada sistem komputer tersebut .

19. *Pasal 21.* Barangsiapa menggunakan nama domain milik orang lain sehingga merugikan pemiliknya yang sah.
20. *Pasal 22.* Barangsiapa menggunakan surat elektronik untuk mengumumkan, menawarkan atau menjual barang dan atau jasa yang sifatnya melanggar hukum.
21. *Pasal 23.* Barangsiapa memalsukan atau menggunakan alamat surat elektronik milik orang lain tanpa seijin yang berhak.
22. *Pasal 24.* Barangsiapa menggunakan teknologi informasi untuk mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seijin yang bersangkutan.
23. *Pasal 25.* Barangsiapa menyalahgunakan peralatan teknologi informasi di luar sebagaimana yang telah diperuntukkannya dan menimbulkan kerugian material bagi pihak lain.

Sedangkan apabila memperhatikan perkembangan pengaturan yang dilakukan dalam *Convention for Cyber Crime* yang ditandatangani oleh 30 Negara dari Dewan Eropa pada bulan November 2001 di Budapest Hungaria maka kategori delik *cyber crime* adalah:¹⁸³

1. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk didalamnya: mengakses sistem komputer tanpa hak, tanpa hak menangkap/mendengar pengiriman dan pemancaran, tanpa hak merusak data, tanpa hak mengganggu sistem, menyalahgunakan perlengkapan.
2. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer)
3. Delik-delik yang bemuatan pornografi anak
4. Delik-delik yang berhubungan dengan hak cipta.

Bertolak dari uraian diatas, maka dilihat dari sudut kebijakan hukum pidana (*penal policy*), kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/merumuskan/memformulasikan perbuatan apa yang dapat dipidana

¹⁸³ Mardjono Reksodiputro, *Op... cit*, hlm. 3-4.

(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.

Oleh karena itulah pada intinya kebijakan kriminalisasi *cyber crime* ini seyogyanya dikaji masalah harmonisasi materi/substansi tindak pidana dan harmonisasi kebijakan formulasi tindak pidana di bidang *cyber crime*. Selanjutnya Barda Nawawi Arief menjelaskan, harmonisasi eksternal/global ini mutlak diperlukan, mengingat sifat hakiki dari *cyber crime* ini sebagai *global crime*.¹⁸⁴, Maka perlu adanya suatu asas yang memungkinkan menarik pelaku yang berada di luar wilayah Indonesia yang merugikan Indonesia.

Kalau kita lihat draft *Convention on Cyber Crime*. Dalam artikel 22 draft tersebut antara lain :

1. Tiap pihak (negara) akan mengambil langkah-langkah legislatif dan langkah lain yang diperlukan untuk menetapkan yurisdiksi terhadap setiap tindak pidana yang ditetapkan sesuai dengan Pasal 2 sampai Pasal 11 konvensi ini, apabila tindak pidana itu dilakukan:
 - a. Di dalam wilayah teritorialnya; atau
 - b. Di atas kapal yang mengibarkan bendera negara yang bersangkutan, 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 atau apabila tindak pidana itu dilakukan di luar yurisdiksi teritorial setiap negara.
2. Tiap negara berhak untuk tidak menerapkan atau hanya menerapkan aturan yurisdiksi sebagaimana disebutkan dalam ayat (1) b - ayat (1) d pasal ini dalam kasus-kasus atau kondisi-kondisi tertentu.

¹⁸⁴ Barda Nawawi Arief, *Kapita Selekta Hukum Pidana... Op.cit*, hlm. 259.

3. Tiap pihak (negara) akan mengambil langkah-langkah yang diperlukan untuk menetapkan yurisdiksi terhadap tindak pidana yang ditunjuk dalam Pasal 24 ayat (1) konvensi ini (pasal tentang ekstradisi).
4. Konvensi ini tidak meniadakan yurisdiksi kriminal yang dilaksanakan sesuai dengan hukum domestik (hukum negara yang bersangkutan).
5. Apabila lebih dari 1 (satu) pihak (negara) menyatakan berhak atas yurisdiksi tindak pidana dalam konvensi ini, maka para pihak yang terlibat akan melakukan konsultasi untuk menetapkan yurisdiksi yang paling tepat untuk penuntutan.

Dalam KUHP sebenarnya sudah ada ketentuan yang memungkinkan hal tersebut dalam ketentuan Pasal 4. Walaupun demikian, pasal tersebut hanya mengatur delik tertentu saja. Demikian juga Pasal 5 KUHP.

Berkaitan dengan masalah yurisdiksi Barda Nawawi Arief menganjurkan untuk menerapkan prinsip "*ubikuitas*", maksudnya adalah prinsip yang menyatakan, bahwa delik-delik yang terjadi di sebagian wilayah teritorial negara dan sebagian di luar teritorial negara, harus dapat dibawa kedalam yurisdiksi.¹⁸⁵

Dalam Rancangan Undang-Undang Teknologi Informasi tentang yurisdiksi ini diatur dalam Pasal 25 dan 26. Akan tetapi RUU ini tidak menggunakan istilah "*ubikuitas*". Walaupun demikian dari ketentuan kedua pasal tersebut mengandung makna prinsip tersebut (*ubikuitas*).

Di samping memodernisasi hukum pidana nasional Indonesia juga harus aktif dalam kesepakatan internasional tentang kejahatan ini. Terutama sekali terhadap konvensi tentang ekstradisi yang berkenaan dengan *cyber crime*.

¹⁸⁵ *Ibid*, hlm. 265.

Memang dalam bidang hukum pidana, kita mempunyai asas yang memperluas tuntutan pidana (ketentuan Pasal 4 sampai 8), yang memberi wewenang dalam melakukan proses peradilan pidana atas perbuatan yang dilakukan di luar wilayah Indonesia. Namun demikian, tanpa adanya kesepakatan Internasional, misalnya ekstradisi tentu tidak akan bisa memaksakan berlakunya hukum nasional kepada negara lain. Di samping itu juga, dalam berlakunya perluasan jangkauan penuntutan terbatas pada delik dan subjek hukum (pelaku) tertentu saja.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan uraian dan analisis terhadap permasalahan yang diteliti, maka dapat ditarik kesimpulan dan saran sebagai berikut :

1. *Cyber crime* dalam hukum pidana positif Indonesia, apabila diperhatikan telah memiliki pengaturan. Pengaturan itu dapat dilihat pada ketentuan di dalam KUHP, Pasal 112 tentang pembocoran rahasia negara, Pasal 322 tentang membuka rahasia perusahaan, Pasal 282 tentang pornografi, Pasal 362 Pencurian, Pasal 369 tentang pemerasan dan pengancaman, Pasal 378 tentang penipuan, Pasal 372 tentang pengelapan, Pasal 382 bis tentang pelanggaran nama domain, Pasal 406 tentang perusakan, Pasal 506 tentang prostitusi (Pelanggaran Ketertiban Umum).

Di samping KUHP beberapa ketentuan perundang-undang diluar KUHP seperti, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Namun demikian, pengaturan *cyber crime* dalam hukum pidana positif Indonesia ada beberapa dari *cyber crime* yang dapat dijerat dengan hukum pidana Indonesia, dan sebagian lagi tidak dikarenakan kejahatan ini relatif baru, oleh karena itu, timbul berbagai permasalahan dalam prakteknya. Misalnya masalah *hacking* karena tidak memenuhi unsur-unsur didalam KUHP, dengan demikian terjadi kekosongan hukum untuk menjangkau kejahatan ini apabila dikaitkan dengan unsur-unsur delik yang diatur dalam

KUHP. Bertolak dari hal tersebut maka menurut hemat penulis perlu adanya kebijakan kriminalisasi atau pembaharuan hukum pidana (KUHP).

2. Kebijakan kriminalisasi *cyber crime* dalam konteks hukum pidana yang akan datang (*Ius Constituendum*), dimana upaya untuk mengantisipasi atas *cyber crime* ini, telah dilakukan dalam hal ini dituangkan dalam Konsep Rancangan Undang-Undang KUHP yang baru (konsep 2005/2006): Buku I Pasal 158 pengertian "*Anak kunci*", Pasal 165 pengertian "*Barang*", Pasal 186 pengertian "*Masuk*", Pasal 174 pengertian "*Jaringan telepon*", Pasal 203 pengertian "*Pornografi*", Pasal 204 pengertian "*Ruang*", Pasal 207 pengertian "*Surat*."

Buku II Pasal 300 tentang Menyadapan pembicaraan, Pasal 301 Memasang alat bantu teknis, Pasal 373 Penggunaan dan kerusakan informasi elektronik, Pasal 374 Pengubahan informasi yang masih dalam proses transaksi, Pasal 376 tanpa hak mengakses komputer dan sistem elektronik, Pasal 377 mengubah dan merusak atau menghilangkan informasi milik pemerintahan, Pasal 378 menggunakan dan mengakses tanpa hak, Pasal 379 Pornografi anak melalui komputer, Pasal 735-736 pencucian uang atau *Money Laundering*, dan juga kebijakan kriminalisasi *cyber crime* ini dengan Rancangan Undang-Undang RUU Informasi dan Transaksi Elektronik dan Tindak Pidana di Bidang Teknologi Informasi.

B. Saran-Saran

1. Segera disahkan Undang-undang yang berkaitan dengan *cyber law* umumnya dan *cyber crime* khususnya.
2. Sebelum adanya aturan khusus tentang *cyber crime*, hakim, aparat penegak hukum lainya harus berani melakukan "*rechtsvinding*" (penemuan hukum).
3. Dalam kebijakan kriminalisasi *cyber crime* tersebut perlu mempertimbangkan draft internasional yang telah ditandatangani di Budapest pada tanggal 23 November 2001, (*draft Conventional on Cyber Crime*") yang berkaitan dengan *cyber crime*, mengingat kejahatan ini merupakan "*global crime*" maka perlu adanya suatu asas yang memungkinkan menarik pelaku yang berada di luar wilayah Indonesia yang merugikan Indonesia, dikarenakan yurisdiksi kejahatan ini tidak jelas.

DAFTAR PUSTAKA

A. Buku

- Andi Zainal Abidin, 1987. *Asas-asas Hukum Pidana Baigan Pertama*, ctk. Pertama, Alumni, Bandung.
- Andi Hamzah, 1994. *Asas-Asas Hukum Pidana*, ctk. Kedua, Rineka Cipta, Jakarta.
- Al. Wisnusobroto, 1999. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Universitas Atmajaya, Yogyakarta.
- Ade Manan Suherman, 2000. *Aspek Hukum dalam Ekonomi Global*, ctk. Pertama, Ghalian Indonesia, Jakarta.
- Agus Raharjo, 2002. *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, ctk. Pertama, Citra Aditya Bakti, Bandung.
- Abdul Wahid, 2002. *Kriminologi dan Kejahatan Kontemporer*, ctk. Pertama, Lembaga Penerbit Fakultas Hukum Unisba, Malang.
- , *et.al*, 2005. *Kejahatan Mayantara (Cyber Crime)*, ctk. Pertama, Refika Aditama, Bandung, 2005.
- Ahmad M. Ramli, 2004. *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, ctk. Pertama, Refika Aditama, Bandung.
- Bernard Arief Sidharta, 2000. *Refleksi Tentang Struktur Ilmu Hukum*, Bandar Maju, Bandung.
- Barda Nawawi Arief, 2002. *Bunga Rampai Kebijakan Hukum Pidana*, ctk. Kedua, PT. Citra Aditya Bakti, Bandung.
- , 2003. *Kapita Selekta Hukum Pidana*, ctk. Pertama, Citra Aditiya Bakti Bandung.
- CST. Kansil, 1989. *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, Balai Pustaka, Jakarta.
- Eliot D. Chappie, 1989. *Mengurangi Pita Merah*, dalam Lewis H. Lapham, *Teknologi Canggih dan Kebebasan Manusia*, ctk. Pertama, Yayasan Obor Indonesia, Jakarta.

- Edmon Makarim, 2003. *Kompilasi Hukum Telematika*, ctk. Pertama, Raja Grafindo Persada, Jakarta.
- Francois Raillon, 1990. *Indonesia Tahun 2000 (Tantangan Teknologi dan Industri)*, (terjemahan Nasir Tamara), ctk. Pertama, CV Haji Masagung, Jakarta.
- I.S. Susanto, 1995. *Kriminologi*, FH UNDIP Semarang.
- J.E. Sahetapy *et.al*, 1983. *Paradoks Dalam Kriminologi*, ctk. Pertama, CV Rajawali, Jakarta.
- , 1984. *Pisau Analisa Kriminologi*, ctk. Kedua, Armico, Bandung.
- Kartini Kartono, 1983. *Patologi Sosial*, ctk. Pertama, CV Rajawali, Jakarta.
- Moeljanto, 1987. *Asas-asas Hukum Pidana*, ctk. Keempat, Bina Aksara, Jakarta.
- , 1993. *Asas-Asas Hukum Pidana*, ctk. Kelima, Rineka Cipta, Jakarta.
- Muladi. *et.al.*, 1992. *Bunga Rampai Hukum Pidana*, ctk. Pertama, Alumni, Bandung.
- , *et.al*, 2005. *Teori-teori dan Kebijakan Pidana*, ctk. Ketiga, Alumni, Bandung.
- Mulyana W. Kusuma, 1982. *Realitas Sosial Kejahatan*, Prisma, LP3ES, Jakarta.
- M. Zaenal Arifin *et.al*, 2003. "Modus Operandi Cyber Crime di Indonesia Makin Canggih" Artikel dalam Analisis Hukum 2002, Jangan Tunggu Langit Runtuh, Jakarta, *hukumonline.com*, Justika Siar Publika, Jakarta.
- P.A.F. Lamintang, 1997. *Dasar-Dasar Hukum Pidana Indonesia*, ctk. Ketiga, Citra Aditya Bakti, Bandung.
- Paul Suparno, 2001. *Filsafat Konstruktivisme Dalam Pendidikan*, Kanisius, Yogyakarta.
- Romli Atmasasmita, 1983. *Kapita Selekta Kriminologi*, ctk. Kedua, Armico, Bandung.
- R. Soesilo, 1994. *KUHP Serta Komentar-komentarnya Lengkap Pasal Demi Pasal*, Politeia, Bogor.

Saswinadi Sasmojo *et.al*, tanpa tahun, *Budaya Sains, Teknologi dan Perubahan Masyarakat*, ctk. Pertama, Seri Penerbitan Sains, Teknologi dan Masyarakat.

Soeharto, 1993. *Hukum Pidana Materil (Unsur Objektif sebagai Dasar Dakwaan)*, ctk. Pertama, Sinar Grafika, Jakarta.

Sudarto, 1983. *Hukum Pidana dan Perkembangan Masyarakat*, ctk. Pertama. Sinar Baru, Bandung.

-----, 1986. *Hukum dan Hukum Pidana*, ctk. Pertama, Alumni, Bandung.

-----, 1990. *Hukum Pidana I*, ctk. Kedua, Penerbit Yayasan Sudarto, UNDIP, Semarang.

Suwondo, 1998. *Himpunan Karya Tentang Hukum Pidana*, Yogyakarta : Liberti, Yogyakarta.

Sumarni Prijohutomo, 1999. "Buku Ajar Hukum Pidana", *Fakultas Hukum Unilak*, Pekanbaru.

Soerjono Soekanto *et.al.*, 1986. *Kriminologi, Suatu Pengantar*, ctk. Pertama. Ghalian Indonesia, Jakarta.

T. Jacob, 1996. *Menuju Teknologi Berperikemanusiaan*, ctk. Pertama, Yayasan Obor Indonesia, Jakarta.

-----, 1993. *Manusia, Ilmu dan Teknologi*, ctk. Kedua, PT Tiara Wacana, Yogyakarta.

B. Makalah, Jurnal, Naskah Pidato, Materi kuliah

Aroma Elmina Martha, 2006. "Diktat Hukum Pidana dan Perkembangan Teknologi Informasi", *Pasca Sarjana Ilmu Hukum UII*, Yogyakarta.

Al Wisnubroto, 2000. "Cyber Crime Permasalahan dan Penanggulangan dari Aspek Hukum Pidana", *Diskusi Bagian Kepidanaan*, FH UMY, 6 Juli 2000.

Barda Nawawi Arief, 1994. *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Hukum Pidana*, Laporan Simposium Pembaharuan Hukum Pidana Nasional 1980 di Semarang. BP UNDIP Semarang.

- , 1994. "Beberapa Aspek Pengembangan Ilmu Hukum Pidana: Menyongsong Generasi Baru Hukum Pidana Indonesia", *Naskah Pidato Pengukuhan Guru Besar dalam Ilmu Hukum Pidana*, Universitas Diponegoro Semarang, 15 Juli 1994.
- , 2001. "Kebijakan Kriminalisasi dan Masalah Yurisdiksi Tindak Pidana Mayantara", Makalah *Seminar Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi*, Semarang, 26 Juli 2001.
- , 2001. "Antisipasi Penanggulangan *Cyber Crime* Dengan Hukum Pidana", Makalah pada *Seminar Nasional Cyberlaw*, diselenggarakan STH Bandung, 9 April 2001.
- Clinard & Yeager, 1980 *Corporate Crime*, The Free Press A Division of Mac Millan Publishing Co. Inc, New York.
- Chairul Huda, 2000. "Perkembangan Teknologi dan Tuntutan Reformasi Hukum," *Jurnal Magister Hukum UII*, Vol.2 No. 1, Februari 2000, hlm. 100-101.
- , 2004. "Kesalahan dan Pertanggungjawaban Pidana", *Ringkasan Disertasi Program Doktor*, Fakultas Hukum UI, Jakarta.
- H. Daud Silalahi, 1997. *Rencana Undang-Undang Alih Teknologi: Perbandingan Perspektif*, *Prisma*, No. 4 Th. XVI, April 1987, hlm. 40.
- I.S. Susanto, 1997. "Menciptakan Lingkungan Hidup yang Nyaman", *Pidato Dies Natalis UNDIP ke-40*, Semarang, 15 Oktober 1997.
- , 1990. "Statistik Kriminal Sebagai Konstruksi Sosial (Penyusunan, Penggunaan dan Penyebarannya, Suatu Studi Kriminologi)", *Ringkasan Disertasi untuk memperoleh Gelar Doktor dalam Ilmu Hukum di UNDIP*, Semarang. 10 Maret 1990.
- J.E. Sahetapy, 1994. "White Collar Crime, Sebuah Perspektif Viktimologi", *Jurnal Ilmu-ilmu Sosial 5* (Kejahatan Keras Putih), PAD IS UI dan PT Gramedia Pustaka Utama. Jakarta, Januari 1994, hlm. 3.
- Joann L. Miller, 1994. "White Collar Crime", *Jurnal Ilmu-ilmu Sosial 5* (Kejahatan Keras Putih), PAU IS UI dan PT Gramedia Pustaka Utama, Jakarta, Januari 1994, hlm. 31
- Johannes Sutoyo dan Adrianus Meliala, 1994. "Politik Kejahatan Terhadap Pelaku White Collar Crime", *Jurnal Ilmu-ilmu Sosial 5*, PAU IS UI dan PT Gramedia Pustaka Utama, Jakarta.

- Juwono Sudarsono, 1992. "Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial-Politik, Masyarakat", *Jurnal Sosiologi*, No. 3 Vol. 2, FISIP UI-Gramedia, Jakarta, 1992, hlm. 4.
- Mas Wigrantoro Roes Setiyadi, 2003. *Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, GIPI-Indonesia.
- , 2002 "Sistem Hukum Indonesia Dalam Menghadapi Potensi Kriminalitas di Dunia Cyber", disampaikan sebagai *Makalah dalam pelatihan Information Security, diselenggarakan oleh STT Telkom Bandung*, 4 April 2002.
- M. Abdul Kholiq, 2006. "Tinjauan Politik Hukum Pidana Tentang RUU APP", Makalah disampaikan pada *Kuliah Program Pasca Sarjana*, UII, Yogyakarta.
- Miftah Wirahadikusumah, 1992. "Logika dan Gramar Teknologi: Sebuah Tinjauan Psikoanalisis, Masyarakat": *Jurnal Sosiologi*, No. 5 Vol. 3, FISIP UI-Gramedia, Jakarta, 1992, hlm. 30.
- Marjono Reksodiputro, 2002. "Cyber Crime: Intellectual Property Rights, Ecommerce", *Penataran Nasional Hukum Pidana dan Kriminologi Indonesia (ASPEHUPIKI)* di FH Universitas Surabaya, 13-19 Januari 2002.
- Nandang Sutrisno, 2001. "Cyber Law: Problem dan Prospek Pengaturan Aktivitas Internet". Artikel dalam *Jurnal Hukum UII Yogyakarta*, No. 16. Vol.8. hlm. 37.
- Ridwan Kairandy, 1997. "Francise dan Kaitannya Sebagai Sarana Alih Teknologi: Suatu Tinjauan Hukum", *Jurnal Hukum Ius Quia Iustum*, No. 7 Vol. 4, FH UII Yogyakarta, 1997, hlm. 115-116.
- Ronny Hanitijo Soemitro, "Hukum dan Perkembangan Ilmu Pengetahuan dan Teknologi di dalam Masyarakat", *Pidato Pengukuhan Guru Besar Tetap Fakultas Hukum UNDIP*, Semarang 6 Desember 2004.
- Salman Luthan, 1999. "Kebijakan Kriminalisasi dalam Reformasi Hukum Pidana", *Jurnal Hukum*, Fakultas Hukum UII Yogyakarta, No. 11 Vol.6. 1999, hlm. 3.
- T. Mulya Lubis, 1987. "Alih Teknologi: Antara Harapan dan Kenyataan", *Prisma*, No. 4 Th. XVI, April 1987, hlm. 11.

C. Peraturan Perundang-Undangan

Undang-Undang Nomor Undang-Undang Dasar 1945

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 8 tahun 1981 tentang Hukum Acara Pidana

Undang-Undang Nomor 4 tahun 2004 Tentang Ketentuan-Ketentuan Pokok Kekuasaan Kehakiman

Undang-Undang Nomor 36 tahun 1992 tentang Telekomunikasi

Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta

Undang-Undang Nomor 25 tahun 2003 tentang Pencucian Uang

Ketentuan *Convention On Cybercrime* 2001 yang terkait dengan Hukum Positif Indonesia

D. Surat Kabar

Republika, Tanggal 27 Mei 2001.

Pikiran Rakyat, Tanggal 31 Agustus 2003.

Riau Mandiri, Tanggal 3 Agustus 2005.

Bisnis Indonesia, Tanggal 23 Maret 2006

Pikiran Rakyat, Tanggal 31 Agustus 2003.

Riau Post, Tanggal, 19 Maret 2007.

E. Data Elektronik

Achmad Ali, 2003. "Hukum dan Teknologi" *Makalah dalam seri diskusi panel PII*, Bandung, 17 Mei 2003 dapat dijumpai dalam situs di Internet: <http://www.pii.or.id/dunia-ir/di0803no02seminar1.html>.

Ari Julianto, *Cyber Crime: Sebuah Fenomena di Dunia Maya*, dapat dijumpai dala situs di internet, <http://www.Theceli.com/dokumen/jurnal/ajo/a002.shtml>.

Budi Rahardjo, "Implikasi Teknologi dan Internet Terhadap Pendidikan, Bisnis dan Pemerintahan, Siapkah Indonesia", Makalah pada *seminar di Riau*, dapat dijumpai di <http://budi.insan.co.id/articles/riau-it.doc>.

<http://www.mediaindo.co.id/cetak/berita.asp/>, 12 Juli 2006, 10.00

<http://students.ukdw.ac.id/-22033149/dani.htm>, 20 Desember 2006. 21.30

<http://www.Tempointeraktif.com/news/2003%5C6%5C24/1,1,25,id.html>, Yogyakarta Pusat Kejahatan Informasi/, 25 Juni 2003. 15.00

WWW. pemantauperadilan.com. Lihat: Eva Achjani Zulfa, *Ketika Jaman Meninggalkan Hukum*, 01 April 2003, [www. pemantauperadilan.com./](http://www.pemantauperadilan.com/), 20 Juli 2006. 16.00

<http://personal.tmlp.com/ddemelo/crime/classical.html>

Hotmilk@www.com. *Republika*, 16 Januari 2000, hlm. 15.

<http://www.law.gonzaga.edu/border...yberlaw.htm>

<http://dhani.singcat.com/internet/modul.php>. 18 Maret 2007.

<http://www.theceli.com.dokumen/jurnal/a0/a002.shtml>, 25 Nopember 2006.

[http://www. Sinarharapan. co.id/berita/0304/05/opi01.html](http://www.Sinarharapan.co.id/berita/0304/05/opi01.html). 23 Desember 2006.

<http://cybertech.cbn.net.id/detil.asp.kategori=Feature&newsno=14>.

<http://www.komputekonline.com/detail.cfm?ID=43>. 27 Januari 2007

Sumber Data, *Mabes Polri, Berita Buser Siang RCTI*, Tanggal 26 Maret 2007.

Tb. Rony R. Nitibaskara, "Problem Yuridis Cyber Crime". Kompas Online, dapat dijumpai dalam situs di internet: [http://www. kompas.com/kompas-cetak/007/31/poin/prob04.htm](http://www.kompas.com/kompas-cetak/007/31/poin/prob04.htm), 5 Mei 2006.

Widi Prajo, *Internet Fraud; Suatu Tantangan Bagi Auditor*, tulisan ini dapat dijumpai secara online di internet dalam situs Budi Raharjo, 12 Nopember 2006.