PERTEMUAN 12

Privacy Dan Kejahatan Komputer

A. TUJUAN PEMBELAJARAN

Melalui risetasi, mahasiswa diharapkan mampu:

1.1 Mengenal kejahatan komputer yang sering terjadi di masyarakat.

1.2 Mempelajari proses pengadilan kejahatan dunia maya, dan implikasinya di masyarakat dunia usaha.

B. URAIAN MATERI

1.1 Privacy dan Kejahatan Komputer

✓ **Kejahatan Komputer**

Definisi kejahatan komputer atau computer crime terus berubah seiring dengan penggunaan dan penyalahgunaan komputer yang merambah-ranah baru. Ketika komputer pertama diperkenalkan, kejahatan komputer hanya didefinisikan sebagai bentuk kejahatan kerah putih yang dilakukan dalam suatu sistem komputer. Disaat aplikasi komputer meluas, terutama dalam telekomunikasi, kejahatan komputer juga merebak dan mulai masuk pelanggaran, komputer digunakan secara langsung atau tidak langsung dalam tindak kejahatan.

Definisi paling sesuai untuk kejahatan komputer saat ini adalah segala tindakan ilegal dengan menggunakan pengetahuan teknologi komputer untuk melakukan tindak kejahatan. Pencurian perangkat keras dan lunak (hardware dan software), manipulasi data, pengaksesan sistem komputer secara ilegal dengan telepon, dan mengubah program kesemuanya masuk definisi ini. Kejahatan yang ditimbulkan karena penggunaan komputer secara ilegal. Kejahatan komputer terus berkembang seiring dengan kemajuan teknologi komputer saat ini. Beberapa jenis kejahatan komputer meliputi Denial of Services (melumpuhkan layanan sebuah sistem komputer), penyebaran virus, spam, carding (pencurian melalui internet) dan lain-lain.

Karakteristik lain dalam definisi ini adalah komputer dapat secara aktif atau pasif terlibat dalam suatu tindak kejahatan. Pengubahan data secara ilegal dalam

suatu database, perusakan file, dan penggunaan program pendobrak (hacking) untuk mendapatkan akses ke dalam suatu sistem merupakan contoh-contoh keterlibatan komputer secara aktif. Sebaliknya, keterlibatan pasif berarti komputer menjadi alat dalam tindak kejahatan, tetapi tuduhan kejahatan komputer mungkin tidak relevan.

Kejahatan komputer internal merupakan pengubahan program yang menghasilkan tampilan fungsi tidak resmi (unauthorized) dalam suatu sistem komputer. Pelanggaran itu yang biasanya dilakukan oleh programer komputer memerlukan pengetahuan komputer yang luas. Seorang programer mampu mengubah program yang ada sehingga tampak berjalan normal, tetapi sebenarnya menjalankan fungsi yang tidak diinginkan ketika kondisi logis tertentu dipenuhi. Dalam keadaan itu, programer mampu menghapus file, mengubah data, atau menyebabkan kerusakan sistem. Karena kejahatan terjadi bertahun-tahun, mereka diberi nama, misalnya Trojan horses, logic bombs, dan trap doors untuk menandai teknik pemrograman yang berbeda dalam menjalankan fungsi tidak resmi. Virus yang menjadi tipe kejahatan komputer internal terbaru merupakan seperangkat instruksi yang tidak hanya menjalankan fungsi tidak resmi, tetapi juga menyisipkannya secara diam-diam pada program lain. Dengan proses penyebaran, virus menular melalui suatu sistem ke sistem lain ketika program yang terinfeksi disalin atau dikirimkan. Kejahatan telekomunikasi meliputi akses ilegal atau penggunaan sistem komputer lewat hubungan telepon. Program hacking berusaha menemukan kode akses yang sahih untuk suatu sistem komputer dengan terus-menerus memanggil sistem itu dengan kode yang dibangkitkan secara acak. Dengan sebuah kode sahih yang ditemukan dengan cara seperti ini, sistem dapat diakses dan biaya dibebankan pada pelanggan yang tidak tahu-menahu. Phreaking telephone merupakan tindak kejahatan lewat telepon yang dilakukan dengan piranti elektronik yang mengeluarkan nada (tone) yang memberi sinyal transaksi jarak jauh normal pada sistem telepon. Piranti ilegal itu menipu sistem telepon agar percaya bahwa tarif jarak jauh sedang diproses secara resmi. Kejahatan manipulasi komputer melibatkan pengubahan data atau penciptaan record dalam suatu sistem untuk pengembangan kejahatan lain. Pada dasarnya segala

penggelapan dalam lembaga keuangan dibuat dengan menciptakan account atau modifikasi data palsu dalam account yang ada untuk menggelapkan.

Database yang dikembangkan oleh operator obat-obatan ilegal untuk pelacakan distribusi termasuk dalam kategori mendukung organisasi kejahatan. Penyitaan obat-obatan dilakukan di tempat informasi yang terkomputerisasi memainkan peran utama dalam pendakwaan pelaku kejahatan. Sering kepolisian lokal tidak mampu menganalisis kejahatan komputer, atau tidak percaya informasi itu akan menjadi data bernilai. Bulletin board komputer menjadi sumber informasi lain yang mendukung aktivitas ilegal. Bulletin board memungkinkan simpanan informasi yang akan dikembalikan oleh seseorang yang menghubungi sistem itu. Penyimpanan informasi pada bulletin board dengan sendirinya tidak ilegal, tetapi penggunaannya telah memperluas peluang berbagai aktivitas ilegal. Tindak kejahatan yang sering terjadi adalah pembajakan perangkat lunak yang didefinisikan sebagai menyalin secara ilegal paket perangkat lunak yang berhak cipta. Bentuk pembajakan paling kentara terjadi ketika seseorang membeli program berhak cipta, menggandakannya, lalu menjual salinannya demi mengeruk keuntungan.

Law Enforcement Response (Respons Penegakan Hukum) Berbagai badan Federal (nasional) pada dasarnya telah menangani kejahatan komputer alih-alih badan di tingkat negara bagian dan lokal. Wewenang legislatif berdasarkan ayat 1029 (“Pemalsuan dan Tindakan Sejenis dalam Piranti Akses”) dan ayat 1030 (“Pemalsuan dan Tindakan Sejenis dalam Bidang Komputer”) pada Pasal 18 UU AS. FBI, Internal Revenue Service (IRS), dan United States Secret Service (USSS) adalah badan Federal terkemuka yang telah melatih para penyelidik untuk melacak kejahatan komputer. Pada 1979, hanya enam negara bagian yang mempunyai peraturan kejahatan komputer. Kian banyaknya negara bagian yang mempunyai hukum kejahatan komputer merupakan tanda makin awasnya legislatif.

Kejahatan Komputer semakin meningkat karena :

- Aplikasi bisnis berbasis TI dan jaringan computer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).

- Desentralisasi server.
- Transisi dari single vendor ke multi vendor.
- Meningkatkatnya Kemampuan pemakai (user).
- Kesulitan penegak hokum dan belum adanya ketentuan yang pasti.
- Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
- Berhubungan dengan internet.

A. Pelanggaran Hukum di Dunia Maya

1. Pelanggaran Isi Situs Web

   Merupakan pelanggaran yang paling banyak terjadi, dengan menampilkan gambar, cerita ataupun gambar bergerak. misalkan:

   - Situs-situs porno
   - Pelanggaran Hak Cipta berupa : Memberikan fasilitas download gratis, Menampilkan gambar-gambar yang dilindungi tanpa izin pembuat gambar, merekayasa gambar atau foto hasil karya oranglain tanpa izin.

2. Kejahatan dalam perdagangan secara elektronik (E-Commerce)

   Penipuan Online Ciri-cirinya yaitu harga produk yang banyak diminati sangat rendah, penjual tidak menyediakan nomor telepon, tidak ada respon terhadap pertanyaan melalui e-mail, menjanjikan produk yang sedang tidak tersedia.

3. Pelanggaran Lainnya

   Yaitu hacker tingkat pemula yang umumnya bertujuan hanya intuk menjebol suatu system dan menunjukkan kegagalan atau kurang andalnya system keamanan pada suatu perusahaan.

B. Motif Kejahatan di Internet

Motif Intelektual, yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekayasadan mengimpelementasikan bidang teknologi informasi.

Motif ekonomi, politik, dan kriminal, yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain.

C. Kriminalitas di Internet (Cybercrime)

Kriminalitas dunia maya (cybercrime) atau kriminalitas di Internet adalah tindakan pidana kriminal yang dilakukan pada teknologi internet (cyberspace), baik yang menyerang fasilitas umum didalam cyberspace ataupun kepemilikan pribadi.

Secara teknik tindak pidana tersebut dapat menjadi off-line crime, semi on-line crime, dan cybercrime. Masing-masing memiliki karakteristik tersendiri, namun perbedaan utama antara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

D. Empat Ruang Lingkup Kejahatan Komputer

1. Komputer sebagai instrumenuntuk melakukan kejahatan tradisional, seperti digunakan untuk melakukan pencurian, penipuan, dan pemalsuan melalui internet, disamping kejahatan lainnya seperti pornografi terhadap anak-anak, porsitusi online, dan lain-lain.
2. Komputer dan perangkatnya sebagai objek penyalahgunaan, di mana data-data didalam computer yang menjadi objek kejahatan dapat saja diubah, dimodifikasi, dihapus, atau di duplikasi secara tidak sah.
3. Penyalahgunaan yang berkaitan dengan komputer atau data, yang dimaksud dengan penyalahgunaan disini yaitu manakala digunakan secara illegal atau tidak sah.
4. Unauthorized acquision, disclosure or use information and data, yang berkaitan dengan masalah penyalahgunaan hak akses dengan cara-cara yang illegal.

Keamanan Komputer

Tindakan pencegahan yang diambil untuk menjaga komputer dan informasi yang ada didalamnya tetap aman dari pengaksesan yang tidak berhak. Pengamanan yang disarankan :

- Terapkan rencana pengamanan untuk mencegah pembobolan.
- Miliki rencana jika pembobolan terjadi

- Buatlah Backup
- Hanya ijinkan akses untuk pegawai tertentu
- Ubah Password secara teratur
- Jagalan Informasi yang tersimpan dengan aman
- Rekrut tenaga kerja / pegwai yang bisa dipercaya

a. Beberapa kendala di internet akibat lemahnya system keamanan komputer (Bernstein, 1996) :
   - Kata sandi seseorang dicuri ketika terhbung ke system jaringan dan ditiru atau digunakan oleh pencuri
   - Jalur komunikasi disadap dan rahasia perusahaan pun dicuri melalui jaringan komputer.
   - Sistem informasi dimasuki oleh pengacau
   - Server jaringan dikirm data dalam ukuran sangat besar sehingga system macet.

b. Masalah Kemanan berhubungan dengan lingkungan hukum :
   - Kekayaan intelektual dibajak
   - Hak cipta dan paten dilanggar dengan melakukan peniruan dan tidak membayar royalty.
   - Terjadi pelanggaran terhadap ketentuan penggunaan teknologi tertentu.
   - Dokumen rahasia disiarkan melalui maling list atau bulletin boards.
   - Pegawai menggunakan internet untuk tindakan asusila seperti pornografi.

c. Sistem keamanan yang berkaitan dengan masalah keuangan dan e-commerce
   - Data keungan dapat dicuri atau diubah oleh intruder atau hacker
   - Dana atau kas disalahgunakan oleh petugas yang memegangnya
   - Pemalsuan uang
   - Seseorang dapat berpura-pura sebagai orang lain dan melakukan transaksi keuangan atas nama orang lain tersebut.

d. Keamanan Internet

- Firewall – hardware dan software yang dirancang untuk menjaga agar user yang tidak berhak tidak dapat masuk ke system jaringan
- Pencegahan virus : Install software antivirus, Buat data cadangan, Hindari pemakaina program bebas yang tidak dikenal, hapus email dari sumber yang tidak dikenal.

✓ **Privacy Dalam IT**

Pengertian Privacy :

- Menurut Standing Committee on Human Rights and The Status of Persons with Dissabilities , privasi adalah "inti dari nilai manusia yang menjiwai perlindungan martabat dan otonomi manusia".
- Profesor Alan Westin, pakar hukum dan pemerintahan dari University of Columbia mendefinisikan privasi sebagai "hak individu untuk menentukan informasi pribadi yang boleh atau tidak boleh diketahui publik".

Sampai saat ini masalah privacy masih menjadi pro dan kontra. Pihak pro yang diwakili oleh ahli hukum dan masyarakat yang peduli atas hak – hak mereka, mengambil sudut pandang privasi sebagai sebuah kekayaan intelektual atau hak milik pribadi. Pemerintah sebagai pihak yang kontra mengedepankan alasan – alasan keamanan negara sebagai pembenaran terhadap aktivitas pengawasan dinamika masyarakat beserta atribut informasi yang melekat padanya.

Wujud konkritnya adalah disahkannya peraturan yang melindungi hak privasi individu. Misalnya, Amerika Serikat memiliki antara lain Privacy Act (1974), Electronic Communications Privacy Act (1986), dan Childrens's Online Privacy Protection (1994), sementara Uni Eropa memiliki European Privacy Directive 8 (1998). Dampak signifikannya terhadap perlindungan privasi baru akan terasa bilamana hukum menjadi rujukan utama dalam penanganan masalah sosial.

Menurut Louis Alvin Day dalam bukunya yang berjudul (Etics in Media Communication, 2006, p. 132), mengatakan bahwa Invasi privasi oleh media meliputi spektrum yang luas, mulai dari reporter, hingga pengiklan. Pengiklan mengubah persoalan etik menjadi persoalan ekonomi. Dalam kondisi persaingan

media yang makin ketat, proses invasi tersebut merupakan hal yang tak dapat dihindari. Namun demikian, tetap saja hal tersebut menimbulkan dilema antara media dan audiensnya.

Day sendiri mendefinisikan privasi sebagai hak untuk dibiarkan atau untuk mengontrol publikasi yang tidak diinginkan tentang urusan personal seseorang. Yang menjadi masalah adalah sifat dasar media itu sendiri yang tidak akan membiarkan seseorang dengan kesendiriannya. Tendensi media adalah pengungkapan [revelation], bukan penyembunyian [concealment]. Privasi sebagai terminologi tidaklah berasal dari akar budaya masyarakat Indonesia. Samuel D Warren dan Louis D Brandeis menulis artikel berjudul "Right to Privacy" di Harvard Law Review tahun 1890. Mereka seperti hal nya Thomas Cooley di tahun 1888 menggambarkan Right to Privacy sebagai Right to be Let Alone atau secara sederhana dapat diterjemahkan sebagai hak untuk tidak di "usik" dalam kehidupan pribadinya. Hak atas Privasi dapat diterjemahkan sebagai hak dari setiap orang untuk melindungi aspek-aspek pribadi kehidupannya untuk dimasuki dan dipergunakan oleh orang lain (Donnald M Gillmor, 1990 : 281). Setiap orang yang merasa privasinya dilanggar memiliki hak untuk mengajukan gugatan yang dikenal dengan istilah Privacy Tort.

Nilai Privacy IT

Ada sejumlah jawaban mengapa privasi penting bagi kita, yakni:

1. Privasi memberikan kemampuan untuk menjaga informasi pribadi yang bersifat rahasia sebagai dasar pembentukan otonomi individu.
2. Privasi dapat melindungi dari cacian dan ejekan orang lain, khususnya dalam masyarakat dimana toleransi masih rendah, dimana gaya hidup dan tingkah laku aneh contoh nyata.
3. Privasi merupakan mekanisme untuk mengontrol reputasi seseorang. Semakin banyak orang tahu tentang diri kita semakin berkurang kekuatan kita untuk menentukan nasib kita sendiri. Contoh peredaran video mesum Yahya Zaini

dan Maria Eva, dimana rekaman tersebut sejatinya merupakan privasi dari keduanya.

4. Privasi merupakan perangkat bagi berlangsungnya interaksi sosial. Berbagai regulasi yang mengatur penyusupan membuktikan bahwa privasi penting bagi interaksi sosial. Begitu juga regulasi yang mengatur soal pemakaian lensa tele.
5. Privasi merupakan benteng dari kekuasaan pemerintah. Sebagaimana slogan yang berbunyi "pengetahuan adalah kekuatan", maka privasi menjaga agar kekuasaan tidak disalahgunakan. Pada satu sisi pemerintah memiliki privasi berupa rahasia negara yang tidak boleh dibuka dalam kondisi tertentu, pada sisi lain masyarakat juga memiliki privasi sehingga penguasa tidak berlaku semena-mena.

Dengan semakin maraknya kejahatan elektronik (carding, cracking, sniffing, spoffing, dll), dan semakin pesatnya teknologi informasi, privacy data dalam dunia IT semakin mudah untuk dilanggar, tetapi semakin mudah pula untuk diamankan, semua tergantung pengetahuan/kemampuan kita sebagai pengguna.

Untuk menjaga privacy, menurut saya harus dimulai oleh si pemilik data, bagaimana kita mengamankan data yang kita miliki, sebagai contoh, mengamankan data jati diri yang tertera dimedia sosial, dengan tidak memampangkan data diri untuk semua orang, cukup untuk user saja atau teman. Untuk memperoleh keamanan data mulailah dari bagaimana kita mengamankan data-data yang kita miliki.

1.2 Privacy dan Confidentiality

A. Privacy

Privacy terkait dengan kerahasiaan data-data pribadi, seperti nama lengkap, alamat, tempat tanggal lahir, status pernikahan, nama istri/suami, nama anak, tempat pekerjaan, nama ibu (mother's maiden name), status kesehatan (pernah mengidap penyakit apa saja), dan seterusnya.

Banyak yang tidak menganggap penting untuk merahasiakan hal ini, padahal dia sangat penting untuk dirahasiakan. Sebagai contoh, jika saya tahu nama anda,

tempat tanggal lahir, alamat, dan nama ibu anda, saya bisa mencoba untuk membatalkan kartu kredit anda. Saya tinggal telepon ke bank anda dimana anda memperoleh kartu kredit dan berpura-pura menjadi anda. Saya laporkan bahwa kartu kredit saya (anda dalam hal ini) hilang. Ketika ditanya nama, alamat, tempat tanggal lahir, dan nama ibu, saya bisa menjawabnya. Maka kartu kredit anda dinyatakan hilang dan diblokir. Meskipun tidak ada yang dicuri, anda akan kerepotan karena tidak bisa menggunakan kartu kredit anda. Bayangkan jika anda sangat membutuhkan kartu kredit tersebut.

Data-data pribadi yang diberikan kepada pihak lain, misalnya ke bank, disebutkan confidential . Pihak kedua ini (bank, dalam contoh ini) tidak boleh menggunakan data-data tersebut untuk keperluan lain. Mereka tidak boleh menjual data-data tersebut ke kartu kredit, atau ke pihak-pihak lain. Untuk itu perhatikan kesepakatan (agreement) yang ada.

Privasi dan kerahasiaan juga didukung oleh dua prinsip Laporan Belmont:

- Menghormati orang - Individu harus diperlakukan sebagai agen otonom mampu menjalankan otonomi mereka semaksimal mungkin, termasuk hak untuk privasi dan hak untuk memiliki informasi pribadi tetap rahasia.
- Kebaikan - Menjaga privasi dan kerahasiaan membantu melindungi peserta dari potensi bahaya termasuk bahaya psikologis seperti rasa malu atau tertekan, kerugian sosial seperti kehilangan pekerjaan atau kerusakan berdiri keuangan seseorang, dan pertanggungjawaban pidana atau perdata.

Privasi adalah kontrol atas tingkat, waktu, dan keadaan berbagi diri (secara fisik, perilaku, atau intelektual) dengan orang lain. Misalnya, orang-orang mungkin tidak ingin terlihat memasuki tempat yang mungkin menstigmatisasi mereka, seperti pusat konseling kehamilan secara jelas diidentifikasi oleh tanda-tanda di depan gedung. Evaluasi privasi juga melibatkan pertimbangan bagaimana peneliti mengakses informasi dari atau tentang calon peserta (misalnya, proses perekrutan). Anggota IRB mempertimbangkan strategi untuk melindungi kepentingan privasi yang berhubungan dengan kontak dengan calon peserta, dan akses ke informasipribadi. Privasi adalah Tentang orang-orang Sebuah rasa

berada dalam kontrol akses yang lain harus diri kita sendiri. Sebuah hak untuk dilindungi Apakah di mata peserta, bukan peneliti atau IRB

B. Confidentiality (Kerahasiaan)

Kerahasiaan berkaitan dengan pengobatan informasi bahwa seseorang telah diungkapkan dalam hubungan kepercayaan dan dengan harapan bahwa hal itu tidak akan diungkapkan kepada orang lain tanpa izin dengan cara yang tidak sesuai dengan pemahaman tentang pengungkapan aslinya.Selama proses informed consent, jika berlaku, subyek harus diberitahu tentang tindakan pencegahan yang akan diambil untuk melindungi kerahasiaan data dan dapat informasi dari pihak-pihak yang akan atau mungkin memiliki akses (misalnya, tim penelitian, FDA, OHRP). Hal ini akan memungkinkan subyek untuk memutuskan tentang kecukupan perlindungan dan penerimaan dari kemungkinan pelepasan informasi pribadi kepada pihak yang berkepentingan.

Kerahasiaan Adalah tentang data diidentifikasi, merupakan perpanjangan dari privasi. Apakah kesepakatan tentang pemeliharaan dan siapa yang memiliki akses ke data diidentifikasi.

Confidentiality juga terkait dengan data-data lain yang bukan data-data pribadi. Password (kata sandi untuk masuk ke sistem) dan PIN (kombinasi angka untuk mengakses account di bank melalui mesin ATM) merupakan contoh data yang harus dirahasiakan dan bersifat confidential . Pemahaman atas pentingnya kerahasiaan data-data ini umumnya lebih mudah diterima atau dimengerti ketimbang privacy . Tetapi masih ada saja orang yang tertipu sehingga data-data yang sifatnya confidential itu bisa bocor ke tangan orang yang tidak berhak. Pencurian password dapat dilakukan dengan menyadap data yang lalu lalang di jaringan komputer dengan menggunakan program yang dikenal dengan nama atau istilah sniffer . Atau, cara lain yang dapat digunakan adalah dengan memasang program “ keylogger ” yang mencatat semua yang diketikkan oleh pemakai ke dalam sebuah berkas. Hal semacam ini semestinya dapat dikategorikan sebagai cybercrime.

Dalam hal HIPAA, melindungi pasien dari pengungkapan yang tidak tepat "Informasi Kesehatan Protected" (PHI). Privasi adalah tentang orang. Kerahasiaan

adalah tentang data.Apa yang Harus Peneliti Tahu? IRB harus memutuskan atas dasar protokol-protokol demi apakah ada ketentuan yang memadai untuk melindungi privasi subyek dan untuk menjaga kerahasiaan data diidentifikasi pada setiap segmen dari penelitian dari perekrutan untuk pemeliharaan data.

Metode pengumpulan data (focus group, wawancara individu, observasi tertutup)

Akankah subyek merasa nyaman memberikan informasi dengan cara ini?
Jika pasif mengamati subjek, bisa individu memiliki harapan privasi (misalnya, chat room untuk pasien kanker)?
Akankah peneliti mengumpulkan informasi tentang individu pihak ketiga yang menganggap swasta (misalnya, penyakit mental, penyalahgunaan zat dalam keluarga)?

Jika ya, informed consent harus diperoleh dari pihak ketiga?
Privasi adalah di mata peserta, bukan peneliti atau IRB

Menjaga Kerahasiaan

Protokol harus dirancang untuk meminimalkan kebutuhan untuk mengumpulkan dan memelihara informasi identitas tentang subjek penelitian. Jika memungkinkan, data harus dikumpulkan secara anonim atau pengidentifikasi harus dihapus dan dimusnahkan sesegera mungkin dan akses ke data penelitian harus didasarkan pada "kebutuhan untuk mengetahui" dan "minimum yang diperlukan" standar.

Bila diperlukan untuk mengumpulkan dan memelihara data yang diidentifikasi, IRB akan memastikan bahwa protokol termasuk pengamanan yang diperlukan untuk menjaga kerahasiaan data diidentifikasi dan keamanan data yang sesuai dengan tingkat risiko dari pengungkapan.

1.3 Kejahatan Komputer vs Kejahatan Biasa

Di Dunia bisnis, mayoritas dari transaksi moneter, diadministrasikan oleh komputer dalam bentuk deposito, neraca dibuat dengan bantuan komputer. Seringkali beberapa produksi dari suatu bank tergantung sekali kepada

kemampuan fungsional dari sistem pengolahan data mereka dan sekaligus sebagai sarana penyimpan data rahasia bank yang sangat penting.

Dengan berkembangnya penggunaan sarana komputer juga membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan.

David I. Bainbridge dalam bukunya Komputer dan Hukum membagi beberapa macam kejahatan dengan menggunakan sarana computer :

1. Memasukkan instruksi yang tidak sah, yaitu seseorang memasukkan instruksi secara tidak sah sehingga menyebabkan sistem komputer melakukan transfer uang dari satu rekening ke rekening lain, tindakan ini dapat dilakukan oleh orang dalam atau dari luar bank yang berhasil memperoleh akses kepada sistem komputer tanpa ijin.
2. Perubahan data input, yaitu data yang secara sah dimasukkan kedalam komputer dengan sengaja diubah. Cara ini adalah suatu hal yang paling lazim digunakan karena mudah dilakukan dan sulit dilacak kecuali dengan pemeriksaan berkala.
3. Perusakan data, hal ini terjadi terutama pada data output, misalnya laporan dalam bentuk hasil cetak komputer dirobek, tidak dicetak atau hasilnya diubah.
4. Komputer sebagai pembantu kejahatan, misalnya seseorang dengan menggunakan komputer menelusuri rekening seseorang yang tidak aktif, kemudian melakukan penarikan dana dari rekening tersebut.
5. Akses tidak sah terhadap sistem komputer atau yang dikenal dengan hacking. Tindakan hacking ini berkaitan dengan ketentuan rahasia bank, karena seseorang memiliki akses yang tidak sah terhadap sistem komputer bank, sudah tentu mengetahui catatan tentang keadaan keuangan nasabah dan hal-hal lain yang harus dirahasiakan menurut kelajiman dunia perbankan.

Dengan demikian pengamanan terhadap system jaringan komputer tidak saja dalam perhitungan keuangan secara otomatis yang sering dipakai dalam bidang

perbankan, system pengupahan, transaksi lintas negara (salah satunya electronic transfer), namun yang tidak kalah penting untuk mendapat perhatian yaitu menyangkut pengamanan terhadap data itu sendiri. Dalam suatu transaksi dibidang perbankan ada berbagai hal yang perlu menjadi perhatian.

Kejahatan komputer akan dibatasi dalam pengertian :

1. Kejahatan yang memanfaatkan kemampuan komputer dalam memproses data dan kemudian memanipulasi data tersebut dengan akibat timbulnya kerugian bagi pihak lain; atau
2. Kejahatan yang dilakukan dengan cara memasuki system komputer orang lain, baik komputer pribadi ataupun komputer yang terhubung ke dalam satu jaringan komputer tanpa ijin.

Dari definisi di atas maka yang dimaksud dengan kejahatan komputer bukanlah penggunaan komputer dalam tindak pidana pemalsuan surat, misalnya perbuatan mendesain kop surat palsu menggunakan komputer dan kemudian mencetaknya dengan menggunakan printer yang memiliki resolusi tinggi. Namun yang dimaksud adalah tindak pidana modern yang berkaitan dengan kemampuan komputer melakukan pemrosesan data seperti memasuki jaringan komputer tanpa ijin (unauthorized access), manipulasi terhadap data-data yang dikirim melalui jaringan elektronik, ataupun penyadapan atas suatu informasi antar para pihak oleh pihak ketiga yang tak berkompeten.

Jadi tidak semua kejahatan yang menggunakan komputer adalah kejahatan komputer. Karena dapat saja terjadi suatu tindak pidana biasa, sedangkan komputer digunakan sebatas alat yang membuat kejahatan itu menjadi lebih sempurna dan meyakinkan. Titik perbedaannya adalah pada kejahatan komputer, esensi kejahatan itu terdapat pada komputer itu sendiri, yaitu kemampuannya melakukan pemrosesan data. Sedangkan pada kejahatan biasa komputer hanya menjadi pengganti alat-alat Bantu lainnya. Misalnya dalam pemalsuan surat dengan komputer maka komputer hanyalah pengganti mesin cetak. Untuk lebih jelasnya dapat kita lihat perbandingan berikut ini

Kejahatan Komputer

1. Memasuki jaringan komputer orang lain tanpa ijin, misalnya melalui internet (hacking)
2. Menyadap transmisi data orang lain, misalnya surat elektronik (e-mail).
3. Memanipulasi data seseorang, misalnya kartu kredit seseorang dan kemudian menggunakan informasi kartu kredit tersebut untuk berbelanja di internet.
4. Memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki kedalam program komputer. Misalnya programmer yang bertugas mendesain system penggajian pegawai negeri. Sang programmer kemudian membuat suatu program system penggajian dan menyisipkan perintah dalam program komputer tersebut untuk memotong 1 persen gaji setiap pegawai dan kemudian mengirimkan potongan tersebut ke rekeningnya tiap bulan.
5. Memalsukan surat dengan cara mendesain surat palsu menggunakan perangkat komputer. Mengubah data yang tersimpan dalam komputer, misalnya dilakukan oleh karyawan suatu perusahaan dengan cara mengganti data-data yang terdapat didalam komputer perusahaan sebagai bagian dari kejahatan pokoknya, misalnya penggelapan. Pada dasarnya perbuatan karyawan tersebut adalah penggelapan biasa, namun mengingat pembukuan perusahaan terdapat di dalam komputer dan bukan di atas kertas maka data yang ia ubah adalah data dalam komputer tersebut. Jadi dalam kejahatan ini tidak ada unsure pemrosesan data, melainkan sekedar pengubahan data saja untuk menutupi penggelapannya.

Berdasarkan definisi dan perbandingan di atas maka dalam kejahatan komputer dimungkinkan adanya delik formil dan delik meteril sekaligus. Delik formil terdapat dalam perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, misalnya melalui jaringan internet, atau delik materil yaitu perbuatan yang menimbulkan akibat kerugian bagi orang lain. Satu contoh delik materil ini adalah perbuatan seseorang yang memasuki jaringan komputer perbankan kemudian mengubah catatan keuangan si penyusup atau orang lain.

Kelemahan Hukum Acara Pidana Dalam Kejahatan Komputer

Masalah yang cukup memusingkan penegak hukum saat ini adalah bagaimana menjaring perbuatan yang mengusik rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku. Kendala yang klasik adalah sulitnya menghukum si pelaku mengingat belum lengkapnya ketentuan pidana yang mengatur tentang kejahatan komputer. Masalah utama adalah belum diterimanya dokumen elektronik (misalnya file komputer) sebagai alat bukti oleh konsep yang dianut UU No 8/1981. Pasal 184 ayat (1) dari Undang undang ini secara definitive membatasi alat-alat bukti hanyalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa saja.

Satu fiksi hukum berikut ini cukup memberikan gambaran kendala tersebut : Seorang pegawai di sebuah instansi pertahanan pemerintah menyalin data-data rahasia yang tersimpan di dalam media penyimpan komputer ke dalam sebuah disket yang memang tersedia di tempat kerja tersebut.

Ketika sedang menyerahkan disket yang berisi rahasia negara tersebut kepada pihak lawan, pegawai tersebut berhasil ditangkap oleh dinas Intelijen pemerintah. Studi terhadap masalah hukum yang muncul atas fiksi hukum di atas adalah sulitnya menjaring si pelaku atas sangkaan pembocoran rahasia negara. Kalaupun kasus dilanjutkan maka yang terjadi adalah sebuah kontroversi yang cukup menggelikan, yaitu sangkaan terhadap si pelaku sebagai penggelapan sebuah disket.

Fiksi hukum di atas memang bukanlah contoh kejahatan komputer. Namun mengingat kejahatan komputer banyak berhubungan dengan data elektronik yang tersimpan di dalam disket, hard disk, CD ROM, dan sebagainya, akan sulit bagi Jaksa untuk mendakwa si pelaku mengingat tidak diakuinya dokumen elektronik sebagai alat bukti oleh KUHAP.

1.4 Alat Bukti Elektronik Pada Proses Pengadilan

Mengingat kelemahan KUHAP tersebut, dalam menjalankan tugasnya penyidik harus dengan cerdik menggunakan definisi dokumen elektronik yang dapat diterima sebagai alat bukti. Pada dasarnya dalam praktik peradilan hakim sudah menerima dokumen elektronik sebagai alat bukti, meskipun hal ini mungkin dilakukan tanpa sadar. Dalam kasus-kasus pidana yang berhubungan

dengan perbankan umumnya rekening koran atau dokumen apapun yang berisikan data nasabah berikut laporan keuangannya dihadirkan sebagai alat bukti surat.

Padahal yang dimaksud dengan rekening koran sebenarnya adalah cetakan (*printout*) laporan keuangan nasabah yang dalam bentuk aslinya berupa dokumen elektronik (file komputer).

Prosedur system perbankan modern saat ini seluruhnya menggunakan komputer sebagai petugas yang secara otomatis mendebat rekening nasabah (misalnya pengambilan lewat ATM atau pengambilan melalui cek dan giro), atau secara otomatis menambahkan bunga atas dana nasabah. Seluruh proses ini dicatat oleh komputer dan disimpan dalam bentuk file.

Dengan demikian seluruh proses pembuktian kasus-kasus perbankan dalam kaitannya dengan dana nasabah sangatlah mustahil didasarkan pada dokumen yang aslinya berbentuk kertas. Kalaupun ada dokumen berbentuk kertas maka itu hanyalah cetakan file komputer pada bank yang bersangkutan.

Dengan diterimanya rekening koran tersebut sebagai alat bukti surat maka hal ini dapat menjadi dasar bagi penyidik untuk menggunakan cetakan file komputer sebagai alat bukti surat.

Doktrin tentang hal ini juga diberikan oleh Subekti. Menurut Subekti, pembuktian adalah upaya meyakinkan hakim akan hubungan hukum yang sebenarnya antara para pihak dalam perkara, dalam hal ini antara bukti-bukti dengan tindak pidana yang didakwakan.

Dalam mengkonstruksikan hubungan hukum ini, masing-masing pihak menggunakan alat bukti untuk membuktikan dalil-dalilnya dan meyakinkan hakim akan kebenaran dalil-dalil yang dikemukakan. Untuk itu hakim patut menerima dalil-dalil para pihak (jaksa ataupun terdakwa) tanpa harus dikungkung oleh batasan alat-alat bukti sepanjang dalil tersebut memenuhi prinsip-prinsip logika.

Untuk memperjelas pendapat Subekti tersebut, ilustrasi dibawah ini mungkin akan memberikan pemahaman yang lebih memperluas cakrawala berpikir : Pernah dipersoalkan, apakah selain lima macam “alat bukti” yang disebutkan dalam pasal 1866 Kitab Undang-undang Hukum Perdata, Pasal 164 RIB (Kini oleh KUHAP

diatur dalam Pasal 184 ayat (1) atau pasal 283 RDS, tidak terdapat lagi alat-alat bukti lainnya.

Persoalan tersebut lazimnya dijawab, bahwa penyebutan alat-alat bukti dalam pasal-pasal tersebut tidak berarti melarang alat-alat bukti lainnya yang bukan tulisan. Pasal 1887 Kitab Undang-undang Hukum Perdata misalnya menyebutkan "tongkat berkelar" yang dapat dipakai untuk membuktikan penyerahan-penyerahan barang. Ada juga yang mengatakan bahwa bukti lain itu yang tidak berupa tulisan, kesaksian, pengakuan, atau sumpah, seyogyanya saja dianggap sebagai "persangkaan", tetapi pendapat yang demikian itu tidak tepat.

Kita juga tidak boleh melupakan bahwa undang-undang yang kita pakai sekarang ini dibuat seratus tahun yang lalu. Dengan kemajuan dalam berbagai bidang teknologi yang pesat dalam setengah abad yang lalu ini muncullah beberapa alat baru, seperti fotocopy, tape recorder, dan lain-lain yang dapat dipakai sebagai alat bukti.

C. SOAL LATIHAN/TUGAS

1. Sebutkan macam-macam kejahatan computer?
2. Bagaimana cara mencegah kejahatan momputer?
3. Apa kaitan antara privacy dengan kejahatan computer?

D. DAFTAR PUSTAKA

Bagio Budiarjo. *Komputer dan Masyarakat*. PT.Elex Media Komputindo, Jakarta