ISSN 1412-1344

ASPEK-ASPEK HUKUM PIDANA BAGI HACKER

Azis Muhammad, SH, M.Hum [1]
Deddy Hidayat, S.Kom [2]
Surohmat [3]

ABSTRAKSI

Kemajuan teknologi informasi yang menjadi starting points dari keberadaan cyber crime, secara yuridis dapat membawa dampak pada hukum yang mengatur tentang hal tersebut. Perhatian terhadap cyber crime tersebut dikarenakan dampak dari adanya cyber crime bersifat negatif yang dapat merusak terhadap seluruh bidang kehidupan modern saat ini, oleh karena kemajuan teknologi komputer menjadi salah satu piranti atau pendukung kehidupan masyarakat. Bahkan kekhawatiran dampak negatif dari keberadaan cyber crime ini secara internasional pernah diutarakan dalam "International Information Industry Congress 2000 Millennium Conggres" di Quebec, yang menyatakan bahwa: "Cyber crime is a real growing threat to economic and social development around the world. Information technology touches every aspect of human life so can electronically enable crime." (Kejahatan dunia maya merupakan suatu pertumbuhan nyata yang mengancam pembangunan ekonomi dan sosial dunia. Teknologi informasi menyentuh setiap aspek kehidupan manusia yang secara elektronik dapat menimbulkan kejahatan.) Dalam KUHP, tindak pidana pencurian dimuat dalam Pasal 362, sedang variasinya diatur dalam Pasal 363 (pencurian dengan pemberatan), Pasal 364 (pencurian ringan), Pasal 365 (pencurian yang disertai dengan kekerasan/ancaman kekerasan, Pasal 367 (pencurian di lingkungan keluarga). Dalam hal pencurian/pembobolan sistem komputer yang dimaksudkan untuk mendapatkan uang tunai melalui transfer dapat diterapkan Pasal 363 KUHP dimana dalam pasal tersebut memperluas pengertian kunci palsu dan perintah palsu sehingga "password" atau "test-key" yang digunakan dalam pencurian tersebut termasuk di dalamnya.

1. Dosen Jurusan Teknik Informatika Perguruan Tinggi Raharja
2. Dosen Jurusan Teknik Informatika Perguruan Tinggi Raharja
3. Dosen Tetap Fakultas Hukum UMJ

PENDAHULUAN

Kemajuan di bidang ilmu pengetahuan dan teknologi mempunyai dampak positif dan negatif bagi tatanan kehidupan manusia secara umum, misalnya dengan ditemukannya suatu perangkat teknologi komputer sebagai penyimpan, pengolah dan pemroses data dan informasi yang membuat pekerjaan menjadi lebih mudah untuk dilakukan, bahkan hal ini tidak terikat pada satu komputer yang terletak pada suatu tempat atau wilayah saja melainkan dapat dihubungkan atau berhubungan dengan komputer yang berada di tempat dan/atau wilayah lain dalam suatu sistem jaringan yang mempergunakan bantuan teknologi komunikasi (satelit). Hal ini menciptakan suatu ruang dan/atau tempat yang dikenal dengan istilah Cyber Space (Dunia Maya).

Keberadaan Cyber Space menjadikan arus data dan informasi secara mudah dapat diakses (dilihat atau dikunjungi) tanpa menghiraukan batas dan/atau lintas wilayah negara. Menjadikan hubungan antar manusia, masyarakat dan bahkan negara menjadi semakin intensif dan berirama dinamis.

Namun kedinamisan yang muncul akibat kemajuan teknologi di bidang komputer yang ditunjang oleh kemajuan di bidang telekomunikasi (satelit) tersebut, yang menciptakan dunia maya bukanlah tanpa dampak negatif. Negatifitas dari keberadaan dunia maya tersebut muncul seiring dengan semakin padatnya arus lalu lintas pada dunia maya, sehingga menimbulkan permasalahan-permasalahan yang perlu mendapat perhatian dan penanganan serius dari masyarakat internasional.

Secara umum permasalahan tersebut dikategorikan sebagai suatu "Cyber Crime" (kejahatan dunia maya).

Cyber Crime sebagai suatu istilah yang dipergunakan untuk menyebut "kejahatan dunia maya" merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari masyarakat Internasional.

Perhatian terhadap *cyber crime* tersebut dikarenakan dampak dari adanya *cyber crime* bersifat negatif yang dapat merusak terhadap seluruh bidang kehidupan modern saat ini, di mana kemajuan teknologi komputer menjadi salah satu piranti atau pendukung kehidupan masyarakat. Bahkan kekhawatiran dampak negatif dari keberadaan *cyber crime* ini secara internasional pernah diutarakan dalam *"International Information Industry Congress 2000 Millennium Conggres" di Quebec,* yang menyatakan bahwa: *"Cyber crime is a real growing threat to economic and social development around the world. Information technology touches every aspect of human life so can electronically enable crime."* [1](Kejahatan dunia maya merupakan suatu pertumbuhan nyata yang mengancam

pembangunan ekonomi dan sosial dunia. Teknologi informasi menyentuh setiap aspek kehidupan manusia yang secara elektronik dapat menimbulkan kejahatan.)

Kemajuan teknologi informasi yang menjadi *starting points* dari keberadaan *cyber crime*, secara yuridis juga membawa dampak pada hukum yang mengatur tentang hal tersebut, sebagaimana dikemukakan Prof. Mr. Roeslan Saleh: *"Akibat dari masuknya produk-produk teknologi informatica dalam masyarakat ditimbulkan banyak dan berbagai pernyataan yuridis. Beberapa diantaranya terutama bersifat pragmatis. Misalnya kontrak-kontrak otomatisasi. Dalam kejadian lain, karena ketiadaan instrumen-instrumen juridis untuk memecahkan masalah-masalahnya. Hal ini terjadi misalnya dalam menangani beberapa bentuk kriminalitas komputer, dan pada masalah perlindungan terhadap privasi. Dalam kejadian lain pula keadaannya lebih kompleks lagi, oleh karena masalahnya berkaitan dengan keadaan bahwa dogmatic dan sistematika, dan kadang-kadang dasar dari stelsel hukum kita tidak memberikan ruangan untuk ditempatkannya dibawahnya itu adalah fenomena dari "masyarakat informasi".*[2]

Pembatasan dan Perumusan Masalah

Fenomena dari masyarakat informasi, sebagaimana dikemukakan oleh Prof. Mr. Roeslan Saleh tersebut di atas, pada kenyataannya tidak hanya berdampak pada ketidaksiapan beberapa masyarakat negara dalam mengantisipasi keberadaan teknologi infornasi yang mempergunakan komputer, melainkan juga memunculkan perbuatan-perbuatan yang pada dasarnya adalah sebagai penyalahgunaan komputer, yang dikategorikan sebagai *cyber crime* (kejahatan dunia maya).

Kejahatan dunia maya pada kenyataannya dapat dilakukan dalam bentuk: [3]

1. Penyusupan/Pembobolan Sistem Komputer
2. *Vandalisme* Komputer
3. *Hacking*
4. *Phreaker*
5. Penyerobotan atas Nama Domain
6. *Typosquating*
7. Pembajakan Nama Domain

Dari kesemua bentuk kejahatan tersebut pada prinsipnya merupakan perbuatan yang melibatkan adanya suatu perbuatan yang secara hukum tidak dibenarkan atau melawan hukum sehingga mengakibatkan orang atau pihak lain tidak dapat mempergunakan data dan informasi yang dimuat dalam suatu komputer dan jaringannya sesuai dengan peruntukkannya sebagaimana mestinya.

Pada tulisan ini penulis membatasi perbuatan, yang terkategori sebagai kejahatan dunia maya sebagaimana tersebut diatas, adalah *hacking.*

Hacking adalah suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa ijin atau melawan hukum, dari pemilik sah jaringan komputer tersebut. Jadi jika ada seseorang asing hendak masuk ke sistem jaringan komputer tanpa ijin atau sepengetahuan dari pemilik terminal komputer terdahulu atau pemilik/penanggungjawab sistem jaringan komputer, maka perbuatan itu dinamakan *hacking.* Seseorang yang melakukan hacking disebut dengan istilah ***"Hacker"***.

Untuk itu penulis akan membatasi permasalahan secara khusus yang berkaitan dengan perbuatan-perbuatan seorang hacker dilihat dari sudut pandang hukum pidana.

Dengan demikian permasalahan dalam paper ini dirumuskan sebagai berikut:

1. Bagaimana perbuatan *hacker* dalam dunia maya *(cyber space)?*
2. Apakah perbuatan *hacker* sebagaimana disebut pada point 1 di atas mempunyai aspek-aspek pidana, dan ketentuan-ketentuan mana saja dalam Kitab Undang-Undang Hukum Pidana yang dapat dipergunakan dan diterapkan untuk menanggulangi dan mencegah perbuatan para *hacker* tersebut ?

Hacker dan Cyber Space

Segala sesuatu yang berhubungan dengan pelaku kejahatan dunia maya, yang dilakukan oleh sekelompok orang ataupun perorangan disebut *Hacker,* walaupun tidak semua *hacker* melakukan kejahatan (ada pula *hacker* yang bekerja untuk pemerintah atau suatu perusahaan).

Kelompok *hacker,* mungkin merupakan bagian masyarakat bawah tanah komputer yang paling legendaris. Definisi *hacker* telah berkembang dari masa ke masa, namun *hacker* pada masa kini dapat didefinisikan sebagai "orang-orang yang gemar mempelajari seluk beluk sistem komputer dan bereksperimen dengannya." [4]

Eric Raymond, Penyusun *The New Hacker's Dictionary,* menuliskan 5 (lima) ciri *hacker,* yaitu:

1. Gemar mempelajari detail sistem komputer atau bahasa pemrograman.
2. Gemar melakukan praktek pemrograman daripada hanya menteorikannya.
3. Mampu menghargai hasil *hacking* orang lain
4. Mempelajari pemrograman dengan cepat.
5. Mahir dalam sistem operasi/bahasa pemrograman tertentu.

Penggolongan Hacker

Di dalam dunia maya, *hacker* diketahui terdapat dua golongan, sebagaimana dijelaskan oleh Suhemi dalam bukunya Kejahatan Komputer, yaitu:

1. *True Hacker* di sisi terang

True hacker ini seolah-olah sudah merupakan sosok lain dari *hacker,* sebenarnya *true hacker* berbeda dengan *hacker.* Jika sistem komputer anda kedatangan seorang *true hacker* maka dapat dikatakan bahwa komputer anda tidak dalam keadaan bahaya bahkan dapat dikatakan beruntung. *True hacker* tidak akan merusak ataupun menghapus sistem komputer yang dikunjunginya. Berbeda dengan *hacker,* maka biasanya akan melakukan hal-hal yang merugikan sistem komputer yang diakses, seperti mengirim program virus, menghapus data-data penting, mengubah sistem operasi dan bahkan berusaha menghancurkan dan menghentikan jalannya komputer.

True hacker atau *hacker* sejati bukanlah kelompok kriminal perusak jaringan seperti kebanyakan anggapan orang. Namun memang harus diakui bahwa dari waktu kewaktu terdapat cukup banyak *hacker* yang menyalahgunakan kemampuan dan pengetahuannya untuk hal-hal yang bersifat negatif bahkan *destruktif,* melakukan berbagai kejahatan atau berbuat usil dengan mengacaukan dan merusak *file* orang.

2. *Hacker* di sisi gelap

Hacker ini mempunyai motif dan tujuan yang berbeda-beda antara satu dengan yang lainnya, diantaranya:

a. hacker yang bermaksud mencuri informasi dan memanipulasi data
b. hacker yang hanya ingin mempelajari sistem komputer
c. hacker yang mempunyai hobi menghancurkan sistem

Para *hacker* ini biasanya tertarik pada komputer-komputer besar yang biasanya dimiliki oleh instansi pemerintah dan perusahaan besar.

Menurut Gede Artha A.P., *hacker* disisi gelap ini disebut sebagai *hacker* jahat. Para *hacker* tipe ini, menyalahgunakan kemampuan mereka untuk melakukan kejahatan komputer serius, mulai dari pencurian nomor kartu kredit hingga perngrusakan jaringan atau perusahaan penyedia jasa internet.

Umumnya *hacker* ini tidak memulai karir hacking mereka dengan motivasi kriminal. Mereka biasanya memulai karir *hacking* mereka dengan rasa ingin tahu, namun seiring dengan waktu, mereka mulai berpikir untuk menyalahgunakan apa yang mereka pelajari

di masa awal karir *hacking* mereka. Namun tentu saja kejahatan mereka tidak dapat ditolerir dan perlu diperhatikan juga bahwa *hacker* yang tergolong kriminal menurut media dan kepolisian, belum tentu dikategorikan sebagai *hacker* jahat oleh dunia bawah komputer. Semua ini kembali pada kode etik *hacker.*

Para *hacker* sejati selalu mempunyai dan memegang kode etik mereka sebagai *hacker.* Kode etik para *hacker* ini muncul dan berkembang sejak *hacker* MIT pada tahun 1960-an, dan kode etik pertama tercatat dalam buku: *Hackers: Heroes of the Computer Revolution*, karya Stephen Levy.

Meski telah beberapa kali mengalami perubahan dan perkembangan, namun para *hacker* sejati setuju bahwa pada prinsipnya mereka "tidak merusak".

Sedangkan prinsip-prinsip dasar lainnya adalah sebagai berikut:

a. Tidak mengubah file apapun, kecuali dalam upaya menghilangkan jejak.
b. Para *hacker* sejati tidak berusaha agar kehadirannya diketahui atau disadari oleh pemilik sistem yang dimasukinya. Untuk itu mereka tidak akan berbuat macam-macam dalam sistem yang mereka masuki.
c. Tidak mengambil uang
d. Tidak mempercayai penguasa
e. Komputer dapat membuat hidup menjadi lebih baik
f. Kebebasan komunikasi dengan rekan-rekan
g. Berusaha melampaui batasan yang ada. *Hacker* yang paling top tidak perlu komputer super canggih dengan peralatan mahal. *Hacker* sejati sering hanya dengan mempergunakan komputer sederhana mampu mengadakan perubahan agar komputer mereka berada di atas kemampuan aslinya.
h. Tidak ada kriteria palsu, para *hacker* sejati menilai *hacker* lain murni berdasarkan keahlian. Usia, jenis kelamin, suku bangsa, agama dan lain-lain semacam itu tidak menjadi pertimbangan dalam menentukan posisi seorang *hacker* di mata *hacker* lain. *Anonimitas* yang ditawarkan oleh jaringan komputer amat mendukung cara pandang yang demikian.
i. Menghargai *privasi,* seorang *hacker* tidak mengganggu *privasi* orang lain. Penyadapan *e-mail* maupun pembicaraan pribadi juga tidak dibenarkan.
j. Kebebasan informasi, *hacker* sejati percaya bahwa informasi dan pengetahuan adalah hak tiap orang dan tidak boleh dimonopoli oleh pihak tertentu. Lebih jauh mereka berpendapat bahwa akses tersebut harus total, dan mereka berusaha menghilangkan penghalang antara manusia dengan teknologi.

HASIL DAN PEMBAHASAN

Dari sudut pandang Hukum Pidana, perbuatan seorang *Hacher* dapat diuraikan sebagai berikut :

A. Aspek-Aspek Pidana dari Perbuatan Hacker

Sebagaimana telah diuraikan pada pembahasan di atas, bahwa *hacking* adalah suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa ijin atau melawan hukum, dari pemilik sah jaringan komputer tersebut. Jadi jika ada seseorang asing hendak masuk ke sistem jaringan komputer tanpa ijin atau sepengetahuan dari pemilik terminal komputer terdahulu atau pemilik/ penanggungjawab sistem jaringan komputer, maka perbuatan itu dinamakan *hacking.*

Seseorang yang melakukan *hacking* disebut pula dengan istilah ***"Hacker"***. Dengan demikian perbuatan seorang *hacker* yang jahat mempunyai aspek-aspek pidana apabila perbuatan itu adalah:

1. Perbuatan memasuki atau melintasi wilayah orang lain tanpa hak
2. Perbuatan Pencurian
3. Perbuatan Penghancuran atau Perusakan Barang.

Penyalahgunaan komputer termasuk di dalamnya kejahatan dunia maya bukan merupakan "delik-delik khusus" yang berdiri sendiri sehingga ketentuan-ketentuan hukum positif yang ada dapat diterapkan terhadapnya. Konsep tersebut nampaknya sederhana namun pada kenyataannya tidaklah demikian. Hal ini disebabkan karena karakteristik penyalahgunaan komputer bersifat khas, sehingga tidak mudah untuk menafsirkan rumusan ketentuan perundang-undangan hukum pidana yang ada untuk diterapkan terhadap bentuk-bentuk penyalahgunaan komputer tertentu secara tepat.

B. Tinjauan Pasal-Pasal dalam KUHP yang Berkaitan dengan Hacker

Dengan asumsi bahwa perbuatan yang dilakukan oleh para *hacker* (yang jahat) merupakan delik umum yang dilakukan dengan sarana komputer beserta sarana penunjangnya, maka rumusan pasal-pasal yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP) dapat dipergunakan dan diterapkan untuk menanggulangi kejahatan para *hacker.*

Ketentuan-ketentuan dimaksud adalah sebagai berikut:

1. *Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain tanpa hak.*

Hal ini diatur dalam Pasal 167 dan Pasal 551 KUHP.

Pasal 167 KUHP menyatakan bahwa:

(1) Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain 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 barangsiapa tidak setahu yang berhak lebih dahulu serta bukan karena kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk.

(3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, dipidana menjadi paling lama satu tahun empat bulan.

(4) Pidana tersebut dalam ayat (1) dan (3) dapat ditambah sepertiga, jika yang melakukan kegiatan dua orang atau lebih dengan bersekutu.

Pasal 551 KUHP menyatakan:

"Barangsiapa tanpa wenang, berjalan atau berkendaraan di atas tanah yang oleh pemiliknya, dengan cara yang jelas dilarang memasukinya di ancam dengan denda paling banyak dua ratus dua puluh lima rupiah."

Dalam rumusan pasal-pasal tersebut nampak bahwa wilayah yang tidak boleh dimasuki atau dilalui tanpa hak tersebut merupakan wilayah fisik (baik rumah, ruangan atau pekarangan tertutup) sehingga sulit untuk diterapkan pada perbuatan tanpa hak memasuki sistem komputerr yang dianggap sebagai wilayah *"non fisik".*

Perkembangan teknologi komputer yang digabungkan dengan teknologi komunikasi telah memunculkan apa yang disebut dengan Sistem Jaringan Komputer, dikenal dengan istilah LAN *(Local Area Network)* dan/atau WAN *(Wide Area Network).* Pemakaian LAN dan/atau WAN tersebut bersifat eksklusif, dalam arti tidak semua orang dapat "memasukinya" tanpa ijin atau tanpa menjadi peserta jaringan komputer tersebut.

Jikalau terjadi pelanggaran terhadap *eksklusifitas* jaringan komputer ini, dimana telah terjadi perbuatan menyambung terminal komputer baru pada suatu jaringan komputer, dan pemilik jaringan telah mengingatkan agar si pelaku segera "keluar" dari sistem jaringan yang dimasukinya secara *illegal,* namun tidak mengindahkan (dikenal dengan istilah *Hacking*), maka terhadap *hacker* tersebut dapat diterapkan Pasal 167 dan Pasal 155 KUHP.

Penerapan kedua pasal tersebut dapat diuraikan sebagai berikut:

Dalam hal ini sistem jaringan komputer ditafsirkan sebagai lingkungan atau wilayah sebagaimana halnya dengan ruangan atau pekarangan, namun demikian wilayah dalam jaringan komputer bersifat non fisik karena tidak dapat dilihat dengan mata. Oleh sebab itu perlu dilakukan penafsiran *ekstensif* untuk memperluas pengertian "memasuki rumah, ruangan atau pekarangan secara melawan hukum" sebagai "memasuki sistem jaringan komputer secara melawan hukum", dan untuk memperluas pengertian kendaraan dalam Pasal 551 KUHP sehingga komputer beserta sarana penunjangnya termasuk di dalamnya dan memperluas pengertian kunci palsu dalam Pasal 167 ayat (2) KUHP sehingga kunci *sinyal elektronis* seperti *test-key* dan *password* termasuk di dalamnya.

2. *Ketentuan-Ketentuan yang berkaitan dengan Perbuatan Pencurian*

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

Pasal 362 KUHP menyatakan bahwa: "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 sembilan ratus rupiah". Pasal 362 KUHP tersebut dapat diterapkan untuk perbuatan yang berkaitan dengan pencurian data atau program komputer.

Pengertian "mengambil" dalam pasal tersebut diperluaskan sebagai "mengcopy" atau "merekam" dan pengertian barang atau benda dalam pasal tersebut diperluas sedemikian rupa sehingga data atau program komputer yang terdapat dalam media komputer termasuk di dalamnya.

Dalam hal pencurian/pembobolan sistem komputer yang dimaksudkan untuk mendapatkan uang tunai melalui transfer dapat diterapkan Pasal 363 KUHP dimana dalam pasal tersebut memperluas pengertian kunci palsu dan perintah palsu sehingga *"password"* atau *"test-key"* yang digunakan dalam pencurian tersebut termasuk di dalamnya.

3. *Ketentuan Yang Berkaitan Dengan Perbuatan Penghancuran atau Perusakan Barang.*

Pengertian mengenai penghancuran atau perusakan barang diatur dalam Pasal 406 KUHP, sedangkan variasi diatur dalam Pasal 407 sampai Pasal 412 KUHP.

Pasal 406 KUHP menyatakan Bahwa:

(1) Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tidak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak empat ribu lima ratus rupiah.

(2) Dijatuhkan pidana yang sama terhadap orang, yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tidak dapat digunakan atau menghilangkan hewan, yang seluruhnya atau sebagian adalah kepunyaan orang lain.

(3) Beberapa pengertian dalam Pasal 406 ayat (1) KUHP tersebut di atas dapat dijelaskan sebagai berikut:

a. Pengertian "menghancurkan" Menghancurkan (membinasakan) dimaksudkan sebagai merusak sama sekali, misalnya membanting gelas, piring sehingga berkeping-keping.
b. Pengertian "merusakkan" Merusakkan dimaksudkan sebagai memperlakukan suatu barang sedemikian rupa namun kurang daripada membinasakan.
c. Pengertian "membikin (membuat) tidak dapat dipakai lagi"Di sini tindakan itu harus sedemikian rupa, sehingga barang itu tidak dapat dipakai lagi.
d. Pengertian "menghilangkan" Yang dimaksud dengan menghiangkan adalah membuat sehingga barang itu tidak ada lagi, misalnya dibakar sampai habis.

Sedangkan pengertian "menghancurkan, merusakkan membuat tidak dapat dipakai lagi dan menghilangkan sesuatu barang" dalam penyalahgunaan komputer *(cyber crime)* dapat dijelaskan sebagai berikut: [5]

a. Yang dimaksud dengan tindakan "menghancurkan" pada kasus penyalahgunaan komputer adalah suatu perbuatan menghancurkan disket dan sejenisnya yang berisikan data atau program komputer sehingga mengakibatkan disket atau sejenisnya beserta data atau program di dalamnya tidak dapat dimanfaatkan lagi.
b. Yang dimaksud dengan tindakan "merusak" pada kasus penyalahgunaan komputer adalah suatu perbuatan merusak isi disket atau media penyimpanannya.
c. Yang dimaksud dengan "membuat tidak dapat dipakai lagi" (membuat tidak berguna) pada kasus penyalahgunaan komputer adalah suatu perbuatan yang dilakukan sedemikain rupa sehingga data atau program komputer yang seharusnya dapat dimanfaatkan sesuai dengan fungsinya menjadi tidak dapat dimanfaatkan. Hal ini disebabkan karena data atau program tersebut telah dirubah seluruhnya atau pada beberapa bagiannya, atau dirusak seluruhnya atau beberapa bagiannya, atau dihapus

seluruhnya atau beberapa bagiannya, maka maksud penggunaan data atau program komputer tersebut terhalangi (tidak dapat dipakai lagi sesuai dengan fungsinya), dan tidak dapat diperbaiki lagi.

d. Yang dimaksud dengan "menghilangkan" pada kasus kejahatan komputer adalah suatu perbuatan menghilangkan, menghapus data atau program yang tersimpan di dalam disket dan media penyimpanan sejenis lainnya sehingga mengakibatkan semua data atau program yang disimpan itu menjadikan disket dan sejenisnya itu menjadi kosong dan tidak dapat dimanfaatkan lagi.

Berdasarkan penjelasan tersebut di atas, nampak adanya kesesuaian antara pengertian peusakan barang dengan pengertian perusakan data atau program komputer yang dalam hal ini data atau prigram komputer menjadi terganggu. [6]

Penerapan Pasal 406 ayat (1) KUHP dapat diterapkan pada perbuatan hacking, dimana perbuatan tersebut dilakukan untuk melakukan penghancuran, perusakan dan penghilangan data atau program komputer yang di "kunjungi" nya.

KESIMPULAN

Dari uraian tersebut di atas, penulis berkesimpulan sebagai berikut:

1. Perbuatan yang dilakukan oleh seseorang untuk masuk dan/atau mengunjungi suatu sistem jaringan komputer tanpa ijin atau sepengetahuan dari pemilik dan/ atau penanggungjawab dari sistem jaringan yang bersangkutan adalah perbuatan melawan hukum.
2. Perbuatan melawan hukum sebagaimana tersebut pada angka 1 di atas dapat mengakibatkan dipidananya seorang *hacker* berdasarkan pada ketentuan-ketentuan yang terdapat dalam hukum pidana di Indonesia.
3. Meskipun KUHP tidak secara tegas mengatur perbuatan melawan hukum yang dilakukan oleh seorang *hacker* tetapi apabila dilakukan penafsiran secara *ekstensif* maka ketentuan-ketentuan yang terdapat dalam Pasal 167, 551, 362, 406 dapat dipergunakan untuk menghukum seorang *hacker* yang jahat.

Oleh karena itu dalam rangka menegakan hukum pidana di Indonesia yang berkaitan dengan pencegahan dan penanggulangan perbuatan-perbuatan seorang *hacker* yang jahat, maka penulis menyarankan dan merekomendasikan bahwa perlu dilakukan hal sebagai berikut:

1. Pembaharuan hukum terhadap ketentuan-ketentuan yang berkenaan dengan penanggulangan kejahatan dunia maya pada umumnya dan pencegahan dan penanggulangan perbuatan *hacker* pada khususnya. Hal ini dapat dilakukan dengan

melakukan perubahan atas KUHP atau membuat dan menerbitkan serta memberlakukan peraturan perundang-undangan yang berkaitan dengan kejahatan dunia maya termasuk kejahatan seorang *hacker.*

2. Perlu diadakan upaya pemerintah dan masyarakat untuk memberikan pengetahuan dan pemahaman kepada pengguna komputer agar tidak melakukan perbuatan-perbuatan yang dilarang dan/atau terlarang dalam penggunaan komputer pada dunia maya. Hal ini dapat dilakukan dengan kegiatan-kegiatan penyuluhan dan gerakan kesadaran hukum masyarakat pengguna dan penghuni dunia maya. Inilah yang sangat *krusial* dan penting dilakukan, karena menurut penulis sebagus dan secanggih apapun hukum dan teknologi yang dibuat dan dikembangkan tidak akan mampu untuk menanggulangi kejahatan pada dunia maya tanpa diiringi dengan kesadaran pribadi pengguna dan penghuni dunia maya yang dilandasi nilai-nilai moral *religius* dan etika kemanusiaan.

DAFTAR PUSTAKA

1. Al Wisnobroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*: Yogyakarta: Universitas Atmajaya Yogyakarta, 1999
2. Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika, 1987
3. Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan,* Bandung:PT.Citra Aditya Bakti,2001
4. Chandra Purnama, *Penanggulangan Kejahatan Dunia Maya (Cyber Crime) Melalui Internet (Skripsi S.1),* Jakarta: Fakultas Hukum Universitas Muhammadiyah Jakarta, 2002
5. Gede Artha Azriadi Prana, *Hacker Sisi Lain Legenda Komputer:* Jakarta:Medikom Pustaka Mandiri, 2001
6. Roeslan Saleh, Prof.Mr., *Hukum Informatika,* Jakarta: Fakultas Hukum Universitas Muhammadiyah Jakarta,1995.