SKRIPSI

CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA INDONESIA

BERNARDUS K. DANIBAO
NIM: 030010852-U

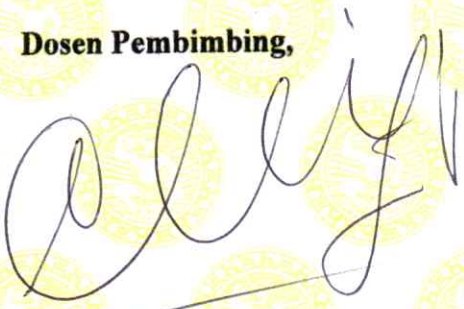
FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2005

CYBERCRIME DALAM PERSPEKTIF HUKUM PIDANA INDONESIA

SKRIPSI

DIAJUKAN UNTUK MELENGKAPI TUGAS DAN MEMENUHI SYARAT GUNA MEMPEROLEH GELAR SARJANA HUKUM

Dosen Pembimbing,



Didik Endro Purwoleksono, S.H., M.H.
NIP: 131 570 341

Penyusun,

Bernardus K. Danibao
NIM: 030010852-U

FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2005

Skripsi ini telah diuji dan dipertahankan di hadapan Panitia Penguji

Pada hari Jum'at, tanggal 25 Pebruari 2005

Panitia Penguji Skripsi :

Ketua : **Muhammad Zaidun, S.H., M.Si.**

Anggota : **1. Didik Endro Purwoleksono, S.H., M.H.**

2. Nur Basuki Minarno, S.H., M.Hum

3. Toetik Rahayuningsih, SH., M.Hum.

MOTTO :

"I may not totally perfect

but parts of me are excellent;

Thus, I always expect for the best

and prepare for the worst"

KATA PENGANTAR

Syukur dan Pujian penulis haturkan kepada Allah Tri Tunggal Terkudus karena hanya atas kasih dan penyertaan-Nya, penulis boleh menyelesaikan skripsinya yang berjudul "*CYBERCRIME* DALAM PERSPEKTIF HUKUM PIDANA INDONESIA".

Ucapan terimakasih dan rasa syukur, juga penulis haturkan buat semua pihak, yang telah dengan caranya masing-masing membantu penulis sejak awal hingga akhir dari penulisan skripsi ini, khususnya kepada :

1. Bapak Didik Endro Purwoleksono, S.H., M.H., yang telah dengan sangat sabar membimbing penulis dalam menyelesaikan skripsi ini.
2. Bapak Muhammad Zaidun, S.H., M.Si., Bapak Nur Basuki M., S.H., M.Hum. dan Ibu Toetik Rahayuningsih, S.H., M. Hum., yang telah berkenan menjadi penguji skripsi ini.
3. Bapa dan Mamaku (Markus Tolan dan Kelara Keri), Saudara dan Saudariku (P. Damas, SVD., P. John, SVD., Sr. Damiana, SSPS., Dionisia Ana, Margaretha Somi, Laurensius Danibao, dan Gerterudis Danibao). Terimakasih untuk doa dan kasihmu yang sangat penulis rasakan dalam penyelesaian skripsi ini.
4. *My bossom friend* 'Anna Rullia *or* Ollien' yang selalu mengingatkan dan setia membantu penulis dalam penyelesaian skripsi ini.

5. Teman-teman seangkatan, Hendrik, Marhaniyanto, Fendy, Rudy, Iwan, Rosita, Ilham dan Ika Rindri. Setiap sapaan dan teguranmu merupakan pendorong bagiku untuk segera menyelesaikan skripsi ini.

Penulis menyadari bahwa 'tak ada gading yang tak retak', dan tak ada tulisan yang sempurna. Demikian pun dengan skripsi penulis ini. Karena itu, setiap kritik dan saran yang konstruktif akan penulis terima dengan senang hati. Semoga dalam keterbatasannya, skripsi ini masih berguna bagi yang memerlukan informasi seputar *cybercrime* dan ketentuan hukum pidana yang berkaitan dengan kejahatan mayantara di negeri kita yang tercinta ini.

Surabaya, 21 February 2005

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

BAB I

PENDAHULUAN

1. Latar Belakang dan Rumusan Masalah

Perkembangan teknologi informasi dan telekomunikasi dewasa ini mengalami peningkatan yang sangat cepat. Hal ini ditandai dengan lahirnya berbagai macam jasa dan fasilitas telekomunikasi serta semakin canggihnya produk teknologi informasi yang mampu mengintegrasikan semua media informasi. Salah satu diantaranya adalah apa yang disebut dengan *the international network of interconnected computers* atau yang lebih dikenal dengan sebutan internet[1].

Internet adalah sebuah alat penyebaran informasi secara global, sebuah mekanisme penyebaran informasi, dan sebuah media untuk berkolaborasi dan berinteraksi antar individu dengan menggunakan komputer tanpa terhalang batas geografis. Internet adalah sebuah contoh sukses dari investasi teknologi yang telah menghadirkan berbagai kemudahan bagi setiap orang, bukan saja untuk berkomunikasi, tetapi juga untuk melakukan banyak hal lainnya seperti transaksi bisnis[2].

---

[1] Internet ditahun 2000-2005, dapat ditemukan di http://search yahoo.com. hukum kejahatan internet.

[2] Agus Raharjo, Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Jilid I, Citra Aditya Bakti, Bandung, 2002, h. 59

Kehadiran internet telah membuka cakrawala baru dalam kehidupan manusia. Internet dengan segala fasilitas yang menyertainya seperti *e-mail*, *chatting*, *video telekonferensi* dan *situs web site* telah memungkinkan dilakukannya penyebaran informasi dan komunikasi secara global tanpa batas teritorial dengan biaya murah, akses cepat dan langsung. Internet telah membawa manusia kepada ruang atau dunia baru yang tercipta yang dinamakan *cyberspace*. *Cyberspace* adalah suatu istilah yang populer saat ini untuk media atau ruang informasi dan komunikasi yang begitu luas di internet sebagaimana yang ditulis oleh Agus Raharjo sebagai berikut:

> *Cyberspace* menampilkan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat, melainkan realitas virtual (*virtual reality*), dunia maya, dunia tanpa batas. Inilah yang dimaksud dengan *borderless world* karena memang dalam *cyberspace* tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu dan tempat sehingga penghuni-penghuninya bisa berhubungan dengan siapa saja dan dimana saja[3]:

Penggunaan internet dalam perkembangannya, selain berdampak positif juga membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti-sosial dan perilaku kejahatan yang selama ini dianggap tidak mungkin terjadi. Sebagaimana sebuah teori mengatakan, "*crime is a product of society itself*", yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas suatu masyarakat, semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat itu. Dengan kata lain, telah berkembang tindak pidana dibidang internet atau yang lazim disebut *cybercrime*

---

[3] Ibid h. 4-5

yakni suatu perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih[4].

Sisi negatif dari keberadaan internet juga diungkapkan oleh Neill Barret, Mark D. Rasch sebagaimana dikutip oleh Agus Raharjo sebagai berikut:

> *However, along the information superhighway are information superhighwaymen. They do not shout the electronic equivalent of 'stand and deliver'. Rather, computer criminals, organized crime figures, drug cartels, international money lounderers, hackers and 'cyberpunk' are all roaming the internet—seeking money, information or simply an opportunity to wreak havoc and destruction. ...computer and computer bulletin boards have been used to facilitate child pornography and child abduction rings, software piracy, theft of cable services, computerized stalking, terrorist rings, narcotick dealing, as well as other forms of criminal activities including plain theft*[5].

Senada dengan hal ini, dalam bukunya "*The Perfect Crime*", Jean Baundrillard menyatakan bahwa internet telah melahirkan kejahatan dan kriminalitas yang telah berkembang sedemikian rupa sehingga mencapai tingkat yang sempurna atau hiperkriminalitas (*hypercriminality*) yang juga melampaui batas realitas (*beyond reality*). Kejahatan internet menjadi satu wacana yang telah direncanakan, diorganisir dan dikontrol secara sempurna melalui teknologi tinggi (*high technology*), managemen tinggi (*high management*) dan politik tinggi (*high politics*) sehingga melampaui otoritas hukum, kemampuan akal sehat dan jangkauan nilai-nilai budaya. Interaksi antar pengguna dalam mayantara telah menimbulkan penyimpangan

---

[4] Widyopramono, Kejahatan di bidang Komputer, Jilid I, Pustaka Sinar Harapan, Jakarta,1994, h. 28

[5] Agus Raharjo, op.cit., h. 6

hubungan sosial berupa kejahatan internet yang khas dan memiliki karakteristik tersendiri[6].

Munculnya tindak pidana yang demikian sempurna dan canggih, sudah barang tentu membawa dampak atau akibat hukum yang secara eksplisit belum terjangkau oleh peraturan perundang-undangan yang berlaku saat ini di Indonesia, sehingga timbul kesan bahwa kejahatan teknologi berbasis internet atau yang popular di sebut *cybercrime* yang dilakukan di Indonesia tidak bisa tersentuh oleh hukum pidana Indonesia. Banyak orang bertanya-tanya apakah pelaku kejahatan *cybercrime* di Indonesia bisa diadili di Indonesia dengan menggunakan hukum pidana Indonesia yang berlaku saat ini.

Dari data yang terungkap dalam pertemuan *Asia Pacific Economic Cooperation and Communication* (APEC Tel.) ke-29 yang diselenggarakan di Hongkong bulan Maret 2004 yang lalu, diketahui bahwa Indonesia kini menempati rangking pertama dalam urusan kejahatan kartu kredit melalui internet. Mengikuti Indonesia adalah Nigeria, Pakistan, Ghana dan Israel[7]. Hasil temuan Perusahaan *Internet Verisgn* ini, jelas merupakan sebuah berita buruk bagi Indonesia. Sebelumnya, berdasarkan survey A.C. Neilsen tahun 2001, Indonesia "cuma" menempati posisi ke-enam dunia atau ke-empat di Asia dalam urusan tindak

---

[6] Ibid, h. 198.

[7] Perampok Lihai di Dunia Maya, Forum Keadilan, No. 44, 4 April 2004, h.12

kejahatan melalui internet[8]. Namun sekarang, Indonesia menjadi pemuncak klasmen dalam hal persentase *fraud*, -kejahatan pembobolan kartu kredit melalui internet. Bahkan selama tahun 2003, Asosiasi Kartu Kredit Indonesia (AKKI) mencatat total kerugian sebesar Rp 60 miliar sebagai akibat dari tindak kejahatan kartu kredit melalui internet dan diperkirakan akan terus mengalami peningkatan bila bila tidak ada perbaikan dalam masalah hukum[9].

Selain itu, terungkap pula bahwa hanya beberapa kasus *cybercrime* yang berhasil diidentifikasi. Tahun 2002, Direktorat Reserse Polda Jawa Tengah berhasil mengungkap kejahatan pembobolan *master card* yang dilakukan oleh 27 carder (pembobol kartu kredit secara illegal) di Semarang dan Salatiga. Sedangkan pada Bulan july 2003, aparat dari Polda Jawa Barat membekuk tujuh mahasiswa dalam kasus yang sama. Terungkapnya kasus-kasus ini pun berkat adanya laporan dari interpol Amerika Serikat yang datang ke Indonesia untuk menyelidiki kasus pembobolan sekitar delapan juta kartu kredit dari sebuah perusahaan kartu kredit di Amerika yang disinyalir bahwa banyak diantara pembobol itu adalah orang Indonesia[10].

Cybercrime atau kejahatan melalui internet adalah bentuk tindak kriminalitas yang tergolong baru di Indonesia, namun kenyataanya bahwa kejahatan jenis ini telah menyebar ke berbagai kota di Indonesia dan telah menempatkan Indonesia sebagai

---

[8] Kompas, 21 Maret 2002, dapat ditemukan di http://www.Kompas.com/internet/news

[9] Upaya Bank Menghadang Carding, Forum Keadilan, No.44, 4 April 2004, h. 18

[10] Ibid h. 20

sarang tindak pidana *cybercrime* nomor satu di dunia. Selain karena faktor kemampuan teknologi yang belum mencukupi, langkah para penegak hukum di Indonesia juga terkesan tidak tegas. Masyarakat mempertanyakan keseriusan dan kemampuan aparat penegak hukum dalam menyelesaikan berbagai permasalahan tersebut, karena dalam kenyataan banyak kasus *cybercrime* atau kejahatan internet yang dilaporkan justru akhirnya berhenti ditengah jalan atau ketika dimajukan ke pengadilan mengalami kegagalan dengan hakim yang beranggapan tidak ada hukum yang mengatur.

Berdasarkan uraian di atas, dapatlah dirumuskan beberapa permasalahan yang akan dibahas dan dikaji dalam skripsi ini yaitu:

1. Bagaimanakah pengaturan tentang hal-hal yang berkaitan dengan *cybercrime* dalam hukum pidana di Indonesia?
2. Bagaimanakah penerapan ketentuan-ketentuan hukum pidana yang berkaitan dengan *cybercrime* di Indonesia?

2. Penjelasan Judul

Berdasarkan rumusan masalah di atas akan ditulis skripsi dengan judul "*CYBERCRIME* DALAM PRESPEKTIF HUKUM PIDANA INDONESIA". Untuk mendapatkan pemahaman yang jelas dan menghindari penafsiran yang berbeda tentang skripsi ini, maka akan diberikan penjelasan sebagai berikut:

Hingga saat ini belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai arti *cybercrime*. Namun sebagai batasan, saya mengutip

pendapat Nazura Abdul Manap yang mengartikan *cybercrime* sebagai *"... any illegal act commited virtually through internet on line"*.[11] Berdasarkan batasan ini, *cybercrime* dapat terjadi di negara manapun di dunia yang terhubung oleh jaringan internet melalui komputer termasuk di negara Indonesia.

Media *cybercrime* yang dibicarakan di dalam tulisan ini hanya difokuskan dalam hal penggunaan media internet, mengingat penggunaan media internet yang saat ini paling populer digunakan oleh banyak orang, selain merupakan hal dikategorikan sebagai hal yang sedang '*booming*'. Perlu digarisbawahi, dengan adanya perkembangan teknologi yang semakin canggih, terbuka kemungkinan adanya penggunaan media jaringan lain selain internet dalam melakukan *cybercrime*. Jadi pembahasan ini hanya terfokus pada penggunaan internet yang terhubung oleh jaringan komputer sebagai media dalam melakukan *cybercime*.

Sedangkan hukum pidana yang dimaksud dalam tulisan ini adalah hukum pidana materiil yang memuat ketentuan-ketentuan pidana berkaitan dengan tindak pidana *cybercrime* sebagaimana yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP), dan Undang-Undang Khusus di luar KUHP yang berkaitan dengan *cybercrime* seperti UU No. 36/1999 tentang Telekomunikasi, UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, UU No. 20/2001 tentang Perubahan Atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi, dan UU No. 32/2002 tentang Penyiaran.

---

[11] Agus Raharjo, op.cit., h. 227.

3. Alasan Pemilihan Judul

Perkembangan penggunaan internet dalam beberapa tahun terakhir ini meningkat cukup pesat termasuk di negara kita ini. Satu hal yang mungkin patut disayangkan adalah ketika perkembangan penggunaan internet ini tidak segera diikuti juga dengan perkembangan pengetahuan hukum positif kita, maka akan muncul berbagai tindak pidana baru yang sulit ditegakkan.

Hal ini jelas merupakan suatu tantangan baru bagi dunia hukum kita. Para penegak hukum dituntut untuk bekerja keras karena teknik dan modus operandi tindak pidana melalui internet semakin canggih dan akan terus berkembang. Selain karena faktor kemampuan teknologi yang belum memadai, langkah para penegak hukum kita juga terhalang oleh belum adanya payung hukum yang khusus (*cyberlaw*) untuk menindak para pelakunya. Pemerintah memang sudah menyusun Rancangan Undang-Undang Informasi Elektronik dan Transaksi Elektronik (IETE) untuk mengatur segala hal yang berkaitan dengan internet, namun hingga kini belum disahkan menjadi undang-undang. Untuk itu, perlu diadakan analisa yang menyeluruh mengenai keberadaan hukum pidana positif yang berkaitan dengan *cybercrime*. Sebab bila tidak segera dilakukan langkah-langkah penegakkan hukum yang memadai, bukan tidak mungkin Indonesia akan dikucilkan dalam setiap transaksi berbasis teknologi informasi terutama transaksi bisnis melalui kartu kredit dari Indonesia. Akibatnya, tidak saja merusak citra Indonesia sebagai suatu bangsa yang berdaulat, tetapi juga berdampak langsung pada dikucilkannya komunitas teknologi informasi Indonesia oleh komunitas teknologi informasi dunia.

4. Tujuan Penulisan

Tujuan yang hendak dicapai dalam penulisan skripsi ini adalah sebagai berikut:

1. Untuk memperoleh gambaran mengenai *cybercrime* dan ketentuan-ketentuan hukum pidana di Indonesia yang berkaitan dengan *cybercrime*.
2. Untuk memberikan sumbangan pemikiran dalam rangka menjawab permasalahan hukum yang timbul dalam kaitannya dengan penerapan hukum pidana dalam hal *cybercrime* di Indonesia.
3. Untuk memenuhi salah satu persyaratan memperoleh gelar sarjana hukum pada Fakultas Hukum Universitas Airlangga, Surabaya.

5. Metode Penulisan

a. Pendekatan Masalah

Pendekatan masalah yang dipakai dalam penulisan ini adalah metode pendekatan yuridis normatif yaitu mengkaji obyek yang menjadi pokok permasalahan dengan melandaskan pada perundang-undangan yang berlaku, baik yang terdapat dalam Kitab Undang-Undang Hukum Pidana maupun undang-undang khusus lain yang berkaitan dengan *cybercrime*.

b. Bahan Hukum

Bahan Hukum diperoleh dari bahan hukum primer yaitu berasal dari peraturan hukum pidana materiil yang berlaku saat ini seperti Kitab Undang-Undang Hukum Pidana (KUHP), dan Undang-Undang Khusus di luar

KUHP seperti UU No. 36/1999 tentang Telekomunikasi, UU No. 20/2001 tentang Perubahan Atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi, UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, UU No. 30/2002 Komisi Pemberantasan Tindak Pidana Korupsi, dan UU No. 32/2002 tentang Penyiaran. Selain itu bahan hukum diperoleh dari bahan hukum sekunder yaitu literatur- literatur, tulisan-tulisan ilmiah, artikel dalam internet, majalah dan koran yang berkaitan langsung dengan topik permasalahan.

c. Prosedur Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum adalah studi kepustakaan. Hal ini dimaksudkan untuk mencari ketentuan peraturan perundang-undangan yang berlaku maupun pendapat-pendapat para sarjana yang berkaitan dengan topik pembahasan dan selanjutnya disusun secara sistematik untuk mendapatkan gambaran dari kenyataan yang terjadi dan kemudian ditarik kesimpulan.

d. Analisis Bahan Hukum

Metode analisis bahan hukum yang digunakan adalah analisis interpretatif dengan memperhatikan asas-asas hukum yang berkaitan dengan topik permasalahan yang dibahas.

6. Pertanggungjawaban Sistematika

Skripsi ini terdiri dari 4 (empat) bab. Bab I merupakan bab pendahuluan yang memaparkan tentang latar belakang dan rumusan permasalahannya, penjelasan judul skripsi dan alasan pemilihan judul, tujuan penulisan skipsi ini, pendekatan masalah, sumber bahan hukum, prosedur pengumpulan dan pengolahan bahan hukum serta analisa bahan hukumnya dan diakhiri dengan pertanggungjawaban sistematika penulisan skripsi.

Bab II merupakan isi dan pembahasan tentang ketentuan-ketentuan hukum pidana di Indonesia yang berkaitan dengan tindak pidana c*ybercrime*. Bagian ini, akan diawali dengan uraian mengenai aktivitas dalam dunia maya (*cyberspace)* dan kejahatan *cyberspace* (*cybercrime*) di Indonesia. Selain itu, dibahas pula mengenai pasal-pasal hukum pidana yang berkaitan dengan *cybercrime* dan diakhiri dengan pemaparan tentang pendapat-pendapat pro dan kontra mengenai perlunya dibuatkan undang-undang khusus yang memuat pengaturan tentang *cybercrime* di Indonesia.

Bab III merupakan kelanjutan isi dan pembahasan yang akan memaparkan tentang penerapan hukum pidana materiil dalam hal *cybercrime* di Indonesia. Ada 3 (tiga) hal pokok yang akan dibahas yaitu tentang asas legalitas, asas kesalahan (*asas culpabilitas*) dan yurisdiksi berlakunya hukum pidana menurut tempat (*Teori locus delicti* - tempat terjadinya perbuatan pidana).

Bab IV merupakan penutup dari rangkaian penyusunan penulisan Karya Ilmiah (skripsi) ini, yang terdiri dari simpulan dan saran.

BAB II

KETENTUAN HUKUM PIDANA DI INDONESIA YANG BERKAITAN DENGAN *CYBERCRIME*

BAB II

KETENTUAN HUKUM PIDANA DI INDONESIA YANG BERKAITAN DENGAN *CYBERCRIME*

1. Aktivitas dalam Dunia Maya (*Cyberspace)* dan Kejahatan *Cyberspace (cybercrime)* di Indonesia

Saat ini akivitas dalam dunia maya (*cyberspace*) dengan memanfaatkan teknologi jaringan komputer atau internet tidak lagi menjadi hal asing bagi masyarakat Indonesia. Teknologi jaringan komputer atau internet yang dulu dianggap barang canggih dan mahal, dan hanya dimiliki dan digunakan oleh orang-orang kaya dan berpendidikan tinggi, dewasa ini telah menjadi aktivitas yang biasa dan lumrah bagi masyarakat. Keberadaan internet tidak lagi menjadi monopoli masyarakat yang tinggal di kota-kota besar, tetapi juga sudah mulai dinikamati oleh masyarakat dikota-kota kecil atau masyarakat yang tinggal di daerah. Bahkan orang yang tidak tahu menggunakan komputer atau memanfaatkan internet dianggap 'gaptek' atau gagap teknologi dan ketinggalan zaman.

Penggunaan *cyberspace* yang berbasis jaringan komputer atau internet dipilih oleh kebanyakan orang sekarang ini karena kemudahan-kemudahan yang dimiliki oleh jaringan internet seperti:

1. Internet sebagai jaringan publik yang sangat besar (*huge/widespread network*) sehingga memiliki kemudahan sebagaimana yang dimiliki suatu jaringan publik elektronik, yaitu murah, cepat dan kemudahan akses.

2. Internet menggunakan data elektronik sebagai media penyampaian pesan/data sehingga dapat dilakukan pengiriman dan penerimaan informasi secara mudah, ringkas dan cepat baik dalam bentuk data elektronik analog maupun digital.
3. Dapat meningkatkan transaksi perdagangan dan bisnis[12].

Berdasarkan sejarah perkembangannya, akitivitas *cyberspace* di Indonesia, baru dimulai pada tahun 1994 dipelopori oleh Ipteknet. Namun perkembangan penggunaan internet di Indonesia telah menunjukkan peningkatan yang signifikan dari tahun ke tahun. Hal ini dapat dilihat pada tabel berikut ini:

TABEL 1

PENINGKATAN JUMLAH
PELANGGAN DAN PENGGUNA INTERNET DI INDONESIA

NO.	TAHUN	PELANGGAN	PENGGUNA
1	1996	31.000	110.000
2	1997	75.000	384.000
3	1998	134.000	512.000
4	1999	256.000	1.000.000
5	2000	760.000	1.900.000
6	2001	1.680.000	4.200.000

Sumber: APJII, January 2001[13]

[12] Patricia Gaby, Kerangka Hukum Digital Signature Dalam Electronic Commerce, dapat dijumpai di hhtp://www.amwibowo@excite.com. Jakarta, Juni 1999

[13] Hendrika Yunapritta, R. Cipto Wahyana, Inilah Wajah Netter Indonesia, Profil Pengguna Internet di Indonesia, dapat dijumpai di http:// www.apjii.or.id, 23 Juli 2002.

Dari tabel di atas, telihat adanya peningkatan jumlah pelanggan dan pengguna internet dari tahun ke tahun yakni dari 110.000 orang pengguna pada tahun 1996 menjadi 4.200.000 orang pada tahun 2001 atau terjadi peningkatan jumlah pengguna internet sebanyak 818.000 orang setiap tahunnya. Namun demikian, bila dibandingkan dengan negara-negara Asia yang lebih maju, seperti Singapura, Taiwan dan Hongkong, Indonesia masih ketinggalan jauh. Indikasi yang kuat adalah masih terbatasnya jumlah pelanggan internet yang baru berkisar 1.680.000 pelanggan sampai dengan tahun 2001 (APJII) atau tidak lebih 5 persen dari total jumlah rumah tangga di perkotaan, padahal di negara-negara Asia tersebut di atas, jumlah pelanggannya sudah mencapai di atas 30% dari jumlah penduduknya. Ditinjau dari gambaran statistik di atas maka tidak berlebihan jika dikatakan bahwa masyarakat pengguna internet di Indonesia masih baru taraf pengenalan atau masih merupakan pasar yang baru mulai muncul[14].

Walaupun Indonesia masih dalam tahap awal perkembangan pasar internet, namun tidak berarti Indonesia ketinggalan dalam hal penyalahgunaan media internet untuk melakukan kejahatan. Satu hal yang sangat mengejutkan dan memalukan bangsa kita adalah bahwa pada tahun 2004, Indonesia mendapat julukan sebagai 'sarang' penjahat dunia maya nomor satu dunia dalam hal pemalsuan kartu kredit melalui internet (*card fraud*). Pada hal, sebelumnya jarang sekali kita membaca atau

---

[14] Ibid

mendengar berita tentang kejahatan internet atau lazim disebut *cybercrime* melalui media cetak dan elektronik di Indonesia. Suhemi mengidentifikasi ada 2 (dua) kemungkinan mengapa kita jarang sekali mendengar atau membaca kasus-kasus kejahatan internet yang melibatkan orang-orang Indonesia, baik sebagai pelaku atau korbannya, yaitu:

1. Kejahatan internet sudah sering terjadi tapi beritanya tidak disebarluaskan melaui media massa. Kemungkinan ini cukup masuk akal, karena umumnya para korban kejahatan internet yang biasanya melibatkan perusahaan-perusahaan besar tidak mau melaporkan kejadian yang dialaminya, dengan alasan untuk menjaga kredibilitas perusahaan di mata masyarakat dan para pesaingnya. Akibatnya tidak banyak kasus *cybercrime* yang bisa diekspose kepada publik melalui media massa.
2. Kejahatan internet sudah terjadi di Indonesia tetapi belum diketahui keberadaannya. Kemungkinan ini pun bisa diterima karena di Indonesia kejahatan melalui internet adalah kejahatan yang tergolong baru dan kita belum memiliki tenaga-tenaga penegak hukum yang memiliki keahlian yang bisa diandalkan dalam menjerat para pelaku kejahatan internet ke pengadilan. Disamping itu, aparat penegak hukum juga belum dilengkapi dengan alat-alat teknologi canggih yang bisa mendeteksi jenis-jenis kejahatan dan keberadaan pelaku kejahatan internet[15].

---

[15] Suhemi, Kejahatan Komputer, Cet. I., Andi Offset, Yogyakarta, 1991, h. 5-8

Fenomena berkembangnya jenis-jenis *cybercrime* di Indonesia harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Ia dapat dilakukan oleh siapa saja, dari mana saja dan kapan saja tanpa melalui proses yang berbelit-belit. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas dari perkembangan *cybercrime* ini.

Kejahatan yang berhubungan erat dengan aktivitas yang dilakukan dalam dunia maya (*cybercrime*), dalam beberapa literatur dan praktiknya dapat dikelompokkan dalam beberapa bentuk, antara lain:

Kongres PBB ke-10 di Vienna pada tanggal 10-17 April 2000, membagi 2 (dua) subkategori *cybercrime* yaitu :

1) Cybercrime in a narrow sense (computer crime) is any illegal behavior directed by means of electronic operations that targets the security of computer system and data.

2) *Cybercrime in a broader sense (computer related crime) is any illegal behavior committed by means of,or in relation to a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network*[16].

Sedangkan Kepala Biro Hukum Kejaksaan Agung RI, H.M. Salamoen Muslim H., mengidentifikasi *cybercrime* dalam 2 kelompok besar yakni :

1. Kejahatan biasa (konvensional) yang menggunakan jaringan komputer sebagai medianya. Kejahatan jenis ini antara lain:

[16] Agus Raharjo, op.cit., h. 229

a) Penipuan biasa yang dilakukan dengan cara menawarkan barang/jasa atau saham di internet;

b) Penipuan menggunakan nomor kartu kredit orang lain di internet untuk berbelanja di luar negeri;

c) Kejahatan di bidang bank offence/fismondef di internet;

d) Pornografi di internet;

e) Menawarkan jasa sex di internet;

f) Mengancam atau menghina seseorang dengan menggunakan email;

g) Pemerasan dengan menggunakan email;

h) Propaganda atau terorisme di internet ;

2. Kejahatan yang memanfaatkan sistem komputer untuk mencari korbannya dan komputer sebagai korbannya. Jenis kejahatan dalam kelompok ini adalah :

a) DdoS Attack yaitu penyerangan terhadap sistem operasional ;

b) Merubah tampilan website atau *deface ;*

c) Masuk ke suatu sistem komputer secara ilegal atau *transpassing* ;

d) Mengendus atau membajak password milik orang lain atau *sniffing*;

e) Tindakan-tindakan lainnya yang dikategorikan sebagai *hacking/ cracking/phreaking ;*

f) Membuat atau menyebarkan program yang bersifat merusak (*malicious code*) dalam bentuk *Worm, Virus, TrojanHorse* dsb ;

g) Penyalahgunaan perijinan *Volp (Voice over internet protocol) ;*

h) Sengketa atau kejahatan yang menyangkut domain (penamaan atau alamat website) ;

i) Pelanggaran terhadap peraturan-peraturan dalam bidang teknologi Informasi [17];

Sedangkan Nazura Abdul Manap membedakan tipe-tipe *cybercrime* menjadi 3 (tiga) yaitu :

1) *Cybercrimes against Property, meliputi Theft (berupa theft of information, theft, theft of property dan theft of services), Fraud/Sheating, Forgery, dan Mischief.*
2) *Cybercrimes against person, meliputi pornography, cyberharassment, cyber-stalking, dan cyber-trespass. Cyber-trespass meliputi Spam E-mail, hacking a Web Page dan breaking into personal computer.*
3) *Cyber-terrorism*[18].

Philip Renata menggolongkan beberapa type *cybercrime* sebagai berikut :

a) *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer.

b) *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.

c) T*he Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus , menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain.

---

[17] H.M. Salamoen Nuslim H., Problematika Penuntutan Tindak Pidana Cyber/Teknolodi Informasi, Makalah yang disampaikan di seminar Problematika Penegakan Hukum Cybercrime di Indonesia, Unair, 9 Oktober 2004

[18] Agus Raharjo, op.cit., h. 228

d) *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.

e) *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah *input* data, atau *output* data.

f) *To frustate data communication* atau penyia-nyiaan data komputer.

g) S*oftware piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI[20].

Dari berbagai penggolongan jenis *cybercrime* di atas, Roy M. Suryo, mengidentifikasi kasus-kasus *cybercrime* yang banyak terjadi di Indonesia setidaknya ada 3 (tiga) tiga jenis berdasarkan modusnya, yaitu:

1. Pencurian Nomor Kredit.

Pencurian nomor kartu kredit milik orang lain di internet merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line*. Nama dan kartu kredit milik orang lain yang diperoleh di berbagai tempat (restaurant, hotel, atau segala tempat yang

---

[20] Bisnis dan Teknologi, Warta Ekonomi No. 24 edisi Juli 2000, h. 52, dapat dijumpai di http:// www.solusi hukum.com , 8 November 2004

melakukan transaksi pembayaran dengan kartu kredit) lalu dimasukkan di dalam aplikasi pembelian barang di internet.

2. Memasuki, memodifikasi, atau merusak *Homepage (Hacking)*

Pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank

3. Penyerangan situs atau *e-mail* melalui virus atau *spamming.*

Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail.* Menurut Roy M. Suryo, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya[21].

Sedangkan menurut As'ad Yusuf kasus-kasus *cybercrime* yang sering terjadi di Indonesia dapat digolongkan menjadi lima, yaitu:

a. Pencurian nomor kartu kredit.

b. Pengambilalihan situs *web* milik orang lain.

c. Pencurian akses *internet* yang sering dialami oleh ISP.

d. Kejahatan nama *domain.*

---

[21] Warta Ekonomi No. 9, 5 Maret 2001 h.12, dapat ditemukan di http:// www.solusi hukum.com , 8 November 2004

e. Persaingan bisnis dengan menimbulkan gangguan bagi situs saingannya[22].

Sampai saat ini, di Indonesia belum ada data yang pasti tentang persentase frekuensi terjadinya masing-masing jenis *cybercrime*. Namun yang pasti, tahun ini Indonesia menempati urutan pertama dalam persentase kejahatan internet pertransaksi. Memang sangat disayangkan bahwa kehadiran internet yang seharusnya dipergunakan untuk mempermudah hidup manusia dalam melakukan aktivitasnya, justru dipergunakan oleh sebagian orang yang tidak bertanggungjawab untuk melakukan kejahatan.

Ironisnya di Indonesia, para pelaku kejahatan internet justru menganggap dirinya sebagai pahlawan karena berhasil menjebol beberapa situs pengaman negara lain atau berhasil memesan barang-barang dari luar negeri dengan menggunakan nomor kartu kredit orang lain. Mereka bahkan menganggap perbuatannya lebih baik, lebih terpuji dan lebih terhormat daripada perbuatan para koruptor Indonesia karena mereka tidak mencuri kekayaan masyarakat Indonesia. Hal ini dapat terlihat dalam pengakuan *bLaCkApRiL*, *Nickname "bA"*, seorang carder yang juga mengelola situs Yogya *carding* tentang aktivitas *carding* sebagai berikut :

> Ironi dan menyedihkan.... ;(Sementara pihak Bea Cukai, telah mendapatkan input berupa pajak masuk barang import yang dibayar seorang carder. Ada apa sebenarnya? Mengapa justru kegiatan carding yang tidak merugikan negara (dari segi finansial) dijadikan trend investigasi? Kenapa tidak mengusut sampai tuntas kasus mantan Presiden Suharto, seorang tokoh yang telah membohongi rakyat selama 32 tahun? Tapi justru rakyat kecil yang hanya melakukan kegiatan carding (itupun menggunakan account milik orang luar negeri) yang dijadikan sasaran utama. Jika dibandingkan, seberapa parahkah antara seorang carder dengan seorang oknum (dari

[22] Ibid

> instansi terkait yang lebih cenderung mengkhianati negara)? Jika ada orang yang menyebut seorang carder = pencuri, maka bA menyebut oknum dari instansi terkait tadi = PENGKHIANAT BANGSA!! Sungguh keadilan hanya dilipat dalam saku, dan dijadikan judul seminar dengan kontribusi finansial yang selangit. So, tangkap dulu yang semestinya ditangkap, jangan membabi buta menangkapi carder yang mulai sedikit nakal mempelajari teknik hacking/cracking. carder tidak akan pernah MEMAKAN dan MENGGEROGOTI uang rakyat Indonesia yang makin hari makin susah kehidupannya akibat ulah para elite![23]

Pengakuan jujur yang cenderung membenarkan salah satu bentuk *cybercrime* ini, hendaknya ditanggapi secara serius oleh penegak hukum kita karena pelaku *cybercrime* telah menganggap perbuatannya sebagai sebuah perbuatan yang wajar dan terpuji. Mereka tidak menyadari bahwa sebenarnya perbuatan mereka telah mencoreng nama bangsa, menghambat kepentingan masyarakat Indonesia untuk kemajuan pendidikan, teknologi, dan berbisnis secara teknologi informasi. Sangatlah disayangkan kalau bangsa ini memiliki sebuah generasi yang telah kehilangan 'moral' sebagai sebuah bangsa yang beradab dan berperikemanusiaan.

Tentu saja tidak semua orang bisa melakukan *cybercrime* sebab tindak pidana berbasis teknologi informasi ini adalah merupakan salah satu bentuk tindak pidana canggih yang dilakukan dengan teknik tinggi/teknik intelektual sehingga sangat sulit untuk dimengerti oleh orang awam. Menurut Todung Mulya Lubis, tindak pidana internet ini termasuk "*White Collar Crime*" yaitu tindak pidana yang dilakukan oleh kalangan tertentu dan menggunakan teknik yang canggih dan rumit. Hal ini dapat

---

[23] Cyber Crime di Bandung Resahkan Dunia, TEMPO Interaktif, dapat ditemukan di http://www.tempo.com/internet/news, Jakarta, 04.April 2002

dilakukan secara perorangan, kelompok atau suatu badan dengan motivasi untuk mendapatkan keuntungan yang sebesar-besarnya atau untuk membuka rahasia perusahaan/negara dalam rangka menggoyahkan perusahaan/negara[24].

Mengingat bentuk kejahatan melaui media informasi terus berkembang dari waktu ke waktu, maka sudah seyoyanya pemerintah Indonesia, para wakil rakyat yang duduk di lembaga legislatif (DPR), aparat penegak hukum, dan juga para pakar dan ahli di bidang teknologi informasi berusaha memikirkan cara yang efektif untuk mencegah meluasnya wabah *cybercrime* ini di Indonesia. Sebab bila tidak segera dilakukan langkah-langkah antisipasi dan penyelesaian yang memadai maka sangat besar kemungkinan Indonesia akan dikucilkan dalam setiap transaksi informasi dan bisnis dari dan ke Indonesia. Hal ini jelas akan merugikan bangsa Indonesia sendiri.

2. Pasal -pasal Hukum Pidana Indonesia yang Berkaitan dengan *Cybercrime*

Mengingat saat ini Indonesia belum memiliki undang-undang khusus yang mengatur tentang *cybercrime*, maka dalam menindak pelaku *cybercrime*, aparat penegak hukum menggunakan pasal-pasal hukum pidana yang berlaku saat ini, yang pengaturannya dapat ditemukan dalam:

---

[24] Widyopramono, op.cit., h. 21

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

Beberapa ketentuan dalam KUHP yang dapat digunakan untuk menuntut perbuatan pidana *cybercrime* berdasarkan identifkasi jenis kasus sebagaimana yang diungkapkan oleh Andi Hamzah adalah sebagai berikut:

a) Terhadap perbuatan seseorang yang telah menggunakan jaringan komputer yang terhubung internet secara tidak sah atau tanpa izin, dan menggunakannya melampaui wewenang yang diberikan (*joycomputing*), maka terhadap pelaku yang demikian dapat diterapkan ketentuan Pasal 362 KUHP yang menyatakan "Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau denda paling banyak enam puluh rupiah".

b) Terhadap perbuatan seorang pelaku yang telah melakukan penyambungan dengan cara menambah terminal komputer baru pada sistim jaringan komputer tanpa izin dari pemilik sah jaringan tersebut (*hacking)* yang berakibat pada hilang atau tidak dapat dipakainya sistem jaringan komputer tersebut, maka dapat dikenakan ketentuan Pasal 167 dan 551 KUHP. Adapun ketentuan masing-masing pasal adalah sebagai berikut:

Pasal 167 KUHP (1) "Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan cara melawan hukum, atau berada di situ dengan melawan hukum, dan atas

permintaan yang berhak tidak segera pergi, diancam dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah". (2) "Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barangsiapa tidak setahu yang berhak lebih dahulu serta bukan karena kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk".

Sedangkan ketentuan Pasal 551 KUHP menyatakan "Barangsiapa tanpa wewenang, berjalan atau berkendaraan di atas tanah yang oleh pemiliknya, dengan cara jelas dilarang memasukinya, diancam dengan denda paling banyak lima belas rupiah".

c) Untuk menjerat pelaku perbuatan memanipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi *(The trojan horse)*, maka dapat digunakan beberapa pasal KUHP seperti:

i. Ketentuan tentang penggelapan sebagaimana terdapat dalam Pasal 372 dan 374 KUHP. Kedua pasal ini berbicara tentang penggelapan, sehingga dapat diterapkan pada seseorang yang telah menggunakan jaringan internet melalui komputer dalam lingkup pekerjaannya untuk menguntungkan dirinya sendiri.

ii. Ketentuan tentang kejahatan menghancurkan atau merusakan barang milik orang lain sebagaimana yang terdapat dalam Pasal 406 KUHP. Dengan demikian pasal ini dapat diterapkan pada seseorang yang telah menimbulkan kerusakan atau kehancuran atau kerugian bagi orang lain pada saat berinteraksi melaui jaringan internet.

iii. Ketentuan tindak pidana korupsi dapat dikenakan, bilamana perbuatan tersebut berkaitan dengan jabatan dalam lingkup pegawai negeri dan merugikan keuangan negara. Perbuatan ini dapat diancam dengan Undang-undang Pemberantasan Tindak Pidana Korupsi yakni UU No.3/1971 yang kemudian diperbarui dengan UU No.20/2001 tentang Perubahan Atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi.

d) Apabila perbuatan seseorang itu menyangkut bocornya data keluar terutama mengenai data yang harus dirahasiakan (*Data leakage)* maka ketentuan yang dapat diterapkan adalah:

i. Jika menyangkut rahasia negara atau menyangkut kejahatan terhadap keamanan negara, maka perbuatan tersebut bisa dijerat dengan ketentuan Pasal 112, 113, 114,115 dan 116 KUHP.

ii. Jika perbuatan tersebut dilakukan oleh seseorang yang wajib menyimpan rahasia karena jabatannya atau pencariannya, maka bisa dikenakan ancaman pidana Pasal 322 KUHP.

iii. Menyangkut rahasia suatu perusahaan, maka perbuatan tersebut bisa dikenakan ketentuan Pasal 323 KUHP.

e) Ketentuan yang berkaitan dengan kejahatan pemalsuan surat sebagaimana yang diatur dalam Pasal 263 KUHP. Dengan demikian pasal ini dapat diterapkan kepada pelaku perbuatan yang mengubah data valid atau sah dengan cara yang tidak sah yaitu dengan mengubah input data atau output sehingga menyebabkan tidak dapat terpakainya data tersebut melalui internet.

b. UU No. 36/1999 tentang Telekomunikasi mengancam tindak pidana terhadap perbuatan:

i. Memanipulasi akses ke jaringan telekomunikasi dan larangan melakukan perbuatan tanpa hak, tidak sah, atau manipulasi akses ke jaringan telekomunikasi, jasa telekomunikasi, dan ke jaringan telekomunikasi khusus, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah). (Pasal 22 jo Pasal 50).

ii. Menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi diancam dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)(Pasal 38 jo Pasal 55).

iii. Menyadap informasi melalui jaringan telekomunikasi dalam bentuk apapun dikenakan ancaman dipidana penjara paling lama 15 (lima belas) tahun.(Pasal 40 jo Pasal 56).

iv. Semua tindak Pidana dalam UU No. 36/1999 dinyatakan sebagai kejahatan dan diancam dengan pidana penjara dan denda sesuai dengan ketentuan pasal yang dilanggar.(Pasal 59)

c. UU No. 20/2001 tentang Perubahan Atas UU No. 31/1999 tentang Pemberantasan Tindak Pidana Korupsi. Ketentuan yang dapat diterapkan berkaitan dengan *cybercrime* adalah:

i. Ketentuan dalam Pasal 2 ayat 1 yang menyatakan bahwa setiap orang secara melawan hukum memperkaya diri sendiri atau orang lain yang dapat merugikan keuangan negara atau perekonomian negara dipidana dengan pidana penjara seumur hidup atau pidana penjara paling singkat empat tahun dan paling lama dua puluh tahun dan denda paling sedikit dua ratus juta rupiah dan paling banyak satu milyar rupiah. Ketentuan ini dapat diterapkan terhadap pelaku yang melakukan kejahatannya dengan menggunakan jaringan komputer atau internet.

ii. Ketentuan Pasal 26-a yang memuat perluasan pengertian alat bukti sebagaimana yang terdapat dalam pasal 188 (2) Kitab Undang-Undang Hukum Acara Pidana. Pasal ini menegaskan diakuinya alat bukti lain berupa informasi atau dokumen yang diucapkan, dikirim, diterima dan atau disimpan secara elektronik dengan alat optik atau yang serupa dengan

itu, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna. Dengan adanya perluasan pengertian tentang alat bukti ini, maka persoalan tentang alat bukti elektronik dalam kasus *cybercrime* dapat diatasi dengan mengacu pada Pasal 26 (a) undang-undang ini.

d. UU No. 15/2002 tentang Tindak Pidana Pencucian Uang. Ada beberapa pasal yang dapat diterapkan terhadap setiap transaksi keuangan melalui jaringan internet yang dapat menimbulkan hubungan hukum seperti yang terdapat dalam Pasal 2 yakni menempatkan, mentransfer, membayarkan atau membelanjakan, menitipkan, menyembunyikan atau menyamarkan asal-usul harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana, dipidana karena tindak pidana pencucian uang dengan pidana penjara paling singkat 5 (lima) tahun dan paling lama 15 (lima belas) tahun dan denda paling sedikit Rp 5.000.000.000,00 (lima milyar rupiah) dan paling banyak Rp 15.000.000.000,00 (lima belas milyar rupiah). Selain itu, Pasal 38 undang-undang ini memuat ketentuan yang memperluas pengertian alat bukti yang tidak hanya mencakup surat sebagai bukti tertulis, tetapi juga alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan, secara elektronik dengan alat optik atau yang serupa dengan itu.

e. UU No. 30/2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi, Pasal 44 ayat (2) yang menyatakan bahwa bukti permulaan yang cukup dianggap telah ada apabila telah di temukan sekurang-kurangnya 2 (dua) alat bukti,

termasuk dan tidak terbatas pada informasi atau data yang di ucapkan, dikirim, diterima, atau disimpan baik secara biasa maupun elektronik atau optik.

f. UU No. 32 /2002 tentang Penyiaran. Undang-undang ini memiliki beberapa pasal yang dapat diterapkan terhadap kasus *cybercrime* seperti, Pasal 57 jo 36 (5) dan (6) yang mengancam pidana terhadap siaran yang memfitnah, mengahasut, menyesatkan, cabul, atau yang memperolokkan, merendahkan, melecehkan dan/atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasonal, dan Pasal 58 jo. 46 (3) mengancam pidana terhadap siaran iklan niaga yang menyesatkan.[25]

Pengakuan alat bukti elektronik dalam sidang di pengadilan terhadap kasus *cybercrime* merupakan sebuah terobosan yang baik dalam sistem perundang-undangan kita. Namun hal ini tidak berarti bahwa permasalahan *cybercrime* dapat terselesaikan dengan adanya perluasan pengertian alat bukti saja. Beberapa istilah lain dalam KUHP masih sering dipermasalahkan bila diimplementasikan secara harafiah terhadap perbuatan pidana *cybercrime.* Untuk itu, perlu dibuat penjelasan terhadap beberapa istilah sebagai berikut:

a. Pengertian benda atau '*eniggoed*', menurut hukum pidana terdapat dalam penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud (misalnya listrik, gas) dan mempunyai nilai di dalam kehidupan ekonomi bagi seseorang. Berkaitan dengan komputer, data atau program

---

[25] Barda Nawawi Arief, Masalah Pertanggungjawaban Pidana Cybbercrime, Makalah pada Seminar "Problematika Hukum Cybercrime di Indonesia", FH UNAIR, 9 Oktober 2004, hal. 3-5

tersimpan di dalam disket atau *hard disk* sehingga tidak dapat diketahui wujudnya jika tidak dicetak dalam kertas. Namun mengingat data atau informasi tersebut memiliki nilai ekonomis dan bermanfaat bagi seseorang, maka data atau program tesebut dapat dikategorikan sebagai benda seperti penjelasan Pasal 362 KUHP.

b. Pengertian 'mengambil'. Sesuai penjelasan Pasal 362 KUHP, pengertian mengambil adalah perbuatan yang bertujuan untuk melepaskan kekuasaan atas benda dari pemiliknya untuk dikuasainya sendiri dan benda tersebut sudah berpindah dari tempatnya asalnya. Dalam kaitan dengan aktivitas dunia maya, kata 'mengambil' memiliki 2 macam bentuk yaitu:

1) Mengambil dalam arti nyata yaitu mengambil disket, *hard disk* atau media penyimpan lainnya yang berisikan data atau program yang memiliki nilai ekonomis. Dengan demikian pengertian 'mengambil' sesuai dengan ketentuan Pasal 362 KUHP.

2) Mengambil dalam arti mengcopy, yaitu merekam data atau program yang tersimpan di disket atau *hard disk* komputer dengan cara memberikan instruksi-instruksi tertentu pada komputer. Dengan demikian data atau program tetap utuh dan tidak berubah. Dalam kasus ini, timbul permasalahan mengenai pengertian 'mengambil' karena data/informasi atau program yang tersaji dalam komputer atau internet tidak berpindah dari tempat asalnya atau berubah karena hanya dicopy. Namun dengan tetap berpegang pada pengertian 'melepaskan kekuasaan atas benda itu

dari pemiliknya untuk dikuasai sendiri secara melawan hukum atau tanpa seizin dari pemiliknya, maka perbuatan ini tetap dapat dikategorikan sebagai perbuatan 'mengambil' sebagaimana yang dimaksud dalam penjelasan Pasal 362 KUHP.

c. Pengertian 'memiliki/menghaki', yakni keinginan untuk menguasai atau mempunyai hak atas suatu barang atau benda dalam hal ini data atau program yang terdapat di dalam komputer secara tidak sah atau melawan hukum. Unsur yang sama juga terdapat dalam Pasal 362 KUHP. Hanya saja dalam, pengertian 'memiliki/menghaki' yang ditekankan adalah unsur subyektif yakni keinginan untuk memiliki bagi dirinya sendiri barang atau data yang diambil.

d. Pengertian 'kekerasan', menurut Pasal 89 KUHP adalah setiap perbuatan yang mempergunakan tenaga badan yang dapat mengakibatkan orang pingsan atau tidak berdaya lagi. Akan tetapi, kekerasan dalam kasus *cybercrime* yaitu suatu perbuatan untuk mengambil dan menguasai data atau program yang tersimpan di dalam disket dan sejenisnya dengan disertai tindakan kekerasan dan atau ancaman kepada pihak yang bertanggung jawab atas penyimpangan tersebut. Apabila kekerasan dalam *cybercrime* dikaitkan dengan delik-delik yang terdapat dalam pasal-pasal KUHP, maka dapat dikategorikan sebagai berikut:

1) Sebagai perbuatan tanpa wewenang memaksa atau mendesak yang disertai kekerasan atau ancaman dengan kekerasan (Pasal 368 (1) KUHP).

2) Sebagai perbuatan pencurian yang didahului atau disertai dengan kekerasan, (Pasal 365 (1) KUHP).

e. Pengertian informasi tertulis/surat. Sesuai penjelasan Pasal 263 dikatakan bahwa yang dimaksud dengan surat adalah segala surat baik yang ditulis dengan tangan, dicetak, maupun ditulis memakai mesin tik dan lain-lain (*paper based).* Namun dengan adanya komputer, media penyimpanan data atau program menjadi *paperless based* karena tersimpan dalam disket atau *hard disk* komputer yang bentuknya tidak tertulis. Namun data atau program yang *paperless based* ini dapat dikategorikan sebagai surat atau informasi tertulis karena data atau program yang terdapat dalam komputer dapat dituangkan dalam bentuk naskah tulisan yang kasat mata sehingga sesuai dengan Kitab Undang-Undang Hukum Pidana yang menginginkan alat bukti secara tertulis untuk menyatakannya dan bersifat tahan lama[26].

Walaupun telah ada pasal-pasal hukum pidana yang berkaitan dengan tindak pidana *cybercrime*, namun keberadaan pasal-pasal hukum pidana ini tentunya belum dapat memberikan jaminan keamanan dan perlindungan sepenuhnya bagi para pengguna internet, apalagi untuk menghentikan penyebaran wabah *cybercrime.* Memang haruslah diakui bahwa peraturan yang ada sekarang tidak didesain untuk menangkal kejahatan-kejahatan *cyberspace* sehingga menimbulkan keraguan bila diimplementasikan.

Merupakan kewajiban pemerintah untuk mencari cara yang lebih efektif dan canggih dalam mengentaskan *cybercrime* dari bumi Indonesia. Memang diakui

---

[26] Andi Hamzah, op.cit., h. 29-35

sendiri oleh Yusril Izha Mahendara (mantan Menteri Kehakiman Indonesia) bahwa sampai saat ini Indonesia belum memiliki peraturan khusus yang mengatur tentang aktivitas *cybercrime* dengan segala aspek negatifnya. Namun hal ini tidak berarti bahwa pemerintah kurang peka terhadap perkembangan teknologi dan informasi, tetapi untuk mendapatkan sebuah produk hukum yang 'mumpuni' mengenai aktivitas *cyberspace*, memerlukan waktu yang lama untuk membuat kajian-kajian yang cermat dan mendalam sehingga tidak menimbulkan problem hukum baru dalam implementasinya[27].

Mengingat penggunaan media internet di berbagai bidang terus meningkat dan tak bisa dibendung, padahal keberadaan hukum positif yang khusus mengatur tentang *cyberspace* masih sebatas rancangan yang tak pasti pengesahannya, maka tuntutan untuk memanfaatkan pasal-pasal hukum pidana yang ada, yang berkaitan dengan aktivitas *cyberspace* adalah sebuah keharusan yang tak bisa ditunda. Dibutuhkan keberanian para penegak hukum untuk menerapkan peraturan yang ada, tentunya dengan pertimbangan-pertimbangan yuridis yang bisa diterima oleh masyarakat pencari keadilan.

---

[27] Agus Raharjo, op. cit., h. 202

3. Pendapat Tentang Perlunya Pengaturan Cybercrime Secara Khusus dalam Hukum Pidana Indonesia

Urgensi keberadaan '*cyberlaw*' untuk mengatur aktivitas dalam dunia maya (*cyberspace*), hingga saat ini masih menimbulkan perdebatan. Selama pemerintah sebagai lembaga eksekutif dan para wakil rakyat (DPR) sebagai lembaga legislatif belum memiliki ketetapan hati untuk melahirkan sebuah undang-undang khusus yang mengatur tentang akvitas di internet, maka diskusi mengenai eksistensi hukum pidana saat ini dalam mengatur aktivitas di internet masih relevan untuk dibicarakan. Berkaitan dengan hal ini, muncul berbagai pandangan mengenai perlu tidaknya dibuatkan suatu ketentuan khusus yang mengatur tentang aktivitas dunia maya melalui internet di Indonesia. Secara umum terdapat dua perbedaan pendapat mengenai hal ini, yakni:

a. Pendapat yang menyatakan tidak perlu dibuatkan ketentuan baru tentang *cybercrime*.

i. Mantan Jaksa Agung Muda Bidang Tindak Pidana Khusus Kejakasaan Agung RI, Himawan menyatakan bahwa hal terpenting dalam menilai kasus *cybercrime* adalah perbuatannya dan bukan dengan apa kejahatan itu dilakukan. Ia mengatakan bahwa internet merupakan suatu media informasi dan komunikasi sehingga hubungan hukum yang berlangsung dalam internet, sepanjang subtansi dari hubungan hukum tersebut dikenal (teridentifikasi) oleh masyarakat (pengguna) maka peraturan yang berlaku di dunia nyata dapat diterapkan dalam dunia maya. Konsekuensi logisnya

jika masyarakat mengenal (mengidentifikasi) subtansi dari suatu hubungan hukum tersebut maka ketentuan yang berlaku dalam dunia nyata dapat diberlakukan terhadap segala aktifitas yang berlangsung dalam dunia maya. Selanjutnya beliau menyatakan, bahwa apapun bentuk kejahatan yang dilakukan dengan komputer sebagai media masih bisa ditangkal dengan undang-undang yang ada[28].

ii. Achmad Ali. (Guru Besar Ilmu Hukum Fakultas Hukum Universitas Hasanudin) mengatakan bahwa internet adalah suatu perpaduan dari teknologi komputer, komunikasi dan informasi. Internet merupakan suatu alat yang digunakan untuk melakukan kejahatan sehingga interaksi dengan menggunakan internet tidaklah membawa perubahan konsepsi perbuatan hukum yang terjadi. Menurutnya, pencurian dengan menggunakan internet tetap saja dapat dikategorikan sebagai perbuatan melanggar hukum, sehingga ketentuan atau pasal mengenai pencurian di dalam KUHP (Pasal 362) dapat diterapkan dalam kasus pencurian barang lewat internet. Mungkin persoalan lainnya yang muncul adalah masalah pembuktian. Persoalan pembuktian ini akan lebih sulit jika barang yang dicuri adalah barang yang berbentuk elektronik bila dibandingkan dengan barang fisik. Di sinilah diperlukan keberanian polisi, jaksa dan penasehat hukum dalam menemukan bukti-bukti yang memiliki hubungan dengan kasus ini dan

---

[28] Widypramono, op.cit., h. 42

menggunakannya di pengadilan. Ia juga menambahkan bahwa hukum tidaklah berubah, teknologilah yang terus berubah. Perkembangan teknologi tidaklah mengubah ketentuan hukum yang berlaku, sepanjang masyarakat mampu mendefinisikan perbuatan hukum tersebut[29].

iii. Hasan Yahya, direktur utama PT Sumberdaya Info Prima, sebuah perusahaan yang bergerak dalam bisnis konsultasi teknologi informasi mengatakan bahwa peraturan mengenai Internet (*cyberlaw*) tidak perlu dibuat secara khusus, cukup dimasukkan dalam peraturan lain yang terkait. Teknologi informasi merupakan sektor yang baru dan masih akan terus berkembang dengan pesat. Arah perkembangan teknologinya belum bisa ditebak dan pasti akan berpengaruh terhadap cara hidup masyarakat, maka sebaiknya tidak perlu diatur secara khusus. Untuk itu, pemerintah perlu mengembangkan struktur regulasi dengan memanfaatkan peraturan perundangan yang telah ada sekarang seperti UU Perlindungan Konsumen, UU Antimonopoli, serta peraturan perdagangan dan investasi. Jadi tidak perlu dibuat aturan khusus dan terpisah. Lebih lanjut ia menambahkan bahwa semua negara mengalami persoalan yang sama dengan perkembangan internet. Persoalan regulasi seperti *e-commerce* bukan hanya dihadapi Indonesia, sehingga perkembangan teknologi informasi tidak perlu diatur terlebih dahulu sampai ada kejelasan arah

---

[29] Hukum dan Teknologi, http://www.indo.net news, Jakarta, 10 Juni 2002.

perkembangan di bidang teknologi informasi. Teknologi informasi masih akan mengalami perkembangan dengan pesat sehingga kebijakan yang dibuat pemerintah akan terus ketinggalan. Namun pemerintah perlu memberikan kerangka pendukung seperti iklim investasi yang baik[30].

b. Pendapat yang menyatakan perlu dibuatkan ketentuan khusus dalam KUHP atau undang-undang khusus yang mengatur tentang *cybercrime*.

i. J.E. Sahetapy, Guru Besar Hukum Pidana Universitas Airlangga, Surabaya, mengatakan bahwa hukum pidana yang ada tidak siap mengahadapi *cybercrime*, karena tidak gampang menganggap *cybercrime* berupa pencurian data sebagai pencurian. Bila dikatakan pencurian tentu harus ada barang hilang, pada hal dalam *cybercrime*, data sipemilik masih ada kendati sudah dicuri orang lain. Selain itu, sulitnya pembuktian dan besarnya kerugian yang mungkin terjadi maka sangat diperlukan produk hukum baru yang dapat menangkal dampak-dampak kemajuan teknologi, agar dakwaan terhadap terdakwa dalam kasus tindak pidana *cyber* tidak meleset[31].

ii. Todung Mulya Lubis, Mantan Ketua Yayasan LBHI berpendapat bahwa sudah saatnya Indonesia memiliki undang-undang khusus yang mengatur tenatng akvitas di internet. Ia beralasan bahwa tindak pidana *cybercrime*

---

[30] Patricia Gaby, loc.cit

[31] Widyopramono, op.cit., h. 44

menggunakan teknik yang canggih dan rumit sehingga sulit untuk dapat dibuktikan hanya dengan pasal-pasal pidana yang terdapat dalam KUHP. Selain itu, ancaman dari pasal-pasal pidana itu tidak memadai dengan akibat yang ditimbulkan tindak pidana *cybercrime*. Kelemahan lain dari undang-undang pidana yang ada adalah subyek hukum pasal-pasal pidana yang hanya menyebutkan manusia sebagai pelaku tindak pidana, pada hal dalam perkembangan ilmu dan teknologi, subyek hukum itu tidak lagi hanya manusia tapi juga perusahaan dan bahkan mungkin komputer yang dipakai sebagai alat untuk melakukan tindak pidana *cybercrime*[32].

iii. Direktur Reserse Kriminal Khusus, Edmon Ilyas mengatakan bahwa KUHP tidak efektif jika diterapkan apa-adanya terhadap *cybercrime* sebab *cybercrime* umumnya berada di luar jangkauan hukum pidana yang konvensional. Padahal untuk dapat menjatuhkan sanksi pidana terhadap suatu perbuatan tertentu maka terlebih dahulu perbuatan tersebut harus secara tegas dinyatakan sebagai kejahatan atau pelanggaran dengan ancaman sanksi tertentu yang ditentukan oleh undang-undang yang berlaku sebelum perbuatan itu dilakukan. Ini dikenal sebagai azas legalitas. Pernyataannya ini dapat terungkap jelas saat mengomentari penangkapan seorang penjual VCD porno melalui internet:

> Kita bisa saja meminta instansi terkait menutup akses situs yang berbau pornografi dari dan ke luar negeri, tapi kita dapat dituntut balik

[32] ibid

> karena penutupan yang kita lakukan itu tak ada dasar hukumnya. Karena itu, Polisi berharap segera disusun undang-undang tentang internet sehingga polisi tidak ragu dalam mengambil tindakan hukum yang tegas[33].

Terhadap kedua pandangan tersebut di atas, penulis beranggapan bahwa terlalu naif untuk menilai hukum pidana kita saat ini sudah baik dan dapat menjangkau aktivitas di internet sehingga tidak diperlukan perubahan dan perbaikan atau sebaliknya menilai bahwa hukum pidana kita terlalu kuno untuk diterapkan dalam kejahatan yang memanfaatkan keunggulan teknologi internet. Penulis beranggapan bahwa beberapa prinsip hukum pidana yang ada saat ini masih aktual untuk merespons persoalan hukum yang timbul dalam aktivitas di internet sebagaimana telah diuraikan di atas. Namun demikian, perubahan atau amandemen terhadap hukum pidana yang ada sudah merupakan tuntutan yang tidak bisa didiamkan karena teknik dan modus operandi *cybercrime* akan terus berkembang dan menjadi semakin canggih dan rumit. Namun hal ini sebaiknya dilakukan secara cermat dan mendalam agar tidak menimbulkan persoalan hukum baru dalam implementasinya.

Trisno Raharjo dalam tulisannya tentang 'Perbandingan Kebijakan Kriminalisasi Tindak Pidana Mayantara di Indonesia dan Belanda' mengungkapkan

---

[33] Hukum dan Teknologi, Seri Diskusi Panel 50 tahun PII, Bandung 17 Mei 2003, dapat ditemukan di http://www.indo.net.news,

bahwa dalam mengkriminalisasikan tindak pidana mayantara, hendaknya dipertimbangkan tiga hal berikut:

1) Hendaknya dipilih perbuatan-perbuatan yang benar-benar merugikan dan dapat menimbulkan akses serius agar pengaturan tersebut tidak bersifat *overcriminalization.*
2) Hendaknya dipertimbangkan dengan biaya yang dikeluarkan untuk menyusun, mengawasi dan menegakan ketentuan tersebut.
3) Hendaknya dipertimbangkan kemampuan aparat penegak hukum sehingga tidak bersifat *overbelasting* (sulit ditegakkan dalam praktek di lapangan)[34]

Aturan hukum yang tegas dan jelas bukanlah merupakan jaminan mutlak bagi penegakan hukum *cybercrime*. Dibutuhkan komitmen yang tinggi dari aparat penegak hukum agar selama bangsa kita belum memiliki peraturan yang khusus mengatur tentang aktivitas di internet, upaya penegakan hukum tetap dilakukan dengan memanfaatkan peraturan pidana yang berlaku saat ini.

---

[34] Trisno Raharjo, Perbandingan Kebijakan Kriminalisasi Tindak Pidana Mayantara di Indonesia dan Belanda, dapat ditemukan dalam http://www.detik.com., Jakarta, 25 September 2002

BAB III

PENERAPAN HUKUM PIDANA BERKAITAN DENGAN *CYBERCRIME* DI INDONESIA

BAB III

PENERAPAN HUKUM PIDANA BERKAITAN DENGAN *CYBERCRIME* DI INDONESIA

1. Asas Legalitas

Dasar pokok dalam menjatuhkan pidana atas pelaku *cybercrime* di Indonesia, pertama-tama harus memenuhi kualifikasi perbuatan pidana. Menurut doktrin hukum pidana Indonesia sebagaimana yang dikemukan oleh Moeljatno dalam bukunya tentang 'Asas-Asas Hukum Pidana Indonesia" dikatakan bahwa, untuk dapat digolongkan sebagai suatu perbuatan pidana, maka suatu perbuatan itu harus terlebih dahulu dilarang dan diancam dengan pidana dalam suatu perundang-undangan yang berlaku. Persyaratan pemidanaan ini dikenal dengan sebutan asas legalitas (*Principle of legality*). Dalam bahasa Latin dikenal dengan "*Nullum delictum nulla poen sine praevia lege"* dan dalam bahasa Indonesia diterjemahkan sebagai tidak ada delik, tidak ada pidana tanpa peraturan lebih dahulu atau dengan kalimat sederhana : "Tiada suatu perbuatan yang dapat dipidana selain telah ada kekuatan ketentuan perundang-undangan pidana yang mendahuluinya"[35].

Lebih lanjut Moeljatno menambahkan bahwa penerapan asas legalitas dalam hukum pidana Indonesia mengandung 3 (tiga) pengertian yaitu:

---

[35] Moeljatno, Asas-Asas Hukum Pidana, Cet. VII, Rineka Cipta, Jakarta, September 2002, h. 23.

a. Suatu perbuatan tidak dapat dipidana kalau terhadap perbuatan itu tidak ada ketentuan perundang-undangan yang mengaturnya. Hal ini nampak jelas dalam ketentuan Pasal 1 ayat (1) KUHP yang berbunyi "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam peraturan perundang-undangan yang telah ada sebelum perbuatan dilakukan".

b. Tidak boleh menggunakan analogi dalam menentukan adanya suatu perbuatan pidana. Suatu analogi terhadap aturan hukum pidana dilarang karena analogi bersifat subyektif, tidak berpegang pada aturan yang ada tetapi menggunakan ratio terhadap maksud dan inti dari aturan yang ada sehingga dapat berakibat pada ketidakadilan dalam suatu putusan peradilan.

c. Tidak berlakunya asas retroaktif (berlaku surut) terhadap aturan-aturan hukum pidana. Namun dalam perkembangan akhir-akhir ini, telah diperbolehkan berlakunya asas retroaktif ini dalam batas-batas tertentu seperti terhadap pelaku kejahatan/pelanggaran HAM berat[36].

Berdasarkan persyaratan asas legalitas ini, maka pemidanaan terhadap pelaku *cybercrime* tentunya harus didasarkan pada sumber hukum yang berlaku saat ini yakni Kitab Undang-undang Hukum Pidana Indonesia (KUHP) maupun peraturan perundang-undangan lain di luar KUHP yang berkaitan dengan *cybercrime*. Padahal, dalam kenyataan tidak semua pasal dalam KUHP maupun Peraturan perundang-undangan lain di luar KUHP dapat menjangkau permasalahan *cybercrime*.

---

[36] Ibid., h. 25

Sebagai contoh keterbatasan hukum pidana yang ada untuk dapat dipakai dalam menangani kasus *cybercrime* adalah masalah pemalsuan kartu kredit dan transfer dana elektronik. Dalam KUHP tidak ada ketentuan khusus mengenai 'pembuatan kartu kredit palsu'. Yang ada hanya ketentuan mengenai:

a) Sumpah/ Keterangan Palsu, bab IX, Pasal 242

b) Pemalsuan Mata Uang dan Uang Kertas, bab X Pasal-pasal 244-252

c) Pemalsuan Materai dan Merek, bab XI, Pasal-pasal 253-262

d) Pemalsuan Surat, bab XII, Pasal-pasal 263-276

Keterbatasan ketentuan hukum pidana yang berkaitan dengan *cybercrime* ini, menimbulkan keraguan bagi aparat penegak hukum dalam menangani kasus *cybercrime* yang melibatkan warga negara Indonesia. Alasan klasik adalah tidak ada dasar hukum formal yang mengatur. Hal ini dapat terlihat dalam pernyataan Direktur Reserse Kriminal Khusus, Edmon Ilyas mengomentari penangkapan seorang penjual VCD porno melalui internet bahwa mereka (polisi) tidak dapat meminta sebuah instansi atau perusahaan yang mengekspose situs-situs pornografi untuk menutup akses-aksesnya dari dan ke luar negeri karena khawatir upayanya ini akan dituntut balik mengingat belum ada dasar hukum yang mengaturnya[37].

Selain alasan belum ada dasar hukumnya, pasal-pasal hukum pidana yang ada sekarang memang tidak didisain untuk merespons kejahatan yang berbasis teknologi informasi, sehingga dalam penerapannya, terlebih dahulu harus dibuat

---

[37] Hukum dan Teknologi, Seri Diskusi Panel 50 tahun PII, Bandung 17 Mei 2003, dapat ditemukan di http://www.indo.net.news

interpretasi dan perluasan makna dari pasal-pasal tersebut. Namun interpretasi yang dibuat masih menjadi bahan perdebatan, dan tidak mengikat hakim dalam menjatuhkan putusan, sehingga hakim cenderung membebaskan pelakunya daripada menghukumnya tanpa ada dasar hukum yang kuat.

Sebagai contoh, perbedaan pendapat mengenai pengertian 'barang' sebagaimana yang terdapat dalam rumusan delik pencurian dalam Pasal 362 KUHP, delik penggelapan dalam Pasal 372 KUHP, dan delik perusakan dalam Pasal 406 KUHP. Orang tidak bolehmenyamakan kata 'barang' dalam pasal-pasal tersebut dapat sebagai termasuk 'data/angka' atau dokumen elektronik' yang terdapat dalam komputer yang dipakai sebagai media untuk melakukan *cybercrime*.

Ditinjau dari segi hukum, benda atau barang itu mempunyai arti yang bermacam-macam. Menurut hukum pidana, pengertian benda dapat diperoleh dari penjelasan Pasal 362 KUHP yaitu "segala sesuatu yang berwujud atau tidak berwujud (misalnya listrik, gas) dan mempunyai nilai di dalam kehidupan ekonomi seseorang. Berdasarkan pemahaman ini, apakah data/angka atau dokumen yang tersimpan dalam memori komputer atau disket yang tidak dapat diketahui wujudnya itu dapat dikategorikan sebagai barang atau benda sesuai pengertiannya dalam KUHP?

Sebagai bahan perbandingan, penulis mengutip keterangan dari komisi di negeri Belanda yang berpendapat bahwa 'data' (gegevens) itu tidak dapat diartikan sebagai 'barang' seperti yang terdapat dalam perumusan suatu delik. Dengan demikian, bila dalam suatu delik ditemukan unsur 'barang', maka kata barang tidak dapat diartikan sama dengan data/dokumen elektronik sebagaimana yang terdapat

dalam komputer[38]. Hal ini menegaskan bahwa di antara para ahli hukum sendiri belum terdapat kesepakatan mengenai pengertian 'barang' yang dapat dipersamakan dengan 'data/angka elektronik' yang terdapat dalam komputer. Perbedaan penafsiran dan pemahaman terhadap makna ketentuan undang-undang pidana yang ada telah turut meperumit penyelesaian hukum secara tepat terhadap kasus *cybercrime*.

Salah satu contoh kasus yang menunjukan bahwa KUHP kita terlalu riskan untuk diterapkan dalam penyelesaian kasus *cybercrime* adalah Putusan Mahkamah Agung RI tentang perkara Pencurian dalam '*Unauthorized* Transfer' yang mempergunakan sarana komputer pada BNI 1946 Cabang New York (1986). Dalam kasus itu, Mahkamah Agung mengidentikkan 'transfer tidak sah' dengan 'delik pencurian' menurut Pasal 362 KUHP, yaitu mengenai unsur 'mengambil'. Namun dalam perkara ini, terdakwa SA kemudian dinyatakan tidak terbukti melakukan pencurian, karena yang ditransfer ke Bank Panama City, bukanlah uang cash tapi hanya berupa data/angka dan nilai dari angka ini tidak pernah dicairkan menjadi uang. Karena itu, menurut pertimbangan hakim, kasus ini bukanlah delik pencurian sehingga terdakwa SA hanya di jatuhkan hukuman ringan saja. Pada hal Bank BNI'46 nyaris kebobolan $ 18.732.500 atau Rp 29 milyar[39].

Selain itu, permasalahan lain yang sering diperdebatkan adalah mengenai pemalsuan surat/akta atau dokumen. Dalam penjelasan Pasal 263 KUHP dikatakan bahwa yang dimaksud dengan surat adalah segala surat baik yang ditulis dengan

---

[38] Andi Hamzah, op.cit., h. 79
[39] Widyopramono, op.cit., h. 80.

tangan, dicetak, maupun ditulis dengan mesin tik dan lain-lain. Dengan demikian, biasanya suatu surat/akta otentik atau dokemen itu, ditulis atau dicetak diatas kertas (*paper based*). Namun dengan hadirnya teknologi komputer, data/akta atau dokumen dapat disimpan dalam disket, dan memori disk (*paperless based*). Yang menjadi persoalan disini adalah apakah informasi yang tersaji dalam media disket atau *storage disk* itu dapat dikategorikan sebagai surat/atau data otentik sehingga dapat dipakai sebagai alat bukti atas suatu fakta atau kejadian? Ironis memang kalau pencurian atau pemalsuan data/dokumen penting yang tersaji dalam *disket atau memori disk*, hanya dipandang sebagai pencurian terhadap sebuah disket.

Dengan adanya keterbatasan-keterbatasan ini, berarti asas legalitas konvensional menghadapi tantangan serius dalam penerapan terhadap kasus *cybercrime*. Hal ini dapat dimaklumi karena:

1) *Cybercrime* berada di lingkungan elektronik dan dunia maya yang sulit diidentifikasi secara pasti, sedangkan asas legalitas konvensional bertolak dari perbuatan riel dan kepastian hukum.
2) *Cybercrime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah sedangkan asas legalitas konvensional bertolak dari sumber hukum formal yang statis.
3) *Cybercrime* melampaui batas-batas negara, sedangkan perundang-undangan suatu negara pada umumnya hanya berlaku di wilayah teritorialnya sendiri[40].

---

[40] Barda Nawawi Arief, op.cit. 7

Mengingat kegiatan komunikasi dan transaksi dengan media internet di Indonesia masih merupakan hal yang baru dan belum diatur secara khusus dalam suatu peraturan perundang-undangan, maka hal ini dapat menimbulkan keraguan di dalam penggunaannya. Akan tetapi untuk adanya kepastian hukum dan perlindungan hukum, Barda Nawawi Arief menganjurkan agar seyogyanya para penegak hukum memiliki keberanian dan inovasi untuk mengefektifkan peraturan yang ada dengan melakukan interpretasi atau konstruksi hukum yang bersumber pada ilmu hukum, pendapat para ahli, jurisprudensi, atau bersumber dari ide-ide dasar yang secara konseptual dapat dipertanggungjawabkan[41].

Usaha interpretasi ekstentif yang dilakukan tidak hanya sebatas pada peraturan-peraturan yang ada di dalam Kitab Undang-undang Hukum Pidana saja akan tetapi juga terhadap hukum-hukum positif yang berlaku di Indonesia yang mempunyai aspek pidana. Adapun mengenai contoh-contoh terhadap Interpretasi Ekstentif dalam hukum pidana, antara lain adalah sebagai berikut :

1. Data komputer sebagai barang

Interpretasi ekstentif ini berawal dari penafsiran ektensif dari kasus pencurian listrik dimana ada pendapat bahwa tenaga listrik adalah barang dengan alasan :

a. Listrik itu tidak dapat dipisahkan secara sendiri-sendiri.

b. Energi listrik dapat diangkut dan dikumpulkan.

---

[41] Ibid ,

c. Energi listrik mempunyai nilai karena untuk membangkitkan energi listrik memerlukan biaya dan usaha dan dapat dipakai sendiri maupun dapat dipakai orang lain.

Dengan demikian data komputer yang dapat juga dikuasai, dapat dialihkan, dapat digandakan dan mempunyai harga/nilai secara hubungan ekonomi sehingga dapat pula dipandang sebagai benda/barang[42].

2. SURAT (dari Pasal 263 KUHP tentang membuat surat palsu dan memalsukan surat)

a. Segala surat baik yang ditulis dengan tangan, dicetak maupun ditulis memakai mesin ketik dan lain-lainnya.

b. Surat yang dipalsu itu harus suatu surat yang:

1) dapat menimbulkan suatu perjanjian.

2) dapat menerbitkan suatu pembebasan utang.

3) dapat menerbitkan suatu hak.

4) suatu surat yang boleh dipergunakan sebagai suatu keterangan bagi sesuatu perbuatan atau peristiwa[43].

Dengan penafsiran yang diperluas dari pengertian yang ada dalam pasal-pasal tersebut, maka dokemen atau data elektronik yang tersaji dalam komputer dapat digolongkan ke dalam pengertian surat sebagaimana tersebut di atas. Namun demikian, haruslah diingat bahwa perluasan makna yang dibuat ini tidak mengikat

---

[42] Patricia Gaby, loc.cit.
[43] Ibid.

hakim dalam menjatuhkan putusan tetapi hanya sebagai panduan yang tidak memiliki kekuatan hukum apa-apa. Konsekuensinya, di dalam memberikan pertimbangan hukum terhadap putusan sebuah kasus c*ybercrime*, hakim bebas untuk untuk memilih pertimbangan hukum sesuai dengan keyakinannya. Pertanyaannya, apakah para hakim di Indonesia memiliki keyakinan yang sama terhadap perluasan makna pasal-pasal KUHP sebagaimana yang dianjurkan oleh para ahli hukum Indonesia di dalam menjatuhkan putusan terhadap kasus-kasus *cybercrime*?.

b. Asas Kesalahan (*Asas Culpabilitas*)

Disamping persyaratan asas legalitas sebagaimana telah dijelaskan di atas, penjatuhan pidana terhadap pelaku *cybercrime* harus pula memenuhi persyaratan pencelaan subjektif, artinya secara subjektif pelaku *cybercrime* patut dicela atau dipersalahkan atas tindak pidana yang dilakukannya sehingga ia patut dipidana. Persyaratan yang demikian ini lazim dikenal dengan sebutan asas kesalahan (*asas culpabilitas*)[44].

Bila asas legilitas menekankan pada prinsip dipidananya pelaku tindak pidana karena perbuatannya termasuk kualifikasi perbuatan pidana menurut suatu peraturan perundangan yang berlaku maka *asas culpabilitas* menekankan pada dipidananya seseorang karena unsur kesalahan yakni apakah dalam melakukan suatu perbuatan pelaku memiliki kesalahan. Hal ini menimbulkan konsekuensi bahwa seseorang yang melakukan perbuatan pidana belum tentu dipidana karena tidak

[44] Barda Nawawi Arief, op. cit., h. 1

terbukti bersalah (*actus non facit reum nisi mens sit rea*) atau dengan kata lain jika hakim ragu-ragu untuk menentukan adanya unsur kesalahan ini, maka dia tidak boleh menetapkan adanya perbuatan pidana. Dengan demikian pelaku/terdakwa harus diputus bebas[45]. Hal ini sesuai dengan ketentuan Pasal 191 (1) KUHAP yang menyatakan bahwa apabila dari hasil pemeriksaan, kesalahan terdakwa tidak terbukti secara sah dan meyakinkan maka terdakwa diputus bebas.

Menurut Moeljatno, unsur-unsur kesalahan yang harus terpenuhi agar seorang pelaku perbuatan pidana dapat dipidana adalah:

a) Melakukan perbuatan pidana (sifat melawan hukum) yaitu perbuatan-perbuatan yang dilarang dan diancam dengan pidana.

b) Mampu bertanggungjawab. Hal ini berkaitan dengan usia dan keadaan psikis seorang pelaku. Bila seorang pelaku perbuatan pidana terbukti mengalami gangguan jiwa karena cacat atau penyakit, tidak dapat dipidana (Pasal 44 ayat (1) KUHP).

c) Mempunyai suatu bentuk kesalahan berupa kesengajaan (*dolus*) atau kealpaan (*culpa*).

d) Tidak adanya alasan pemaaf yaitu alasan yang menghapuskan kesalahan terdakwa. Perbuatan yang dilakukan terdakwa tetap bersifat melawan hukum tetapi tidak dipidana karena tidak ada unsur kesalahan. Misalnya, Pasal 49 (2) KUHP yang membebaskan seorang pelaku perbuatan pidana dari penjatuhan

---

[45] Moeljatno, op.cit., h. 164

pidana karena adanya alasan bahwa perbuatan pelaku disebabkan oleh pembelaan terpaksa (*noodweer*)[46].

Berdasarkan keempat unsur kesalahan ini, dalam hal *cybercrime*, sifat melawan hukum merupakan persoalan yang sangat rumit karena tidak mudah membuktikan apakah perbuatan yang telah dilakukan oleh seorang pengguna internet itu dilarang dan diancam dengan pidana sehingga ia dapat dipidana. Kejahatan melalui media internet adalah kejahatan dunia maya, dunia tidak kasat mata sehingga sangat sulit untuk mengidentifikasi bukti-bukti perbuatan melawan hukum. Hal ini disebabkan seorang pelaku *cybercrime* dapat melakukan kejahatannya dalam waktu yang relatif sangat cepat dan dapat pula menghilangkan jejaknya tanpa meninggalkan bukti atau petunjuk apapun. Ia dapat melakukan kejahatannya kapan pun dan dari mana saja tanpa bisa dengan mudah dilacak keberadaannya.

Salah satu contoh sulitnya membuktikan sifat melawan hukum dari suatu tindak pidana dunia siber apabila terhadap perbuatan itu, diterapkan anasir pasal-pasal KUHP adalah Kejahatan pornografi dalam internet. Pasal 282 KUHP mensyaratkan unsur dilakukannya kejahatan terhadap kesusilaan di muka umum. Persoalannya penayangan pornografi di internet dalam kenyataanya dapat dilakukan dimana saja bahkan mungkin dilakukan di sebuah tempat tertutup tanpa dilihat oleh orang lain sehingga kita tidak bisa begitu saja menganalogikannya sebagai perbuatan yang dilakukan di muka umum.

---

[46] Ibid, h. 134

Sifat tidak pasti dari perbuatan pidana dalam dunia maya ini membuat aparat penegak hukum ragu-ragu dalam mengambil tindakan hukum yang tegas terhadap pelaku *cybercrime* sehingga timbul kesan bahwa aparat penegak hukum tidak serius dalam upaya memberantas tindak pidana dunia maya (*cybercrime*).

Mengingat sulitnya membuktikan adanya sifat melawan hukum dalam suatu tindak pidana dunia siber, maka sangat diperlukan adanya persamaan persepsi dan kerjasama yang memadai antar aparat penegak hukum baik ditingkat pusat maupun daerah bahkan antar negara agar persoalan mengenai pembuktian kesalahan atau sifat melawan hukum dari suatu perbuatan pidana siber, tidak mengalami kendala atau hambatan dalam penanganannya.

c. Yurisdiksi Berlakunya Hukum Pidana Menurut Tempat *(Teori Locus Delecti)*

Disamping masalah asas legalitas seperti dikemukakan di atas, sisi lain dari aspek pertanggungjawaban *cybercrime* adalah masalah jurisdiksi, khususnya yang berkaitan dengan masalah ruang berlakunya hukum pidana menurut tempat (*locus delicti*). Dalam hukum pidana Indonesia dikenal beberapa teori mengenai ruang berlakunya hukum pidana menurut tempat (*locus delecti*) yaitu:

1) Teori Perbuatan Materiil. Menurut teori ini yang menjadi *locus delicti* (tempat terjadinya perbuatan pidana) adalah tempat di mana pelaku melakukan perbuatan yang dapat menimbulkan perbuatan pidana yang bersangkutan.

2) Teori Alat Yang Dipergunakan. Teori ini menyatakan bahwa yang menjadi locus delicti adalah tempat dimana alat yang dipergunakan untuk melakukan perbuatan pidana itu berada.

3) Teori Akibat. Menurut teori ini yang menjadi locus delicti adalah tempat keberadaan akibat dari perbuatan pidana itu[47].

Pemahaman yang benar terhadap asas-asas ruang berlakunya hukum pidana sangat penting dalam mengajukan penuntutan terhadap pelaku *cybercrime* karena:

1) Menentukan berlakunya undang-undang pidana nasional bagi perbuatan pidana tersebut.

2) Menentukan kompetensi relatif (kewenangan untuk mengadili) bagi hakim yang mengadili perkara ini[48].

Namun demikian, asas-asas ruang berlakunya hukum pidana menurut tempat yang konvensional ini, akan menghadapi tantangan dalam penerapannya terhadap kasus *cybercrime*. Hal ini disebabkan *cybercrime* bersifat *trans-nasional* dan *extraterritorial* yang dapat melibatkan banyak negara dengan *locus delicti* yang dapat terjadi dimana saja dan korbannyapun bisa di negara manapun di dunia yang tersambung dengan jaringan internet. Pada hal, dalam sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas territorial) dan warga negaranya sendiri (asas personal/nasional aktif).

---

[47] Patricia Geby, op.cit
[48] Ibid

Hal ini memunculkan pertanyaan mengenai negara mana atau pihak mana yang berwewenang mengadili pelaku kejahatan *cybercrime* yang melibatkan pelaku dan korban yang berasal dari wilayah negara yang berbeda? Mengingat keterbatasan hukum nasional dalam menjangkau pelaku *cybercrime* yang bersifat transnasional ini, maka seyogyanya dalam penanganan perkara *cybercrime* diterapkan yurisdiksi hukum internasional yang sudah diakui dan dipraktekkan oleh masyarakat internasional.

Berdasarkan hukum internasional, terdapat tiga jenis yurisdiksi yang berlaku dalam penanganan kasus *cybercrime* yaitu,

1) Yurisdiksi untuk menetapkan undang-undang (*the jurisdiction to prescribe).*

2) Yurisdiksi untuk menegakan hukum (*the jurisdiction to enforce*).

3) Yurisdiksi untuk menuntut (*the jurisdiction to adjudicate*)[48].

Sedangkan untuk menentukan yuridiksi hukum yang berlaku, harus diperhatikan prinsip-prinsip hukum internasional seperti:

a. Asas *subjectif territoriality,* yaitu asas yang menentukan keberlakuan hukum berdasarkan tempat dimana pelaku perbuatan *cybercrime* itu berada. Jadi kalau pelaku *cybercrime* adalah orang Indonesia yang pada saat melakukan perbuatan pidana *cyber* berada di Indonesia sedangkan korbannya berasal dari negara lain. maka berdasarkan asas teritorial subyektif ini, negara yang berhak mengadili pelaku *cybercrime* adalah negara Indonesia.

---

[48] H. Ajmad M. Ramli, Cyberlaw Dalam Sistem Hukum Indonesia, Refika Aditama Bandung, Oktober 2004, h. 19

b. Asas *objectif territoriality,* yaitu asas yang menentukan keberlakuan hukum berdasarkan tempat dimana akibat perbuatan itu berada. Dalam hal ini, negara yang menjadi korban dan paling dirugikan dengan adanya perbuatan *cybercrime* berhak untuk mengadili pelaku *cybercrime* walaupun pelakunya bukan warganegaranya sendiri.

c. Asas *aktif nationality,* yaitu asas yang menekankan yurisdiksi berdasarkan kewarganegaraan pelaku.

d. Asas *pasif nationality,* yaitu asas yang menekankan yurisdiksi berdasarkan kewarganegaraan korban.

e. Asas *protective principle*, yaitu asas yang mendasarkan yurisdiksinya pada keinginan negara untuk melindungi kepentingan negaranya apabila korbannya adalah negara atau pemerintah.

f. Asas *universality,* yaitu asas yang menyatakan bahwa setiap negara berhak menangkap dan mengadili pelaku kejahatan. Dalam hal ini, *cybercrime* dapat dipandang sebagai *piracy* (pembajakan) terhadap kepentingan orang lain sehingga dapat diadili oleh negara manapun di dunia demi menjaga keamanan dan kestabilan nasional dan internasional[49].

Masalah yurisdiksi *cybercrime* ini termasuk masalah yang sangat serius karena cybercrime dapat bersinggungan dengan negara lain yang memiliki kepentingan dan sistem hukum sendiri dalam menangani suatu kasus yang melibatkan negaranya. Barbara Etter, di dalam tulisannya yang berjudul "*Critical Issues in Hi-*

[49] Ibid, h. 20

tech Crime" mengidentifikasi beberapa masalah utama yang menyebabkan timbulnya masalah yurisdiksi ini dalam konteks internasional, yaitu

1. *The lack of global consensus on what types of conduct should constitute a computer related crime.*
2. *The lack of global consensus on the legal definition of criminal conduct.*
3. *The lack of expertise on the part of the police, prosecutors and the courts in this field.*
4. *The inadequacy of legal powers for the investigations and access to computer systems, including the inapplicability of seizure powers to intangibles such as computerized data.*
5. *The lack of harmonization between the different national procedural laws concerning the investigation of computer-related crimes.*
6. *The transnational character of many computer crimes.*
7. *The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation, or the inability of existing treaties to take into account the dynamics and special requirements of computer crime investigation*[50].

Mengingat kompleksitas permasalahan mengenai kewenangan dalam menentukan hukum yang berlaku terhadap pelaku kejahatan internasional, Matthew Burnstein memberikan tiga alternatif penyelesaiannya yakni:

1) Unifikasi pilihan hukum (*a unification of choice of law*). Dalam hal ini dibuat kesepakatan internasional tentang kewenangan mengadili pelaku kejahatan *cybercrime* dalam bentuk konvensi internasional.

2) Unifikasi substansi hukum internet (*a unification of a substantive internet law*). Disini dibuatkan ketentuan hukum internasional yang mengikat semua negara, sehingga penyelesaian hokum terhadap pelaku *cybercrime* dapat diterima masyakat internasional.

---

[50] Barda Nawawi Arief, op.cit. h. 13.

3) Membentuk Badan Arbitrase Intenet Internasional (*International Internet Arbitration Board*) yang khusus menangani kasus-kasus *cybercrime*[51].

Di Indonesia, menurut Romli Atmasasmita, sebagai langkah antisipasi terhadap persoalan yurisdiksi hukum ini adalah dengan memasukkan secara khusus ketentuan mengenai kerja sama internasional seperti *ekstradisi dan mutual assitance in criminal matters* ke dalam rancangan undang-undang yang berkaitan dengan dunia siber[52].

---

[51] Kenny Wiston, The Internet : Issues of Jurisdiction and Controversies Surrounding Domain Names, Citra Aditya Bakti, Bandung 2002, h. 9-11

[52] RUU Tak Sentuh Kejahatan Internasoanal, dapat dijumpai http://www.kompas.com/ internet/news, 22 Oktober 2003

BAB IV

PENUTUP

BAB IV

PENUTUP

1. Simpulan

Berdasarkan pemaparan saya tentang pengaturan *cybercrime* dalam hukum pidana Indonesia dan permasalahan hukum yang timbul dalam penerapan hukum pidana yang berkaitan dengan *cybercrime* di Indonesia, dapatlah ditarik beberapa kesimpulan sebagai berikut:

a) Mengingat Indonesia belum memiliki peraturan khusus yang mengatur tentang aktivitas dalam dunia maya di internet maka dalam menindak pelaku *cybercrime*, aparat penegak hukum menggunakan ketentuan hukum pidana yang ada yang berkaitan dengan *cybercrime* seperti Kitab Undang-undang Hukum Pidana (KUHP), UU No. 36 tahun 1999 tentang Telekomunikasi, UU No. 20/2001 tentang Pemberantasan Tindak Pidana Korupsi, UU No. 15/2002 tentang Tindak Pidana Pencucian Uang, dan UU No. 32/2002 Tentang Penyiaran.

b) Penerapan ketentuan hukum pidana sebagaimana tersebut di atas, dalam realisasinya banyak mengalami kendala terutama berkaitan pemenuhan persyaratan pemidanaan umum yaitu asas legalitas, asas culpabilitas (sifat melawan hukum) dan yurisdiksi dalam penerapan hukum. Interpretasi hukum yang dilakukan terhadap ketentuan hukum pidana yang ada, terkadang kurang tepat sehingga menimbulkan kesan bahwa aparat penegak hukum tidak mampu

dalam menangani persoalan hukum yang berkaitan dengan kejahatan dalam dunia maya di internet. Hal ini terbukti dengan maraknya aktivitas *cybercrime* di Indonesia sahingga menempatkan Indonesia ditingkat pertama di dunia dalam jenis *cybercrime 'card fraud'* atau pemalsuan kartu kredit.

2. Saran

Mengingat maraknya aktivitas dunia maya dan kejahatan yang timbul di dalamnya serta rumitnya persoalan hukum yang dihadapi dalam penyelesaian kasus-kasus *cybercrime* di Indonesia sebagaimana yang telah diuraikan dalam skripsi ini, maka saya mengharapkan:

a) Agar pemerintah dan para wakil rakyat yang terhormat (DPR) segera membahas dan mensahkan Rancangan Undang-Undang yang berkaitan dengan aktivitas mayantara agar dapat dipakai sebagai landasan formal dalam menuntut pelaku perbuatan pidana *cybercrime*.

b) Agar aparat penegak hukum baik ditingkat pusat maupun daerah, melakukan koordinasi dan kerjasama yang memadai, baik dalam skala nasional maupun internasional dalam upaya menyelesaikan kasus-kasus *cybercrime* di Indonesia. Misalnya, menyamakan persepsi tentang penggunaan istilah-istilah hukum pidana sebagaimana yang terdapat dalam KUHP terhadap hal-hal yang berkaitan dengan kejahatan mayantara agar tidak terdapat perbedaan penafsiran (*missmeaning*) diantara aparat penegak hukum sendiri..

c) Agar aparat penegak hukum lebih meningkatkan kewaspadaannya dalam mengahadapi kasus-kasus *cybercrime* di internet karena karekteristik *cybercrime* sangat canggih dan rumit. Hal ini dapat dilakukan dengan merekrut penegak hukum yang memiliki integritas moral yang tinggi, melakukan pelatihan untuk meningkatkan professionalismenya sehingga tidak timbul kesan aparat hukum 'gaptek' (gagap teknologi), dan mendatangkan peralatan bantu seperti *forensik computing* untuk mempermudah upaya pembuktian *cybercrime*.

d) Agar pemerintah, aparat penegak hukum, para pendidik (guru dan dosen) pengusaha warung internet, dan pihak-pihak lain yang berkompeten di bidang teknologi internet, lebih menyebarluaskan atau mengajarkan etika penggunaan internet/komputer kepada warga masyarakat terutama kepada kalangan pengakses internet melalui media pendidikan, seminar, media massa baik cetak maupun elektronik atau forum-forum lainnya. Sangatlah disayangkan bila pelaku *cybercrime* justru menganggap dirinya sebagai 'pahlawan' dan 'orang pintar' karena berhasil menjebol situs pengaman internet pihak lain atau mendapatkan barang mewah tanpa mengeluarkan biaya sepeser pun karena kelincahannya memanfaatkan keunggulan teknologi internet.

DAFTAR BACAAN

DAFTAR BACAAN

1. BUKU & MAKALAH :

Arief, Barda Nawawi, Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana, Citra Aditya Bakti, Bandung, 1998.

_____, Masalah Pertanggungjawaban Pidana Cybercrime, Makalah Seminar Nasional "Problematika Hukum Cybercrime", Fakultas Hukum Universitas Airlangga, Surabaya, 9 Oktober 2004.

Gudono, Mengenal Kejahatan Komputer dan Upaya Pengamanannya, FajarAgung, Jakarta, Desember 1989.

Hamzah, Andi Aspek-Aspek Pidana di Bidang Komputer, Cet. II, Sinar Grafika, Jakarta, 1987.

Moeljatno, Asas-Asas Hukum Pidana, Cet. VII, Rineka Cipta, Jakarta, September 2002

Muslim, Salamoen H.M., Problematika Penuntutan Tindak Pidana Cyber/Teknologi Informasi, Makalah Seminar Nasional "Problematika Hukum Cybercrime", Fakultas Hukum Universitas Airlangga, Surabaya, 9 Oktober 2004.

Raharjo, Agus, Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Citra Aditya Bakti, Bandung, 2002.

Ramli, M. Ahmad., Cyberlaw Dalam Sistem Hukum Indonesia, Refika Aditama Bandung, Oktober 2004

Suhemi, Kejahatan Komputer, Andi Offset, Yogyakarta, 1991.

Tim Fakultas Hukum Universitas Airlangga, Problematika Penegakan Hukum Cybercrime di Indonesia, Makalah Seminar Nasional "Problematika Hukum Cybercrime", Fakultas Hukum Universitas Airlangga, Surabaya, 9 Oktober 2004.

Widyopramono, Kejahatan di Bidang Komputer, Pustaka Sinar Harapan, Jakarta, 1994.

Wiston, Kenny, The Internet : Issues of Jurisdiction and Controversies Surrounding Domain Names, Citra Aditya Bakti, Bandung 2002.

2. MAJALAH & KORAN

FORUM KEADILAN, No. 44, 4 April 2004.

Kompas, 17 Maret 2004, 23 April 2004.

3. INTERNET

hhtp://www.amwibowo@excite.com.

http://www.apjii.or.id.com.

http://www.indo.net news.com.

http://www.pikiran-rakyat.com.

http://www.solusi hukum.com.

http://students.ukdw.ac.id/~22033149/dani.htm.

http://search yahoo.com. hukum kejahatan internet.

http://www.tempo.com/internet/news.com.