

SISTEM INFORMASI

Etika dan Keamanan Dalam Sistem Informasi

Rianto, S.Kom., M.Eng.

Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : rianto@mti.ugm.ac.id Website : <http://www.rianto.com>

Mobile : 0815 787 02873

Etika dalam Sistem Informasi

- Etika : kepercayaan tentang hal yang benar dan salah atau yang baik dan yang tidak
- Etika dalam SI dibahas pertama kali oleh Richard Mason (1986), yang mencakup PAPA:
 1. Privasi
 2. Akurasi
 3. Properti
 4. Akses

Etika dalam Sistem Informasi

- **PRIVASI** menyangkut hak individu untuk mempertahankan informasi pribadi dari pengaksesan oleh orang lain yang memang tidak diberi izin untuk melakukannya
- Kasus:
 - *Junk mail*
 - Manajer pemasaran mengamati *e-mail* bawahannya
 - Penjualan data akademis

Etika dalam Sistem Informasi

- **AKURASI** terhadap informasi merupakan faktor yang harus dipenuhi oleh sebuah sistem informasi
- Ketidakakurasian informasi dapat menimbulkan hal yang mengganggu, merugikan, dan bahkan membahayakan.
- Kasus:
 - Terhapusnya nomor keamanan sosial yang dialami oleh Edna Rismeller (Alter, 2002, hal. 292)
 - Kasus kesalahan pendeteksi misil Amerika Serikat

Etika dalam Sistem Informasi

- Perlindungan terhadap hak PROPERTI yang sedang digalakkan saat ini yaitu yang dikenal dengan sebutan HAKI (hak atas kekayaan intelektual).
- HAKI biasa diatur melalui hak cipta (*copyright*), paten, dan rahasia perdagangan (*trade secret*).

Etika dalam Sistem Informasi

- **Hak cipta** adalah hak yang dijamin oleh kekuatan hukum yang melarang penduplikasian kekayaan intelektual tanpa seizin pemegangnya
- Hak seperti ini mudah untuk didapatkan dan diberikan kepada pemegangnya selama masa hidup penciptanya plus 70 tahun.

Etika dalam Sistem Informasi

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

Etika dalam Sistem Informasi

- **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 diserahkan pada orang lain atau dijual.

Etika dalam Sistem Informasi

- Berkaitan dengan kekayaan intelektual, banyak masalah yang belum terpecahkan (Zwass, 1998); Antara lain:
 - Pada level bagaimana informasi dapat dianggap sebagai properti?
 - Apa yang harus membedakan antara satu produk dengan produk lain?
 - Akankah pekerjaan yang dihasilkan oleh komputer memiliki manusia penciptanya? Jika tidak, lalu hak properti apa yang dilindunginya?

Etika dalam Sistem Informasi

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

Keamanan Sistem Informasi

- Keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi
- Tujuannya adalah untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem.

Keamanan Sistem Informasi

- Ancaman terhadap sistem informasi dapat dibagi menjadi dua macam: ancaman aktif dan ancaman pasif
- **Ancaman aktif** mencakup kecurangan dan kejahatan terhadap komputer
- **Ancaman pasif** mencakup kegagalan sistem, kesalahan manusia, dan bencana alam

Keamanan Sistem Informasi

Macam Ancaman	Contoh
Bencana alam dan politik	Gempa bumi, banjir, kebakaran, perang
Kesalahan manusia	• Kesalahan pemasukan data, Kesalahan penghapusan data, Kesalahan operator (salah memberi label pada pita magnetik)
Kegagalan perangkat lunak dan perangkat keras	Gangguan listrik, Kegagalan peralatan Kegagalan fungsi perangkat lunak
Kecurangan dan kejahatan komputer	• Penyelewengan aktivitas, Penyalahgunaan kartu kredit, Sabotase, Pengaksesan oleh orang yang tidak berhak
Program yang jahat/usil	Virus, cacing, bom waktu, dll

Keamanan Sistem Informasi

- Metode yang umum digunakan oleh orang dalam melakukan penetrasi terhadap sistem berbasis komputer ada 6 macam (Bodnar dan Hopwood, 1993), yaitu
 1. Pemanipulasian masukan
 2. Penggantian program
 3. Penggantian berkas secara langsung
 4. Pencurian data
 5. Sabotase
 6. Penyalahgunaan dan pencurian sumber daya komputasi.

Keamanan Sistem Informasi

- 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 terhadap 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 *e-mail* atau Web dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti *password* atau nomor kartu kredit

Keamanan Sistem Informasi

- Penggunaan Kode yang Jahat:
 1. Virus
 2. Cacing (worm)
 3. Bom waktu
 4. Kuda Trojan

Terima Kasih dan Selamat Belajar

Rianto, S.Kom., M.Eng.

www.rianto.com

rianto@mti.ugm.ac.id

0815 787 02873