BAB II

ASPEK HUKUM TENTANG SITUS INTERNET DAN TINDAK PIDANA PERUSAKAN SITUS

A. Teori-Teori Mengenai Situs Internet

Internet adalah jaringan informasi komputer yang berkembang sangat pesat dan pada saat ini dapat dikatakan sebagai jaringan informasi terbesar di dunia, sehingga sudah seharusnya para profesional mengenal manfaat apa yang dapat diperoleh melalui jaringan ini.

Secara harfiah, internet (kependekan dari *interconnected-networking*) ialah rangkaian komputer yang terhubung dalam beberapa rangkaian. Internet (huruf 'I' besar) ialah sistem komputer umum, yang berhubung secara global dan menggunakan *TCP/IP* sebagai protokol pertukaran paket (*packet switching communication protocol*). Rangkaian internet yang terbesar dinamakan *Internet*. Cara menghubungkan rangkaian dengan kaedah ini dinamakan *internetworking*.[1]

Internet dapat diartikan sebagai gabungan dari jaringan-jaringan komputer dalam skala luas dan besar yang mana masing-masing komputer dapat saling berkomunikasi satu dengan yang lainnya menggunakan sebuah bahasa jaringan, sedangkan secara kata per kata internet berarti jaringan antara atau penghubung. Internet menghubungkan berbagai jaringan yang tidak saling bergantung pada satu sama lain sedemikian

[1] *http://id.wikipedia.org/ wiki/ Internet # Internet_pada_saat_ini*, 15 Februari 2010, Pkl. 23:13:34

rupa, sehingga mereka dapat berkomunikasi. Sistem apa yang digunakan pada masing-masing jaringan tidak menjadi masalah.

Internet mengatasi perbedaan berbagai sistem operasi dengan menggunakan bahasa yang sama oleh semua jaringan dalam pengiriman data. Pada dasarnya inilah yang menyebabkan besarnya dimensi Internet. Dengan demikian, Internet ialah tiada lain sebagai jaringannya jaringan, dengan menciptakan kemungkinan komunikasi antar jaringan di seluruh dunia tanpa bergantung kepada jenis komputernya.

Selain itu, internet yang merupakan hubungan antar berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya yang mana hubungan tersebut memanfaatkan kemajuan media komunikasi (telepon dan satelit).

Sebuah *situs web* sendiri adalah sebutan bagi sekelompok halaman *web* (*webpage*), yang umumnya merupakan bagian dari suatu nama *domain* (*domain name*) atau *subdomain* di *World Wide Web* (*WWW*) di Internet. *WWW* terdiri dari seluruh *situs web* yang tersedia kepada publik. Halaman-halaman sebuah *situs web* diakses dari sebuah *URL* yang menjadi "akar" (*root*), yang disebut *homepage* (halaman induk; sering diterjemahkan menjadi "beranda", "halaman muka"), dan biasanya disimpan dalam *server* yang sama. Tidak semua *situs web* dapat diakses dengan gratis. Beberapa *situs web* memerlukan pembayaran agar dapat menjadi pelanggan, misalnya *situs-situs* yang menampilkan pornografi, *situs-situs* berita, layanan surat elektronik (*e-mail*), dan lain-lain.[2] Oleh karena itu, *situs* pemerintah adalah sekelompok halaman *web* milik

[2] *http://id.wikipedia.org/wiki/Situs_web*, 8 Februari 2010, Pkl. 22:12:45

pemerintah, yang merupakan bagian dari suatu nama *domain* atau *subdomain* di *World Wide Web* di Internet.

Secara terminologi, *website* adalah kumpulan dari halaman-halaman *situs*, yang biasanya terangkum dalam sebuah *domain* atau *subdomain*, yang tempatnya berada di dalam *World Wide Web* (*WWW*) di Internet. Sebuah halaman *web* adalah dokumen yang ditulis dalam format *HTML* (*Hyper Text Markup Language*), yang hampir selalu bisa diakses melalui *HTTP*, yaitu protokol yang menyampaikan informasi dari *server website* untuk ditampilkan kepada para pemakai melalui *web browser*. Semua publikasi dari *website-website* tersebut dapat membentuk sebuah jaringan informasi yang sangat besar.

Halaman-halaman dari *website* akan bisa diakses melalui sebuah *URL* yang biasa disebut *Homepage*. *URL* ini mengatur halaman-halaman *situs* untuk menjadi sebuah hirarki, meskipun, *hyperlink-hyperlink* yang ada di halaman tersebut mengatur para pembaca dan memberitahu mereka sususan keseluruhan dan bagaimana arus informasi ini berjalan.

Beberapa *website* membutuhkan subskripsi (data masukan) agar para *user* bisa mengakses sebagian atau keseluruhan isi *website* tersebut. Contohnya, ada beberapa *situs-situs* bisnis, *situs-situs e-mail* gratisan, yang membutuhkan subkripsi agar kita dapat mengakses *situs* tersebut.

Hacker atau Peretas itu sendiri adalah orang yang mempelajari, menganalisa, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi sistem yang terdapat di sebuah perangkat seperti perangkat lunak komputer dan perangkat keras

komputer seperti program komputer, administrasi dan hal-hal lainnya, terutama keamanan.[3]

Adapula istilah-istilah yang dikenal dalam dunia *hacker*, antara lain:[4]

1. *White hat hacker* adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada peretas yang secara etis menunjukkan suatu kelemahan dalam sebuah sistem komputer. *White hat* secara umum lebih memfokuskan aksinya kepada bagaimana melindungi sebuah sistem, yang bertentangan dengan *black hat* yang lebih memfokuskan aksinya kepada bagaimana menerobos sistem tersebut. Topi putih atau peretas putih adalah pahlawan atau orang baik, terutama dalam bidang komputer, yang mana disebut etika *hacker* atau penetrasi penguji yang berfokus pada mengamankan dan melindungi *IT* sistem.

   White hat hacker atau peretas suci, juga dikenal sebagai "*good hacker*," yaitu ahli keamanan komputer, yang berspesialisasi dalam penetrasi pengujian, dan pengujian metodologi lain, untuk memastikan bahwa perusahaan sistem informasi yang aman. Pakar keamanan ini dapat memanfaatkan berbagai metode untuk melaksanakan uji coba mereka, termasuk rekayasa sosial taktik, penggunaan alat-alat *hacking*, dan upaya untuk menghindari keamanan untuk mendapatkan masuk ke daerah aman.

[3] *http://id.wikipedia.org/wiki/Hacker*, 8 Februari 2010, Pkl. 23:15:41
[4] *http://id.wikipedia.org/wiki/Situs_web*, 8 Februari 2010, Pkl. 22:12:45

2. *Black hat hacker* adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada para peretas yang menerobos keamanan sistem komputer tanpa izin, umumnya dengan maksud untuk mengakses komputer-komputer yang terkoneksi ke jaringan tersebut.

Cybercrime atau kejahatan internet dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Teknologi, *internet* selain memberi manfaat juga menimbulkan dampak negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Pada jaringan komputer seperti *internet*, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas dalam *internet* atau *cybercrime* pada dasarnya adalah suatu tindak pidana yang berkaitan dengan *cyberspace,* baik yang menyerang fasilitas umum di dalam *cyberspace* ataupun kepemilikan pribadi.

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.[5]

Kejahatan dalam bidang teknologi informasi secara umum dapat dikategorikan menjadi dua kelompok. Pertama, kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantunya. Pada kejahatan ini terjadi peningkatan modus operandinya dari semula menggunakan

[5] J.E. Sahetapy dikutip dalam Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer*, Lembaga Penerbitan Fakultas Hukum UNISMA, Malang, 2002, hlm. 21

peralatan biasa, sekarang telah memanfaatkan teknologi informasi. Dampak kejahatan biasa yang telah menggunakan teknologi informasi ternyata cukup serius, terutama jika dilihat dari jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pencurian uang dengan cara pembobolan bank atau pembelian barang menggunakan kartu kredit curian melalui media internet dapat menimbulkan korban di wilayah hukum negara lain. Kedua, kejahatan yang muncul setelah adanya internet, yang mana 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.

Jenis-jenis kejahatan dalam *internet* terbagi dalam berbagai versi. Salah satu versi menyebutkan bahwa kejahatan ini terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasan pribadi. Jenis kedua adalah kejahatan dengan motif politik, ekonomi atau kriminal yang berpotensi menimbulkan kerugian bahkan perang informasi. Versi lain membagi *cybercrime* menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan.[6]

[6] *http://blog.poltek-malang.ac.id/ media/ 3/ 20090528-3.% 20 RUANG % 20 LINGKUP % 20 KEJAHATAN % 20 SISTEM%20INFORMASI.doc*, 7 Februari 2010, Pkl. 22:22:25

Adapun ruang lingkup kejahatan komputer terbagi menjadi empat bagian, diantaranya:[7]

1. Komputer sebagai instrumen untuk melakukan kejahatan tradisional, seperti digunakan untuk melakukan pencurian, penipuan, dan pemalsuan melalui internet, di samping kejahatan lainnya seperti pornografi terhadap anak-anak, prostitusi online, dan lain-lain.
2. Komputer dan perangkatnya sebagai objek penyalahgunaan, yang mana data-data dalam komputer yang menjadi objek kejahatan dapat saja diubah, dimodifikasi, dihapus, atau diduplikasi secara tidak sah.
3. Penyalahgunaan yang berkaitan dengan komputer atau data, yang dimaksud dengan penyalahgunaan disini pada saat komputer dan data-data yang terdapat dalam komputer digunakan secara ilegal atau tidak sah.
4. *Unauthorized acquisition*, *disclosure or use of information and data*, yang berkaitan dengan masalah penyalahgunaan hak akses dengan cara-cara yang ilegal.

Selain ruang lingkup, dikenal pula tipe-tipe *cybercrim*e, yaitu:[8]

1. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer;
2. *Hacking,* yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal;

---

[7] *http://mohtar.staff.uns.ac.id/files/2009/03/cybercrime.pdf*, 7 Februari 2010, Pkl. 22:25:21

[8] *http://kepriprov.go.id/ id /index. php? Option = com_content & task = view & id = 110 & Itemid = 97*, 7 Februari 2010, Pkl. 22:35:12

3. *The 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 pribadi atau orang lain;
4. *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu;
5. *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah *input* data atau *output* data;
6. *To frustate data communication* atau penyia-nyiaan data computer;
7. *Software piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI.

Berdasarkan ketujuh tipe c*ybercrime* tersebut, nampak bahwa inti *cybercrime* adalah penyerangan di *content, computer system* dan *communication system* milik orang lain atau umum di dalam *cyberspace*.

Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas wilayah dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan, dapat dipastikan dengan sifat global *internet*, semua negara yang melakukan kegiatan *internet* hampir pasti akan terkena imbas perkembangan *cybercrime* ini.

Pengertian Hacking itu sendiri adalah memasuki, memodifikasi atau merusak homepage (hacking). Istilah *hacker* biasa dipakai untuk menyebut seseorang yang memiliki keahlian khusus di bidang komputer. Seorang *hacker* mampu berpikir dan bekerja dengan efektif dan efisien dan sering kali menyelesaikan permasalahan yang dihadapi dengan metode yang "*out of the box"*, di luar pemikiran yang biasa digunakan orang.

Pengertian *Hacker* dan *Cracker* itu sendiri adalah sebagai berikut:[9]

1. ***Hacker*** adalah sebutan untuk orang atau sekelompok orang yang memberikan sumbangan bermanfaat untuk dunia jaringan dan sistem operasi, membuat program bantuan untuk dunia jaringan dan komputer. Hacker juga dapat dikategorikan sebagai perkerjaan yang dilakukan untuk mencari kelemahan suatu sistem dan memberikan ide atau pendapat yang dapat memperbaiki kelemahan sistem yang di temukannya.
2. ***Cracker*** adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang dimasuki seperti: pencurian data, penghapusan, dan banyak yang lainnya.

Hacker juga mempunyai tingkatan-tingkatan, tiap tingkatan dibedakan dengan kemampuan dan ilmu yang dimiliki *hacker*, antara lain:[10]

1. *Elite,* ciri-cirinya adalah mengerti sistem operasi luar dan dalam, sanggup mengkonfigurasi dan menyambungkan jaringan secara global, melakukan pemrograman setiap harinya, efisien dan trampil, menggunakan pengetahuannya dengan tepat,

[9] *http://fleahlit.web.id/pengertian-hacker-dan-cracker/,* 7 Februari 2010, Pkl. 23:20:12

[10] *http://id.wikipedia.org/wiki/Situs_web, Loc. Cit*

tidak menghancurkan data-data, dan selalu mengikuti peraturan yang ada. Tingkat *Elite* ini sering disebut sebagai ‘suhu’.

2. *Semi Elite*, ciri-cirinya adalah lebih muda dari golongan *elite*, mempunyai kemampuan dan pengetahuan luas tentang komputer, mengerti tentang sistem operasi (termasuk lubangnya), kemampuan programnya cukup untuk mengubah program *eksploit*.
3. *Developed Kiddie*, ciri-cirinya adalah umurnya masih muda dan masih sekolah, mereka membaca tentang metoda *hacking* dan caranya di berbagai kesempatan, mencoba berbagai sistem sampai akhirnya berhasil & memproklamirkan kemenangan ke lainnya, umumnya masih menggunakan *Grafik User Interface* (*GUI*) dan baru belajar basic dari *UNIX* tanpa mampu menemukan lubang kelemahan baru di sistem operasi.
4. *Script Kiddie*, ciri-cirinya adalah seperti *developed kiddie* dan juga seperti *Lamers*, mereka hanya mempunyai pengetahuan teknis *networking* yang sangat minimal, tidak lepas dari *GUI, hacking* dilakukan menggunakan *trojan* untuk menakuti dan menyusahkan hidup sebagian pengguna internet.
5. *Lammer,* ciri-cirinya adalah tidak mempunyai pengalaman dan pengetahuan tapi ingin menjadi *hacker* sehingga *lamer* sering disebut sebagai “*wanna-be*” *hacker*, penggunaan komputer mereka terutama untuk main *game*, *IRC*, tukar menukar *software private*, mencuri kartu kredit, melakukan *hacking* dengan menggunakan *software trojan*, *nuke* dan *DoS*, suka

menyombongkan diri melalui *IRC channel*, dan sebagainya. Karena banyak kekurangannya untuk mencapai *elite*, dalam perkembangannya mereka hanya akan sampai level *developed kiddie* atau *script kiddie* saja.

Sedangkan Cracker tidak mempunyai hirarki khusus karena sifatnya hanya membongkar dan merusak.

Komunitas hacker di Indonesia kebanyakan terdiri dari siswa dan mahasiswa yang memiliki ketertarikan di bidang keamanan jaringan komputer. Kelompok ini memiliki banyak waktu luang untuk mencari informasi mengenai bagaimana cara-cara yang bisa dipakai untuk memanfaatkan kelemahan yang ada pada jaringan komputer milik orang lain.

Informasi seperti ini banyak tersedia di internet. Kadang-kadang cara yang biasa dipakai untuk masuk ini sudah disediakan dalam bentuk *script* yang tinggal diambil dan dijalankan, layaknya menjalankan aplikasi komputer biasa. Orang-orang yang masuk ke dalam kelompok ini sering disebut sebagai *script kiddies* (sebuah istilah yang menggambarkan bahwa anak kecil pun bisa melakukannya). Apa yang Orang-orang butuhkan hanyalah informasi awal mengenai produk perangkat lunak apa dan versi berapa yang dipakai di *server* yang akan mereka rusak.

B. Ketentuan Hukum Mengenai Perusakan Situs

Indonesia, di antara jenis kejahahatan internet yang populer dan sering terjadi adalah *hacking* yang bahkan mengalahkan *carding* dimana Indonesia sempat menjadi terkenal oleh karena tingkat kasus *carding* yang

sangat tinggi. Tetapi tidak semua orang dapat melakukan *hacking*, karena *hacker* biasanya mempunyai pengetahuan dan keahlian khusus di bidang komputer dan internet, seperti penguasaan ilmu komputer, *programming* dan akses internet. Disamping itu, pelaku juga harus mempunyai akses, baik dalam kepemilikan maupun infrastruktur *TI*.

Hacking dapat dilakukan dari tempat terpisah dan bersifat *borderless* (tanpa batas wilayah) bahkan *transnasional* (lintas batas wilayah), dan yang terjadi di Indonesia, para *hacker* kebanyakan adalah remaja, seperti kasus *hacking* website Komisi Pemilihan Umum (KPU), April 2004, dengan terpidana Dani Firmansyah, serta kasus *hacking website* Partai Golkar baru-baru lalu oleh Iqra Syafaat. Keduanya termasuk kedalam usia remaja.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, tidak ada ketentuan hukum yang secara khusus mengatur kejahatan *cyber* termasuk tindak pidana *hacking*. Namun dengan berlakunya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, maka sudah ada ketentuan yang menjamin kepastian hukum dan memberikan perlindungan kepada masyarakat, khususnya bagi mereka yang memanfaatkan *TI* serta mencegah terjadinya kejahatan berbasis *TI*.

keberadaan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik belum mampu mengatur semua kejahatan internet. Kesiapan hakim sendiri dalam menyelesaikan kasus-kasus yang terkait dengan TI, belum siap secara rata-rata. Namun Undang-Undang Nomor 11 Tahun 2008 perlu disosialisasikan, termasuk kepada

para hakim, sebab undang-undang tanpa sosialisasi tidak akan berlaku efektif.

Perusakan situs resmi suatu instansi pemerintah telah diatur dalam Pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik."

Pasal di atas menegaskan bahwa bilamana seseorang dengan sengaja mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik atau yang lebih dikenal sebagai "*situs*", merupakan salah satu perbuatan yang dilarang karena telah melanggar isi pasal tersebut.

Unsur-unsur yang terdapat dalam Pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tersebut adalah :

1. Unsur Objektif

   Setiap orang, dimana manusia oleh hukum diakui sebagai penyandang hak dan kewajiban, sebagai subyek hukum atau sebagai orang.

2. Unsur Subjektif

   Melawan hukum/ menambah/ merusak, dimana dalam undang-undang diatur bahwa pada perbuatan tersebut seseorang terikat kepada akibat hukum yang muncul karena kehendaknya sendiri.

Berdasarkan unsur-unsur di atas, maka setiap orang yang mengalami kerusakan suatu Informasi Elektronik yang dilakukan oleh seseorang dengan cara melawan hukum atau tanpa hak, dapat menggunakan pasal ini untuk menjerat setiap pelanggaran yang dilakukan oleh seseorang dengan cara melawan hukum tersebut.

Pada Pasal tersebut dinyatakan bahwa seseorang yang dengan sengaja mengubah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dapat dipidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi:

> “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).”

Uraian di atas menegaskan bahwa bilamana seseorang dengan sengaja dan tanpa hak atau melawan hukum/ menambah/ merusak suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik, akan dikenakan sanksi pidana sebagaimana diatur dalam Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.