BAHAN E-LEARNING

ETIKA PROFESI TEKNOLOGI INFORMASI DAN KOMUNIKASI

UNIVERSITAS BINA SARANA INFORMATIKA

www.bsi.ac.id

PERTEMUAN 1

TINJAUAN UMUM ETIKA

A. PENGERTIAN ETIKA

Dalam pergaualan hidup bermasyarakat, bernegara hingga pergaualan hidup tingkat internasional diperlukan suatu sistem yang mengatur bagaimana seharusnya manusia bergaul. Sistem pengaturan pergaulan tersebut menjadi saling menghormati dan dikenal dengan sebutan sopan santun, tata krama, protokoler dan lain-lain.

Maksud pedoman pergaulan tidak lain untuk menjaga kepentingan masing-masing yang terlibat agar mereka senang, tenang, tentram, terlindungi tanpa merugikan kepentingannya serta terjamin agar perbuatannya yang tengah dijalankan sesuai dengan adat kebiasaan yang berlaku dan tidak bertentangan dengan hak-hak asasi umumnya. Hal itulah yang mendasari tumbuh kembangnya etika di masyarakat kita.

Menurut para ahli maka etika tidak lain adalah aturan prilaku, adat kebiasaan manusia dalam pergaulan antara sesamanya dan menegaskan mana yang benar dan mana yang buruk.

Perkataan Etika atau lazim juga disebut Etik, berasal dari kata yunani yaitu ETHOS yang berarti norma-norma, nilai-nilai, kaidah-kaidah dan ukuran-ukuran bagi tingkah laku manusia yang baik, seperti yang dirumuskan oleh beberapa ahli berikut :

- Drs. O. P. Simorangkir : Etika atau etik sebagai pandangan manusia dalam berprilaku menurut ukuran dan nilai yang baik.
- Drs. Sidi Gajalba dalam sistematika filsafat : Etika adalah teori tentang tingkah laku perbuatan manusia dipandang dari segi baik dan buruk, sejauh yang dapat ditentukan oleh akal.

- Drs. H. Burhanuddin Salam : Etika adalah cabang Filsafat yang berbicara mengenai nilai dan norma moral yang menentukan prilaku manusia dalam hidupnya.

Menurut kamus besar Bahasa Indonesia terbitan Departemen Pendidikan dan Kebudayaan (1988), terdapat tiga pengertian etika :

1. Ilmu tentang apa yang baik dan buruk, tentang hak dan kewajiban moral.
2. Kumpulan asas atau nilai yang berkenaan dengan akhlak
3. Nilai mengenai benar atau salah yang dianut di masyarakat.

Menurut Profesor Salomon dalam Wahyono (2006:3), Etika dikelompokkan dalam dua definisi, yaitu :

1. Etika merupakan karakter individu, disebut pemahaman manusia sebagai individu beretika.
2. Etika merupakan hukum sosial. Sebagai hukum yang mengatur, mengendalikan serta membatasi prilaku manusia.

Secara umum etika terbagi menjadi dua bagian besar yaitu Etika Umum dan Etika Khusus.

1. **Etika Umum** : Etika tentang kondisi dasar dan umum bagaimana manusia harus bertindak secara etis.
2. **Etika Khusus** : Penerapan prinsip-prinsip moral dasar dalam bidang kehidupan khusus.

Etika Khusus dikelompokkan menjadi :

1. **Etika Individual** : Etika yang menyangkut hubungan individu dengan dirinya sendiri.
2. **Etika Sosial** : Etika yang menyangkut hubungan individu dengan lingkup kehidupannya.

Perlu diperhatikan bahwa etika individual dan etika sosial tidak dapat dipisahkan satu sama lain dengan tajam, karena kewajiban manusia terhadap diri sendiri dan sebagai anggota umat manusia saling berkaitan.

Etika sosial menyangkut hubungan manusia dengan manusia baik secara langsung maupun secara kelembagaan (keluarga, masyarakat, negara), sikap kritis terhadpa pandangan-pandangana dunia dan idiologi-idiologi maupun tanggung jawab umat manusia terhadap lingkungan hidup.

Dengan demikian luasnya lingkup dari etika sosial, maka etika sosial ini terbagi atau terpecah menjadi banyak bagian atau bidang. Dan pembahasan bidang yang paling aktual saat ini adalah sebagai berikut :

1. Sikap terhadap sesama
2. Etika keluarga
3. Etika profesi
4. Etika politik
5. Etika lingkungan
6. Etika idiologi

Sistem Penilaian Etika :

- Titik berat penilaian etika sebagai suatu ilmu, adalah pada perbuatan baik atau jahat, susila atau tidak susila.
- Perbuatan atau kelakuan seseorang yang telah menjadi sifat baginya atau telah mendarah daging, itulah yang disebut akhlak atau budi pekerti. Budi tumbuhnya dalam jiwa, bila telah dilahirkan dalam bentuk perbuatan namanya pekerti. Jadi suatu budi pekerti, pangkal penilaiannya adalah dari dalam jiwa; dari semasih berupa angan-angan, cita-cita, niat hati, sampai ia lahir keluar berupa perbuatan nyata.
- Burhanuddin Salam, Drs. menjelaskan bahwa sesuatu perbuatan di nilai pada 3 (tiga) tingkat :
  a. **Tingkat pertama**, semasih belum lahir menjadi perbuatan, jadi masih berupa rencana dalam hati, niat.
  b. **Tingkat kedua**, setelah lahir menjadi perbuatan nyata, yaitu pekerti.
  c. **Tingkat ketiga**, akibat atau hasil perbuatan tersebut, yaitu baik atau buruk.

Etika dalam perkembangannya sangat mempengaruhi kehidupan manusia. Etika memberi manusia orientasi bagaimana ia menjalani hidupnya melalui rangkaian tindakan sehari-hari. Itu berarti etika membantu manusia untuk mengambil sikap dan bertindak secara tepat dalam menjalani hidup ini. Etika pada akhirnya membantu kita untuk mengambil keputusan tentang tindakan apa yang perlu kita lakukan dan yang pelru kita pahami bersama bahwa etika ini dapat diterapkan dalam segala aspek atau sisi kehidupan kita, dengan demikian etika ini dapat dibagi menjadi beberapa bagian sesuai dengan aspek atau sisi kehidupan manusianya.

B. PENGERTIAN MORAL

Moral berasal dari bahasa latin “Mos” yang juga berarti adat kebiasaan. Secara etimologis, Moral sama dengan Etika yaitu nilai dan norma yang menjadi pegangan seseorang. Magnis Suseno (1975) mengemukakan hal yang menjadi dasar norma moral untuk mengakui perbuatan baik atau buruk yaitu “Kebiasaan”. Hobbes dan Rousseau seperti dikutip oleh Huijbers (1995) mengemukakan “kesepakatan masyarakat” sebagai dasar pengakuan perbuatan.

Menurut Lowrence Konhberg dalam Wahyono (2006:6) Keenam tahapan perkembangan moral dikelompokkan ke dalam tiga tingkatan: pra-konvensional, konvensional, dan pasca-konvensional.

Tingkat 1 (Pra-Konvensional)

1. Orientasi kepatuhan dan hukuman
2. Orientasi minat pribadi

(*Apa untungnya buat saya?*) *Tingkat 2 (Konvensional)*

3. Orientasi keserasian interpersonal dan konformitas

(*Sikap anak baik*)

4. Orientasi otoritas dan pemeliharaan aturan sosial

(*Moralitas hukum dan aturan*)

Tingkat 3 (Pasca-Konvensional)

5. Orientasi kontrak sosial
6. Prinsip etika universal

(*Principled conscience*)

Pra-Konvensional

Tingkat pra-konvensional dari penalaran moral umumnya ada pada anak-anak, walaupun orang dewasa juga dapat menunjukkan penalaran dalam tahap ini. Seseorang yang berada dalam tingkat pra-konvensional menilai moralitas dari suatu tindakan berdasarkan konsekuensinya langsung. Tingkat pra-konvensional terdiri dari dua tahapan awal dalam perkembangan moral, dan murni melihat diri dalam bentuk egosentris.

Dalam ***tahap pertama***, individu-individu memfokuskan diri pada konsekuensi langsung dari tindakan mereka yang dirasakan sendiri. Sebagai contoh, suatu tindakan dianggap salah secara moral bila orang yang melakukannya dihukum. Semakin keras hukuman diberikan dianggap semakin salah tindakan itu. Sebagai tambahan, ia tidak tahu bahwa sudut pandang orang lain berbeda dari sudut pandang dirinya. Tahapan ini bisa dilihat sebagai sejenis otoriterisme.

Tahap dua menempati posisi *apa untungnya buat saya*, perilaku yang benar didefinisikan dengan apa yang paling diminatinya. Penalaran tahap dua kurang menunjukkan perhatian pada kebutuhan orang lain, hanya sampai tahap bila kebutuhan itu juga berpengaruh terhadap kebutuhannya sendiri, seperti "kamu garuk punggungku, dan akan kugaruk juga punggungmu." Dalam tahap dua perhatian kepada oranglain tidak didasari oleh loyalitas atau faktor yang berifat intrinsik. Kekurangan perspektif tentang masyarakat dalam tingkat pra-konvensional, berbeda dengan kontrak sosial (tahap lima), sebab semua tindakan dilakukan untuk melayani kebutuhan diri sendiri saja. Bagi mereka dari tahap dua, perpektif dunia dilihat sebagai sesuatu yang bersifat relatif secara moral.

Konvensional

Tingkat konvensional umumnya ada pada seorang remaja atau orang dewasa.

Orang di tahapan ini menilai moralitas dari suatu tindakan dengan membandingkannya

dengan pandangan dan harapan masyarakat. Tingkat konvensional terdiri dari tahap ketiga dan keempat dalam perkembangan moral.

Dalam ***tahap tiga***, seseorang memasuki masyarakat dan memiliki peran sosial. Individu mau menerima persetujuan atau ketidaksetujuan dari orang-orang lain karena hal tersebut merefleksikan persetujuan masyarakat terhadap peran yang dimilikinya. Mereka mencoba menjadi seorang *anak baik* untuk memenuhi harapan tersebut, karena telah mengetahui ada gunanya melakukan hal tersebut. Penalaran tahap tiga menilai moralitas dari suatu tindakan dengan mengevaluasi konsekuensinya dalam bentuk hubungan interpersonal, yang mulai menyertakan hal seperti rasa hormat, rasa terimakasih, dan *golden rule*. Keinginan untuk mematuhi aturan dan otoritas ada hanya untuk membantu peran sosial yang stereotip ini. Maksud dari suatu tindakan memainkan peran yang lebih signifikan dalam penalaran di tahap ini; 'mereka bermaksud baik.

Dalam ***tahap empat***, adalah penting untuk mematuhi hukum, keputusan, dan konvensi sosial karena berguna dalam memelihara fungsi dari masyarakat. Penalaran moral dalam tahap empat lebih dari sekedar kebutuhan akan penerimaan individual seperti dalam tahap tiga; kebutuhan masyarakat harus melebihi kebutuhan pribadi. Idealisme utama sering menentukan apa yang benar dan apa yang salah, seperti dalam kasus fundamentalisme. Bila seseorang bisa melanggar hukum, mungkin orang lain juga akan begitu - sehingga ada kewajiban atau tugas untuk mematuhi hukum dan aturan. Bila seseorang melanggar hukum, maka ia salah secara moral, sehingga celaan menjadi faktor yang signifikan dalam tahap ini karena memisahkan yang buruk dari yang baik.

Pasca-Konvensional

Tingkatan pasca konvensional, juga dikenal sebagai tingkat berprinsip, terdiri dari

tahap lima dan enam dari perkembangan moral. Kenyataan bahwa individu-individu adalah

entitas yang terpisah dari masyarakat kini menjadi semakin jelas. Perspektif seseorang harus dilihat sebelum perspektif masyarakat. Akibat 'hakekat diri mendahului orang lain' ini membuat tingkatan pasca-konvensional sering tertukar dengan perilaku pra-konvensional.

Dalam ***tahap lima***, individu-individu dipandang sebagai memiliki pendapat-pendapat dan nilai-nilai yang berbeda, dan adalah penting bahwa mereka dihormati dan dihargai tanpa memihak. Permasalahan yang tidak dianggap sebagai relatif seperti kehidupan dan pilihan jangan sampai ditahan atau dihambat. Kenyataannya, tidak ada pilihan yang pasti benar atau absolut - 'memang anda siapa membuat keputusan kalau yang lain tidak'? Sejalan dengan itu, hukum dilihat sebagai kontrak sosial dan bukannya keputusan kaku. Aturan-aturan yang tidak mengakibatkan kesejahteraan sosial harus diubah bila perlu demi terpenuhinya *kebaikan terbanyak untuk sebanyak-banyaknya orang*. Hal tersebut diperoleh melalui keputusan mayoritas, dan kompromi. Dalam hal ini, pemerintahan yang demokratis tampak berlandaskan pada penalaran tahap lima.

Dalam ***tahap enam***, penalaran moral berdasar pada penalaran abstrak menggunakan prinsip etika universal. Hukum hanya valid bila berdasar pada keadilan, dan komitmen terhadap keadilan juga menyertakan keharusan untuk tidak mematuhi hukum yang tidak adil. Hak tidak perlu sebagai kontrak sosial dan tidak penting untuk tindakan moral *deontis*. Keputusan dihasilkan secara kategoris dalam cara yang absolut dan bukannya secara hipotetis secara kondisional. Hal ini bisa dilakukan dengan membayangkan apa yang akan dilakukan seseorang saat menjadi orang lain, yang juga memikirkan apa yang dilakukan bila berpikiran sama. Tindakan yang diambil adalah hasil konsensus. Dengan cara ini, tindakan tidak pernah menjadi cara tapi selalu menjadi hasil; seseorang bertindak *karena* hal itu benar, dan bukan karena ada maksud pribadi, sesuai harapan, legal, atau sudah disetujui sebelumnya. Walau Kohlberg yakin bahwa tahapan ini

ada, ia merasa kesulitan untuk menemukan seseorang yang menggunakannya secara konsisten. Tampaknya orang sukar, kalaupun ada, yang bisa mencapai tahap enam dari model Kohlberg ini.

Aliran yang digunakan untuk menyatakan perbuatan moral itu baik atau buruk :

1. **Aliran Hedonise** (Aristippus pendiri mazhab Cyrene 400SM, Epicurus 341271 SM)

   Perbuatan manusia dikatan baik apabila menghasilkan kenikmatan atau kebahagiaan bagi dirinya sendiri atau orang lain (perbuatan itu bermanfaat bagi semua orang).
2. **Aliran Utilisme** (Jeremy Bentham 1742-1832, John Struart Mill 1806-1873)

   Perbuatan itu baik apabila bermanfaat bagi manusia, buruk apabila menimbulkan mudharat bagi manusia.
3. **Aliran Naturalisme** (J.J. Rousseau)

   Perbuatan manusia dikatan baik apabila bersifat alami, tidak merusak alam.
4. **Aliran Vitalisme** (Albert Schweizer abad 20)

   Perbuatan baik adalah perbuatan yang menambah daya hidup, perbuatan buruk adalah perbuatan yang mengurangi bahkan merusak daya hidup.

C. PENGERTIAN NORMA

Sony Keraf (1991), ada dua macam norma :

1. Norma Umum

Norma yang memiliki sifat universal, terbagi menjadi tiga :

a. **Norma Sopan Santun** : disebut juga norma etiket adalah norma yang mengatur pola prilaku dan sikap lahiriah manusia.

b. **Norma Hukum** : adalah norma yang dituntut keberlakuannya secara tegas oleh masyarakat karena dianggap perlu dan niscaya demi keselamatan dan kesejahteraan manusia dalam kehidupan bermasyarakat.

c. **Norma Moral** : yaitu aturan mengenai sikap dan prilaku manusia sebagai manusia. Norma ini menyangkut aturan tentang baik-buruknya, adil tidaknya tindakan dan prilaku manusia sejauh dilihat sebagai manusia.

2. Norma Khusus

Aturan yang berlaku dalam bidang kegiatan atau kehidupan khusus misalnya aturan yang berlaku dalam bidang pendidikan, keolahragaan, bidang ekonomi dan sebagainya. Norma ini hanya berlaku pada lingkup bidangnya dan tidak berlaku jika memasuki bidang lainnya.

Berdasarkan Nilai dan Norma yang terkandung didalamnya, Etika dikelompokkan menjadi :

1. Etika Deskriptif

Etika yang berbicara tentang fakta, yaitu nilai dan pola perilaku manusia yang terkait dengan situasi dan realitas yang membudaya dalam masyarakat

2. Etika Normatif

Etika yang memberikan penilaian serta himbauan kepada manusia tentang bagaimana harus bertindak sesuai dengan norma yang berlaku.

Sanksi yang timbul atas pelanggaran Etika :

1. Sanksi Sosial

Berupa teguran dari masyarakat, pengucilan dari masyarakat

2. Sanksi Hukum

Hukum pidana dan hukum perdata.

Sumaryono (1995) mengklasifikasikan moralitas menjadi dua golongan :

1. **Moralitas Obyektif**, moralitas yang melihat perbuatan sebagaimana adanya, terlepas dari segala bentuk modifikasi kehendak bebas pelakunya
2. **Moralitas Subyektif**, moralitas yang melihat perbuatan sebagai dipengaruhi oleh pengetahuan dan perhatian pelakunya, latar belakang, stabilitas emosional dan perlakuan persoanal lainnya.

D. Etika danTeknologi

- Teknologi adalah segala sesuatu yang diciptakan manusia untuk memudahkan pekerjaannya.
- Kehadiran teknologi membuat manusia “kehilangan” beberapa sense of human yang alami. (otomatiasi mesin→refleks/ kewaspadaan melambat)
- Cara orang berkomunikasi, by or by surat, membawa perubahan signifikan, dalam sapaan/tutur kata
- Orang berzakat dengan SMS, implikasi pada silaturahmi yang “tertunda”
- Emosi (“touch”) yang semakin tumpul karena jarak dan waktu semakin bias dalam Teknologi Inf.

PERTEMUAN 2
ETIKA PROFESI

A. Pengertian Profesi

Abdulkadir Muhammad (2001) tentang klasifikasi kebutuhan manusia:

1. Kebutuhan ekonomi
2. Kebutuhan psikis
3. Kebutuhan biologis
4. Kebutuhan pekerjaan

Kebutuhan pekerjaan merupakan kebutuhan yang bersifat praktis untuk memenuhi kebutuhan yang lain.

Thomas Aquinas menyatakan bahwa setiap wujud kerja mempunyai 4 macam tujuan, yaitu:

1. Memenuhi kebutuhan hidup
2. Mengurangi tingkat pengangguran dan kriminalitas
3. Melayani sesama
4. Mengontrol gaya hidup

Profesi merupakan bagian dari pekerjaan, tetapi tidak semua pekerjaan adalah profesi. Profesi adalah suatu pekerjaan yang mengharuskan pelakunya memiliki pengetahuan tertentu yang diperoleh melalui pendidikan formal dan ketrampilan tertentu yang didapat melalui pengalaman bekerja pada orang lain yang terlebih dahulu menguasai ketrampilan tersebut, dan terus memperbaharui ketrampilannya sesuai dengan perkembangan teknologi.

Nilai moral profesi menurut Frans Magnis Suseno (1975) :

- Berani berbuat untuk memenuhi tuntutan profesi
- Menyadari kewajiban yang harus dipenuhi selama menjalankan profesi
- Idealisme sebagai perwujudan makna misi organisasi profesi

B. Ciri-ciri Profesi

Secara umum ada beberapa ciri atau sifat yang selalu melekat pada profesi, yaitu :

1. Adanya pengetahuan khusus, yang biasanya keahlian dan ketrampilan ini dimiliki berkat pendidikan, pelatihan dan pengalaman yang bertahun-tahun.
2. Adanya kaidah dan standar moral yang sangat tinggi. Hal ini biasanya setiap pelaku profesi mendasarkan kegiatannya pada kode etik profesi.
3. Mengabdi pada kepentingan masyarakat, artinya setiap pelaksana profesi harus meletakkan kepentingan pribadi dibawah kepentingan masyarakat.
4. Adanya izin khusus untuk menjalankan suatu profesi. Setiap profesi akan selalu berkaitan dengan kepentingan masyarakat, dimana nilai-nilai kemanusian berupa keselamatan, keamanan, kelangsungan hidup dan sebagainya, maka untuk menjalankan suatu profesi harus terlebih dahulu ada izin khusus.
5. Kaum profesional biasanya menjadi anggota dari suatu profesi.

Gilley Dan Eggland mengutip pendapat Bulle : “Profesi adalah bidang usaha manusia berdasarkan pengetahuan, dimana keahlian dan pengalaman pelakunya diperlukan oleh masyarakat”.

Tercatat ada profesi khusus yang dibedakan dari profesi-profesi pada umumnya:

1. Profesi tertentu yang melibatkan hajat hidup orang banyak, misalnya dokter.

2. Profesi luhur yang merupakan profesi yang menekankan pengabdian kepada masyarakat, misalnya guru, penasehat hukum, pengacara, dll.

Sifat-sifat yang harus dimiliki seorang pelaku profesi:

1. Menguasai ilmu secara mendalam dalam bidangnya.
2. Mampu mengkonversikan ilmu menjadi ketrampilan.
3. Selalu menjunjung tinggi etika dan integritas profesi (kode etik profesi) yang bersangkutan.

C. Pengertian Etika Profesi

Kode Etik yaitu norma atau azas yang diterima oleh suatu kelompok tertentu sebagai landasan tingkah laku sehari-hari di masyarakat maupun di tempat kerja.

Menurut UU No.8 (Pokok-pokok Kepegawaian), Kode Etik Profesi adalah pedoman sikap, tingkah laku dan perbuatan dalam melaksanakan tugas dan dalam kehidupan sehari-hari.

Prinsip-prinsip dasar didalam Etika Profesi :

a. Prinsip Standar Teknis

   Setiap anggota profesi harus melaksanakan jasa profesionalnya yang relevan dengan bidang profesinya.

b. Prinsip Kompetensi

   Setiap anggota profesi harus melaksanakan pekerjaan sesuai jasa profesionalnya dengan kehati-hatian, kompetensi dan ketekunan.

c. Prinsip Tanggung Jawab Profesi

   Dalam melaksanakan tanggungjawabnya, setiap anggota harus menggunakan pertimbangan moral dan profesional.

d. Prinsip Kepentingan Publik

Setiap anggota berkewajiban senantiasa bertindak dalam kerangka pelayanan kepada publik, menghormati kepercayaan publik.

e. Prinsip Integritas

Harus menjungjung tinggi nilai tanggung jawab profesional dengan integritas setinggi mungkin.

f. Prinsip Obyektifitas

Harus menjaga obyektifitas dan bebas dari benturan kepentingan dalam pemenuhan kewajibannya.

g. Prinsip Kerahasiaan

Harus menghormati kerahasiaan informasi yang diperoleh.

h. Prinsip Prilaku Profesional

Harus berprilaku konsisten dengan reputasi profesi yang baik dan menjauhi tindakan yang dapat mendeskreditkan profesinya.

D. Pentingnya Etika Profesi

Kata Etik atau Etika berasal dari bahasa Yunani yaitu Ethos yang berarti Karakter, Watak Kesusilaan atau Adat. Sebagai suatu subyek, Etika akan berkaiatan dengan konsep yang dimiliki oleh individu ataupun kelompok untuk menilai apakah tindakan-tindakan yang telah dikerjakan itu salah atau benar, buruk atau baik.

Menurut Martin (1993), etika didefinisikan sebagai “the discpline which can act as the performance index or reference for our control system”. Dengan demikian, etika akan memberikan semacam batasan maupun standar yang akan mengatur pergaulan manusia di dalam kelompok sosialnya. Dalam pengertiannya yang secara khusus dikaitakan dengan seni pergaualan manusia, etika ini kemudian dirupakan dalam bentuk aturan (kode) tertulis

yang secara sistematik sengaja dibuat berdasarkan prinsip-prinsip moral yang ada. Pada saat yang dibutuhkan akan bisa difungsikan sebagai alat untuk menghakimi segala macam tindakan yang secara logika-rasional umum (common sense) dinilai menyimpang dari kode etik. Dalam pengertiannya yang secara khusus dikaitkan dengan seni pergaulan manusia, etika ini kemudian dirupakan dalam bentuk aturan (code) tertulis yang secara sistematik sengaja dibuat berdasarkan prinsip-prinsip moral yang ada dan pada saat yang dibutuhkan akan bisa difungsikan sebagai alat untuk menghakimi segala macam tindakan yang secara logika-rasional umum (common sense) dinilai menyimpang dari kode etik. Dengan demikian etika adalah refleksi dari apa yang disebut dengan "self control", karena segala sesuatunya dibuat dan diterapkan dari dan untuk kepenringan kelompok sosial (profesi) itu sendiri.

Selanjutnya, karena kelompok profesional merupakan kelompok yang berkeahlian dan berkemahiran yang diperoleh melalui proses pendidikan dan pelatihan yang berkualitas dan berstandar tinggi yang dalam menerapkan semua keahlian dan kemahirannya yang tinggi itu hanya dapat dikontrol dan dinilai dari dalam oleh rekan sejawat, sesama profesi sendiri. Kehadiran organisasi profesi dengan perangkat "built-in mechanism" berupa kode etik profesi dalam hal ini jelas akan diperlukan untuk menjaga martabat serta kehormatan profesi, dan di sisi lain melindungi masyarakat dari segala bentuk penyimpangan maupun penyalah-gunaan kehlian (Wignjosoebroto, 1999).

Oleh karena itu dapatlah disimpulkan bahwa sebuah profesi hanya dapat memperoleh kepercayaan dari masyarakat, bilamana dalam diri para elit profesional 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 semual 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.

E. Etika Komputer

Menurut Moor (1985) dalam bukunya "What is Computer Ethics", Etika Komputer diartikan sebagai bidang ilmu yang tidak terkait secara khusus dengan teori filsafat manapun dan kompatibel dengan pendekatan metodologis yang luas pada pemecahan masalah etis.

Isu-isu pokok etika komputer

1. Kejahatan Komputer

   Kejahatan yang dilakukan dengan komputer sebagai basis teknologinya. Contoh : virus, spam, penyadapan, carding, denial of service (DoS)/melumpuhkan target.

2. Cyber Ethics

   Implikasi dari internet, memungkinkan pengguna IT semakin meluas, tak terpetakan, tak teridentifikasi dalam dunia anonymouse.

3. E-Commerce

   Otomatis bisnis dengan internet dan layanannya, mengubah bisnis proses yang telah ada dari transaksi konvensional kepada yang berbasis teknologi, melahirkan implikasi negatif, bermacam-macam kejahatan, penipuan, kerugian karena ke-anonymouse-an tadi.

4. Pelanggaran Hak Atas Kekayaan Intelektual

   Masalah pengakuan hak atas kekayaan intelektual, pembajakan, cracking, illlegal software dst.

5. Tanggung Jawab Profesi

   Sebagai bentuk tanggung jawab moral, perlu diciptakan ruang bagi komunitas yang akan saling menghormati. Misal IPKIN (Ikatan Profesi Komputer & Informatika-1974)

F. Profesional dan Profesionalisme

Profesional adalah pekerja yang menjalankan profesi. Dalam menjalankan tugas profesi, para profesional harus bertindak objektif, artinya bebas dari rasa malu, sentimen, benci, sikap malas dan enggan bertindak. Dengan demikian seorang profesional harus memiliki profesi tertentu yang diperoleh melalui sebuah proses pendidikan maupun pelatihan yang khusus, dan disamping itu pula ada unsur semangat pengabdian (panggilan profesi) didalam melaksanakan suatu kegiatan kerja. Hal ini perlu ditekankan benar untuk membedakannya dengan kerja biasa (occupation) yang semata bertujuan untuk mencari nafkah dan/atau kekayaan materiil-duniawi.

Kelompok Profesional merupakan kelompok yang berkeahlian dan berkemahiran, yang diperoleh melalui proses pendidikan dan pelatihan yang berkwalitas dan berstandar tinggi, yang dalam menerapkan semua keahlian dan kemahirannya yang tinggi itu hanya dapat dikontrol dan dinilai dari dalam oleh rekan sejawat, sesama prefesi sendiri.

Tiga watak kerja seorang profesional :

1. Kerja seorang profesional itu beritikad untuk merealisasikan kebajikan demi tegaknya kehormatan profesi yang digeluti, dan oleh karenanya tidak terlalu mementingkan atau mengharapkan imbalan upah materiil.
2. Kerja seorang profesional itu harus dilandasi oleh kemahiran teknis yang berkwalitas tinggi yang dicapai melalui proses pendidikan dan/atau pelatihan yang panjang, ekslusif dan berat.

3. Kerja seorang profesional, diukur dengan kualitas teknis dan kualitas moral, harus menundukkan diri pada sebuah mekanisme kontrol berupa kode etik yang dikembangkan dan disepakati bersama didalam sebuah organisasi profesi.

Sifat-sifat pelaku profesi :

1. Menguasai ilmu secara mendalam dalam bidangnya
2. Mampu mengkonversi ilmu menjadi ketrampilan
3. Selalu menjunjung tinggi etika dan integritas profesi

Seseorang yang menjalankan profesinya secara benar dan melakukannya menurut etika dan garis-garis profesionalisme yang berlaku dalam profesinya disebut seorang yang profesional.

Sikap-sikap yang dituntut untuk menjadi seorang profesional:

1. Komitmen tinggi
2. Tanggung jawab
3. Berpikir sistematis
4. Penguasaan materi
5. Menjadi bagian masyarakat profesional

Profesionalisme adalah ide, aliran, isme yang bertujuan mengembangkan profesi agar profesi dilaksanakan oleh profesional dengan mengacu kepada norma-norma standar dan kode etik serta memberikan layanan terbaik kepada klien.

Istilah profesionalisme berarti adalah suatu paham terkait profesi, yang juga berarti bahwa nilai-nilai profesional harus menjadi bagian dari jiwa seorang pelaku profesi. Gilley

Dan Eggland menetapkan 4 perspektif pendekatan untuk mengukur profesionalisme seseorang, yaitu:

1. Pendekatan berorientasi filosofis

   Pendekatan berorientasi filosofis melihat 3 hal pokok untuk mengetahui tingkat perofesionalisme seseorang:

   a. Pendekatan lambang profesional : sertifikat, lisensi, akreditasi
   b. Pendekatan sikap individu : individu yang profesional adalah individu yang memberikan pelayanan yang memuaskan dan bermanfaat bagi pengguna jasa profesi tersebut.
   c. Pendekatan electic : bahwa proses profesional dianggap sebagai kesatuan dari kemampuan, hasil kesepakatan, dan standar tertentu.

2. Pendekatan perkembangan bertahap

   Enam orientasi perkembangan ke arah profesional:

   a. Berkumpulnya individu-individu yang memiliki minat yang sama terhadap suatu profesi.
   b. Melakukan identifikasi dan adopsi terhadap ilmu pengetahuan tertentu untuk mendukung profesi yang dijalaninya.
   c. Membentuk organisasi formal yaitu organisasi profesi.
   d. Membuat kesepakatan mengenai persyaratan profesi berdasarkan pengalaman atau kualifikasi tertentu.
   e. Menentukan kode etik profesi.
   f. Revisi persyaratan profesi sesuai tuntutan tingkat pelayanan kepada para pengguna jasa profesi yang bersangkutan.

3. Pendekatan berorientasi karakteristik

   Orientasi ini melihat bahwa proses profesional juga dapat ditinjau dari karakteristik-karakteristik profesi, yaitu:

   a. Kode etik profesi
   b. Pengetahuan yg terorganisir yg mendukung pelaksanaan profesi
   c. Keahlian dan kompetensi yg bersifat khusus
   d. Tingkat pendidikan minimal dari sebuah profesi
   e. Sertifikat keahlian yg harus dimiliki sbg lambang profesional
   f. Proses tertentu sblm memangku profesi misalnya pendidikan, ujian, dan pekerjaan
   g. Diseminasi dan pertukaran ide di antara anggota
   h. Adanya tindakan disiplin dan batasan tertentu jika terjadi malpraktek dan pelanggaran kode etik profesi

4. Pendekatan berorientasi non-tradisional

   Pendekatan berorientasi non-tradisional menyatakan bahwa seseorang dengan bidang ilmu tertentu diharapkan mampu melihat dan merumuskan karakteristik yang unik dan kebutuhan sebuah profesi. Orientasi ini memandang perlunya dilakukan identifikasi elemen-elemen penting untuk sebuah profesi, misalnya standarisasi profesi untuk menguji kelayakannya dengan kebutuhan lapangan, sertifikasi profesional, dll.

Prinsip-prinsip yang menjadi tanggung jawab seorang profesional :

1. Prinsip Holistic (keseluruhan)

   Profesioanal memperhatikan keseluruhan sistem komponen-komponen dari jasa/praktek yang diberikannya agar dapat menghindari dampak negatif terhadap salah satu atau beberapa komponen yang terkait dengan sistem tersebut.

2. Prinsi Optimal (terbaik)

   Profesional selalu memberikan jasa/prakteknya yang terbaik bagi perusahaan.

3. Prinsip Life Long Learner (belajar sepanjang hidup)

   Profesional selalu belajar sepanjang hidupnya untuk menjaga wawasan dan ilmu pengetahuan sekaligus mengembangkannya sehingga dapat memberikan jasa/prakteknya yang lebih berkwalitas daripada sebelumnya.

4. Prinsip Integrity (kejujuran)

   Profesional menjunjung tinggi nilai-nilai kejujuran serta bertanggungjawab atas integritas (kemurnian) pekerjaan atau jasanya.

5. Prinsip Sharp (berpikir tajam)

   Profesional selalu cepat tanggap terhadap permasalahan yang ada dalam jasa/praktek yang diberikannya, sehingga dapat menyelesaikan masalah tersebut secara cepat dan tepat.

6. Prinsip Team Work (kerjasama)

   Profesional mampu bekerja sama dengan profesional lainnya untuk mencapai suatu obyektifitas.

7. Prinsip Innovation (inovasi)

   Profesional selalu berfikir atau belajar untuk mengembangkan kreatiivitasnya agar dapat mengemukakan ide-ide baru sehingga mampu menciptakan peluang-peluang yang baru atas jasa/praktek yang diberikannya.

8. Prinsip Communication (komunikasi)

   Profesional mampu berkomunikasi dengan baik dan benar sehingga dapat menyampaikan obyektifitas pembicaraan yang dimaksudkan secara tepat.

PERTEMUAN 3
PROFESIONALISME KERJA BIDANG IT

A. Gambaran Umum Pekerjaan Bidang IT

TI merupakan teknologi yang berkembang secara revolusioner (seperti pada hardware) maupun bersifat evolusioner (seperti pada software) sehingga menuntut pelaku profesionalisme TI untuk selalu mengikuti perkembangannya.

Dalam menjalankan profesinya, seorang TI memiliki prasyaratan profesionalisme spt:

a. Dasar ilmu yang kuat dibidangnya
b. Penguatan kiat-kiat profesi yang dilakukan berdasarkan riset dan praktis, bukan konsep/teori belaka.
c. Pengembangan kemampuan profesional berkesinambungan.

Penyebab rendahnya profesionalisme pekerja dibidang TI:

a. Masih banyak pekerja di bidang TI yang tidak menekuni profesinya secara total / sekedar sambilan.
b. Belum adanya konsep yang jelas dan terdefinisi tentang norma dan etika profesi pekerja dibidang TI.
c. Masih belum ada (mungkin) organisasi profesional yang menangani para profesional dibidang TI.

B. Kompetensi Bidang TI

Kompetensi profesionalisme dibidang IT, mencakupi beberapa hal :

1. Ketrampilan Pendukung Solusi IT
    - Instalasi dan konfigurasi sistem operasi (windows atau linux)
    - Memasang dan konfigurasi mail server, FTP server dan web server
    - Menghubungkan perangkat keras

- Programming

2. Ketraampilan Pengguna IT
    - Kemampuan pengoperasian perangkat keras
    - Administer dan konfigurasi sistem operasi yang mendukung network
    - Administer perangkat keras
    - Administer dan mengelola network security
    - Administer dan mengelola database
    - Mengelola network security
    - Membuat aplikasi berbasis desktop atau web dengan multimedia
3. Pengetahuan di Bidang IT
    - Pengetahuan dasar perangkat keras, memahami organisasi dan arsitektur komputer
    - Dasar-dasar telekomunikasi, mengenal perangkat keras komunikasi data serta memahami prinsip kerjanya
    - Bisnis internet, mengenal berbagai jenis bisnis internet.

C. Kelompok Bidang Teknologi Informasi

Dengan posisi tenaga kerja di bidang Teknologi Informasi (TI) yang sangat bervariasi karena menyesuaikan dengan skala bisnis dan kebutuhan pasar, maka sangat sulit untuk mencari standardisasi pekerjaan di bidang ini. Tetapi setidaknya kita dapat mengklasifikasikan tenaga kerja di bidang Teknologi Informasi tersebut berdasarkan jenis dan kualifikasi pekerjaan yang ditanganinya. Berikut ini adalah penggolongan pekerjaan di bidang teknologi informasi yang berkembang belakangan ini.

Secara umum, pekerjaan di bidang Teknologi Informasi setidaknya terbagi dalam 4 kelompok sesuai bidang pekerjaannya.

a. ***Kelompok Pertama***, adalah mereka yang bergelut di dunia perangkat lunak (software) baik mereka yang merancang sistem operasi, database maupun sistem aplikasi. Pada lingkungan kelompok ini terdapat pekerjaan-pekerjaan seperti misalnya :

   - Sistem analis, merupakan orang yang bertugas menganalisa sistem yang akan diimplementasikan, mulai dari menganalisa sistem yang ada, tentang kelebihan dan kekurangannya, sampai studi kelayakan dan desain sistem yang akan dikembangkan.
   - Programmer, merupakan orang yang bertugas mengimplementasikan rancangan sistem analis yaitu membuat program (baik aplikasi maupun sistem operasi) sesuai sistem yang dianalisa sebelumnya.
   - Web designer adalah orang yang melakukan kegiatan perecanaan, termasuk studi kelayakan, analisis dan desain terhadap suatu proyek pembuatan aplikasi berbasis web.

- Web programmer orang yang bertugas mengimplementasikan rancangan web designer yaitu membuat program berbasis web sesuai desain yang telah dirancang sebelumnya.
- dan lain-lain.

b. ***Kelompok kedua***, adalah mereka yang bergelut di perangkat keras (hardware). Pada lingkungan kelompok ini terdapat pekerjaan-pekerjaan seperti :
   - Technical enginer, sering juga disebut sebagai teknisi yaitu orang yang berkecimpung dalam bidang teknik baik mengenai pemeliharaan maupun perbaikan perangkat sistem komputer.
   - Networking Engineer, adalah orang yang berkecimpung dalam bidang teknis jaringan komputer dari maintenance sampai pada *troubleshooting*-nya.
   - dan lain-lain.

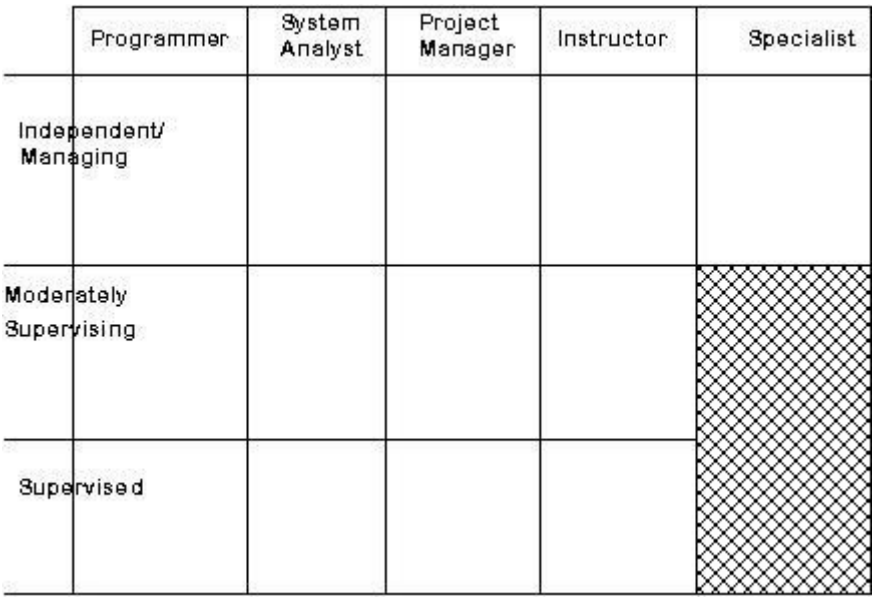
c. ***Kelompok ketiga***, adalah mereka yang berkecimpung dalam operasional sistem informasi. Pada lingkungan kelompok ini terdapat pekerjaan-pekerjaan seperti :
   - EDP Operator, adalah orang yang bertugas untuk mengoperasikan program-program yang berhubungan dengan *electronic data processing* dalam lingkungan sebuah perusahaan atau organisasi lainnya.
   - System Administrator, merupakan orang yang bertugas melakukan administrasi terhadap sistem, melakukan pemeliharaan sistem, memiliki kewenangan mengatur hak akses terhadap sistem, serta hal-hal lain yang berhubungan dengan pengaturan operasional sebuah sistem.
   - MIS Director, merupakan orang yang memiliki wewenang paling tinggi terhadap sebuah sistem informasi, melakukan manajemen terhadap sistem

tersebut secara keseluruhan baik hardware, software maupun sumber daya manusianya.

- dan lain-lain

d. ***Kelompok yang keempat***, adalah mereka yang berkecimpung di pengembangan bisnis Teknologi Informasi. Pada bagian ini, pekerjaan diidentifikasikan oleh pengelompokan kerja di berbagai sektor di industri Teknologi Informasi.

Model SEARCC untuk pembagian job dalam lingkungan TI merupakan model 2 dimensi yang mepertimbangkan jenis pekerjaan dan tingkat keahlian ataupun tingkat pengetahuan yang dibutuhkan. Model sel tersebut dapat digambarkan seperti pada gambar di bawah ini.



Dari gambar diatas, dapat dilihat jenis pekerjaan di bidang TI yang antara lain meliputi :

- ***Programmer***

  Merupakan bidang pekerjaan untuk melakukan pemrograman komputer terhadap suatu sistem yang telah dirancang sebelumnya. Jenis pekerjaan ini memiliki 3 tingkatan yaitu :

  1. *Supervised* (terbimbing). Tingkatan awal dengan 0-2 tahun pengalaman, membutuhkan pengawasan dan petunjuk dalam pelaksanaan tugasnya.
  2. *Moderately supervised* (madya). Tugas kecil dapat dikerjakan oleh mereka tetapi tetap membutuhkan bimbingan untuk tugas yang lebih besar, 3-5 tahun pengalaman
  3. *Independent/Managing* (mandiri). Memulai tugas, tidak membutuhkan bimbingan dalam pelaksanaan tugas.

- ***System Analyst* (Analis Sistem)**

  Merupakan bidang pekerjaan untuk melakukan analisis dan desain terhadap sebuah sistem sebelum dilakukan implementasi atau pemrograman lebih lanjut. Analisis dan desain merupakan kunci awal untuk keberhasilan sebuah proyek-proyek berbasis komputer. Jenis pekerjaan ini juga memiliki 3 tingkatan seperti halnya pada programmer.

- ***Project Manager* (Manajer Proyek)**

  Pekerjaan untuk melakukan manajemen terhadap proyek-proyek berbasis sistem informasi. Level ini adalah level pengambil keputusan. Jenis pekerjaan ini juga memiliki 3 tingkatan seperti halnya pada programmer, terhgantung pada kualifikasi proyek yang dikerjakannya.

- ***Instructor* (Instruktur)**

  Berperan dalam melakukan bimbingan, pendidikan dan pengarahan baik terhadap anak didik maupun pekerja level di bawahnya. Jenis pekerjaan ini juga memiliki 3 tingkatan seperti halnya pada programmer.

- ***Specialist.***

  Pekerjaan ini merupakan pekerjaan yang membutuhkan keahlian khusus. Berbeda dengan pekerjaan-pekerjaan yang lain, pekerjaan ini hanya memiliki satu level saja yaitu *independent* (*managing*), dengan asumsi bahwa hanya orang dengan kualifikasi yang ahli dibidang tersebut yang memiliki tingkat profesi spesialis. Pekerjaan spesialis menurut model SEARCC ini terdiri dari :

  - Data Communication
  - Database Security
  - Quality Assurances
  - IS Audit
  - System Software Support
  - Distributed System
  - System Integration

D. Sertifikasi

Dalam mempertanggungjawabkan kemampuan menjalankan pekerjaan dibidang TI, perlu standarisasi dari sebuah profesi. Cara yang ditempuh adalah melalui sertifikasi, sebagai lambang sebuah profesionalisme.

Beberapa manfaat sertifikasi :

a. Ikut berperan dalam menciptakan lingkungan kerja yang lebih profesional.

b. Pengakuan resmi pemerintah tentang tingkat keahlian individu terhadap sebuah profesi.

c. Pengakuan dari organisasi profesi sejenis (benchmarking), baik pada tingkat regional/internasional.

d. Membuka akses lapangan pekerjaan scr nasional, regional/internasional.

e. Memperoleh peningkatan karier dan pendapatan sesuai perimbangan dengan pedoman skala yang diberlakukan.

Sertifikasi internasional untuk profesi bidang TI relatif pada lingkungan terbatas dan biasanya dikeluarkan berkaitan dengan produk software atau hardware dari perusahaan tertentu, seperti Microsoft, Oracle, Cisco, dll. Pelaksanaan sertifikasi diselenggarakan oleh perusahaan tersebut / lembaga yang ditunjuk sebagai afiliasi, tentunya dengan biaya yang cukup mahal.

Beberapa contoh sertifikasi yang berorientasi produk:

a) Sertifikasi Microsoft

- MCDST (Microsoft Certified Desktop Support Technicians)
- MCSA (Microsoft Certified System Administrations)
- MCSE (Microsoft Certified Systems Engineers)
- MCDBA (Microsoft Certified Database Administations)
- MCT (Microsoft Certified Trainers)
- MCAD (Microsoft Certified Application Developers)
- MCSD (Microsoft Certified Solution Developers)
- Office Specialist (Microsoft Office Specialist)

b) Sertifikasi Oracle

- OCA (Oracle Certified Associate)
- OCP (Oracle Certified Professional)
- OCM (Oracle Certified Master)

c) Sertifikasi Cisco

- CCNA (Cisco Certified Networking Associate)
- CCNP (Cisco Certified Networking Professional)
- CCIA (Cisco Certified Internetworking Expert)

d) Sertifikasi Novell

- Novel CLP (Novel Certified Linux Professional)
- Novel CLE (Novel Certified Linux Engineer)
- Suse CLP (SUSE Certified Linux Professional)
- MCNE (Master Certified Novell Engineer)

Selain sertifikasi yang berorientasi produk, adapula sertifikasi yang tidak berorientasi pada produk.

Beberapa sertifikasi yang berorientasi pd pekerjaan / profesi:

a) Institut for Certification of Computing Professionals (ICCP): Badan Sertifikasi Teknologi Informasi di Amerika

   CDP (Certified Data Processor)

   CCP (Certified Computer Programmer)

   CSP (Certfied Systems Professional)

b) Computing Technology Industry Association (CompTIA): Asosiasi Industri Teknologi Komputer di Amerika

   A+ (Entry Level Computer Services)

Networks+ (Networks Support and Administration)

Security+ (Computer and Information Security)

HTI+ (Home Technology Installation)

IT Project+ (IT Project Management)

Hambatan pelaksanaan sertifikasi :

1. Biaya mahal, untuk mengikuti sertifikasi berstandar internasional dibutuhkan biaya kurang lebih 150 USD, itupun belum tentu lulus.
2. Kemampuan yang kurang memadai terhadap penguasaan materi sertifikasi
3. Dibutuhkan pengetahuan dan kemampuan diatas rata-rata untuk lulus sertifikasi.

PERTEMUAN 4
CYBERCRIME

A. Pengertian Cybercrime

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis *internet* dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalau dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (*cyber crime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat.

Pada awalnya cybercrime didefinisikan sebagai kejahatan komputer. Menurut Mandell dalam suhariyanto (2012:10) disebutkan ada dua kegiatan computer crime :

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembuanyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan.

Pada dasarnya cybercrime meliputi tindak pidana yang berkenaan dengan sistem informasi itu sendiri juga sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

B. Karakteristik Cybercrime

Karakteristik cybercrime yaitu :

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut dilakukan dalam ruang/wilayah cyber sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan melintas batas negara.

C. Bentuk-Bentuk Cybercrime

Klasifikasi kejahatan komputer :

1. Kejahatan yang menyangkut data atau informasi komputer
2. Kejahatan yang menyangkut program atau software komputer
3. Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya
4. Tindakan yang mengganggu operasi komputer
5. Tindakan merusak peralatan komputer atau yang berhubungan dengan komputer atau sarana penunjangnya.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

1. Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi *Internet*/intranet.

Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa *website* milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, *hacker* juga telah berhasil menembus masuk ke dalam *data base* berisi data para pengguna jasa *America Online* (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang *e- commerce* yang memiliki tingkat kerahasiaan tinggi (*Indonesian Observer*, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para *hacker*, yang mengakibatkan tidak berfugsinya situs ini beberapa waktu lamanya.

2. Illegal Contents

Merupakan kejahatan dengan memasukkan data atau informasi ke *Internet* tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang

merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

3. Data Forgery

Merupakan kejahatan dengan memalsukan data pada dokumendokumen penting yang tersimpan sebagai *scripless document* melalui *Internet*. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

4. Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan *internet* untuk melakukan kegiatan matamata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

5. Cyber Sabotage and Extortion

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan *Internet*. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak

berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6. Offense against Intellectual Property

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di *Internet*. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di *Internet* yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. Infringements of Privacy

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

D. Contoh Cybercrime

Hacker dan Cracker

Menurut mansfield, hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi.

Sedangkan cracker adalah sisi gelap dari hacker dan memiliki ketertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer.

Penggolongan Hacker dan Cracker

- Recreational Hackers : kejahatan yang dilakukan oleh netter tingkat pemula untuk sekedar mencoba kekurang handalan sistem sekuritas suatu perusahaan.
- Cracker/Criminal Minded Hackers : pelaku memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase dan pengrusakan data. Tipe kejahatan ini dapat dilakukan dengan bantuan orang dalam.
- Political Hackers : aktifis politis (hacktivist) melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendisskreditkan lawannya.

Denial Of Service Attack

Didalam keamanan komputer, Denial of Service Attack (DoS Attack) adalah suatu usaha untuk membuat suatu sumber daya komputer yang ada tidak bisa digunakan oleh para pemakainya. Secara khas target adalah high-profile web server, serangan ini mengarahkan menjadikan host halaman web tidak ada di internet. Hal ini merupakan kejahatan komputer yang melanggar kebijakan penggunaan internet yang diindikasikan oleh internet arsitecture broad (IAB).

Denial of Service Attack mempunyai dua format umum :

1. Memaksa komputer-komputer korban untuk mereset atau korban tidak bisa lagi menggunakan perangkat komputernya seperti yang diharapkannya.

2. Menghalangi media komunikasi antara para pemakai dan korban sehingga mereka tidak bisa lagi berkomunikasi.

Deniel of Service Attack ditandai oleh suatu usaha eksplisit dengan penyerang untuk mencegah para pemakai memberi bantuan dari penggunaan jasa tersebut. Contoh meliputi :

1. Mencoba untuk "membanjiri" suatu jaringan, dengan demikian mencegah lalu lintas jaringan yang ada.
2. Berusaha untuk mengganggu koneksi antara dua mesin, dengan demikian mencegah akses kepada suatu service.
3. Berusaha untuk mencegah individu tertentu dari mengakses suatu service.
4. Berusaha untuk mengganggu service kepada suatu orang atau sistem spesifik.

Pelanggaran Piracy

Piracy adalah kemampuan dari suatu individu atau kelompok untuk memelihara urusan pribadi dan hidup mereka ke luar dari pandangan publik, atau untuk mengendalikan alir informasi tentang diri mereka.

Pembajakan software aplikasi dan lagu dalam bentuk digital (MP3, MP4, WAV dll) merupakan trend dewasa ini, software dan lagu dapat dibajak melalui download dari internet dan dicopy ke dalam CD room yang selanjutnya diperbanyak secara ilegal dan diperjual belikan secara ilegal.

Fraud

Meruapakan kejahatan manipulasi informasi dengan tujuan mengeruk keuntungan yang sebesar-besarnya. Biasanya kejahatan yang dilakukan adalah memanipulasi informasi

keuangan. Sebagai contoh adanya situs lelang fiktif. Melibatkan berbagai macam aktivitas yang berkaitan dengan kartu kredit. Carding muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Gambling

Perjuadian tidak hanya dilakukan secara konfensional, akan tetapi perjuadian sudah marak didunia cyber yang berskala global. Dari kegiatan ini dapat diputar kembali dinegara yang merupakan "tax heaven", seperti cyman island yang merupakan surga bagi money laundering.

Jenis-jenis online gambling antara lain :

1. Online Casinos

   Pada online casinos ini orang dapat bermain Rolet, Blackjack, Cheap dan lain-lain.

2. Online Poker

   Online Poker biasanya menawarkan Texas hold 'em, Omaha, Seven-card stud dan permainan lainnya.

3. Mobile Gambling

   Merupakan perjuadian dengan menggunakan wereless device, seperti PDAs, Wereless Tabled PCs. Beberapa casino online dan poker online menawarkan pilihan mobil. GPRS, GSM Data, UMTS, I-Mode adalah semua teknologi lapisan data atas nama perjudian gesit tergantung.

Pornography dan Paedophilia

Pornography merupakan jenis kejahatan dengan menyajikan bentuk tubuh tanpa busana, erotis, dan kegiatan seksual lainnya, dengan tujuan merusak moral. Dunia cyber selain mendatangkan kemudahan dengan mengatasi kendala ruang dan waktu, juga telah menghadirkan dunia pornografi melalui news group, chat rooms, dll. Penyebarluasan

obscene materials termasuk pornography, indecent exposure. Pelecehan seksual melalui e-mail, websites atau chat programs atau biasa disebut cyber harrassment.

Data Forgery

Kejahatan ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di Internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database. Dokumen tersebut disimpan sebagai scriptless documen dengan menggunakan media internet.

E. Istilah-istilah dalam Cybercrime

Probing : aktivitas yang dilakukan untuk melihat service-service apa saja yang tersedia di server target.

Pishing : email penipuan yang seakan-akan berasal dari sebuah toko, bank atau perusahaan kartu kredit. Email ini mengajak anda untuk melakukan berbagai hal, misalnya memverifikasi informasi kartu kredit, mengupdate password dan lainnya.

Cyber Espionage :kejahatan yang memanfaatkan internet untuk melakukan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasaran.

Offence Against Intelectual Property : kejahatan yang ditunjukkan terhadap HAKI yang dimiliki pihak lain di Internet.

F. Wajah Kasus Indonesia

- Money Laundering erat kaitannya dengan kegiatan mentransfer dana. Kegiatan transfer dana itu sendiri saat ini banyak dilakukan dengan menggunakan teknologi, semacam wire transfer, ATM, dan masih banyak lagi. Bahkan saat ini metode transfer dana yang banyak digunakan karena sangat cepat adalah dengan menggunakan RTGS (Real Time Gross Settlement)

- Ketika krisis di Timor-Timur sempat terjadi peperangan antara hacker indonesia dan australia. Serta ketika hubungan Indonesia dan Malaysia yang memanas karena masalah perbatasan. Beberapa situs pemerintah Malaysia sempat didevace oleh Hakcer Indonesia, dan dari Malayasia juga membalas dengan mendevace situs pemerintah daerah di Indonesia
- Dani Firmansyah, konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di http://tnp.kpu.go.id dan mengubah nama-nama partai di dalamnya menjadi nama-nama "unik", seperti Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan lain sebagainya. Dani menggunakan teknik SQL Injection(pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari Kamis, 22 April 2004

PERTEMUAN V

KEBIJAKAN HUKUM CYBERCRIME

A. Pendahuluan

Ada beberapa ruang lingkup cyberlaw yang memerlukan perhatian serius di Indonesia saat ini yakni:

- Kriminalisasi Cyber Crime atau kejahatan di dunia maya.
- Aspek Pembuktian.
- Aspek Hak Atas Kekayaan Intelektual di cyberspace.
- Standardisasi di bidang telematika.
- Aturan-aturan di bidang E-Bussiness .
- Aturan-aturan di bidang E-Government.
- Aturan tentang jaminan keamanan dan kerahasiaan Informasi
- Yurisdiksi hukum.

Untuk menegakkan hukum serta menjamin kepastian hukum di Indonesia perlu adanya Cyber Law yaitu Hukum yang membatasi kejahatan siber (kejahatan dunia maya melalui jaringan internet), yang dalam Hukum Internasional terdapat 3 jenis Yuridis yaitu (The Juridiction to Prescribe) *Yuridis untuk menetapkan undang-undang, (*The Juridicate to Enforce) *Yuridis untuk menghukum* dan (The Jurisdiction to Adjudicate) *Yuridis untuk menuntut.*

The Jurisdiction to Adjudicate terdapat beberapa asas yaitu:

a. Asas Subjective Territorial

   berlaku hukum berdasarkan tempat pembuatan dan penyelesaian tindak pidana dilakukan di Negara lain,

b. Asas Objective Territorial

hukum yang berlaku adalah akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi Negara yang bersangkutan,

c. Asas Natonality

hukum berlaku berdasarkan kewarganegaraan pelaku,

d. Asas PassiveNatonality

Hukum berlaku berdasarkan kewarganegaraan korban,

e. Asas Protective Principle

Berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar wilayahnya,

f. Asas Universality

Berlaku untuk lintas Negara terhadap kejahatan yang dianggap sangat serius seperti pembajakan dan terorisme (*crime against humanity*).

B. Pengertian Cyberlaw

Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindakan (prilaku) seseorang dan masyarakat dimana akan ada sangsi bagi yang melanggar. Alasan cyberlaw itu diperlunya menurut Sitompul (2012:39) sebagai berikut :

1. Masyarakat yang ada di dunia virtual ialah masyarakat yang berasal dari dunia nyata yang memiliki nilai dan kepentingan
2. Meskipun terjadi di dunia virtual, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata.

Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya) yang umumnya diasosiasikan dengan internet.

Cyberlaw merupakan aspek hukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan

memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya.

C. Ruang Lingkup Cyberlaw

Jonathan Rosenoer dalam Cyberlaw, the law of internet mengingatkan tentang ruang lingkup cyberlaw diantaranya :

- Hak Cipta (Copy Right)
- Hak Merk (Trade Mark)
- Pencemaran nama baik (Defamation)
- Fitnah, Penistaan, Penghinaan (Hate Speech)
- Serangan terhadap fasilitas komputer (Hacking, Viruses, Illegal Access)
- Pengaturan sumber daya internet seperti IP-Address, domain name
- Kenyamanan individu (Privacy)
- Prinsip kehati-hatian (Duty Care)
- Tindakan kriminal biasa menggunakan TI sebagai alat
- Isu prosedural seperti yuridiksi, pembuktian, penyelidikan dll
- Kontrak/transaksi elektronik dan tandatangan digital
- Pornografi
- Pencurian melalui internet
- Perlindungan konsumen
- Pemanfaatan internet dalam aktivitas keseharian seperti e-commerce, e-goverment, e-education, dll.

D. Pengaturan Cybercrimes dalam UUITE

Saat ini di Indonesia telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber, UU RI tentang Informasi dan Transaksi Elektronik no 11 th 2008 , yang terdiri dari 54 pasal dan disahkan tgl 21 April 2008, yang diharapkan bisa mengatur segala urusan dunia Internet (siber), termasuk didalamnya memberi punishment terhadap pelaku cybercrime.

Rangkuman dari muatan UU ITE adalah sebagai berikut:

- Tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai). Sesuai dengan e-ASEAN Framework Guidelines (pengakuan tanda tangan digital lintas batas)
- Alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHP
- UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia yang memiliki akibat hukum di Indonesia
- Pengaturan Nama domain dan Hak Kekayaan Intelektual
- Perbuatan yang dilarang (cybercrime) dijelaskan pada Bab VII (pasal 27-37):

  -Pasal 27 (Asusila, Perjudian, Penghinaan, Pemerasan)

  -Pasal 28 (Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan)

  -Pasal 29 (Ancaman Kekerasan dan Menakut-nakuti)

  -Pasal 30 (Akses Komputer Pihak Lain Tanpa Izin, Cracking)

  -Pasal 31 (Penyadapan, Perubahan, Penghilangan Informasi)

  -Pasal 32 (Pemindahan, Perusakan dan Membuka Informasi Rahasia)

  -Pasal 33 (Virus?, Membuat Sistem Tidak Bekerja (DOS?))

  -Pasal 35 (Menjadikan Seolah Dokumen Otentik(phising?))

Ada hal pokok yang bisa kita pegang dalam Undang-Undang ini.

Dalam Undang-Undang ini pada Pasal 1 yang dimaksud dengan:

1. Informasi Elektronik

   Satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

2. Transaksi Elektronik

   Perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

3. Teknologi Informasi

   Suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

4. Dokumen Elektronik

   Setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Sistem Elektronik

   Serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

6. Penyelenggaraan Sistem Elektronik

   Adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan

Usaha, dan/atau masyarakat.

7. Jaringan Sistem Elektronik

   Terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.

8. Agen Elektronik

   Perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.

9. Sertifikat Elektronik

   Sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

10. Penyelenggara Sertifikasi Elektronik

    Adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.

11. Lembaga Sertifikasi Keandalan

    Lembaga independen yang dibentuk oleh profesional yang diakui, disahkan,dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.

1. Tanda Tangan Elektronik

   Tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

13. Penanda Tangan

    Subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.

14. Komputer

Alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

15. Akses

Kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.

16. Kode Akses

Angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.

17. Kontrak Elektronik

Perjanjian para pihak yang dibuat melalui Sistem Elektronik.

18. Pengirim

Subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.

19. Penerima

Subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.

20. Nama Domain

Alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.

21. Orang

Orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.

22. Badan Usaha

Perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.

23. Pemerintah

Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Untuk siapakah undang-undang ini berlaku ??

Dalam Pasal 2

Undang- undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

ASAS-ASAS

pasal 3

a. Asas Kepastian Hukum
b. Asas Manfaat
c. Asas kehati-hatian
d. Asas iktikad baik, dan
e. Asas kebebasan memilih teknologi atau netral teknologi.

Pasal 4, pemanfaatan Teknologi Informasi dan Transaksi Elektronik

Bisa dilaksanakan asal bertujuan untuk :

1. Mencerdaskan kehidupan bangsa,
2. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat,
3. Meningkatkan efektivitas dan efisiensi pelayanan publik,
4. Membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi

Informasi seoptimal mungkin

5. Bertanggung jawab. Terakhir, memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi

Pasal 5 mengatur bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan :

Alat bukti hukum yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia sesuai dengan ketentuan yang diatur dalam Undang-Undang ini, kecuali :

a. Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis;
b. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

pasal 6

Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

pasal 7

Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan.

Untuk waktu pengiriman dan penerimaan diatur pada pasal 8 :

1. Kecuali diperjanjikan lain,
    a. Waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik

ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.

b. Waktu penerimaan suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.

2. Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.
3. Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka:
   a. waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim;
   b. waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

Pasal 9.

Sementara itu, bagi pelaku usaha yang menawarkan produk melalui Sistem Elektronik ada pula payung hukumnya. Yakni, harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Pasal 10

Sertifikasi keandalan dapat dilakukan oleh lembaga Sertifikasi Keandalan untuk setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik.

pasal 11- 14

pengaturan terkait tanda tangan elektronik dan pennyelenggara serftifikasi elektronik

1. Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
   a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
   b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
   c. segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
   d. segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
   e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan
   f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.
2. Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya sekurang-kurangnya meliputi:
   a. sistem tidak dapat diakses oleh Orang lain yang tidak berhak;
   b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;
   c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda

Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:

- Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau
- Keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

3. Untuk pembuatan Tanda Tangan Elektronik, setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik yang mana Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.
4. Penyelenggara Sertifikasi Elektronik terdiri atas: (13)
   a. Penyelenggara Sertifikasi Elektronik Indonesia; berbadan hukum Indonesia dan berdomisili di Indonesia dan
   b. Penyelenggara Sertifikasi Elektronik asing, yang beroperasi di Indonesia harus terdaftar di Indonesia.
5. Penyelenggara Sertifikasi Elektronik harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi: (14. P)
   a. metode yang digunakan untuk mengidentifikasi Penanda Tangan;
   b. hal yang dapat digunakan untuk mengetahui data diri pembuat Tanda Tangan Elektronik; dan
   c. hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik.

pasal 15 – 16 ,

Pengaturan Penyelenggaraan Sistem Elektronik

- diatur pada yaitu Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya dan bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya (kecuali dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik)
- Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum:
    a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
    b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
    c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
    d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
    e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

pasal 17- 22

transaksi elektronik dan hal-hal yang terkait dengan transaksi elektronik

1. Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik ataupun privat, yang mana para pihak yang melakukan Transaksi Elektronik wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.
2. Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak, yang mana para tersebut memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya, tetapi jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.
3. Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik internasional yang dibuatnya, tetapi jika para pihak tidak melakukan pilihan forum maka penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional.
4. Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati, kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima, dan persetujuan atas penawaran Transaksi Elektronik tersebut dilakukan dengan pernyataan penerimaan secara elektronik.
5. Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik, dengan ketentuan ,
   a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik

menjadi tanggung jawab para pihak yang bertransaksi;

b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau
c. jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.

- Segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik. Jika kerugian Transaksi Elektronik disebabkanm gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik,
- Segala akibat hukum menjadi tanggung jawab pengguna jasa layanan. Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan,

6. Ketentuan terkait dengan tanggung jawab penyelenggara agen elektronik tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.
7. Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada Agen Elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.

Berdasarkan surat Presiden RI No.R./70/Pres/9/2005 tanggal 5 September 20015, naskah UUITE secara resmi disampaikan kepada DPR RI. Pada tanggal 21 April 2008, undang-undang ini disahkan.

Dua muatan besar yang diatur dalam UUITE adalah :

1. Pengaturan transaksi elektronik
2. Tindak pidana cyber

Tindak pidana yang diatur dalam UUITE diatur dalam bab VII tentang perbuatan yang dilarang, perbuatan tersebut dikategorikan menjadi kelompok sebagai berikut :

1. Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu :
    a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal (kesusilaan, perjudian, berita bohong, dll)
    b. Dengan cara apapun melakukan akses illegal
    c. Intersepsi illegal terhadap informasi atau dokumen elektronik dan sistem elektronik
2. Tindak pidana yang berhubungan dengan gangguan (interfensi), yaitu :
    a. Ganguan terhadap informasi atau dokumen elektronik
    b. Ganguan terhadap sistem elektronik
3. Tindak pidana memfasilitasi perbuatan yang dilarang
4. Tindak pidana pemalsuan informasi atau dokumen elektronik
5. Tindak pidana tambahan dan
6. Pemberatan-pemberatan terhadap ancaman pidana

E. Celah Hukum Cybercrime

Pada dasarnya sebuah undang-undang dibuat sebagai jawaban hukum terhadap persoalan yang ada di masyarakat. Namun pada pelaksanaannya tak jarang suatu undang-undang yang sudah terbentuk menemui kenyataan yang mungkin tidak terjangkau saat undang-undang dibentuk.

Faktor yang mempengaruhi munculnya kenyataan diatas, yaitu :

1. Keterbatasan manusia memprediksi secara akurat apa yang terjadi dimasa yang akan datang
2. Kehidupan masyarakat manusia baik sebagai kelompok dan bangsa

3. Pada saat undang-undang diundangkan lansung "konservatif"

Menurut suhariyanto (2012) celah hukum kriminalisasi cybercrime yang ada dalam UUITE, diantaranya :

1. Pasal pornografi di internet (cyberporn)
2. Pasal perjudian di internet (gambling online)
3. Pasal penghinaan dan atau pencemaran nama baik di internet
4. Pasal pemerasan dan atau pengancaman melalui internet
5. Penyebaran berita bohong dan penghasutan melalui internet
6. Profokasi melalui internet

Pasal Pornografi di Internet (Cyberporn)

Pasal 27 ayat 1 UUITE berbunyi : "Setiap orang dengan sengaja dan tanpa hak mendistribusiakan dan/atau mentransmisikan dan/atau membuat dapat diaksenya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan"

- Pertama, pihak yang memproduksi dan yang menerima serta yang mengakses tidak terdapat aturannya
- Kedua, definisi kesusilaan belum ada penjelasan batasannya.

Pasal Perjudian di Internet (Gambling Online)

Dalam pasal 27 ayat 2 UUITE berbunyi : "Setiap orang dengan sengaja dan tanpa hak mendistribusiakan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian".

Bagi pihak-pihak yang tidak disebutkan dalam teks pasal tersebut, akan tetapi dalam acara perjudian di internet misalnya : para penjudi tidak dikenakan pidana.

Pasal Penghinaan dan atau Pencemaran Nama Baik di Internet

Pasal 27 ayat 3 berbunyi : "Setiap orang dengan sengaja dan tanpa hak dindistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksenya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik".

Pembuktian terhadap pasal tersebut harus benar-benar dengan hati-hati karena dapat dimanfaatkan bagi oknum yang arogan.

Penyebaran Berita Bohong dan Penghasutan melalui Internet

Pasal 28 ayat 1 berbunyi : "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik".

Pihak yang menjadi korban adalah konsumen dan pelakunya produsen, sementara dilain pihak bisa jadi yang menjadi korban sebaliknya.

Profokasi melalui Internet

Pasal 28 ayat 2 yaitu : "Setiaap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat berdasarkan atas suku, agama, ras dan antar golongan (SARA)".

Dipasal tersebut disebutkan istilah informasi dan tidak dijelaskan informasinya yang seperti apa.

PERTEMUAN VI

ETIKA BERINTERNET

A. Perkembangan Dunia Internet

Internet merupakan kepanjangan dari Interconection Networking atau juga telah menjadi International Networking merupakan suatu jaringan yang menghubungkan komputer di seluruh dunia.

Internet pertama kali dikembangkan oleh salah satu lembaga riset di Amerika Serikat, yaitu DARPA (Defence Advanced Research Projects Agency) pada tahun 1973. Pada saat itu DARPA membangun Interconection Networking sebagai sarana untuk menghubungkan beberapa jenis jaringan paket data seperti CS-net, BIT-net, NSF-net, dll.

Tahun 1972, jaringan komputer yang pertama dihasilkan adalah ARPnet yang telah menghubungkan 40 titik dengan menggunakan FTP. Pada perkembangannya titik yang dihubungkan semakin banyak sehingga NCP tak lagi dapat menampung, lalu ditemukan TCP dan IP.

Tahun 1984, host berkembang menjadi DNS dan tahun 1990 terdapat penambahan aplikasi diantaranya www, wais dan ghoper.

Dari segi penggunaan internetpun mengalami perkembangan mulai dari aplikasi sederhana seperti chatting hingga penggunaan VOIP.

Beberapa alasan mengapa internet memberikan dampak besar dalam segala aspek kehidupan :

a. Informasi di Internet dapat diakses 24 jam
b. Biaya relatif murah dan bahkan gratis
c. Kemudahan akses informasi dalam melakukan transaksi
d. Kemudahan membangun relasi dengan pelanggan

e. Materi dapat di update dengan mudah

f. Pengguna internet telah merambah ke segala penjuru dunia.

Karakteristik dunia maya (menurut Dysson, 1994) :

a. Beroperasi secara virtual/maya

b. Dunia cyber selalu berubah dengan cepat

c. Dunia maya tidak mengenal batas-batas teritorial

d. Orang-orang yang hidup dalam dunia maya dapat melaksanakan aktivitasnya tanpa menunjukkan identitas

e. Informasi didalamnya bersifat publik

B. Pentingnya Etika di Dunia Maya

Perkembangan internet yang begitu pesat menuntut dibuatnya aturan-aturan atau etika beraktivitas didalamnya. Berikut ini adalah beberapa alasan pentingnya etika dalam dunia maya :

a. Pengguna internet berasal dari berbagai negara yang memiliki budaya, bahasa dan adat istiadat yang berbeda

b. Pengguna internet merupakan orang yang hidupdalam anonymous, yang mengharuskan pernyataan identitas asli dalam berinteraksi

c. Bermacam fasilitas di internet memungkinkan seseorang untuk bertindak etis / tidak etis

d. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat yang memungkinkan masuknya ‘penghuni’ baru. Untuk itu mereka perlu diberi petunjuk agar memahami budaya internet.

C. Contoh Etika Berinternet

Netiket atau Nettiquette, adalah etika dalam berkomunikasi menggunakan internet yang ditetapkan oleh IETF (The Internet Enginnering Task Force). IETF adalah sebuah komunitas masyarakat internasional yang terdiri dari para perancang jaringan, operator, penjual dan peneliti yang terkait dengan evolusi arsitektur dan pengoperasian internet.

Berikut salah satu contoh etika yang telah ditetapkan oleh IETF : Netiket One to One Communication adalah kondisi dimana komunikasi terjadi antar individu dalam sebuah dialog. Contoh komunikasi via email. Hal-hal yang dilarang :

a. Jangan terlalu banyak mengutip
b. Perlakukan email secara pribadi
c. Hati-hati dalam menggunakan huruf kapital
d. Jangan membicarakan orang lain
e. Jangan menggunakan CC (carbon copy)
f. Jangan gunakan format HTML
g. Jawablah secara masuk akal

D. Tips Aman Berinternet

Bijak dalam memBerikaN data pribadi di Medsos

Peraturan Perlindungan Data Pribadi (PDP) RI hingga saat ini masih dalam pembahasan, seperti PP 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Institusi atau Perusahaan yang mengelola data base pribadi konsumen atau pengguna yang biasa disebut Data Controller disingkat menjadi DCO. DCO bertanggung jawab melindungi Data Pribadi Konsumen sebagai pemilik data. Setiap perlakuan terhadap Data dari seorang klien harus diberikan secara bebas atau berdasarkan keinginan atau tanpa tekanan dengan kata lain harus dengan persetujuan dan ijin dari klien pemilik Data.

Seorang pengguna sosmed, website atau konsumen ecommerce (Data Subject) memiliki hak privasinya:

1. Agar Data Pribadi (Personal) dihapus (delete) atau diremajakan (up to date);
2. Agar Data Pribadi (Privasi) dilindungi kerahasiaannya seperti informasi yang dapat mengidentifikasi (identifier): Nama, nomor ID, lokasi data, atau identifikasi dari faktor seperti fisik, genetik, mental, agama, sosial, budaya dan ekonomi seseorang
3. Agar perekaman, pengambaran dan analisa atas profile suatu objek harus seijin (consent) Data Subjek tersebut termasuk segala bentuk personalisasi, prediksi mengenai kinerja, pekerjaan, ekonomi, keuangan, kesehatan, referensi personal, interest, hobby, kelakuan, lokasi dan pergerakannya.

Tip Akutabilitas Perusahaan (DCO) Menjaga Data Pribadi Konsumen atau Masyarakat:

1. DCO wajib menjaga Keamanan terhadap Pembocoran Data Pribadi (Data Breach). Jika terjadi musibah pembocoran data harus segera melaporkan dalam waktu 72 jam setelah mengetahui (discovery).
2. DCO memproses data konsumen dengan cara Sah, tidak melanggar hukum, fair (adil) dan transparan terhadap konsumen untuk tujuan spesifik, jelas/eksplisit, valid & sah, sesuai dengan tujuan yang sudah disepakati oleh konsumen.
3. DCO menjamin ketepatan, akurasi data konsumen, tidak kadaluwarsa, up to date terus diperbarui, sesuai tujuan penyimpanan data yang disetujui oleh konsumen.
4. DCO menjamin Lokasi & format penyimpanan atau database disetujui konsumen dan UU yang berlaku.
5. DCO menjaga integritas (tidak rusak dan hilang) data dan kerahasian (confidentiality) data subjek dengan enkripsi, password dll.

Penggunaan Enkripsi Untuk Menjaga Integritas Data

Enkripsi (Encryption) adalahsuatu proses untuk merahasiakan berita agar pihak yang tidak berwenang tidak dapat membaca dan mengerti isi berita. Sebuah konversi dari tulisan yang bisa dibaca manusia (plain text) menjadi tulisan yang diacak (cypher text) menggunakan kunci (key). Namun enkripsi dapat dikembalikan dengan dekripsi (decryption) ke tulisan original (plain text) menggunakan kunci (key).

Kriptanalisis (Cryptanalysis) adalah suatu cara untuk mendapatkan kembali informasi yang telah dienkripsi.Kadang melalui proses berulang kali, (salah satu cara dengan Brute Force Attack yaitu serangan yang mencoba semua kemungkinan rangkaian kunci password) oleh peretas enkripsi. Kunci simetris artinya hanya satu kunci untuk mengunci (enkripsi) dan membuka (dekripsi). Asimetris jika ada dua kunci, kunci privat yang harus selalu disimpan/rahasia dan kunci publik/umum yang diumumkan di website misalnya dan digunakan oleh mitra transaksi anda untuk membuka (dekripsi) transaksi atau berita.

Tip mengapa email atau data transaksi perbankan harus dienkripsi jika ingin aman? Upayakan agar email text atau transaksi itu dijaga:

1. Kerahasiannya (Confidential) terhadap upaya penyadapan;
2. Integritasnya (integrity) agar data tidak diubah, dihapus, diganti;
3. Otentikasi (Authentication) dari data agar pengirim ter verifikasi, tidak anonim dan jelas. Certificate Authority (CA) adalah pihak ketiga yang membuat, memverifikasi publik & private key (kunci privat) untuk menjaga otentikasi pemiliknya.

Tangkis Konten Negatif dan Kecanduan

Konten-konten negatif seperti pornografi banyak berseliweran di Internet dan membahayakan pertumbuhan dan pikiran. Meskipun pemerintah sudah melakukan penyensoran satu situs, namun tumbuh 1000 situs baru, karena sifat Internet yang tanpa batas dan industri pornografi yang booming. Berikut tipnya bagi Orang Tua dan Guru:

1. Mengedukasi agar anak-anak dan remaja menjauhi konten pornografi (namun juga pornoaksi, SARA, narkoba, dunia hitam dark web/deep web). Memberikan rasa tanggung jawab dan kepercayaan agar melakukan halhal yang positif seperti kursus dan kegiatan ekstra kurikuler sekolah, sehingga mereka tidak kecanduan menggunakan konten Internet dan Sosmed.
2. Mendidik anak-anak agar mengetahui bahwa Indonesia adalah negara hukum, yang memiliki hukum dan sangsi terkait pornografi, yang diatur dalam UU Pornografi No 44/2008 dan UU ITE No 11/ 2008. Penyebarluasan muatan yang melanggar kesusilaan, pornografi melalui Internet diatur dalam pasal 27 ayat 1 UU ITE mengenai Perbuatan yang dilarang dan dikenakan pidana penjara hingga enam tahun dan/atau denda hingga Rp 1 milyar.
3. Menemani anak-anak ketika sedang mengakses Internet atau letakan laptop atau perangkat lainnya di tempat yang terjangkau dari pengawasan orang tua.
4. Menggunakan alat pengontrol internet yang aman di gawai dan memonitor apa saja yang si-kecil lakukan di gawainya seperti apa yang ditonton atau games yang dimainkan memanfaatkan fitur Parental Control.
5. Memberi batas waktu bermain Internet kepada anak-anak, untuk mencegah anakanak kecanduan bermain Internet.

Menghindari & menangkal spaM, Malware, ransoMware, virus & spyware :

1. Rajin Update Sistem

   Malware/virus selalu mencari kelemahan (vulnerability) di setiap sistem agar bisa dibobol. Sistem operasi, software anti virus komputer dan smartphone harus diperbarui (update) sesuai rekomendasi pabrik, sehingga sistem keamanan sudah menggunakan sistem yang terbaru dan sudah diuji coba terhadap malware versi sebelumnya
2. Gunakan & Update Anti Virus (AV)/ Anti Spam atau Anti Spyware/Worm untuk PC,

Gawai dan Smartphone, agar selalu mempunyai penangkal virus/spam terbaru. Scan secara menyeluruh dan berkala untuk mencegah program malware, virus, spam, worm yang ingin masuk ke dalam komputer/smartphone anda

3. Backup dokumen, foto atau berkas penting lainnya ke flashdisk, harddisk cadangan (offline) atau ke layanan google dropbox (online). Agar memiliki data cadangan. Jika data anda hilang karena virus atau di sandera oleh ransomware yang meminta uang tebusan, maka dapat dipulihkan (recovery) dengan data backup
4. Jangan klik link web atau download file yang tidak dikenal. Karena dapat membangunkan malaware, virus, ransomware yang ada di file yang didownload atau attachment yang diklik, konsekwensinya data dalam gawai anda sudah terkontaminasi, termasuk daftar alamat (address book) digunakan oleh peretas untuk fase duplikasi malware dan penyebaran berikutnya
5. Berhati-hati gunakan wfi public. Terutama jika anda ingin melalukan transaksi keuangan, perbankan, ecommerce, credit cards serta aplikasi yang kritis dan strategis
6. Tidak gunakan perangkat pribadi di tempat bekerja, untuk memproses pekerjaan perusahaan

Cara penjagaan berlapis serangan cracker dari Internet dan dalam Sistem:

1. Memasang proteksi perimeter di peripheri (pagar) seperti Firewall, Router untuk sistem LAN internal perusahaan anda. Proxy di peripheri untuk memisahkan IP Internet Siber yang beresiko (compromised) dengan IP Private untuk semua PC dan gadget dilingkungan LAN Perusahaan. Proxy untuk memisahkan IP dunia cyber yang berbahaya (compromised) dengan IP Private untuk semua PC dan gadget dilingkungan LAN Perusahaan.
2. Anti virus, Anti Spam, Anti Malware, Sensor konten di Server dan disetiap PC serta peralatan Anti Insider Threat yang merupakan pertahanan berlapis (defence in depth)

bagi sebuah korporasi dan enterprise

Bahaya dan cara hindari Penipuan Phishing & social engineering di internet

Sosial Engineering (SosEng) menggunakan metode penyamaran, misalnya menyaru sebagai bos perusahaan dan menelpon satpam atau admin web untuk mendapatkan informasi rahasia seperti password. Modus SosEng yang lain adalah mengaku customer service sebuah bank atau kartu kredit dan minta informasi pribadi seperti pin atau data pribadi lainnya.

Phishing adalah upaya menyaru sebuah situs untuk melakukan penipuan. Kasus phishing terkenal pernah menimpa Klikbca.com Si cracker ini menyaru Klikbca.com dengan membuat beberapa situs yang mirip misalnya clickbca.com, clikbca.com atau Klik-bca.com. Nah korban yang tidak teliti membaca domain akan tertipu masuk situs phishing milik cracker. Selanjutnya cracker ini akan melakukan data mining pasword, login yang diketik oleh si korban, karena si korban sekarang bukan masuk ke situs BCA resmi tapi masuk ke situs si Cracker. Akhirnya si Cracker memiliki login dan password si korban dan dengan cepat menguras saldo si korban dengan cara phishing

1. Jangan panik dan tetap tenang menghadapi serangan phishing.
2. Segera hubungi call center atau datangi kantor dari perusahaan yang asli atau sebenarnya. Jelaskan anda ditenggarai menjadi korban phishing, agar informasi rahasia korban yang sudah dimiliki pelaku phishing segera di reset dan diubah agar pelaku phishing tidak dapat menguras rekening bank si korban.
3. Laporkan ke polisi agar situs penyamar pelaku phishing segera di blokir, ditutup dan pelaku phishing dikejar.
4. Rubah semua password dan login informasi agar tidak disusupi oleh cracker tersebut.

E. Bisnis di Bidang Teknologi Informasi

Beberapa alasan yang membuat bisnis perlu dilandasi oleh suatu etika :

a. Selain mempertaruhkan barang dan uang untuk tujuan keuntungan, bisnis juga

mempertaruhkan nama, harga diri bahkan nasib umat manusia yang terlibat didalamnya.

b. Bisnis adalah bagian penting dari masyarakat, sebagai hubungan antar manusia bisnis membutuhkan etika yang mampu memberi pedoman bagi pihak yang melakukannaya.

c. Bisnis adalah kegiatan yang mengutamakan rasa saling percaya. Etika dibutuhkan untuk menumbuhkan dan memperkuat rasa saling percaya.

Sony keraf (1991) dalam buku Etika Bisnis : Membangun Citra Bisnis sebagai Profesi Luhur, memcatat beberapa hal yang menjadi prinsip dari etika bisnis, antara lain :

a. Prinsip otonomi
b. Prinsip kejujuran
c. Prinsip berbuat baik dan tidak berbuat jahat
d. Prinsip keadilan
e. Prinsip hormat pada diri sendiri

Beberapa kategori bisnis dibidang TI :

a. Bisnis dibidang Industri Perangkat Keras

   Bergerak dibidang rekayasa perangkat keras, contoh IBM, Compaq, dll.

b. Bisnis dibidang Rekayasa Perangkat Lunak

   Dilakukan oleh perusahaan yang menguasai teknik rekayasa, yaitu kegiatan engineering yang meliputi analisis, desain, spesifikasi, implementasi dan validasi untuk menghasilkan produk perangkat lunak. Contoh : Microsoft, Adobe, dll.

c. Bisnis dibidang Distribusi dan Penjualan Barang

   Bisnis yang bergerak dibidang pemasaran produk komputer baik vendor ataupun secara pribadi.

d. Bisnis dibidang Pendidikan Teknologi Informasi

   Bisa berupa lembaga-lembaga kursus komputer sampai dengan perguruan tinggi bidang komputer. Contoh : BSI

e. Bisnis dibidang Pemeliharaan Teknologi Informasi

   Pemeliharaan bisa dilakukan oleh pengembang melalui divisi technical support atau spelialisasi bidang maintenance dan teknisi.

Tantanga umum bisnis di bidang TI :

a. Tantangan inovasi dan perubahan yang cepat
b. Tantangan pasar dan pemasaran di era globalisasi
c. Tantangan pergaulan internasional
d. Tantangan pengembangan sikap dan tanggung jawab pribadi
e. Tantangan pengembangan sumber daya manusia

PERTEMUAN 9

Jawablah pertanyaan berikut :

1. Berikan 3 contoh perubahan proses bisnis/sosial akibat teknologi yang “melunturkan” nilai etika tradisional. Untuk tiap contoh, sebutkan teknologinya, model kerjanya, nilai etika tradisional yang hilang.
2. Pelanggaran terhadap etika akan mendapatkan sanksi sosial dan sanksi hukum. Kapan pelanggaran etika memperoleh sanksi sosial dan memperoleh sanksi hukum. Berikan contoh.

Ketentuan pengerjaan :

1. Dikerjakan secara individu
2. Jawaban diketik menggunakan format word

PERTEMUAN 10

Jawablah pertanyaan berikut :

1. Berikan contoh etiket atau pelanggaran berinternet yang anda ketahui dalam:
   a. berkirim surat melalui email
   b. berbicara dalam chatting
2. Jelaskan berbagai macam kegiatan apa saja yang bisa dilakukan pada dua kegiatan di atas
3. Jelaskan apa yang dimaksud dengan "proses professional" dalam mengukur sebuah profesionalisme
4. Jelaskan bagaimana bentuk profesionalisme dalam profesi seperti: polisi, hakim, dokter, programmer, data entri operator, database administrator dan sebagainya. (Pilihlah satu profesi bidang IT dan satu profesi bidang non-IT)

Ketentuan pengerjaan :

1. Dikerjakan secara individu
2. Jawaban diketik menggunakan format word

PERTEMUAN 11

Jawablah pertanyaan berikut :

1. Kejahatan yang terjadi di internet terdiri dari berbagai macam jenis dan cara yang bisa terjadi. Menurut anda motif apakah yang dapat mempengaruhi kejahatan TI
2. Sebutkan contoh-contoh kasus kejahatan TI yang sedang trend (viral) saat ini. Dan menurut anda apa motif kejahatan tersebut
3. Berdasarkan contoh kasus (sesuai jawaban no.2), menurut anda apakah upaya-upaya yang dapat kita lakukan untuk menanggulangi kejahatan TI
4. Berdasarkan jawaban no.2, sebutkan pasal yang mengaturnya dalam UUITE

Ketentuan pengerjaan :

1. Dikerjakan secara individu
2. Jawaban diketik menggunakan format word

PERTEMUAN 12

Jawablah pertanyaan berikut :

1. Sebutkan menurut anda apa saja tips-tips aman berinternet

Ketentuan pengerjaan :

1. Dikerjakan secara individu
2. Jawaban diketik menggunakan format word

PERTEMUAN 13

Ketentuan :

1. Buatlah makalah dengan tema : **Unauthorized Access to Computer System / Illegal Contents / Data Forgery** (pilih salah satu)
2. Melakukan presentasi sesuai tema yang diplih (seluruh anggota kelompok wajib hadir (mengikuti) presentasi tersebut.
3. Tugas dikerjakan secara berkelompok maksimal 5 orang dalam dua bentuk yaitu :
   a. Paper/makalah dalam format pdf
   b. Blog/Web
4. Susunan Makalah sebagai berikut :

   Bab I Pendahuluan menjelaskan tentang latar belakang masalah dari kejahatan komputer yang diangkat

   Bab II Landasan Teori
   Teori Cybercrime dan Cyberlaw yang sesuai dengan kejahatan yang diangkat

   Bab III Pembahasan /Analisa Kasus
   Motif, penyebab dan penanggulangannya

   Bab IV Penutup
5. Tuliskan Link Blog/Web dari materi tersebut pada cover makalah
6. Secara individu, mahasiswa wajib menyampaikan tugas projek melalui sistem elearning Universitas Bina Sarana Informatika. **Penting** : Bagi mahasiswa yang tidak login dan tidak meyampaikan tugas projek, maka mahasiswa tidak mendapatkan nilai projek.
7. Kriteria Penilaian :
   a. Dapat menganalisa, menjelaskan, menyebutkan, melengkapi serta mengevaluasi mengenai Konten (sesuai tema) yang telah dibuat (50 %)
   b. Akurat dan tepat dalam mengidentifikasi masalah (25 %)
   c. Blog/web (25 %)

PERTEMUAN 14

Ketentuan :

1. Buatlah makalah dengan tema : **Cyber Espionage / Cyber Sabotage and Extortion**
2. Melakukan presentasi sesuai tema yang diplih (seluruh anggota kelompok wajib hadir (mengikuti) presentasi tersebut.
3. Tugas dikerjakan secara berkelompok maksimal 5 orang dalam dua bentuk yaitu :
   a. Paper/makalah dalam format pdf
   b. Blog/Web
4. Susunan Makalah sebagai berikut :

   Bab I Pendahuluan menjelaskan tentang latar belakang masalah dari kejahatan komputer yang diangkat

   Bab II Landasan Teori
   Teori Cybercrime dan Cyberlaw yang sesuai dengan kejahatan yang diangkat

   Bab III Pembahasan /Analisa Kasus
   Motif, penyebab dan penanggulangannya

   Bab IV Penutup
5. Tuliskan Link Blog/Web dari materi tersebut pada cover makalah
6. Secara individu, mahasiswa wajib menyampaikan tugas projek melalui sistem elearning Universitas Bina Sarana Informatika. **Penting** : Bagi mahasiswa yang tidak login dan tidak meyampaikan tugas projek, maka mahasiswa tidak mendapatkan nilai projek.
7. Kriteria Penilaian :
   a. Dapat menganalisa, menjelaskan, menyebutkan, melengkapi serta mengevaluasi mengenai Konten (sesuai tema) yang telah dibuat (50 %)
   b. Akurat dan tepat dalam mengidentifikasi masalah (25 %)
   c. Blog/web (25 %)

PERTEMUAN 15

Ketentuan :

1. Buatlah makalah dengan tema : **Intellectual Property / Infringements of Privacy**
2. Melakukan presentasi sesuai tema yang diplih (seluruh anggota kelompok wajib hadir (mengikuti) presentasi tersebut.
3. Tugas dikerjakan secara berkelompok maksimal 5 orang dalam dua bentuk yaitu :
   a. Paper/makalah dalam format pdf
   b. Blog/Web
4. Susunan Makalah sebagai berikut :

   Bab I Pendahuluan menjelaskan tentang latar belakang masalah dari kejahatan komputer yang diangkat

   Bab II Landasan Teori
   Teori Cybercrime dan Cyberlaw yang sesuai dengan kejahatan yang diangkat

   Bab III Pembahasan /Analisa Kasus
   Motif, penyebab dan penanggulangannya

   Bab IV Penutup
5. Tuliskan Link Blog/Web dari materi tersebut pada cover makalah
6. Secara individu, mahasiswa wajib menyampaikan tugas projek melalui sistem elearning Universitas Bina Sarana Informatika. **Penting** : Bagi mahasiswa yang tidak login dan tidak meyampaikan tugas projek, maka mahasiswa tidak mendapatkan nilai projek.
7. Kriteria Penilaian :
   a. Dapat menganalisa, menjelaskan, menyebutkan, melengkapi serta mengevaluasi mengenai Konten (sesuai tema) yang telah dibuat (50 %)
   b. Akurat dan tepat dalam mengidentifikasi masalah (25 %)
   c. Blog/web (25 %)