

PENANGGULANGAN KEJAHATAN *HACKING* DI INDONESIA

(Suatu Kajian dalam Perspektif Kebijakan Hukum Pidana
Saat ini dan Wacana Kebijakan Hukum Pidana Akan Datang)

Oleh : Suhartono, S.Ag., SH., MH.

(Hakim PA Martapura)

E-mail: suhartono_71@yahoo.com

Abstrak

Cybercrime merupakan fenomena sosial yang membuka cakrawala keilmuan dalam dunia hukum, betapa suatu kejahatan yang sangat dasyat dapat dilakukan dengan hanya duduk manis di depan computer. *Cybercrime* merupakan sisi gelap dari kemajuan teknologi komunikasi dan informasi yang membawa implikasi sangat luas dalam seluruh bidang kehidupan karena terkait erat dengan *economic crime* dan *organized crimes*.

Dari beberapa jenis *cybercrime*, Kongres PBB X di Wina menetapkan *hacking* sebagai *first crime*. Persoalannya apakah hukum pidana positif dapat menjangkau kejahatan *hacking*, setidaknya ada dua wacana yang berkembang di antara para pakar hukum pidana. Pertama, kejahatan computer *-hacking-* sebenarnya bukanlah kejahatan baru dan masih terjangkau oleh KUHP untuk menanganinya. Menurut pendapat ini pengaturan untuk menangani kejahatan komputer *-hacking-* sebaiknya diintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri. Kedua, pendapat ini menyatakan perlu pembaharuan hukum pidana dengan membentuk Undang-Undang baru yang mengatur masalah kejahatan komputer *-hacking-*. Hal ini dilandasi kenyataan bahwa kejahatan ini memiliki karakteristik yang berbeda dengan tindak pidana konvensional, sementara instrument hukum pidana yang ada masih kesulitan untuk menanggulangi perkembangan kejahatan *ini*.

Ada dua isu hukum (*legal issues*) yang menarik untuk dikaji. *Pertama*, mengenai kejahatan *hacking* dalam perspektif kebijakan hukum pidana yang berlaku saat ini. *Kedua*, penanggulangan kejahatan *hacking* dalam perspektif wacana kebijakan hukum pidana yang akan datang.

Kata Kunci : internet, *cyberspace*, *cybercrime*, *hacking*, Kebijakan Hukum Pidana.

A. Pendahuluan

J.E. Sahetapy menyatakan bahwa kejahatan erat kaitannya dan bahkan menjadi bagian dari hasil budaya itu sendiri. Artinya semakin tinggi

tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu bentuk, sifat dan cara pelaksanaannya.¹

Kejahatan dalam bidang teknologi informasi secara umum dapat dikategorikan menjadi dua kelompok. *Pertama*, kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantu. Dalam kejahatan ini terjadi peningkatan modus dan operandinya dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan teknologi informasi. Dampak dari kejahatan biasa yang telah menggunakan teknologi informasi ternyata berdampak cukup serius, terutama jika dilihat dari jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pencurian uang dengan pembobolan bank atau 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. *Kedua*, kejahatan yang muncul setelah adanya internet, dimana sistem komputer sebagai korbannya. Kejahatan yang menggunakan aplikasi internet adalah salah satu perkembangan dari kejahatan teknologi informasi. Jenis kejahatan dalam kelompok ini makin bertambah seiring dengan kemajuan teknologi informasi. Contoh dari kejahatan kelompok ini adalah perusakan situs internet, pengiriman virus atau program-program komputer yang tujuannya merusak sistem kerja komputer.²

Internet (*interconnected Network*) adalah konvergensi telematika yang merupakan perpaduan antara teknologi komputer, media dan teknologi informasi. Internet merupakan jaringan komputer yang terdiri dari ribuan bahkan jutaan jaringan komputer independent yang dihubungkan satu dengan yang lainnya. Jaringan ini dapat dimanfaatkan untuk kepentingan

¹ Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer*, (Malang: Lembaga Penerbitan Fakultas Hukum UNISMA, 2002) hal. 21.

² Heru Sutadi, *Cybercrime, Apa Yang Bisa Diperbuat?*, <http://www.sinarharapan.co.id/berita/0304/05/opi01.html>.2003

sosial, ekonomi, politik, militer bahkan untuk propaganda maupun terorisme.³

Internet merupakan sebuah ruang informasi dan komunikasi yang menembus batas-batas yurisdiksi antar Negara. Sebuah media yang menawarkan beragam kemudahan-kemudahan bertransaksi tanpa mempertemukan para pihak secara fisik atau materiil. Internet telah membawa kita ke dalam dunia baru yang disebut *cyberspace*, yang dalam perkembangannya tidak hanya membawa efek positif tetapi juga sarat dampak negatif.

Cyberspace sebagai wahana komunikasi yang berbasis computer (*computer mediated communication*), banyak menawarkan realitas baru dalam berinteraksi dalam dunia maya. Adanya interaksi antar pengguna *cyberspace* telah banyak terseret ke arah terjadinya penyelewengan hubungan sosial berupa kejahatan yang khas yang memiliki karakteristik berbeda dengan tindak pidana konvensional yang selama ini sudah dikenal. Namun ada juga yang berpandangan bahwa kejahatan melalui internet (*cybercrime*) memiliki kesamaan bentuk dengan kejahatan yang ada di dunia nyata.⁴

Belum ada definisi yang seragam mengenai istilah *cybercrime*,⁵ istilah ini banyak banyak dipakai terhadap suatu bentuk kejahatan yang berkaitan dengan dunia virtual dan tindakan kejahatan yang menggunakan sarana komputer. Jenis aktivitas kejahatan yang berkaitan dengan komputer sangat

³ Ramos Horta menggunakan internet sebagai media perjuangan untuk memerdekakan Timor-Timur, terutama setelah jajak pendapat Agustus 1999, Ramos Horta dan "pasukan digitalnya" menyerang situs-situs Pemerintah Indonesia, Republika 22 Agustus dan 26 September 1999.

Demikian pula munculnya situs anshar.net sebagai alat propaganda kelompok teroris Dr. Azahari. Dalam situs ini dimuat cara-cara melakukan terror, target serangan dan alas an terror yang mereka lakukan, lihat di www.metrovnews.com.

⁴ Tubagus Ronny Rahman Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi* (Jakarta: Peradaban, 2001), hal. 53.

⁵ Barda Nawawi Arif menggunakan istilah tindak pidana mayantara untuk jenis kejahatan ini, (Seminar Nasional Cyber Law, Bandung, 9 April 2001).

beragam, sehingga banyak muncul istilah-istilah baru di antaranya: *hacking*, *cracking*, *viruses*, *booting*, *troyan horse*, *spamming* dan lain sebagainya.

Untuk mempersempit ruang lingkup pembahasan, maka penulis hanya membatasi dan mengangkat isu hukum seputar penanggulangan kejahatan *hacking* ditinjau dari perspektif kebijakan hukum pidana saat ini dan wacana kebijakan hukum pidana akan datang sebagaimana judul artikel ini.

Hacking dikenal juga dengan sebutan *computer trespass*, yakni tindakan yang melanggar hukum apapun bentuk alasan dan motivasinya. Tidak jarang tindakan ini disertai dengan penipuan, pencurian, penggelapan atau pengrusakan. Kejahatan *hacking* telah mempunyai sejarah perjalanan panjang, bermula diakhir perang dunia II sampai dengan tahun 60-an komputer masih merupakan barang langka, hanya beberapa departemen dan organisasi besar yang memiliki komputer. Pada awalnya beberapa mahasiswa yang berasal dari *Institute of Technology* (MIT) di Massachusetts melakukan eksperimen dengan menggunakan komputer institutnya. Mereka melakukan penyusupan-penyusupan dengan maksud agar penggunaan komputer tersebut dapat dilakukan kapan saja dan dimana saja. Para Mahasiswa tersebut membuat program yang bertujuan mengoptimalkan fungsi dan kerja komputer dan membantu pengembangan bahasa LISP karya John McCarthy.

Selain membuat program, mereka juga bekerja dalam pembuatan proyek MAC (*Multiple Access Computer*). Pada saat inilah pertama kali istilah "*hacker*" digunakan. Istilah ini berawal dari kata "*hack*" yang saat itu artinya teknik pemrograman kreatif yang mampu memecahkan masalah secara jauh dan lebih efisien daripada teknik biasa. Saat itu, sebuah tindakan *hacking computer* sangat bermanfaat karena dapat meningkatkan kemampuan program dan lebih hemat.

Pada tahun 1969, dengan dibangunnya APRANET oleh Departemen Pertahanan dan Keamanan Amerika (awalnya jaringan ini hanya

menghubungkan beberapa perguruan tinggi seperti Stanford dan UCLA, kemudian jaringan ini mampu dikembangkan) semakin mendorong pertumbuhan kelompok *hacker* di universitas-universitas terkemuka, antara lain MIT (pelopor hacker), Carnegie-Mellon dan Stanford AI Lab., Kemudian sejalan dengan perkembangan teknologi komputer dan pesatnya pertumbuhan jaringan internet, mendorong meningkatnya pertumbuhan para *hacker*, khususnya di tahun 90-an, dimana internet telah berkembang dengan pesat. Para *hacker* membentuk komunitasnya sendiri (*cyber community*), dimana mereka sering menunjukkan keahlian mereka, bahkan sering juga disertai dengan tindakan-tindakan yang merugikan. Seperti kerusakan sistem komputer, hilangnya seluruh data dalam komputer, tidak berfungsinya *search engine*; seperti yahoo, CNN yang sempat terhenti beberapa hari, dan tentunya kerugian besar dari segi ekonomi.⁶

Hacking bukanlah suatu bentuk kejahatan sederhana, karena pembuktiannya yang sulit dan seringkali terbentur oleh belum adanya peraturan hukum yang jelas dan tegas. Hal ini terbukti dengan masih enggannya investor luar negeri yang bergerak dalam perdagangan *e-commerce* kurang berminat menjalankan bisnisnya di Indonesia, mereka khawatir karena tidak ada regulasi perlindungan hukum yang jelas mengenai hal tersebut.

B. Kebijakan Dunia Internasional Terhadap *Cybercrime*

Perangkat hukum internasional sudah dibentuk dengan adanya beberapa kongres-kongres PBB, dan hal tersebut wajib untuk diratifikasi oleh Negara anggota. Langkah yang ditempuh adalah memasukkan *cybercrime* dalam sistem hukumnya masing-masing.

⁶ Dewi Lestari, *Kejahatan Komputer (Cybercrime)*, http://www.lkht.net/artikel_lengkap.php?id=6, di akses tanggal 05 November 2007

Dalam rangka menanggulangi *cybercrime*, Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* dan *International Industry Congres (IIIC) 2000 Millenium Congres* di Quebec pada tanggal 19 September 2000 dan Kongres PBB mengenai *The Prevention of Crime anda The Treatment of Offenders*, mengajukan beberapa kebijakan antara lain :⁷

1. Menghimbau Negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan computer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
 - a. Melakukan modernisasi hukum pidana meteriil dan hukum acara pidana;
 - b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
 - c. Melakukan langkah-langkah untuk membuat warga masyarakat, aparat pengadilan dan penegak hukum sensitive terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer (*cybercrime*);
 - d. Memperluas *rules of ethics* dalam penggunaan computer dan mengajarkannya dalam kurikulum informatika;
 - e. Mengadopsi kebijakan perlindungan korban *cybercrime* sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cybercrime*.
2. Menghimbau negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*.
3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*committee on Crime Preventon And Control*) PBB untuk :
 - a. Menyebarkan pedoman dan standar untuk membantu Negara anggota menghadapi *cybercrime* di tingkat nasional, regional dan internasional;

⁷ Barda Nawawi Arif, *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, 1991, hal. 141.

- b. Mengembangkan penelitian dan analisa lebih lanjut guna menemukan cara-cara baru menghadapi problem *cybercrime* di masa depan;
- c. Mempertimbangkan *cybercrime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama di bidang penanggulangan kejahatan.

Kebijakan penanggulangan *cybercrime* yang digariskan dalam Resolusi PBB sebagaimana diuraikan di atas cukup komprehensif. Penanggulangan tidak hanya melalui kebijakan penal (hukum pidana meteril dan formil), tetapi juga kebijakan non penal.⁸ Kebijakan non penal yang dikembangkan adalah upaya mengembangkan dan pengamanan perlindungan computer dan tindakan-tindakan pencegahan (*computer security and prevention measures*), yakni tindakan pencegahan dengan teknologi.

Secara internasional, PBB telah menghimbau Negara-negara anggota untuk menanggulangi *cybercrime* dengan sarana penal, namun dalam kenyataannya tidaklah mudah. Dokumen Kongres PBB X/2000 sendiri mengakui bahwa ada beberapa kesulitan dalam menanggulangi *cybercrime* dengan sarana penal, antara lain:⁹

1. Perbuatan jahat yang dilakukan berada di lingkungan elektronik. Oleh karena itu penanggulangan *cybercrime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia di Negara yang bersangkutan;
2. *Cybercrime* melampaui batas-batas Negara, sedangkan supaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah territorial negaranya sendiri;
3. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (Negara) yang belum mengkriminalisasikan *cybercrime*. Terjadi "*data havens*"

⁸ *Ibid.*

⁹ *Ibid, hal. 9*

(Negara tempat berlindung/singgahnya data, yaitu Negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha Negara lain untuk memberantas kejahatan itu.

Persoalan di atas sebenarnya berkaitan dengan kebijakan hukum pidana (*penal policy*). Marc Ancel mendefinisikan kebijakan hukum pidana sebagai ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dalam hal ini hukum pidana) dirumuskan secara lebih baik.¹⁰

Kebijakan hukum pidana terkait erat dengan proses kriminalisasi terhadap suatu perbuatan. Dalam Kongres PBB/X/2000 disebutkan bahwa dalam jaringan komputer global, kebijakan criminal Negara mempunyai pengaruh langsung pada masyarakat internasional. Para penjahat *cyber* dapat mengarahkan aktifitas elektroniknya melalui suatu negara yang belum melakukan kriminalisasi terhadap kejahatan yang dilakukan itu dan oleh karena ia merasa aman dan terlindungi oleh hukum yang berlaku di negara tersebut. Kendatipun suatu negara tidak mempunyai kepentingan nasional khusus dalam melakukan kriminalisasi terhadap perbuatan tertentu, seyogyanya dipertimbangkan untuk melakukan langkah sebagai upaya menghindari negara tersebut menjadi *data haven* (tempat berlindungnya data) dan menjadi terisolasi secara internasional. Harmonisasi hukum pidana substantif mengenai *cybercrime* merupakan hal yang esensial apabila kerjasama internasional harus dicapai oleh beberapa negara yang berbeda.¹¹

Kekhawatiran terhadap kejahatan mayantara di dunia sebetulnya telah dibahas secara khusus dalam suatu lokakarya (yaitu, "*workshop on crimes to computer networks*") yang diorganisir oleh UNAFEI selama kongres PBB X/2000 berlangsung.

¹⁰ Wisnusubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer* (Yogyakarta: Universitas Atmajaya, 1999) hal. 3.

¹¹ Barda Nawawi Arief, *op.cit.*, hal. 10

Adapun kesimpulan dari lokakarya tersebut adalah sebagai berikut:¹²

- a. CRC (*computer related crime*) harus dikriminalisasikan;
- b. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat cyber (*cybercrimes*);
- c. Harus ada kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman;
- d. Diperlukan kerjasama internasional untuk menelusuri/mencari para penjahat di internet;
- e. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan dan kerjasama teknis dalam penanggulangan CRC.

Dari uraian di atas diketahui bahwa sebenarnya *cybercrime* khususnya kejahatan *hacking* adalah sebuah isu hukum internasional. Perbedaannya adalah di beberapa negara anggota PBB sudah meratifikasi hasil kongres internasional mengenai kejahatan ini dalam sebuah regulasi peraturan perundang-undangan secara khusus, sedangkan di Indonesia belum diatur secara khusus mengenai kejahatan tersebut.

C. Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan *Hacking* saat ini.

Ketentuan-ketentuan mengenai *cybercrime* dalam KUHP masih bersifat global, namun berdasarkan tingkat kemungkinan terjadinya kasus dalam dunia maya (*cyberspace*) dan kategorisasi kejahatan *cyber* menurut *draft convention on cyber crime* maupun pendapat para ahli, Teguh Arifandi (Inspektorat Jendral Depkominfo) mengkatagorikan beberapa hal yang secara khusus diatur dalam KUHP dan disusun berdasarkan tingkat

¹² Teguh Arifiyadi, *Cyber Crime dan Upaya Antisipasinya Secara Yuridis (II)*, http://www.depkominfo.go.id/portal/?act=detail&mod=artikel_itjen&view=1&id=BRT061002182401, diakses tgl. 05 November 2007.

intensitas terjadinya kasus tersebut, -yang berkaitan dengan kejahatan hacking- antara lain:¹³

1. Ketentuan yang berkaitan dengan delik pencurian;
2. Ketentuan yang berkaitan dengan perusakan/ penghancuran barang;
3. Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain;

1. Ketentuan yang Berkaitan dengan Delik Pencurian

Delik tentang pencurian dalam dunia maya termasuk salah satu delik yang paling sering diberitakan di media masa. Pencurian disini tidak diartikan secara konvensional karena barang yang dicuri adalah berupa data digital, baik yang berisikan data transaksi keuangan milik orang lain maupun data yang menyangkut *software* (program) ataupun data yang menyangkut hal-hal yang bersifat rahasia.

Delik pencurian di atur dalam Pasal 362 KUHP dan variasinya diatur dalam Pasal 363 KUHP, yakni tentang pencurian dengan pemberatan; Pasal 364 KUHP tentang pencurian ringan, Pasal 365, tentang pencurian yang disertai dengan kekerasan; Pasal 367 KUHP, tentang pencurian di lingkungan keluarga.

Pasal 362 KUHP berbunyi:

"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 pidana denda paling banyak Sembilan ratus rupiah"

Menurut hukum pidana, pengertian benda diambil dari penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud seperti listrik, dan mempunyai nilai di dalam kehidupan ekonomi dari

¹³ Teguh Arifiyadi, *Menjerat Pelaku Cyber Crime dengan KUHP*, http://www.depkominfo.go.id/portal/?act=detail&mod=artikel_itjen&view=1&id=BRT07062_0115101, diakses tanggal 05 November 2007

seseorang. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya dapat berwujud dengan cara menampilkan pada layar penampil komputer (*screen*) atau dengan cara mencetak pada alat pencetak (*printer*). Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda seperti pada penjelasan Pasal 362 KUHP.

Kendatipun demikian dalam sistem pembuktian kita terutama yang menyangkut elemen penting dari alat bukti (Pasal 184 KUHP ayat (1) huruf c) masih belum mengakui data komputer sebagai bagiannya karena sifatnya yang digital. Padahal dalam kasus *cybercrime* data elektronik seringkali menjadi barang bukti yang ada. Karenanya sangat realistis jika data elektronik dijadikan sebagai bagian dari alat bukti yang sah.¹⁴

Menurut pengertian *computer related crime*, pengertian mengambil adalah dalam arti meng-copy atau mereka data atau program yang tersimpan di dalam suatu disket dan sejenisnya ke disket lain dengan cara memberikan instruksi-instruksi tertentu pada komputer sehingga data atau program yang asli masih utuh dan tidak berubah dalam posisi semula.

Menurut penjelasan pasal 362 KUHP, barang yang sudah diambil dari kekuasaan pemiliknya itu, juga harus berindah dari tempat asalnya, padahal dengan mengambil adalah melepaskan kekuasaan atas benda itu dari pemiliknya untuk kemudian dikuasai dan perbuatan itu dilakukan dengan sengaja dengan maksud untuk dimiliki sendiri, sehingga perbuatan meng-copy yang dilakukan dengan sengaja tanpa ijin dari pemiliknya dapat dikategorikan sebagai perbuatan "mengambil" sebagaimana yang dimaksud dengan penjelasan Pasal 362 KUHP.

Dalam sistem jaringan (*network*), peng-copy-an data dapat dilakukan secara mudah tanpa harus melalui izin dari pemilik data. Hanya sebagian kecil saja dari data internet yang tidak dapat "diambil" oleh para

¹⁴ *Ibid.*

pengguna internet. Pencurian bukan lagi hanya berupa pengambilan barang/benda berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah.

Penggunaan fasilitas *Internet Service Provider* (ISP) untuk melakukan kegiatan *hacking* erat kaitannya dengan delik pencurian yang diatur dalam Pasal 362 KUHP. Pencuri biasanya lebih mengutamakan memasuki sistem jaringan perusahaan financial, misalnya: penyimpanan data kartu kredit, situs-situs belanja *on-line* yang ditawarkan di media internet dan data yang didapatkan secara melawan hukum itu diharapkan memberi keuntungan badi si pelaku.¹⁵

2. Ketentuan yang Berkaitan dengan Kejahatan Perusakan dan Penghancuran Barang

Ketentuan ini erat dengan kejahatan *hacking*. Dalam kejahatan mayantara (*cybercrime*) perbuatan perusakan dan penghancuran barang ini tidak hanya ditujukan untuk merusak/menghancurkan media disket atau media penyimpan sejenis lainnya, namun juga merusak dan menghancurkan suatu data, *web site* ataupun *homepage*. Delik ini juga termasuk di dalamnya perbuatan merusak barang-barang milik publik (*crime against public property*).

Ketentuan mengenai perbuatan perusakan, penghancuran barang diatur dalam Pasal 406-412 KUHP.

Pasal 406 KUHP berbunyi:

- (1) Barangsiapa dengan sengaja melawan hukum menghancurkan, merusakkn, membikin tidak dapat dipakai lagi atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana dipenjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah;
- (2) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin

¹⁵ *Ibid.*

tidak dapat digunakan atau menghilangkan hewan yang seluruhnya atau sebagian adalah kepunyaan orang lain.

Pengertian-pengertian dalam Pasal 406 KUHP dapat dijelaskan sebagai berikut:¹⁶

Pengertian “menghancurkan” (*vermielen*)

Menghancurkan atau membinasakan dimaksudkan sebagai merusak sama sekali sehingga suatu barang tidak dapat berfungsi sebagaimana mestinya.

Pengertian “merusakkan”

Merusakkan dimaksudkan sebagai memperlakukan suatu barang sedemikian rupa namun kurang dan membinasakan (*beschadigen*). Misalnya: perbuatan merusak data atau program komputer yang terdapat di internet dengan cara menghapus data atau program, membuat cacat data atau program, menambahkan data baru ke dalam suatu situs (*web*) atau sejenisnya secara acak. Dengan kata lain, perbuatan tersebut mengacaukan isi media penyimpanannya.

Pengertian “membikin/membuat tidak dapat dipakai lagi”

Tindakan itu harus sedemikian rupa, sehingga barang itu tidak dapat diperbaiki lagi. Kaitannya dengan *cybercrime* adalah perbuatan yang dilakukan tersebut menyebabkan data atau program yang tersimpan dalam media penyimpan (*data base*) atau sejenisnya menjadi tidak dapat dimanfaatkan (tidak berguna lagi). Hal ini disebabkan oleh data atau program telah dirubah sebagian atau seluruhnya, atau dirusak pada suatu bagian atau seluruhnya, atau dihapus pada sebagian atau seluruhnya.

Pengertian “menghilangkan”

Adalah membuat barang itu tidak ada lagi. Kaitannya dengan *cybercrime* yakni perbuatan menghilangkan atau menghapus data yang tersimpan pada data base –bisa juga tersimpan dalam suatu web- atau

¹⁶ *Ibid.*

sejenisnya sehingga mengakibatkan semua atau sebagian dari data atau program menjadi hapus sama sekali.

Berdasarkan pengertian-pengertian mengenai perbuatan "menghancurkan, merusak, membuat tidak dapat dipakai lagi dan menghilangkan", maka dapat disimpulkan bahwa makna dalam perbuatan-perbuatan tersebut terdapat kesesuaian yang pada intinya perbuatan tersebut menyebabkan fugsi dari data atau program dalam suatu jaringan menjadi berubah/berkurang.

Perbuatan penghancuran atau perusakan barang yang dilakukan *cracker* dengan kemampuan *hacking*-nya bukanlah perbuatan yang bisa dilakukan oleh semua orang awam. Kemampuan tersebut dimiliki secara khusus oleh orang-orang yang mempunyai keahlian dan kreatifitas dalam memanfaatkan sistem, program, maupun jaringan. Motif untuk kejahatan ini sangat beragam yakni misalnya motif ekonomi, politik, pribadi atau motif kesenangan semata.

3. Ketentuan yang Berkaitan dengan Perbuatan Memasuki atau Melintasi Wilayah Orang Lain

Penggunaan sarana jaringan melalui media internet di negara-negara dunia dewasa ini semakin berkembang pesat. Kehadiran internet tidak dapat dielakkan lagi dapat menunjang kerja dari komputer sehingga dapat mengolah data yang bersifat umum melalui suatu *terminal system*.

Apabila ada orang asing yang masuk ke dalam jaringan komputer tersebut tanpa ijin dari pemilik terminal ataupun penanggung jawab sistem jaringan komputer, maka perbuatan ini dikategorikan sebagai *hacking*. Kejahatan komputer jenis *hacking* –apabila ia melakukan perusakan atau gangguan- sangat berbahaya karena apabila seseorang berhasil masuk ke dalam sistem jaringan orang lain, maka implikasi hukumnya ia mungkin saja membaca dan menyalin informasi yang mungkin sangat rahasia, atau

mungkin pula menghapus atau mengubah informasi atau program-program yang tersimpan pada sistem komputer. Ada kemungkinan ia mencuri dengan memerintahkan komputer untuk mengirimkan barang kepadanya.

Perbuatan mengakses ke suatu sistem jaringan tanpa ijin tersebut dapat dikategorikan sebagai perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan tanpa haknya berjalan di atas tanah milik orang lain, sehingga pelaku dapat diancam idana berdasarkan Pasal 167 KUHP dan Pasal KUHP.

Pasal 167 KUHP berbunyi :

- (1) *Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau denda paling banyak empat ribu lima ratus rupiah;*
- (2) *Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barang siapa tidak setahu yang berhak lebih dulu bukan karen kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk;*
- (3) *Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan;*
- (4) *Pidana tersebut dalam ayat (1) dan (3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.*

Dari Pasal 167 KUHP, menurut Andi Hamzah ada beberapa hal yang menyulitkan aparat penegak hukum dalam upaya penanganan kejahatan komputer, antara lain:

- Apakah komputer dapat disamakan dengan rumah, ruangan atau pekarangan tertutup;
- Berkaitan dengan cara masuk ke rumah atau ruangan tertutup, apakah test *key* atau *password* yang digunakan oleh seseorang untuk berusaha masuk ke dalam suatu sistem jaringan dapat dikategorikan sebagai kunci palsu, perintah palsu atau pakaian palsu.

Pasal yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain adalah Pasal 551 KUHP.

Pasal 551 KUHP berbunyi:

"Barang siapa tanpa wewenang berjalan atau berkendara di atas tanah yang oleh pemiliknya dengan cara jelas di larang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah".

Berkaitan dengan pasal di atas, ada beberapa hal yang tidak sesuai lagi untuk diterapkan dalam upaya penanggulangan kejahatan *hacking*, yaitu pidana denda yang sangat ringan –dapat mengganti pidana kurungan– padahal *hacking* dapat merugikan finansial yang tidak sedikit bahkan mampu melumpuhkan kegiatan dari pemilik suatu jaringan yang berhasil dimasuki oleh pelaku dan perbuatan *hacking* ini merupakan awal dari maraknya kejahatan-kejahatan tradisional dengan sarana komputer dilakukan. Misalnya: pencurian, penipuan, penggelapan, pemalsuan dan lain-lain. Sebagai contoh: Seseorang yang dapat masuk ke suatu jaringan komputer perusahaan akan dengan mudah melakukan transaksi fiktif yang ia kehendaki atau melakukan perbuatan curang lainnya.¹⁷

D. Wacana Kebijakan Hukum Pidana akan datang.

Penanggulangan terhadap *cybercrime* dalam bentuk *hacking* perlu diimbangi dengan pembenahan dan pembangunan sistem hukum pidana secara menyeluruh, yakni meliputi pembangunan kultur, struktur dan substansi hukum pidana. Dalam hal ini kebijakan hukum pidana menduduki posisi yang strategis dalam pengembangan hukum pidana modern.

Istilah kebijakan berasal dari bahasa Inggris *policy* atau dalam bahasa Belanda *politiek* yang secara umum dapat diartikan sebagai prinsip-prinsip umum yang berfungsi untuk mengarahkan pemerintah dalam mengelolah, mengatur atau menyelesaikan urusan-urusan publik, masalah-

¹⁷ *Ibid.*

masalah masyarakat atau bidang-bidang penyusunan peraturan perundang-undangan dan pengaplikasian hukum/peraturan, dengan suatu tujuan yang mengarah pada upaya mewujudkan kesejahteraan atau kemakmuran masyarakat (warga negara).¹⁸ Oleh karena itu istilah kebijakan hukum pidana dapat pula disebut dengan istilah politik hukum pidana.

Marc Ancel menyatakan, bahwa *modern criminal science* terdiri dari 3 (tiga) komponen, yakni *criminology*, *criminal law* dan *penal policy*. Menurut pandangannya, *penal policy* 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 hanya pada pembuat undang-undang, tetapi juga pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan.¹⁹ Dengan demikian yang dimaksudkan peraturan hukum positif (*the positive rules*) adalah peraturan perundang-undangan pidana.

Dalam kaitannya dengan jenis kejahatan ini, maka kebijakan hukum pidana adalah garis kebijakan untuk menentukan:²⁰

1. Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu diubah atau diperbaharui (*in welk opzicht de bestaande straf bepalingen herzien dienen te worden*);
2. Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana (*wat gedaan kan worden om strafrechtelijk gedrad voorkomen*);
3. Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan (*hoe de opsporing, vervolging, berechting en tenuitvoerlegging van straffen dient te verlopen*).

Penanggulangan kejahatan dengan menggunakan hukum pidana merupakan bagian dari penegakan hukum (*law enforcement*), oleh Karena

¹⁸ Wisnubroto, *Op.Cit.*, hal. 10.

¹⁹ Barda Nawawi Arif, *Bunga Rampai Kebijakan Hukum Pidana* (Bandung: Citra Aditya Bakti, 2002) hal. 21.

²⁰ *Ibid*

itu kebijakan hukum pidana merupakan bagian dari penegakan hukum. Proses pembuatan undang-undang pidana bertujuan memberikan perlindungan masyarakat (*social defence*) dan mencapai kesejahteraan masyarakat (*social welfare*). Berdasarkan tujuan di atas diharapkan sistem hukum pidana yang ada dapat mengantisipasi keadaan *normlessness*²¹ untuk memenuhi rasa keadilan bagi masyarakat.

Kejahatan *hacking* sebagai sebuah kejahatan baru memberikan sebuah pemahaman terhadap keberadaan hukum pidana kita. Disatu sisi penerapannya terbentur asas legalitas, sedangkan di sisi lain kepastian hukum dan rasa keadilan wajib untuk dipenuhi. Asas legalitas (*principle of legality*) sebagai dasar pemidanaan menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan. Hal ini bertujuan untuk memberikan perlindungan hukum bagi warganegara terhadap kekuasaan tanpa batas dari pemerintah.

Kebijakan hukum pidana (tataran aplikatif) sangat dipengaruhi sistem hukum yang berlaku saat ini. Hukum pidana Indonesia yang ada saat ini dan pengembangan ke depan dipengaruhi oleh tradisi hukum *civil law*. Politik hukum yang cenderung mengarah pada tradisi *civil law* mengandung konsekuensi sebagai berikut:

1. Peraturan perundang-undangan harus dirumuskan secara teliti dan lengkap sehingga diharapkan mampu menjangkau semua permasalahan yang timbul.
2. Asas legalitas ditempatkan sebagai landasan yang bersifat fundamental dan dalam pelaksanaannya harus dijunjung tinggi tanpa kecuali.

²¹ Yakni kondisi *inability of norms to control or regulate behaviour*, vide: Romli Atmasasmita, *Teori dan Kapita Selekt Kriminologi*, Eresco, Bandung, 1992, hal. 24.

3. Operasionalisasi peraturan perundang-undangan diupayakan seoptimal mungkin untuk menangani berbagai kasus yang bervariasi dengan pendekatan penafsiran (interpretasi).

Kebijakan hukum pidana dalam penanggulangan kejahatan *hacking* dapat ditempuh dengan pembaharuan hukum pidana, pada hakekatnya adalah suatu upaya untuk melakukan re-orientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosio-politik, sosio filosofik dan sosio cultural masyarakat Indonesia yang melandasi kebijakan social, kebijakan criminal dan kebijakan penegakan hukum Indonesia.²²

Indonesia saat ini sedang melakukan langkah-langkah kebijakan harmonisasi dengan negara-negara lain, khususnya dalam lingkungan ASEAN menyangkut masalah *cybercrime*. Antisipasi masalah *cybercrime* tidak hanya melalui penyusunan RUU ITE oleh tim gabungan Depkominfo dengan perguruan tinggi, namun juga berusaha mengantisipasinya dalam penyusunan konsep KUHP baru. Kebijakan sementara ditempuh di dalam konsep KUHP baru tahun 2002 adalah sebagai berikut:

Konsep KUHP baru memperluas dan memberi kejelasan definisi tentang beberapa aspek yang secara langsung maupun tidak langsung berkaitan dengan masalah *cybercrime*.

Misalnya:

- Pengertian "barang" (Pasal 174) di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon/telekomunikasi/jasa komputer;
- Pengertian "anak kunci" (Pasal 178) di dalamnya termasuk kode rahasia, kunci komputer, kartu magnetic, signal yang telah deprogram untuk membuka sesuatu;

²² Barda Nawawi Arief, *Op.Cit.*, hal.63-64.

- Pengertian "surat" (Pasal 188) termasuk data tertulis atau tersimpan dalam disket, pita magnetic, media penyimpan komputer atau penyimpan data elektronik lainnya;
- Pengertian "ruang" (Pasal 189) termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu;
- Pengertian "masuk" (Pasal 190) termasuk mengakses komputer atau masuk ke dalam sistem komputer;
- Pengertian jaringan "telepon" (Pasal 191) termasuk jaringan komputer atau sistem komunikasi komputer.

Pengertian-pengertian ini menjelaskan bahwa konsep KUHP baru tidak hanya berupaya mengantisipasi masalah *cybercrime* maupun *computer crime* melainkan juga berupaya mengantisipasi *telecommunication crime*.²³

E. Penutup

Ada dua pilihan terhadap kebijakan hukum pidana terhadap *cybercrime* khususnya penanggulangan terhadap kejahatan *hacking*. Pertama, aturan ini cukup dimasukkan dalam konsep rumusan KUHP baru, sehingga aturan ini bersifat umum (*lex generalis*). Kedua, perlu diatur dalam undang-undang yang bersifat khusus (*lex specialist*).

Menurut hemat penulis, langkah yang paling efektif dan efisien adalah dengan tetap dicantumkannya jenis kejahatan ini dalam KUHP baru, akan tetapi sifatnya hanya secara umum, menyangkut norma-norma yang hendak diatur. Selain itu juga dibentuknya undang-undang khusus yang mengatur tentang kejahatan teknologi informasi secara menyeluruh.

²³ Teguh Arifandi, *Op.Cit.*

Efektif dengan maksud bahwa undang-undang ini diharapkan dapat menjadi *umbrella provision* dari seluruh aturan yang menyangkut kejahatan berteknologi. Efisien dalam arti bahwa konsep Rumusan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUU-KUHP) tidak perlu dijelaskan secara spesifik tentang kejahatan ini karena sudah diatur secara khusus dalam undang-undang lain.

DAFTAR PUSTAKA

Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer* (Malang: Lembaga Penerbitan Fakultas Hukum UNISMA, 2002)

Barda Nawawi Arif, *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, 1991.

-----, *Bunga Rampai Kebijakan Hukum Pidana* (Bandung: Citra Aditya Bakti, 2002)

Dewi Lestari, *Kejahatan Komputer (Cybercrime)*, http://www.lkht.net/artikel_lengkap.php?id=6, di akses tanggal 05 November 2007

Heru Sutadi, *Cybercrime, Apa Yang Bisa Diperbuat?*, <http://www.sinarharapan.co.id/berita/0304/05/opi01.html>.2003.

Teguh Arifiyadi, *Cyber Crime dan Upaya Antisipasinya Secara Yuridis(II)*, http://www.depkominfo.go.id/portal/?act=detail&mod=artikel_itjen&view=1&id=BRT061002182401, diakses tgl. 05 November 2007.

-----, *Menjerat Pelaku Cyber Crime dengan KUHP*, http://www.depkominfo.go.id/portal/?act=detail&mod=artikel_itjen&view=1&id=BRT070620115101, diakses tanggal 05 November 2007

Tubagus Ronny Rahman Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi* (Jakarta: Peradaban, 2001).

Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer* (Yogyakarta: Universitas Atmajaya, 1999).