ETIKA DAN PROFESIONALISME

ETIKA DALAM SISTEM INFORMASI

Masalah etika juga mendapat perhatian dalam pengembangan dan pemakaian sistem informasi. Masalah ini diidentifikasi oleh Richard Mason pada tahun 1986 (Zwass, 1998) yang mencakup privasi, akurasi, property, dan akses.

1. Privasi

Privasi menyangkut hak individu untuk mempertahankan informasi pribadi dari pengaksesan oleh orang lain yang memang tidak diberi ijin untuk melakukannya. Contoh isu mengenai privasi sehubungan diterapkannya sistem informasi adalah pada kasus seorang manajer pemasaran yang ingin mengamati *email* yang dimiliki bawahannya karena diperkirakan mereka lebih banyak berhubungan dengan *email* pribadi daripada *email* para pelanggan. Sekalipun manajer dengan kekuasaannya dapat melakukan hal itu, tetapi ia telah melanggar privasi bawahannya.

2. Akurasi

Akurasi terhadap informasi merupakan factor yang harus dipenuhi oleh sebuah sistem informasi. Ketidakakurasian informasi dapat menimbulkan hal yang mengganggu, merugikan, dam bahkan membahayakan. Sebuah kasus akibat kesalahan penghapusan nomor keamanan social dialami oleh Edna Rismeller. Akibatnya, kartu asuransinya tidak bisa digunakan dan bahkan pemerintah menarik kembali cek pensiun sebesar $672 dari rekening banknya. Mengingat data dalam sistem informasi menjadi bahan dalam pengambilan keputusan, keakurasiannya benar-benar harus diperhatikan.

3. Properti

Perlindungan terhadap hak property yang sedang digalakkan saat ini yaitu dikenal dengan sebutan HAKI (Hak Atas Kekayaan Intelektual). Kekayaan Intelektual diatur melalui 3 mekanisme yaitu hak cipta (copyright), paten, dan rahasia perdagangan (trade secret).

a. Hak Cipta

Hak cipta adalah hak yang dijamin oleh kekuatan hukum yang melarang penduplikasian kekayaan intelektual tanpa seijin pemegangnya. Hak cipta biasa diberikan kepada pencipta buku, artikel, rancangan, ilustrasi, foto, film, musik, perangkat lunak, dan bahkan kepingan semi konduktor. Hak seperti ini mudah didapatkan dan diberikan kepada pemegangnya selama masih hidup penciptanya ditambah 70 tahun.

b. Paten

Paten merupakan bentuk perlindungan terhadap kekayaan intelektual yang paling sulit didapat karena hanya akan diberikan pada penemuan-penemuan inovatif dan sangat berguna. Hukum paten memberikan perlindungan selama 20 tahun.

c. Rahasia Perdagangan

Hukum rahasia perdagangan melindungi kekayaan intelektual melalui lisensi atau kontrak. Pada lisensi perangkat lunak, seseorang yang menandatangani kontrak menyetujui untuk tidak menyalin perangkat lunak tersebut untuk diserhakan pada orang lain atau dijual.

4. Akses

Fokus dari masalah akses adalah pada penyediaan akses untuk semua kalangan. Teknologi informasi malah tidak menjadi halangan dalam melakukan pengaksesan terhadap informasi bagi kelompok orang tertentu, tetapi justru untuk mendukung pengaksesan untuk semua pihak.

MASALAH KEAMANAN DALAM SISTEM INFORMASI

Keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi, yang dimaksudkan untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat kerusakan sistem.

Secara garis besar, ancaman terhadap sistem informasi dapat dibagi menjadi 2 macam, yaitu ancaman ak tif dan ancaman pasif. Ancaman aktif mencakup kecurangan dan kejahatan terhadap komputer, sedangkan ancaman pasif mencakup kegagalan sistem, kesalahan manusia dan bencana alam. Kegagalan sistem menyatakan kegagalan dalam peralatan-peralatan komponen (misalnya *hard disk)*.

Tabel 1. Ancaman terhadap sistem informasi

MACAM ANCAMAN	CONTOH
Bencana alam dan politik	- Gempa bumi, banjir, kebakaran, perang.
Kesalahan manusia	- Kesalahan memasukkan data - Kesalahan penghapusan data - Kesalaha operator (salah memberi label pada pita magnetic).
Kegagalan perangkat lunak dan perangkat keras	- Gangguan listrik - Kegagalan peralatan - Kegagalan fungi perangkat lunak
Kecurangan dan kejahatan	- Penyelewengan aktivitas

komputer	- Penyalahgunaan kartu kredit - Sabotase - Pengaksesan oleh orang yang tidak berhak.
Program yang jahat/usil	- Virus, cacing, bom waktu, dll

Bencana alam merupakan faktor yang tak terduga yang bisa mengancam sistem informasi. Banjir, badai, gempa bumi, dan kebakaran dapat meghancurkan sumber daya pendukung sistem informasi dalam waktu singkat.

Kesalahan pengoperasian sistem oleh manusia juga dapat mengancam integritas sistem dan data. Pemasukkan data yang salah dapat mengacaukan sistem.

Gangguan listrik, kegagalan peralatan dan kegagalan fungsi perangkat lunak dapat menyebabkan data tidak konsisten, transaksi tidak lengkap atau bahkan data rusak, Selain itu, variasi tegangan listrik yang terlalu tajam dapat membuat peralatan terbakar.

Ancaman lain berupa kecurangan dan kejahatan komputer. Ancaman ini mendasarkan pada komputer sebagai alat untuk melakukan tindakan yang tidak benar. Penggunaan sistem berbasis komputer terkadang menjadi rawan terhadap kecurangan (*fraud*) dan pencurian.

Metode yang umum digunakan oleh orang dalam melakukan penetrasi terhadap sistem berbasis komputer ada 6 macam :

1. ***Pemanipulasian masukan***
   Pemanipulasian masukan merupakan metode yang paling banyak digunakan, mengingat hal ini bisa dilakukan tanpa memerlukan ketrampilan teknis yang tinggi. Contoh seorang *teller* bank ditemukan mengambil uang dari rekening-rekening bank melalui sistem komputer.

2. ***Penggantian program***
   Pemanipulasian melalui program biasa dilakukan oleh para spesialis teknologi informasi.

3. ***Penggantian berkas secara langsung***
   Pengubahan berkas secara langsung umum dilakukan oleh orang yang punya banyak akses secara langsung terhadap basis data.

4. ***Pencurian data***
   Dengan kecanggihan menebak *password* atau menjebol *password* para pencuri berhasil mengakses data yang seharusnya tidak menjadi hak mereka.

5. ***Sabotase***
   Sabotase dapat dilakukan dengan berbagai cara. Istilah umum digunakan untuk menyatakan tindakan masuk ke dalam suatu sistem komputer tanpa otorisasi, yaitu *hacking*.

   Berbagai teknik yang digunakan untuk melakukan *hacking :*

   - **Denial of Service**

Teknik ini dilaksanakan dengan cara membuat permintaan yang sangat banyak terhadap suatu situs sehingga sistem menjadi macet dan kemudian dengan mencari kelemahan pada sistem si pelaku melakukan serangan pada sistem.

- **Sniffer**
  Teknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi Internet, menangkap *password* atau menangkap isinya.
- **Spoofing**
  Melakukan pemalsuan alamat *email* atau *web* dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti *password* atau nomor kartu kredit.

Berbagai kode jahat atau usil juga menjadi ancaman bagi sistem komputer, kode yang dimaksud adalah :

- **Virus**
  Virus berupa penggalan kode yang dapat menggandakan dirinya sendiri dengan cara menyalin kode dan menempelkan ke berkas program yang dapat dieksekusi (misalnya berkas .exe pada DOS). Selanjutnya, salinan virus ini akan menjadi aktif manakala program yang terinfeksi dijalankan. Beberapa virus hanya "sekedar muncul". Namun sejumlah virus yang lain benar-benar sangat jahat karena akan menghapus berkas-berkas dengan extension tertentu dan bahkan dapat memformat *hard disk*. Contoh virus jahat adalah CIH atau virus Chernobyl, yang melakukan penularan melalui *email*.
- **Cacing (Worm)**
  Cacing adalah program komputer yang dapat menggandakan dirinya sendiri dan menulari komputer-komputer dalam jaringan.
- **Bom Logika atau Bom Waktu (*Logic bomb or time bomb*)**
  Program yang beraksi karena dipicu oleh sesuatu kejadian atau setelah selang waktu berlalu. Sebagai contoh, program dapat diatur agar menghapus *hard disk* atau menyebabkan lalu lintas jaringan macet.
- **Kuda Trojan (Trojan Horse)**
  Program yang dirancang agar dapat digunakan untuk menyusup ke dalam sistem. Sebagai contoh kuda Trojan dapat menciptakan pemakai dengan wewenang supervisor atau superuser. Pemakai inilah yang nantinya dipakai untuk menyusup ke sistem.

6. ***Penyalahgunaan dan pencurian sumber daya komputasi***
   Merupakan bentuk pemanfaatan secara illegal terhadap sumber daya komputasi oleh pegawai dalam rangka menjalankan bisnisnya sendiri.

Trapdoor adalah kemungkinan tindakan yang tak terantisipasi yang tertinggal dalam program karena ketidaksengajaan. Disebabkan sebuah program tak terjamin bebas dari kesalahan, kesalahan-kesalahan yang terjadi dapat membuat pemakai yang tak berwenang dapat

mengakses sistem dan melakukan hal-hal yang sebenarnya tidak boleh dan tidak bisa dilakukan.

BEBERAPA POKOK PEMIKIRAN TENTANG CYBERLAW

Cyberlaw adalah hukum yang digunakan untuk dunia Cyber (dunia maya, yang umumnya diasosiasikan dengan internet. Cyberlaw dibutuhkan karena dasar atau pondasi dari hukum di banyak Negara adalah "ruang dan waktu". Sementara itu, internet dan jaringan komputer telah mendobrak batas ruang dan waktu.

Berikut ini adalah contoh permasalahan yang berhubungan dengan hilanganya ruang dan waktu:

Seorang penjahat komputer yang berkebangsaan Indonesia berada di Australia mengobrak-abrik server di Amerika, yang ditempati atau hosting sebuah perusahaan Inggris.

Hukum apa yang akan dipakai untuk mengadili kejahatan teknologi tersebut?

Di Indonesia telah keluar Rancangan Undang-Undang (RUU) yang salah satunya diberi Nama "RUU Pemanfaatan Teknologi Informasi". Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi. Sebelumnya RUU ini diberi nama "RUU Teknologi Informasi", namun judul ini ditolak karena RUU yang diinginkan penertiban terhadap penggunaannya atau pemanfaatannya bukan terhadap teknologinya. RUU ini dikenal dengan istilah "Cyberlaw". RUU Pemanfaatan Teknologi Informasi (RUU PTI) ini dipelopori oleh Fakultas Hukum Universitas Padjajaran dan Tim Asistensi dari Institut Teknologi Bandung (ITB) dengan jalur Departemen Perhubungan (melalui Diden Postel).

RUU Pemanfaatan Teknologi Informasi ini telah disosialisasikan melalui presentasi dan seminar-seminar di berbagai daerah dengan berbagai peserta, mulai dari mahasiswa, dosen, akademik, pelaku bisnis, birokrat dan pihak pemerintah.

Latar Belakang MuncuInya RUU Pemanfaatan Teknologi Informasi

Munculnya RUU Pemanfaatan Teknologi Informasi bermula dari mulai merasuknya pemanfaatan teknologi informasi dalam kehidupan kita saat-saat ini. Jika kita lihat, kita mulai terbiasa menggunakan ATM untuk mengambil uang, menggunakan handphone untuk berkomunikasi dan bertransaksi melalui mobile banking, menggunakan internet untuk melakukan transaksi (internet banking atau membeli barang), berkirim e-mail atau untuk sekedar menjelajah internet, dan masih banyak yang lainnya. Semua kegiatan ini adalah beberapa contoh dari pemanfaatan Teknologi Informasi.

Selain memberikan kemudahan bagi para user, pemanfaatan Teknologi Informasi ini juga mempunyai dampak negative yang luar biasa, seperti:

- Penyadapan e-mail, PIN (untuk internet banking)
- Pelanggaran terhadap hak-hak privasi
- Masalah domain seperti kasus mustikaratu.com clan klikbca.corn
- Penggunaan kartu kredit milik orang lain.
- Munculnya pembajakan lagu dalam format MP3
- Pornografi