1. Pentingnya etika bagi profesional bidang IT akan mendapat kepercayaan dari masyarakat, bilamana dalam diri para elit profesional TI tersebut ada kesadaran kuat untuk mengindahkan etika profesi pada saat mereka ingin memberikan jasa keahlian profesi kepada masyarakat yang memerlukannya. Tanpa etika profesi, apa yang semua dikenal sebagai sebuah profesi yang terhormat akan segera jatuh terdegradasi menjadi sebuah pekerjaan pencarian nafkah biasa (okupasi) yang sedikitpun tidak diwarnai dengan nilai-nilai idealisme dan ujung-ujungnya akan berakhir dengan tidak-adanya lagi respek maupun kepercayaan yang pantas diberikan kepada para elite profesional ini.

2. Sanksi bila melanggar Etika :

    - Sanksi Sosial : Sanksi ini diberikan oleh masyarakat sendiri, tanpa melibatkan pihak berwenang. Pelanggaran yang terkena sanksi sosial biasanya merupakan kejahatan kecil, ataupun pelanggaran yang dapat dimaafkan. Dengan demikian hukuman yang diterima akan ditentukan leh masyarakat, misalnya membayar ganti rugi dsb, pedoman yang digunakan adalah etika setempat berdasarkan keputusan bersama.
    - Sanksi Hukum : Sanksi ini diberikan oleh pihak berwengan, dalam hal ini pihak kepolisian dan hakim. Pelanggaran yang dilakukan tergolong pelanggaran berat dan harus diganjar dengan hukuman pidana ataupun perdata. Pedomannya suatu KUHP.

3. Menurut saya Kasus pelanggaran etika di bidang teknologi informasi apa yang terbesar saat itu adalah kasus Copas Artikel dari Internet. Dan tanggapan saya mengenai hal itu adalah yaitu copy paste bukanlah suatu kesalahan namun terkadang banyak orang yang menggunakan copy paste secara ilegal, yaitu tidak mencantumkan sumber sumbernya atau mengkopi keseluruhan isi artikel tersebut. Untuk membuatnya lebih baik, artikel yang di copy paste harus di tambahkan dengan pemikiran sendiri, itu tidak akan dipermasalahkan. Karena sesungguhnya, menulis memanglah membutuhkan suatu kreatifitas yang tinggi, dan juga membutuhkan pengetahuan yang luas dari penulisnya. Sebelum menulis haruslah terlebih dahulu senang membaca, karena, Jika membacapun kita tidak suka,menulis adalah hal yang mustahil untuk dilakukan.

4. - Cybercrime

Adalah Cyber crime adalah tindak kejahatan yang dilakukan secara online. Kejahatan ini tidak mengenal waktu dan tidak pilih-pilih target. Bisa terjadi pada individu atau perusahaan di mana pun berada. Jadi, Anda perlu waspada. Tujuan cyber crime sendiri beragam. Bisa sekedar iseng, sampai kejahatan serius yang merugikan korbannya secara finansial.

- Cyberlaw

Adalah adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat mulai "online" dan memasuki dunia cyber atau maya. Pada negara yang telah maju dalam penggunaan internet/elektronik sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju.

5. UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU-ITE), Bab VII Perbuatan yang dilarang, memuat ketentuan pidana bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan:
    - Melanggar kesusilaan; memiliki muatan perjudian; memiliki muatan penghinaan dan/atau pencemaran nama baik; memiliki muatan pemerasan dan/atau pengancaman (Pasal 27).
    - Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik; menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA) (Pasal 28)
    - Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29).

- Mengakses komputer dan/atau sistem elektronik milik orang lain; mengakses komputer dan/atau sistem elektronik dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik; mengakses komputer dan/atau sistem elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30).
- Melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik; melakukan intersepsi elektronik atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik (Pasal 31)
- Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik; memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak; mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya (Pasal 32).
- Terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya (Pasal 33).
- Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki (a) perangkat keras atau perangkat lunak yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud Pasal 27-33; (b) sandi lewat komputer, kode akses, atau hal lain yang sejenis dengan itu yang ditujukan agas sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan dalam Pasal 27-33 (Pasal 34).
- Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olahdata yang otentik (Pasal 35).
- Melakukan perbuatan sebagaimana dimaksud dalam Pasal 27-34 yang mengakibatkan kerugian bagi orang lain (Pasal 36).

- Melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27-36 diluar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah Yurisdiksi Indonesia (Pasal 37).

6. Pada tahun 1982 telah terjadi penggelapan uang di bank melalui komputer sebagaimana diberitakan "Suara Pembaharuan" edisi 10 Januari 1991 tentang dua orang mahasiswa yang membobol uang dari sebuah bank swasta di Jakarta sebanyak Rp. 372.100.000,00 dengan menggunakan sarana komputer. Perkembangan lebih lanjut dari teknologi komputer adalah berupa computer network yang kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet. Pada kasus tersebut, kasus ini modusnya adalah murni criminal, kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan.Sebaiknya internet digunakan untuk kepentingan yang bermanfaat,dan tidak merugikan orang lain.Penyelesaian,karena kejahatan ini termasuk penggelapan uang pada bank dengan menggunakan komputer sebagai alat melakukan kejahatan.Sesuai dengan undang-undang yang ada di indonesia maka,orang tersebut diancam dengan pasal 362 KUHP tentang pencurian,mendapat sanksi hukuman penjara selama 5 Tahun.dan pasal 378 KUHP tentang penipuan,mendapat sanksi hukuman penjara 4 Tahun. Disamping itu,pelaku yang diduga telah melakukan pembobolan tersebut,UU ITE menyebutkan bahwa minimal dapat dijerat dengan Pasal 30 ayat (1). Isi Pasal tersebut menyebutkan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik milik orang lain dengan cara apapun,dan ayat (3) yang menyebutkan,bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar,menerobos,melampaui,atau menjebol sistem pengamanan.Disamping itu,juga dapat dijerat dengan Pasal 32 ayat (2) yang menyebutkan,bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan /atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.