TEKNOSAIN

Etika Profesi Teknologi Informasi dan Komunikasi

Susi Susilowati
Enok Tuti Alawiyah
Dewi Ayu Nur Wulandari

Etika Profesi Teknologi Informasi dan Komunikasi

Etika Profesi Teknologi Informasi dan Komunikasi

Susi Susilowati
Enok Tuti Alawiyah
Dewi Ayu Nur Wulandari

TEKNOSAIN

ETIKA PROFESI TEKNOLOGI INFORMASI DAN KOMUNIKASI

oleh Susi Susilowati; Enok Tuti Alawiah; Dewi Ayu Nur Wulandari

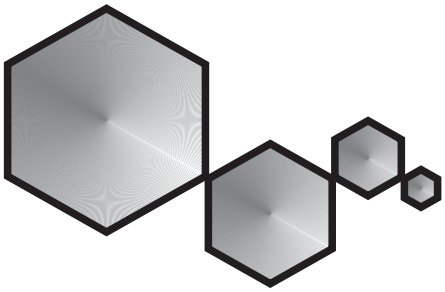
Edisi Pertama; Cetakan Pertama ~ 2021

TEKNOSAIN
Ruko Jambusari 7A Yogyakarta 55283
Telp: 0274-889398; 0274-882262

ISBN: 978-623-6433-06-5

Buku ini tersedia sumber elektronisnya

DATA BUKU:
Format: 17 x 24 cm; Jml. Hal.: viii + 162; Kertas Isi: HVS 70 gram; Tinta Isi: BW; Kertas Cover: Ivori 260 gram; Tinta Cover: Colour; Finishing: Perfect Binding: Laminasi Doff.



KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakaatuh.

Puji syukur alhamdullillah, penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehingga pada akhirnya kami dapat menyelesaikan buku Etika Profesi Teknologi Informasi dan Komunikasi. Buku ini disusun dengan tujuan untuk memudahkan mahasiswa dan para praktisi untuk memahami etika profesi tik.

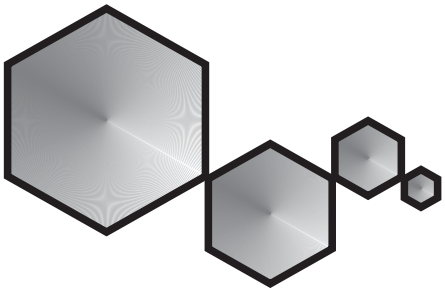
Penulis menyadari buku ini masih jauh dari sempurna, oleh karena itu penulis mengharapkan kritik dan saran yang bersifat membangun sehingga kedepannya buku ini dapat kami sempurnakan.

Akhir kata kami mengucapkan terima kasih kepada semua pihak yang telah membantu terbitnya buku ini. Semoga buku ini dapat memberikan manfaat.

Wassalamu'alaikum Warahmatullahi Wabarakaatuh.

Jakarta, Juli 2020

Penulis



DAFTAR ISI

-oo0oo-

BAB I
TINJAUAN UMUM ETIKA

A. Pengertian Etika

Secara etimologi kata “etika” berasal dari bahasa yunani yang terdiri dari dua kata yaitu Ethos dan ethikos. Ethos berarti sifat, watak kebiasaan, tempat yang biasa. Ethikos berarti susila, keadaban, kelakuan dan perbuatan yang baik. Sedangkan dalam bahasa Arab kata etika dikenal dengan istilah akhlak, artinya budi pekerti. Sedangkan dalam bahasa Indonesia disebut tata susila.

K Bertens dalam buku etikanya menjelaskan lebih jelas lagi. Etika berasal dari bahasa Yunani kuno. Kata Yunani ethos dalam bentuk tunggal mempunyai banyak arti: tempat tinggal yang biasa; padang rumput; kandang; kebiasaan, adat; akhlak, watak; perasaan, sikap, cara berpikir. Dalam bentuk jamak artinya adalah adat kebiasaan. Dalam arti ini, etika berkaitan dengan kebiasaan hidup yang baik, tata cara hidup yang baik, baik pada diri seseorang atau kepada masyarakat. Kebiasaan hidup yang baik ini dianut dan diwariskan dari satu generasi ke generasi lain.

Secara terminologi etika bisa disebut sebagai ilmu tentang baik dan buruk atau kata lainnya ialah teori tentang nilai. Dalam Islam teori nilai mengenal lima kategori baik-buruk, yaitu baik sekali, baik, netral, buruk dan buruk sekali. Nilai ditentukan oleh Tuhan, karena Tuhan adalah maha suci yang bebas dari noda apa pun jenisnya.

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.

Etika disebut juga ilmu normatif, karena didalamnya mengandung norma dan nilai-nilai yang dapat digunakan dalam kehidupan. Sebagian orang menyebut etika dengan moral atau budi pekerti. ilmu etika adalah ilmu yang mencari keselarasan perbuatan-perbuatan manusia dengan dasar yang sedalam-dalamnya yang diperoleh dengan akal budi manusia.

Menurut KBBI, filsafat etika adalah

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

Dengan demikian, pandangan baik dan buruk, dan hakikat nilai dalam kehidupan manusia sangat tergantung pada tiga hal mendasar yaitu:

1. Cara berpikir yang melandasi manusia dalam berprilaku.
2. Cara berbudaya yang menjadi sendi berlakunya norma sosial.
3. Cara merujuk kepada sumber-sumber nilai yang menjadi tujuan pokok dalam bertindak.

Selain itu juga pengertian etika adalah cabang ilmu filsafat yang membicarakan nilai dan moral yang menentukan perilaku seseorang/manusia dalam hidupnya. Etika merupakan sebuah refleksi kritis dan rasional mengenai nilai dan norma moral yang menentukan dan terwujud dalam sikap serta pola perilaku hidup manusia baik sebagai pribadi maupun sebagai kelompok.

Jadi, filsafat etika adalah cabang ilmu filsafat yang mempelajari tingkah laku manusia yang baik dan buruk. Dasar filsafat etika yaitu etika individual sendiri.

Menurut para ahli makna 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.

Dari beberapa pengertian diatas dapat di simpulkan bahwa etika adalah suatu ilmu yang membahas tentang arti baik dan buruk, benar dan salah kemudian manusia menggunakan akal dan hati nuraninya untuk mencapai tujuan hidup yang baik dan benar sesuai dengan tujuan yang dikehendaki. Jadi manusia dapat melakukan apa saja yang dikehendaki yang dianggap baik dan benar, meskipun hati nuraninya menolak dan yang terpenting tujuannya dapat tercapai.

Dalam menelaah ukuran baik dan buruk suatu tingkah laku yang ada dalam masyarakat kita bisa menggolongkan etika, yakni :

1. Etika Deskriptif

Etika deskriptif Merupakan usaha menilai tindakan atau prilaku berdasarkan pada ketentuan atau norma baik buruk yang tumbuh dalam kehidupan bersama di dalam masyarakat. Kerangka etika ini pada hakikatnya menempatkan kebiasaan yang sudah ada di dalam masyarakat sebagai acuan etis. Suatu tindakan seseorang disebut etis atau tidak. Tergantung pada kesesuaiannya dengan yang dilakukan kebanyakan orang.

Etika deskriptif mempunyai dua bagian yang sangat penting, yaitu

a. Sejarah kesusilaan.

   Bagian ini timbul apabila orang menerapkan metode historik dalam etika deskriptif. Dalam hal ini yang di selidiki adalah pendirian-pendirian mengenai baik dan buruk, norma-norma kesusilaan yang pernah berlaku, dan cita-cita kesusilaan yang dianut oleh bangsa-bangsa tertentu apakah terjadi penerimaan dan bagaimana pengolahannya. Perubahan-perubahan apakah yang di alami kesusilaan dalam perjalanan waktu, hal-hal apakah yang mempengaruhinya, dan sebagainya. Sehingga bagaimanapun sejarah etika penting juga bagi sejarah kesusilaan.

b. Fenomenologi kesusilaan. Dalam hal ini istilah fenomenologi dipergunakan dalam arti seperti dalam ilmu pengetahuan agama. Fenomenologi agama mencari makna keagamaan dari gejala-gejala keagamaan, mencari logos, susunan batiniah yang

mempersatukan gejala-gejala ini dalam keselarasan tersembunyi dan penataan yang mengandung makna. Demikian pula dengan fenomenologi kesusilaan. Artinya, ilmu pengetahuan ini melukiskan kesusilaan sebagaimana adanya, memperlihatkan ciri-ciri pengenal, bagaimana hubungan yang terdapat antara ciri yang satu dengan yang lain, atau singkatnya, mempertanyakan apakah yang merupakan hakekat kesusilaan. Yang dilukiskan dapat berupa kesusilaan tertentu, namun dapat juga moral pada umumnya.

Masalah-masalah ini bersifat kefilsafatan. Pertanyaan yang utamanya ialah, apakah kesusilaan harus di pahami dari dirinya sendiri ataukah kesusilaan itu didasarkan oleh sesuatu yang lain. Dengan perkataan lain, apakah kesusilaan mengacu ataukah tidak mengacu kepada sesuatu yang terdapat di atas atau setidak- tidaknya di luar dirinya sendiri. Etika yang menelaah secara kritis dan rasional tentang sikap dan perilaku manusia, serta apa yang dikejar oleh setiap orang dalam hidupnya sebagai sesuatu yang bernilai. Artinya Etika deskriptif tersebut berbicara mengenai fakta secara apa adanya, yakni mengenai nilai dan perilaku manusia sebagai suatu fakta yang terkait dengan situasi dan realitas yang membudaya. Dapat disimpulkan bahwa tentang kenyataan dalam penghayatan nilai atau tanpa nilai dalam suatu masyarakat yang dikaitkan dengan kondisi tertentu memungkinkan manusia dapat bertindak secara etis.

Contohnya: Mengenai masyarakat Jawa yang mengajarkan tatakrama berhubungan dengan orang yang lebih tua dari pada kita.

2. Etika Normatif

Kelompok ini mendasarkan diri pada sifat hakiki kesusilaan bahwa di dalam perilaku serta tanggapan- tanggapan kesusilaannya, manusia menjadikan norma- norma kesusilaan sebagai panutannya. Etika menetapkan bahwa manusia memakai norma-norma sebagai panutannya, tetapi tidak memberikan tanggapan mengenai kelayakan ukuran-ukuran kesusilaan. Sah atau tidaknya norma- norma tetap tidak dipersoalkan yang di perhatikan hanya berlakunya.

Etika normatif tidak dapat sekedar melukiskan susunan - susunan formal kesusilaan. Ia menunjukkan prilaku manakah yang baik dan prilaku manakah yang buruk. Yang demikian ini kadangkadang yang disebut ajaran kesusilaan, sedangkan etika deskriptif disebut juga ilmu kesusilaan. Yang pertama senantiasa merupakan etika material. Etika

normatif memperhatikan kenyataan-kenyataan, yang tidak dapat di tangkap dan diverifikasi secara empirik.

Etika yang berusaha menelaah dan memberikan penilaian suatu tindakan etis atau tidak, tergantung dengan kesesuaiannya terhadap norma-norma yang sudah dilakukan dalam suatu masyarakat. Norma rujukan yang digunakan untuk menilai tindakan wujudnya bisa berupa tata tertib, dan juga kode etik profesi.

Contohnya: Etika yang bersifat individual seperti kejujuran, disiplin, dan tanggung jawab.

3. Etika Deontologi

Etika Deontologi adalah suatu tindakan dinilai baik buruk berdasarkan apakah tindakan itu sesuai atau tidak dengan kewajiban. Dengan kata lain, suatu tindakan dianggap baik karena tindakan itu memang baik pada dirinya sendiri, sehingga merupakan kewajiban yang harus kita lakukan. Sebaliknya suatu tindakan dinilai buruk secara moral karena tindakan itu memang buruk secara moral sehingga tidak menjadi kewajiban untuk kita lakukan. Bersikap adil adalah tindakan yang baik, dan sudah kewajiban kita untuk bertindak demikian.

Etika deontologi sama sekali tidak mempersoalkan akibat dari tindakan tersebut: baik atau buruk. Akibat dari suatu tindakan tidak pernah diperhitungkan untuk menentukan kualitas moral suatu tindakan. Atas dasar itu, etika deontologi sangat menekankan motivasi, kemauan baik dan watak yang kuat untuk bertindak sesuai dengan kewajiban.

Etika deontologi menekankan kewajiban manusia untuk bertindak secara baik. Jadi, etika Deontologi yaitu tindakan dikatakan baik bukan karena tindakan itu mendatangkan akibat baik, melainkan berdasarkan tindakan itu baik untuk dirinya sendiri.

4. Etika Teleologi

Etika Teleologi menilai baik buruk suatu tindakan berdasarkan tujuan atau akibat dari tindakan tersebut. suatu tindakan dinilai baik kalau bertujuan baik dan mendatangkan akibat baik. Jadi, terhadap pertanyaan, bagaimana harus bertindak dalam situasi kongkret tertentu, jawaban teleologi adalah pilihlah tindakan yang membawa akibat baik.

Dengan demikian, bisa dikatakan bahwa etika teleologi lebih bersifat situasional dan subyektif. Kita bisa bertindak berbeda dalam situasi yang lain tergantung dari penilaian kita tentang akibat dari tindakan tersebut. demikian pula, suatu tindakan yang jelas-

jelas bertentangan dengan norma dan nilai moral bisa di benarkan oleh kita teleologi hanya karena tindakan itu membawa akibat yang baik.

Suatu tindakan dikatakan baik jika tujuannya baik dan membawa akibat yang baik dan berguna. Dari sudut pandang "apa tujuannya", etika teleologi dibedakan menjadi dua, yaitu:

a. Teleologi Hedonisme (hedone = kenikmatan) yaitu tindakan yang bertujuan untuk mencari kenikmatan dan kesenangan.
b. Teleologi Eudamonisme (eudemonia = kebahagiaan) yaitu tindakan yang bertujuan mencari kebahagiaan yang hakiki

5. Etika Keutamaan

Etika keutamaan tidak mempersoalkan akibat suatu tindakan. Juga, tidak mendasarkan penilaian moral pada kewajiban terhadap hukum moral universal. Etika keutamaan lebih mengutamakan pengembangan karakter moral pada diri setiap orang.

Dalam kaitan dengan itu, sebagaimana dikatakan Aristoteles, nilai moral ditemukan dan muncul dari pengalaman hidup dalam masyarakat, dari teladan dan contoh hidup yang diperlihatkan oleh tokoh-tokoh besar dalam suatu masyarakat dalam menghadapi dan menyikapi persoalan-persoalan hidup ini.

Dengan demikian, etika keutamaan sangat menekankan pentingnya sejarah kehebatan moral para tokoh besar dan dari cerita dongeng ataupun sastra kita belajar tentang nilai dan keutamaan, serta berusaha menghayati dan mempraktekkannya seperti tokoh dalam sejarah, dalam cerita, atau dalam kehidupan masyarakat. Tokoh dengan teladannya menjadi model untuk kita tiru.

Etika keutamaan sangat menghargai kebebasan dan rasionalitas manusia, karena pesan moral hanya di sampaikan melalui cerita dan teladan hidup para tokoh lalu membiarkan setiap orang untuk menangkap sendiri pesan moral itu. Juga setiap orang dibiarkan untuk menggunakan akal budinya untuk menafsirkan pesan moral itu, artinya, terbuka kemungkinan setiap orang mengambil pesan moral yang khas bagi dirinya, dan melalui itu kehidupan moral menjadi sangat kaya oleh berbagai penafsiran.

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.

Menurut A. Sonny Keraf (dalam Ruslan, 2011), Secara umum etika terbagi menjadi dua bagian besar yaitu Etika Umum dan Etika Khusus.

1. Etika Umum

   Etika umum berbicara mengenai norma dan nilai moral, kondisikondisi dasar bagi manusia untuk bertindak secara etis, bagaimana manusia mengambil keputusan etis, teori-teori etika, lembagalembaga normatif dan semacamnya. Etika umum sebagai ilmu atau filsafat moral dapat dianggap sebagai etika teoretis, istilah ini sesungguhnya tidak tepat karena bagaimanapun juga etika selalu berkaitan degan perilaku dan kondisi praktis dan actual dari

   manusia dalam kehidupannya sehari-hari dan tidak hanya sematamata bersifat teoretis

2. Etika Khusus

   Adalah penerapan prinsip-prinsip atau norma-norma moral dasar dalam bidang kehidupan yang khusus. Dalam hal ini, norma dan prinsip moral diteropongi dalam konteks kekhususan

   bidang kehidupan manusia yang khusus. Etika tidak lagi sekedar meneropong perilaku dan kehidupan manusia sebagai manusia saja, melainkan sebagai manusia dalam bidang kehidupan dan kegiatan khusus tertentu berdasarkan kekhususan situasi dan problematika kehidupan.

   Dalam kaitan dengan ini, etika khusus dianggap sebagai etika terapan karena aturan normatif yang bersifat umum diterapkan secara khusus sesuai dengan kekhususan dan kekhasan bidang kehidupan dan kegiatan khusus tertentu. Dengan demikian, etika khusus dapat dikatakan merupakan kontekstualisasi aturan moral umum dalam bidang dan situasi konkret. Etika Khusus dikelompokkan menjadi :

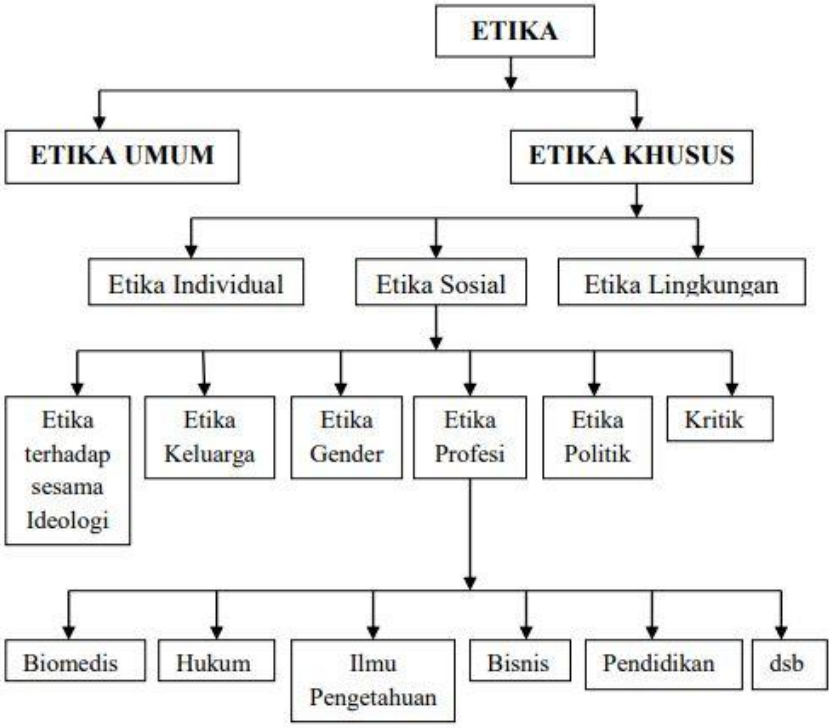
   a. Etika Individual : Etika yang menyangkut menyangkut kewajiban dan perilaku manusia terhadap dirinya sendiri untuk mencapai kesucian kehidupan pribadi, kebersihan hati nurani dan yang berakhlak luhur.
   b. Etika Sosial : Etika yang menyangkut kewajiban, sikap dan perilaku sebagai anggota masyarakat yang berkaitan dengan nilai-nilai sopan santun, tata karma dan saling menghormati, yaitu bagaimana saling berinteraksi yang menyangkut hubungan manusia dengan manusia, baik secara perseorangan dan langsung, maupun secara

bersama-sama atau kelompok dalam bentuk kelembagaan masyarakat dan organisasi formal lainnya.

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.

Secara umum dapat dilihat dari skema etika dibawah ini ;



Gambar 1: Skema Etika

Sistem Penilaian Etika

Etika dalam implementasinya dapat mempengaruhi kehidupan manusia. Etika memberi pedoman perilaku bagaimana seseorang menjalani hidupnya melalui rangkaian tindakan sehari-hari. Itu berarti etika membantu manusia untuk mengambil sikap dan bertindak

secara tepat dalam menjalani hidup sejalan dengan kaidah norma yang berlaku pada kelompok dimana ia berada. Norma sendiri merupakan suatu nilai yang mengatur dan memberikan pedoman bagi setiap orang atau masyarakat dalam berperilaku, dimana norma atau kaidah merupakan standar yang harus dipatuhi dalam kelompok tertentu (Soekanto, 1989). Etika pada akhirnya membantu untuk mengambil keputusan tentang tindakan apa yang perlu kita lakukan dan yang perlu dipahami bersama bahwa etika ini dapat diterapkan dalam segala aspek atau sisi kehidupan. Dalam menilai etika, maka berlaku sistem yang mengaturnya diantaranya adalah sebagai berikut (Isnanto, 2009):

- 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.

B. Pengertian Moral

Secara etimologis, kata moral berasal dari kata mos dalam bahasa Latin, bentuk jamaknya mores, yang artinya adalah tata-cara atau adat-istiadat. Dalam Kamus Besar Bahasa Indonesia (1989: 592), moral diartikan sebagai akhlak, budi pekerti, atau susila. Secara terminologis, terdapat berbagai rumusan pengertian moral, yang dari segi substantif materiilnya tidak ada perbedaan, akan tetapi bentuk formalnya berbeda.

Widjaja (1985: 154) menyatakan bahwa moral adalah ajaran baik dan buruk tentang perbuatan dan kelakuan (akhlak). Al-Ghazali (1994: 31) mengemukakan pengertian akhlak, sebagai padanan kata moral, sebagai perangai (watak, tabiat) yang menetap kuat dalam jiwa

manusia dan merupakan sumber timbulnya perbuatan tertentu dari dirinya secara mudah dan ringan, tanpa perlu dipikirkan dan direncanakan sebelumnya.

Sementara itu Wila Huky, sebagaimana dikutip oleh Bambang Daroeso (1986: 22) merumuskan pengertian moral secara lebih komprehensip rumusan formalnya sebagai berikut :

1. Moral sebagai perangkat ide-ide tentang tingkah laku hidup, dengan warna dasar tertentu yang dipegang oleh sekelompok manusia di dalam lingkungan tertentu.
2. Moral adalah ajaran tentang laku hidup yang baik berdasarkan pandangan hidup atau agama tertentu.
3. Moral sebagai tingkah laku hidup manusia, yang mendasarkan pada kesadaran, bahwa ia terikat oleh keharusan untuk mencapai yang baik , sesuai dengan nilai dan norma yang berlaku dalam lingkungannya.

Agar diperoleh pemahaman yang lebih jelas perlu diberikan ulasan bahwa substansi materiil dari ketiga batasan tersebut tidak berbeda, yaitu tentang tingkah laku. Akan tetapi bentuk formal ketiga batasan tersebut berbeda.

Batasan pertama dan kedua hampir sama, yaitu seperangkat ide tentang tingkah laku dan ajaran tentang tingkah laku. Sedangkan batasan ketiga adalah tingkah laku itu sendiri Pada batasan pertama dan kedua, moral belum berwujud tingkah laku, tapi masih merupakan acuan dari tingkah laku.

Pada batasan pertama, moral dapat dipahami sebagai nilai-nilai moral. Pada batasan kedua, moral dapat dipahami sebagai nilai-nilai moral atau norma-norma moral. Sedangkan pada batasan ketiga, moral dapat dipahami sebagai tingkah laku, perbuatan, atau sikap moral.

Namun demikian semua batasan tersebut tidak salah, sebab dalam pembicaraan sehari-hari, moral sering dimaksudkan masih sebagai seperangkat ide, nilai, ajaran, prinsip, atau norma. Akan tetapi lebih kongkrit dari itu , moral juga sering dimaksudkan sudah berupa tingkah laku, perbuatan, sikap atau karakter yang didasarkan pada ajaran, nilai, prinsip, atau norma.

Ada beberapa pengertian moral. Moral merupakan pengetahuan yang menyangkut budi pekerti manusia yang beradab. Moral juga berarti ajaran yang baik dan buruk

perbuatan dan kelakuan (akhlak). Moralisasi, berarti uraian (pandangan, ajaran) tentang perbuatan dan kelakuan yang baik. Demoralisasi, berarti kerusakan moral.

Menurut asal katanya “moral” dari kata mores dari bahasa Latin, kemudian diterjemahkan menjadi “aturan kesusilaan”. Dalam bahasa sehari-hari, yang dimaksud dengan kesusilaan bukan mores, tetapi petunjuk-petunjuk untuk kehidupan sopan santun dan tidak cabul. Jadi, moral adalah aturan kesusilaan, yang meliputi semua norma kelakuan, perbuatan tingkah laku yang baik. Kata susila berasal dari bahasa Sansekerta, su artinya “lebih baik”, sila berarti “dasar-dasar”, prinsip-prinsip atau peraturan-peraturan hidup. Jadi susila berarti peraturan-peraturan hidup yang lebih baik.

Moral secara ekplisit adalah hal-hal yang berhubungan dengan proses sosialisasi individu tanpa moral manusia tidak bisa melakukan proses sosialisasi. Moral dalam zaman sekarang mempunyai nilai implisit karena banyak orang yang mempunyai moral atau sikap amoral itu dari sudut pandang yang sempit. Moral itu sifat dasar yang diajarkan di sekolah-sekolah dan manusia harus mempunyai moral jika ia ingin dihormati oleh sesamanya. Moral adalah nilai ke-absolutan dalam kehidupan bermasyarakat secara utuh. Penilaian terhadap moral diukur dari kebudayaan masyarakat setempat.

Moral merupakan perbuatan/tingkah laku/ucapan seseorang dalam berinteraksi dengan manusia. apabila yang dilakukan seseorang itu sesuai dengan nilai rasa yang berlaku di masyarakat tersebut dan dapat diterima serta menyenangkan lingkungan masyarakatnya, maka orang itu dinilai mempunyai moral yang baik, begitu juga sebaliknya. Moral adalah produk dari budaya dan Agama. Moral juga dapat diartikan sebagai sikap, perilaku, tindakan, kelakuan yang dilakukan seseorang pada saat mencoba melakukan sesuatu berdasarkan pengalaman, tafsiran, suara hati, serta nasihat, dll.

Pengertian moral menurut para ahli:

1. W. J. S. Poerdarminta menyatakan bahwa moral merupakan ajaran tentang baik buruknya perbuatan dan kelakuan.
2. Dewey mengatakan bahwa moral sebagai hal-hal yang berhubungan dengan nilai-nilai susila.
3. Baron dkk. Mengatakan bahwa moral adalah hal-hal yang berhubungan dengan larangan dan tindakan yang membicarakan salah atau benar.

4. Magnis-Susino mengatakan bahwa moral selalu mengacu pada pada baik buruknya manusia sebagai manusia, sehingga bidang moral adalah bidang kehidupan manusia dilihat dari segi kebaikannya sebagai manusia.

Nilai moral dipengaruhi oleh tiga hal, yaitu ajaran agama, adat istiadat dan ideologi.

- Nilai moral bersumber agama

  Kepatutan yang bersumber pada agama, sehingga hal ini tergantung dari ajaran masing-masing agama contohnya adalah mencuri, berdusta, ingkar janji, menfitnah, tindakan asusila dan lain-lain.
- Nilai moral bersumber adat istiadat

  Kepatutan yang bersumber adat istiadat, contohnya adalah tidak duduk diatas orang yang lebih tua.
- Nilai moral bersumber dari ideology

  Kepatutan yang bersumber dari ideologi atau paham seseorang, misalnya seseorang bersihkukuh agar tidak merokok selama hidupnya.

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.

Fungsi dan Tujuan Moral :

1. Menjamin tegaknya harkat dan martabat pribadi seseorang dan kemanusiaan.
2. Menjamin kebahagiaan jasmani dan rohani manusia karena penunaian fungsi moral tidak menimbulkan konflik-konflik batin, rasa menyesal, perasaan berdosa atau kekecewaan.
3. Menjamin keharmonisan antar hubungan sosial pribadi, karena moral memberikan landasan kepercayaan kepada sesama, percaya atas itikad baik dan kebaikan setiap orang karena moralitasnya yang luhur.
4. Fungsi moral lebih-lebih memberikan motivasi kebaikan dan kebajikan dalam tiap sikap dan tindakan manusia, manusia berbuat kebaikan dan kebajikan didasarkan atas kesadaran kewajiban yang dilandasi moral.

5. Moral memberikan wawasan masa depan baik konsekuensi dan sanksi sosial dalam kehidupan di dunia yang selalu mempertimbangkan sebelum bertindak juga lebih-lebih konsekuensi dan tanggung jawab terhadap Tuhan dalam kehidupan di akhirat.
6. Moral memberikan landasan kesabaran, untuk bertahan terhadap segala dorongan naluri dan keinginan (nafsu) member daya tahan dalam menunda atau menolak dorongan-dorongan yang rendah yang mengancam harkat martabat pribadi manusia.

Jenis-Jenis Moral

1. Moral ketuhanan, keagamaan atau religius. Moral berdasarkan ajaran agama yang berlaku.
2. Moral berdasarkan filsafat dan ideologi Negara bangsa yang berinti jiwa dan semangat kebangsaan, loyal kepada cita-cita bangsa dan Negara.
3. Moral berdasarkan etika kesusilaan yang dijunjung masyarakatnya, bangsa dan Negara secara budaya dan tradisi.
4. Moral dan disiplin berdasarkan hukum yang berlaku dalam masyarakat dan Negara. Moral sosial termasuk dalam bagian moral ilmiah dankode etika professional misalnya: mengutip pikiran dan pendapat orang lain dengan menuliskan sumbernya secara jelas dan sah.

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

Norma adalah petunjuk tingkah laku yang harus dilakukan dan tidak boleh dilakukan dalam hidup sehari-hari, berdasarkan suatu alasan (motivasi) tertentu dengan disertai sanksi. Sanksi adalah ancaman/akibat yang akan diterima apabila norma tidak dilakukan (Widjaja, 1985: 168).

Dalam kehidupan umat manusia terdapat bermacam-macam norma, yaitu norma agama, norma kesusilaan, norma kesopanan, norma hukum dan lain-lain. Norma agama, norma kesusilaan, norma kesopanan, dan norma hokum digolongkan sebagai norma umum. Selain itu dikenal juga adanya norma khusus, seperti aturan permainan, tata tertib sekolah, tata tertib pengunjung tempat bersejarah dan lain-lain.

1. **Norma Agama**

   Norma agama adalah aturan-aturan hidup yang berupa perintah-perintah dan larangan-larangan, yang oleh pemeluknya diyakini bersumber dari Tuhan Yang Maha Esa. Aturan-aturan itu tidak saja mengatur hubungan vertikal, antara manusia dengan Tuhan (ibadah), tapi juga hubungan horisontal, antara manusia dengan sesama manusia. Pada umumnya setiap pemeluk agama menyakini bawa barang siapa yang mematuhi perintah-perintah Tuhan dan menjauhi larangan-larangan Tuhan akan memperoleh pahala. Sebaliknya barang siapa yang melanggarnya akan berdosa dan sebagai sanksinya, ia akan memperoleh siksa. Sikap dan perbuatan yang menunjukkan kepatuhan untuk menjalankan perintah-Nya dan menjauhi larangan-Nya tersebut disebut taqwa.

2. **Norma Kesusilaan**

   Norma kesusilaan adalah aturan-aturan hidup tentang tingkah laku yang baik dan buruk, yang berupa “bisikan-bisikan” atau suara batin yang berasal dari hati nurani manusia. Berdasar kodrat kemanusiaannya, hati nurani setiap manusia “menyimpan” potensi nilai-nilai kesusilaan. Hal ini analog dengan hak-hak asasi manusia yang dimiliki oleh setiap pribadi manusia karena kodrat kemanusiaannya, sebagai anugerah Tuhan Yang Maha Kuasa. Karena potensi nilai-nilai kesusilaan itu tersimpan pada hati nurani setiap manusia (yang berbudi), maka hati nurani manusia dapat disebut sebagai sumber norma kesusilaan. Ini sejalan dengan pendapat Widjaja tentang moral dihubungkan dengan etika, yang membicarakan tata susila dan tata sopan santun. Tata susila mendorong untuk berbuat baik, karena hati kecilnya menganggap baik, atau bersumber dari hati nuraninya, lepas dari hubungan dan pengaruh orang lain (Widjaja, 1985: 154).Tidak jarang ketentuan-ketentuan norma agama juga menjadi ketentuan-ketentuan norma kesusilaan, sebab pada hakikatnya nilainilai keagamaan dan kesusilaan itu berasal dari Tuhan Yang Maha Kuasa. Demikian pula karena sifatnya yang melekat pada diri setiap manusia, maka nilai-nilai kesusilaan itu bersifat universal.

Dengan kata lain, nilai-nilai kesusilaan yang universal tersebut bebas dari dimensi ruang dan waktu, yang berarti berlaku di manapun dan kapanpun juga. Sebagai contoh, tindak pemerkosaan dipandang sebagai tindakan yang melanggar kesusilaan, di belahan dunia manapun dan pada masa kapanpun juga. Kepatuhan terhadap norma kesusilaan akan menimbulkan rasa bahagia, sebab yang bersangkutan merasa tidak mengingkari hati nuraninya. Sebaliknya, pelanggaran terhadap norma kesusilaan pada hakikatnya merupakan pengingkaran terhadap hati nuraninya sendiri, sehingga sebagaimana dikemukakan dalam sebuah mutiara hikmah, pengingkaran terhadap hati nurani itu akan menimbulkan penyesalan atau bahkan penderitaan batin. Inilah bentuk sanksi terhadap pelanggaran norma kesusilaan.

3. Norma Kesopanan

Norma kesopanan adalah aturan hidup bermasyarakat tentang tingkah laku yang baik dan tidak baik baik, patut dan tidak patut dilakukan, yang berlaku dalam suatu lingkungan masyarakat atau komunitas tertentu. Norma ini biasanya bersumber dari adat istiadat, budaya, atau nilai-nilai masyarakat. Ini sejalan dengan pendapat Widjaja tentang moral dihubungkan dengan eika, yang membicarakan tentang tata susila dan tata sopan santun. Tata sopan santun mendorong berbuat baik, sekedar lahiriah saja, tidak bersumber dari hati nurani, tapi sekedar menghargai menghargai orang lain dalam pergaulan (Widjaja, 1985: 154). Dengan demikian norma kesopanan itu bersifat kultural, kontekstual, nasional atau bahkan lokal. Berbeda dengan norma kesusilaan, norma kesopanan itu tidak bersifat universal. Suatu perbuatan yang dianggap sopan oleh sekelompok masyarakat mungkin saja dianggap tidak sopan bagi sekelompok masyarakat yang lain. Sejalan dengan sifat masyarakat yang dinamis dan berubah, maka norma kesopanan dalam suatu komunitas tertentu juga dapat berubah dari masa ke masa. Suatu perbuatan yang pada masa dahulu dianggap tidak sopan oleh suatu komunitas tertentu mungkin saja kemudian dianggap sebagai perbuatan biasa yang tidak melanggar kesopanan oleh komunitas yang sama. Dengan demikian secara singkat dapat dikatakan bahwa norma kesopanan itu tergantung pada dimensi ruang dan waktu. Sanksi terhadap pelanggaran norma kesopanan adalah berupa celaan, cemoohan, atau diasingkan oleh masyarakat. Akan tetapi sesuai dengan sifatnya yang “tergantung” (relatif), maka tidak jarang norma kesopanan ditafsirkan secara subyektif, sehingga menimbulkan perbedaan persepsi tentang sopan atau tidak sopannya perbuatan

tertentu. Sebagai contoh, beberapa tahun yang lalu ketika seorang pejabat di Jawa Timur sedang didengar kesaksiannya di pengadilan dan ketika seorang terdakwa di ibu kota sedang diadili telah ditegur oleh hakim ketua, karena keduanya dianggap tidak sopan dengan sikap duduknya yang "jegang" (menyilangkan kaki). Kasus ini menimbulkan tanggapan pro dan kontra dari berbagai kalangan dan menjadi diskusi yang hangat tentang ukuran kesopanan yang digunakan. Demikian pula halnya ketika advokat kenamaan di ibu kota berkecak pinggang di depan majelis hakim, yang oleh majelis hakim perbuatan itu bukan hanya dinilai tidak sopan, tapi lebih dari itu dinilai sebagai contempt of court (penghinaan terhadap pengadilan), sehingga tentu saja mempunyai implikasi hukum.

4. Norma Hukum

Norma hukum adalah aturan-aturan yang dibuat oleh lembaga negara yang berwenang, yang mengikat dan bersifat memaksa, demi terwujudnya ketertiban masyarakat. Sifat "memaksa" dengan sanksinya yang tegas dan nyata inilah yang merupakan kelebihan norma hukum dibanding dengan ketiga norma yang lain. Negara berkuasa untuk memaksakan aturan-aturan hukum guna dipatuhi dan terhadap orang-orang yang bertindak melawan hukum diancam hukuman. Ancaman hukuman itu dapat berupa hukuman bandan atau hukuman benda. Hukuman bandan dapat berupa hukuman mati, hukuman penjara seumur hidup, atau hukuman penjara sementara. Di samping itu masih dimungkinkan pula dijatuhkannya hukuman tambahan, yakni pencabutan hak-hak tertentu, perampasan barang-barang tertentu, dan pengumuman keputusan pengadilan. Demi tegaknya hukum, negara memiliki aparat-aparat penegak hukum, seperti polisi, jaksa, dan hakim. Sanksi yang tegas dan nyata, dengan berbagai bentuk hukuman seperti yang telah dikemukakan itu, tidak dimiliki oleh ketiga norma yang lain. Sumber hokum dalam arti materiil dapat berasal dari falsafah, pandangan hidup, ajaran agama, nilai-nilai kesusilaam,adat istiadat, budaya, sejarah dan lain-lain. Dengan demikian dapat saja suatu ketentuan norma hukum juga menjadi ketentuan norma-norma yang lain. Sebagai contoh, perbuatan mencuri adalah perbuatan melawan hukum (tindak pidana, dalam hal ini : kejahatan), yang juga merupakan perbuatan yang bertentangan dengan norma agama, kesusilaan (asusila), maupun kesopanan (a sosial). Jadi, diantara norma-norma tersebut mungkin saja terdapat kesamaan obyek materinya, akan tetapi yang tidak sama adalah sanksinya. Akan tetapi, sebagai contoh lagi, seorang

yang mengendari kendaraan bermotor tanpa memiliki SIM, meskipun tidak melanggar norma agama, akan tetapi melanggar norma hukum.

Sony Keraf (1991), ada dua macam norma :

1. **Norma Umum** adalah 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** adalah 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** adalah etika yang berbicara tentang fakta, yaitu nilai dan pola perilaku manusia yang terkait dengan situasi dan realitas yang membudaya dalam masyarakat
2. **Etika Normatif** adalah 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** yaitu sanki yang berupa teguran dari masyarakat, pengucilan dari masyarakat.
2. **Sanksi Hukum** yaitu sanki berupa 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

Seiring dengan pesatnya perkembangan Ilmu Pengetahuan dan Teknologi diharapkan taraf hidup manusia yang seutuhnya dapat dipertahankan dan tingkatkan. Oleh karena itu, disamping memahami dan menggunakan ilmu pengetahuan dan teknologi maka setiap insan manusia yang menggunakan ilmu pengetahuan dan teknologi harus memahami dan mendalami aturan-aturan atau etika yang terkait dengan ilmu pengetahuan dan teknologi itu sendiri.

Pemahaman terhadap etika tersebut harus benar-benar dihayati dan kemudian diterapkan pada saat penggunaan ilmu pengetahuan dan teknologi. Teknologi merupakan hasil ciptaan manusia agar dapat mempermudah pelaksanaan pekerjaan. Namun pada kenyataannya, keberadaan teknologi memberi dampak pada nilai sosial manusia tersebut dimana nilai sosial semakin berkurang, yang artinya teknologi semakin berpengaruh besar pada kehidupan manusia tersebut, misalnya penggunaan teknologi dalam berdemokrasi semakin bebas.

Di era sekarang ini manusia semakin bebas berkreasi dan semakin bebas berpendapat tanpa mempedulikan perasaan orang lain. Kebebasan berpendapat tidak dilarang asalkan pendapat yang disampaikan benar dan tidak merugikan orang lain karena terkadang tanpa disadari oleh manusia tersebut bahwa ia telah melanggar etika sosial bermasyarakat melalui teknologi informasi. Contohnya, penyebaran berita-berita bohong atau hoax. Untuk itu diperlukan aturan-aturan yang mengatur tentang kebebasan berpendapat melalui teknologi informasi. Sebagai contoh Undang-Undang ITE yang membatasi kebebasan berpendapat melalui teknologi informasi.

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 Informasi

BAB II
ETIKA PROFESI

A. Pengertian Profesi

Profesi dapat dikategorikan kedalam 2 bagian yaitu, profesi pada umumnya dan profesi yang luhur (Kansil dan Kansil, 1997). Secara umum Profesi adalah pekerjaan yang dilakukan sebagai kegiatan pokok agar dapat menghasilkan nafkah hidup dan yang mengandalkan/mengedepankan keahlian yang khusus.

Walaupun profesi dibedakan dengan pekerjaan oleh karena persyaratan keahlian yang khusus, namun tidak dapat disangkal bahwa sangat sulit untuk membedakan atau memisahkan kedua istilah tersebut.

Dengan demikian, pengertian Profesi diatas merupakan profesi pada umumnya sedangkan Profesi yang luhur adalah profesi yang pada hakikatnya merupakan suatu pelayanan pada manusia atau masyarakat (Kansil dan Kansil, 1997). Contoh profesi yang luhur adalah rohaniawan, dokter, wartawan, hakim, advokat, notaris, jaksa dan polisi.

Seseorang yang melaksanakan profesinya harus memiliki sifat-sifat, antara lain:

1. Harus menguasai ilmu pengetahuan yang terkait dengan tugas dan tanggung jawabnya atau *hard skills*.
2. Harus mampu menerapkan prinsip-prinsip etika atau *soft skills*
3. Harus memiliki integritas yang tinggi.
4. Harus mampu bekerja secara profesional. Secara profesional berarti hasil yang dikerjakan memuaskan atau akan dirasakan memuaskan oleh atasan yang memberi pekerjaan.

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 (Isnanto, 2009) :

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.

Dengan melihat ciri-ciri umum profesi diatas, maka dapat disimpulkan bahwa kaum profesional adalah orang-orang yang memiliki tolak ukur perilaku yang berada di atas ratarata. Di satu pihak ada tuntutan dan tantangan yang sangat berat, tetapi di lain pihak ada suatu kejelasan mengenai pola perilaku yang baik dalam rangka kepentingan masyarakat. Seandainya semua bidang kehidupan dan bidang kegiatan menerapkan suatu standar profesional yang tinggi, bisa diharapkan akan tercipta suatu kualitas masyarakat yang semakin baik (Isnanto, 2009).

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

Etika Profesi adalah bagian dari etika sosial yaitu filsafat atau pemikiran rasional tentang kewajiban dan tanggung jawab manusia sebagai anggota masyarakat lebih khusus dalam profesi dimaka manusia itu harus memberikan pertanggungjawaban atas apa yang manusia itu lakukan.

Agar supaya etika profesi dapat ditegakkan dengan baik maka baik profesi pada umumnya maupun profesi luhur hendaknya memiliki prinsip-prinsip dan disertai kode etik atau persyaratan-persyaratan yang harus dipatuhi setiap orang yang terlibat dalam suatu organisasi, untuk dapat dijadikan pedoman bagi tercapainya suatu komitmen yang telah

disepakati dalam memajukkan suatu usaha/organisasi terutama dalam memberikan pelayanan kepada masyarakat.

Prinsip-prinsip Etika Profesi pada umumnya dapat berupa prinsip menjalankan profesinya secara bertanggung jawab, komitmen, kejujuran dan hormat terhadap hak-hak orang lain. Sedangkan prinsip-prinsip Etika Profesi yang luhur terdapat pula dua prinsip yaitu mendahulukan kepentingan orang yang dibantu, apakah itu klien atau pasien, dan mengabdi pada tuntutan luhur profesi.

Contohnya, adalah seorang advokat tidak boleh mengelabui hakim dengan menyatakan orang yang dibelanya tidak bersalah demi untuk memenangkan perkara dan mendapat bayaran tinggi dari kliennya. Contoh lainnya, seorang sekretaris, tidak boleh membocorkan rahasia atasannya langsung kepada pimpinan perusahaan yang lain supaya bisa mendapatkan tambahan insentif dari perusahaan.

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. Kode Etik Profesi

Kode etik profesi adalah norma yang ditetapkan dan diterima oleh kelompok profesi yang mengarahkan atau memberi petunjuk kepada anggotanya bagaimana seharusnya berbuat dan sekaligus menjamin mutu moral profesi itu dimata masyarakat (Bartens, 1985).

Kode etik profesi adalah produk etika terapan karena dihasilkan berdasarkan penerapan pemikiran etis atas suatu profesi. Kode etik profesi dapat berubah dan diubah seiring dengan perkembangan ilmu pengetahuan dan teknologi, sehingga anggota kelompok profesi tidak akan ketinggalan jaman.

Selanjutnya, kode etik profesi adalah hasil pengaturan diri profesi yang bersangkutan dan ini perwujudan moral yang hakiki, yang tidak dapat dipaksakan dari luar. Kode etik profesi hanya berlaku efektif apabila dijiwai oleh cita-cita dan nilai-nilai yang hidup dalam lingkungan profesi itu sendiri.

Kode etik profesi pada dasarnya adalah norma perilaku yang sudah dianggap benar dan tentunya lebih efektif lagi apabila norma perilaku itu dirumuskan secara baik, sehingga memuaskan semua pihak. Dengan demikian, kode etik profesi adalah kriteria prinsip profesional yang telah ditetapkan, yang harus diketahui dengan pasti oleh anggota

kelompok profesi, baik yang lama, baru, ataupun yang akan menjadi anggota kelompok profesi. Hal ini berarti bahwa kode etik profesi menentukan standar kewajiban profesional para anggota kelompok profesi.

Kode etik profesi perlu dirumuskan dan dijabarkan secara tertulis agar para pelaku profesi dapat memahami dengan pasti sehingga menerapkan kode etik profesi tersebut.

Menurut Sumaryono (1995), kode etik profesi dapat dijadikan:

a. Sebagai sarana kontrol sosial
b. Sebagai pencegah campur tangan pihak lain
c. Sebagai pencegah kesalahpahaman dan konflik

Ada beberapa hal yang menjadi penyebab pelanggaran kode etik profesi yang biasanya terjadi di lingkungan organisasi (Yoel Hulu, 2015), antara lain :

a. Pengaruh jabatan

   Misalnya yang melakukan pelanggaran kode etik profesi itu adalah pimpinan atau orang yang memiliki kekuasaan yang tinggi pada profesi tersebut, maka bisa jadi orang lain yang posisi dan kedudukannya berada di bawah orang tersebut, akan enggan untuk melaporkan kepada pihak yang berwenang memberikan sangsi, karena kekhawatiran akan berpengaruh kepada jabatan dan posisinya pada profesi tersebut.
b. Pengaruh masih lemahnya penegakan hukum di Indonesia, sehingga menyebabkan pelaku pelanggaran kode etik profesi tidak merasa khawatir melakukan pelanggaran.
c. Tidak berjalannya kontrol dan pengawasan dari masyarakat.
d. Organisasi profesi tidak dilengkapi denga sarana dan mekanisme bagi masyarakat untuk menyampaikan keluhan.
e. Rendahnya pengetahuan masyarakat mengenai substansi kode etik profesi, karena buruknya pelayanan sosialisasi dari pihak profesi sendiri.
f. Belum terbentuknya kultur dan kesadaran dari para pengemban profesi untuk menjaga martabat luhur profesinya.
g. Pengaruh sifat kekeluargaan

   Misalnya, yang melakukan pelanggaran adalah keluarga atau dekat hubungan kekerabatannya dengan pihak yang berwenang memberikan sangsi terhadap pelanggaran kode etik pada suatu profesi, maka ia akan cendrung untuk tidak

memberikan sangsi kepada kerabatnya yang telah melakukan pelanggaran kode etik tersebut.

Faktor yang mempengaruhi pelanggaran etika, antara lain:

a. Kebutuhan individu, contohnya korupsi karena alasan ekonomi
b. Tidak ada pedoman, karena area "abu-abu", sehingga tak ada panduan
c. Perilaku dan kebiasaan individu contohnya kebiasaan yang terakumulasi tak dikoreksi
d. Lingkungan tidak etis contohnya pengaruh dari komunitas
e. Perilaku orang yang ditiru contohnya efek primordialisme yang kebablasan

Sedangkan sangsi pelanggaran etika antara lain:

a. Sanksi Sosial, skala relative kecil, dipahami sebagai kesalahan yang dapat "dimaafkan".
b. Sanksi Hukum, skala besar, merugikan hak pihak lain. Hukum pidana menempati prioritas utama, diikuti oleh hukum Perdata.

F. 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)

G. 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 professional
   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.

BAB III
PROFESIONALISME 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 profesionalberkesinambungan.

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 tentangnorma dan etika profesi pekerja dibidang TI.
c. Masih belum ada (mungkin) organisasi profesional yang menangani para profesional dibidang TI.

B. Kompetensi Bidang Teknologi Informasi

Berikut adalah jenis-jenis kompetensi bidang teknologi informasi yang harus dimiliki:

1. Keterampilan pendukung solusi IT
    a. Mampu menghubungkan perangkat keras.
    b. Mampu melakukan instalasi sistem operasi baik windows maupun linux, dan sistem operasi jaringan.

c. Mampu melakukan konfigurasi mail server, ftp server, web server.

d. Memahami fungsi perangkat jaringan seperti routing, modem, HUB, dll.

e. Memiliki kemampuan mengoperasikan perangkat keras.

f. Memiliki keahlian dalam memperbaiki jaringan komputer.

g. Memiliki keampuan untuk mengelola jaringan komputer.

h. Dapat melakukan monitor terhadap jaringan komputer.

i. Dapat mengelola databse dan melakukan perintah sederhana ke dalam database.

j. Mampu melakukan pengelolaan terhadap website .

k. Memiliki keterampilan dalam memperbaiki kerusakan sederhana komputer dan perangkat keras lainnya.

l. Mengetahui fungsi perangkat input dan output.

2. Keterampilan Pengguna IT

a. Memahami fungsi sistem operasi

b. Dapat menjalankan program sederhana

c. Memahami cara kerja sistem informasi

d. Dapat mengakses database

e. Dapat memahami fungsi sederhana dalam database

f. Dapat melakukan proteksi terhadap keamanan data pribadi

g. Memahami fungsi perangkat input, proses dan ouput

h. Dapat menggunakan teknologi internet

i. Dapat melakukan pengiriman pesan melalui surat elektronik atau aplikasi perpesanan.

j. Dapat mengakses sebuah situs website.

3. Pengetahuan Bidang IT

   a. Mengetahui informasi terbaru mengenai perkembangan sistem informasi

   b. Mengetahui fungsi dasar perangkat komputer

   c. Memiliki pengetahuan yang cukup dalam bisnis di bidang teknologi informasi

   d. Memiliki pengetahuan dalam proses komunikasi digital

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.

     Sistem Analis atau Analis Sistem merupakan seseorang yang bertanggung jawab terhadap suatu bentuk penelitian, perencanaan, pengkoordinasian dan merekomendasikan pemilihan perangkat lunak serta sistem yang memang paling sesuai dengan kebutuhan organisasi suatu bisnis, instansi ataupun perusahaan. Sistem Analiss ini memegang peranan yang sangat penting di dalam suatu proses pengembangan sistem. Seorang analis sistem harus mampu mempunyai berbagai macam keahlian diantaranya yaitu mengalisasi kebutuhan sistem dan user, mampu

melakukan koordinasi manajemen dan tim dan mempunyai kemampuan interpersonal yang baik agar dapat bekerja dengan tim dan komunikasi dengan user.

Sistem Analis harus bisa memahami perilaku organisasi, beserta dengan fungsi-fungsinya. Sistem Analis harus memiliki kemampuan mengidentifikasi segala bentuk kemungkinan terbaik, mrancang rumusan masalah dan melakukan suatu analisis terhadap penyelesaian masalah yang tengah dihadapi.

Keahlian teknis mampu membantu seorang Analis Sistem dalam memahami potensi dan keterbatasan dari Teknologi Informasi. Sistem Analis diharuskan memiliki kemampuan dan menguasai berbagai macam atau jenis bahasa pemrograman, sistem operasi, hingga perangkat keras yang digunakan.

Keahlian manajerial dapat membantu Sistem Analis dalam mengelola proyek, sumber daya, resiko dan adanya suatu bentuk perubahan. Keahlian interpersonal sendiri mampu membantu seorang analis sistem untuk melakukan suatu bentuk interaksi terhadap pengguna akhir sebagaimana halnya dengan analis, programmer dan profesi sistem yang lain

- *Programmer*, merupakan orang yang bertugas mengimplementasikan rancangan sistem analis yaitu membuat program (baik aplikasi maupun sistem operasi) sesuai sistem yang dianalisa sebelumnya. Programmer atau biasa disebut dengan pemrogram komputer, pemrogram, pengembang perangkat lunak atau seorang ahli pengolahan dan penataan merupakan suatu bentuk profesi yang menulis program dengan menggunakan bahasa pemrograman.

  Secara umum Programmer ini dikelompokkan atas 2 kelompok utama, yakni kelompok programmer aplikasi dan programmer sistem. Programmer aplikasi, menulis suatu bentuk program yang digunakan untuk menangani suatu tugas khusus seperti program untuk melacak suatu bentuk persediaan barang yang ada di suatu organisasi yang ada. Programmer aplikasi, menulis suatu bentuk program yang digunakan untuk menangani suatu tugas khusus seperti program untuk melacak suatu bentuk persediaan barang yang ada di suatu organisasi yang ada.

  Sedangkan Programmer sistem adalah programmer yang menulis suatu program dan digunakan untuk memelihara dan mengendalikan perangkat lunak sistem komputer,

seperti sistem operasi dan sistem manajemen basis data (*database*). Programmer sistem akan membuat suatu program yang akan menentukan bagaimana jaringan komputer, komputer, hingga CPU itu bekerja dengan baik. Programmer juga dapat dibedakan melalui kategori pemrograman berbasis aplikasi dan pemrograman berbasis web

- *Web designer* adalah orang yang melakukan kegiatan perecanaan, termasuk studi kelayakan, analisis dan desain terhadap suatu proyek pembuatan aplikasi berbasisweb.

  Web Design atau Perancangan Web merupakan suatu bentuk istilah umum yang biasa digunakan untuk mencakup bagaimana isi web konten tersebut bisa ditampilkan kepada pengguna, yang biasanya itu berupa *hypertext* atau *hypermedia*, yang dikirimkan ke pengguna akhir. Web Designer mengirimkan melalui *World Wide Web* (WWW) yang menggunakan suatu browser web atau perangkat lunak berbasis web. Tujuan dari perancangan tersebut adalah untuk membuat halaman sebuah website yang berisi dokumen dan aplikasi yang ada di server web atau sebuah server. Halaman website adalah tampilan yang berupa sekumpulan teks, gambar, suara dan konten yang lain, yang mana bisa juga memiliki sifat interaktif ataupun statis. Web Designer (Perancang Web) adalah pekerjaan yang memiliki keahlian dalam menciptakan dan merancang konten presentasi yang dikirimkan kepada pengguna akhir melalui sebuah tampilan yang interaktif, statis ataupun dinamis ke dalam sebuah *World Wide Web* (WWW). Tampilan tersebut dapat diakses oleh suatu web browser atau perangkat lunak *web-enabled* yang lain, seperti televisi internet, microblogging, RSS dan lain sebagainya.

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

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.

  Techcnical engineer atau sering disebut teknisi adalah orang yang harus memiliki keterampilan dan penguasaan teknik yang terkait dengan cabang teknik tertentu, dengan adanya pemahaman yang praktis serta mempunyai konsep teknik fundamental umum. Teknisi sering membantu seorang insinyur ataupun orang yang berkecimpung di dalam dunia teknologi yang sedang berada di suatu proyek baik itu dalam penelitian maupun dalam pengembangan. Seorang *Techcnical Engineer* harus mampu beradaptasi dengan lingkungan tempat dimana orang tersebut bekerja dan harus mampu memcahkan teknis sesuai dengan kalibrasi tertentu. *Techcnical Engineer* harus dapat menyelesaikan permasalahan-permasalahan user dan sistem sesuai dengan batasan permasalahannya serta harus dapat melakukan uji coba sistem secara keseluruhan.

- Networking Engineer, adalah orang yang berkecimpung dalam bidang teknis jaringan komputer dari maintenance sampai pada *troubleshooting*-nya. Network Engineer harus dapat bekerja di dalam bidang yang ada kaitannya dengan layanan dari suatu jaringan, melakukan analisa, pemeliharaan jaringan, hingga melakukan *troubleshooting* jaringan. Administrator Jaringan bertugas memelihara infrastruktur komputer dengan penekanan terhadap suatu jaringan. Administrator Jaringan juga bertanggung jawab untuk melakukan monitoring jaringan (memantau), melakukan pengujian jaringan, menginstal dan menerapkan program keamanan jaringan, melakukan evaluasi serta melakukan implementasu pada jaringan. Salah satu sertifikasi yang harus dimiliki orang yang bekerja di dalam jaringan adalah Cisco.

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 organisasilainnya.

  Electronic Data Processing (EDP) merupakan suatu metode di dalam pemrosesan data komersial. Sebagai salah satu bagian dari Teknologi Informasi, maka seorang EDP Operator harus mampu melakukan suatu bentuk pemrosesan data secara berulang kali terhadap data yang sama dengan bentuk pemrosesan yang bisa dikatakan relatif lebih sederhana.Contoh pemrosesan data elektronik ini digunakan sebagai pemutakhiran atau update stock di dalam suatu daftar barang (*inventory*), pemrosesan transaksi nasabah bank, pemrosesan booking untuk tiket (bus, kereta, kapal, hingga pesawat terbang), sistem reservasi dan hotel, sistem pembayaran tagihan online, Sistem penjualan tiket konser, dan lan-lain.

- 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.

  System Administrator atau *sysadmin* merupakan orang yang bertanggung jawab penuh terhadap suatu bentuk pemeliharaan, konfigurasi dan pengoperasian sistem komputer yang andal, terutama dalam komputer multi-user, contohnya server. Seorang System Administrator berusaha untuk memastikan tetap uptime, kinerja, sumber daya, hingga keamanan komputer yang ia monitor mampu memenuhi kebutuhan dari pengguna tanpa harus membebankan anggaran yang lebih. System Administrator harus memiliki kemampuan untuk melakukan upgrade komponen komputer dan perangkat lunak komputer, memberikan pengecekan secara rutin, harus dapat memelihara suatu bentuk kebijakan keamanan, harus dapat memecahkan masalah, memiliki kemampuan untuk melatih atau mengawasi setiap staf, dan maemberikan penawarkan dukungan teknis terhadap suatu proyek.

- 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. MIS Director *(Management Information System),* merupakan orang yang memiliki wewenang paling tinggi terhadap sebuah system informasi, melakukan manajemen terhadap system tersebut secara keseluruhan baik perangkat keras, perangkat lunak maupun sumber daya manusianya. MIS Director bertanggung jawab untuk mengelola orang, hubungan dengan vendor, dan operasi bisnis. MIS Director juga harus dapat melakukan riset teknologi dan industri tren dan menghadiri konferensi bisnis. MIS Director harus memastikan bahwa sistem dan teknologi bekerja secara efektif dan dapat diandalkan. Seorang MIS Director dituntut untuk memastikan bahwa perusahaan menggunakan teknologi komputer aman. Mereka biasanya berkoordinasi dengan keamanan perusahaan untuk melihat bahwa sesuai langkah-langkah yang diambil untuk melindungi perusahaan dan klien. MIS Director juga bertugas untuk mengawasi sistem yang berjalan dan menyusun strategi untuk memenuhi tujuan produksi mereka saat ini tetapi juga harus melihat ke masa depan.

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 TeknologiInformasi.

Secara umum, sebutan lain untuk berbagai jenis pekerjaan di bidang teknologi informasi:

1. *Programmer*

   Membuat program, aplikasiatau sistem operasi dengan menggunakan bahasa pemrograman tertentu.

2. *Software engineering*

   Pekerjaan yang mengharuskan memiliki keterampilan dalam pengembangan sistem informasi dimulai dari tahapn perencanaan, analisa, desain, implementasi hingga pegujian dan pemeliharaan.

3. *Hardware engineering*

   Pekerjaan yang mengharuskan memiliki keahlian dalam mengembangkan pengembangan perangkat keras yang akan digunakan untuk implementasi sistem informasi.

4. *System analyst*

   Pekerjaan yang membutuhkab keahlian untuk menganalisa kebutuhan sistem dan user. System anayst atau analis sistem harus memiliki keahlian dalam membuat analisa kebutuhan user, memahami keingin user, membaca dan membuat gambaran berdasarkan kebutuhan user dan menuangkan ide atau gagasan ke dalam bentuk diagram. System analyst harus teliti menjelaskan kebutuhan sisi user dan mengkombinasikannya ke dalam kebutuhan sistem, merancangan sistem usulan yang dibutuhkan oleh user dan menerjemahkannya ke dalam kebutuhan sistem.

5. *Database administrator*

   Pekerjaan yang membutuhkan keahlian untuk mendesain, mengimplementasikan, memelihara dan mengelola database.

6. *Web administrator*

   Pekerjaan yang membutuhkan keahlian teknis terhadap operasional sebuah situs atau website, bertanggung jawab terhadap pengelolaan situs atau website serta melakukan pemeliharaan terhadap jalannya sebuah situs atau website.

7. *Network engineering*

   Pekerjaan yang membutuhkan keahlian teknis untuk pengembangan jaringan, implementasi jaringan, pemeliharaan jaringan komputer dan perbaikan jaringan komputer serta memahami teknis komunikasi data antara komputer.

8. *Network architecture*

   Pekerjaan yang membutuhkan keahlian dalam mendesain skema jaringan komputer, merancang stopologi jaringan komputer, menghubungkan skema satu komputer dengan komputer lain, memahami fungsi dan perangkat jaringan, membangun dan melakukan pengujian terhadapn jaringan komunikasinya.

9. *Web developer*

Pekerjaan yang membutuhkan keterampilan dalam pengembangan sebuah situs website. Web developer harus mampu merancang kebutuhan sistem dalam pembuatan situs website, dan membuat dapat diaksesnya halaman website dengan menggunakan jaringan komputer. Web developer harus mampu mengembangan sebuah situs website dan menampilkan situs website sehingga dapat diakses oleh user, serta melakukan pemeliharaan sistemnya.

10. *IT support*

Pekerjaan yang membutuhkan keahlian dalam mengatasi masalah umum yang terjadi pada komputer seperti install software, perbaikan hardware, perbaikan jaringan komputer, perbaikan komunikasi jaringan komputer di antara user, pemeliharaan rutin dan sederhana dari sebuah sistem 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.

	Programmer	System Analyst	Project Manager	Instructor	Specialist
Independent/ Managing					
Moderately Supervising					
Supervised					

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

- *Programmer*

  Merupakan bidang pekerjaan untuk melakukan pemrograman komputer terhadapsuatu 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 pelaksanaantugasnya.
  2. *Moderately supervised* (madya). Tugas kecil dapat dikerjakan oleh mereka tetapi tetap membutuhkan bimbingan untuk tugas yang lebih besar, 3-5 tahunpengalaman
  3. *Independent/Managing* (mandiri). Memulai tugas, tidak membutuhkan bimbingan dalam pelaksanaantugas.

- *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:

  - DataCommunication
  - DatabaseSecurity
  - QualityAssurances
  - ISAudit
  - System SoftwareSupport
  - DistributedSystem
  - SystemIntegration

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 tentululus.
2. Kemampuan yang kurang memadai terhadap penguasaan materisertifikasi
3. Dibutuhkan pengetahuan dan kemampuan diatas rata-rata untuk lulussertifikasi.

E. Standarisasi Profesi IT

Pengelompokkan profesi di kalangan teknologi informasi juga dapat didasarkan pada *South East Asia Regional Computer Confideration* (SEARCC) . SEARCC adalah suatu forum atau badan yang beranggotakan himpunan profiesional IT yang terdiri dari 13 negara. SEARCC dibentuk pada Februari 1978 di negara Singapura oleh 6 ikatan komputer yang terdiri dari negara-negara berikut yaitu Hong Kong, Indonesia, Malaysia, Philipina, Singapore dan Thailand.

SEARCC mengadakan konferensi setahun dua kali di tiap negara anggotanya secara berkala.Saat ini jumlah negara yang mengikuti SEARCC semakin bertambah anggotanya, maka konferensi rutin dilakukan setiap tahun.. Negara lain yang saat ini ikut bergabung menjadi anggota SEARCC adalah Sri Lanka, Australia, Hong Kong, India Indonesia, Malaysia, New Zealand, Pakistan, Philipina, Singapore, Korea Selatan, Taiwan, Thailand, Kanada.

Salah satu kegiatan dari SEARCC adalah SRIG-PS (*Special Regional Interest Group on Profesional Standardisation*). SRIG-PS dibentuk karena adanya kebutuhan untuk menciptakan dan menjaga standard profesional yang tinggi dalam dunia Teknologi Informasi, khususnya ketika sumber daya di region ini memiliki kontribusi yang penting bagi kebutuhan pengembangan teknologi informasi secara global.

SRIG-PS dibentuk karena adanya kebutuhan untuk menciptakan dan menjaga standard profesional yang tinggi dalam dunia Teknologi Informasi, khususnya ketika sumber daya di region ini memiliki kontribusi yang penting bagi kebutuhan pengembangan TI secara global. SRIG-PS diharapkan memberikan berupa kode etik , klasifikasi pekerjaan dalam bidang teknologi informasi, panduan metoda sertifikasi dalam TI, dan Promosi dari program yang disusun oleh SRIG-PS di tiap negara anggota SEARCC.

Pada pertemuan yang ke empat di Singapore, Mei 1994, tiga dari empat point tersebut hampir dituntaskan dan telah dipresentasikan pada SEARCC 1994 di Karachi. Dalam pelaksanaannya kegiatan SRIG-PS ini mendapat sponsor dari Center of International Co

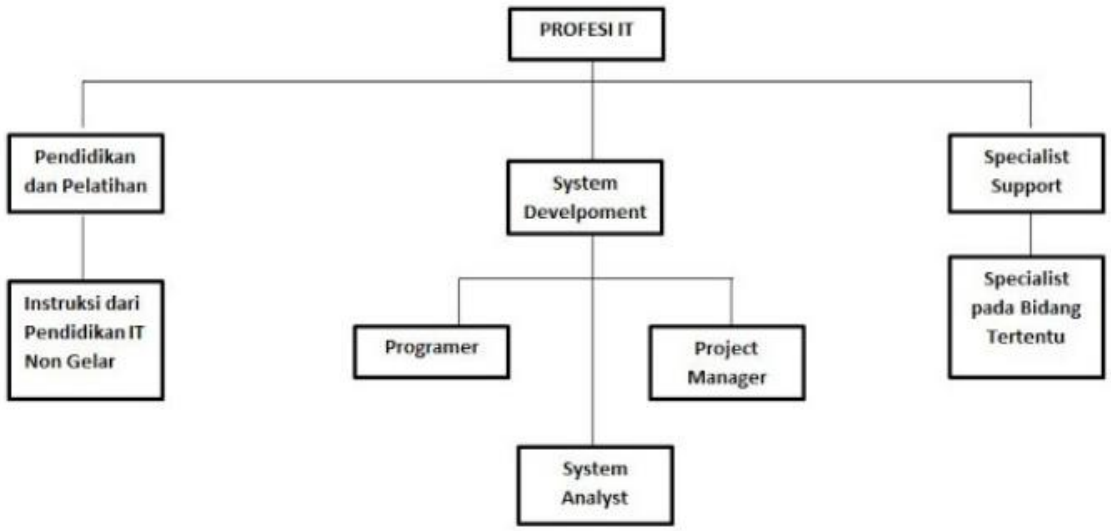
operation on Computerization (CICC). Hasil kerja tersebut dapat diperoleh di Central Academy of Information Technology (CAIT), Jepang. Pelaksanaan SRIG-PS dilakukan dalam 2 phase. Phase 1, hingga pertemuan di Karachi telah diselesaikan. Kini memasuki phase ke 2 hingga diselesaikannya panduan model SRIG-PS, phase ke 2 ini akan diselesaikan di SEARCC 97 di New Delhi.

Beberapa model yang dikembangkan yaitu:

- **Model SEARCC**

  Model SEARCC adalah model dua dimensi yang mempertimbangkan jenis pekerjaan dan tingkat keahlian ataupun tingkat pengetahuan yang dibutuhkan.

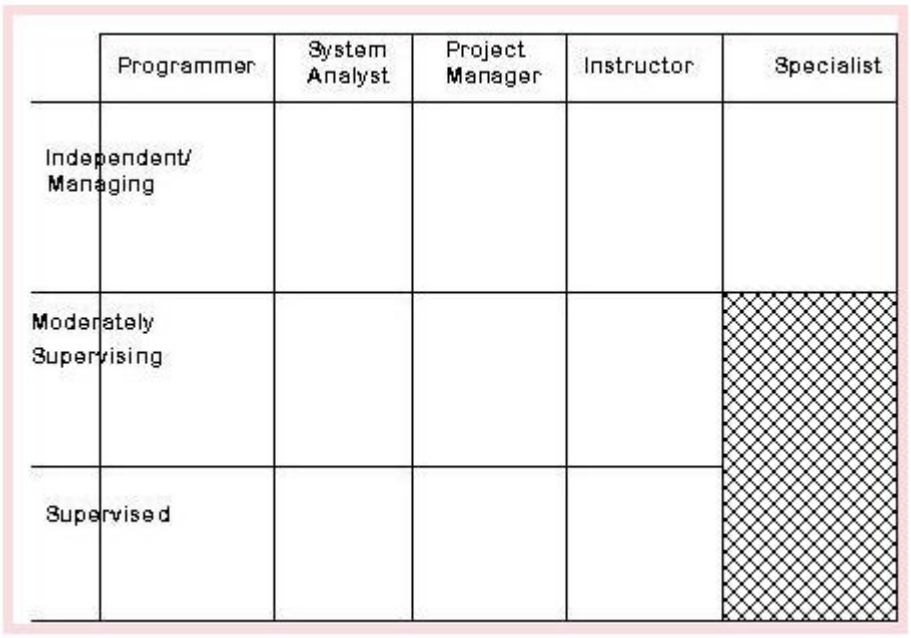
  Berikut adalah gambarannya:



Gambar 3 :Model SEARCC

Beberapa kriteria yang menjadi pertimbangan klasifikasi job model SEARCC :

1. *Cross Country, Cross-enterprise applicability,* job harus relevan dengan kondisi region yang memiliki kesamaan pemahaman
2. Function Oriented *bukan* Tittle Oriented, *gelar bisa berbeda, yang penting fungsinya sama*
3. Testable/Certifiable, *job dapat ditukar atau diuji*
4. Applicable, *harus dapat diterapkan pada mayoritas profesional TI di region masing-masing*



Gambar 4 :Pembagian Job Model SEARCC SRIG-PS

Standar model SRIG-PS SEARCC memiliki dua pendekatan dalam melakukan pengklasifikasian pekerjaan. Kedua pendekatan tersebut adalah:

a. Model yang berbasiskan industri atau bisnis. Pada model ini pembagian pekerjaan diidentifikasikan oleh pengelompokan kerja di berbagai sektor di industri Teknologi Informasi. Model ini digunakan oleh Singapore dan Malaysia.

b. Model yang berbasiskan siklus pengembangan sistem. Pada model ini pengelompokkan dilakukan berdasarkan tugas yang dilakukan pada saat pengembangan suatu sistem. Model pendekatan ini digunakan oleh Japan.

Pengelompokkan profesi IT berdasarkan standar model tersebut adalah

a. Programmer

Bidang pekerjaan yang 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). Tingkatan dengan tugas kecil yang dapat dikerjakan oleh mereka tetapi tetap membutuhkan bimbingan untuk tugas yang lebih besar, 3-5 tahun pengalaman.

3) *Independent/Managing* (mandiri). Tingkatan pekerjaan yang tugasnya dimulai tidak membutuhkan bimbingan dalam pelaksanaan tugas

b. System Analyst

Bidang pekerjaan yang 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.

c. *Project Manager (PM)*

Bidang pekerjaan yang 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.

d. *Instructor*

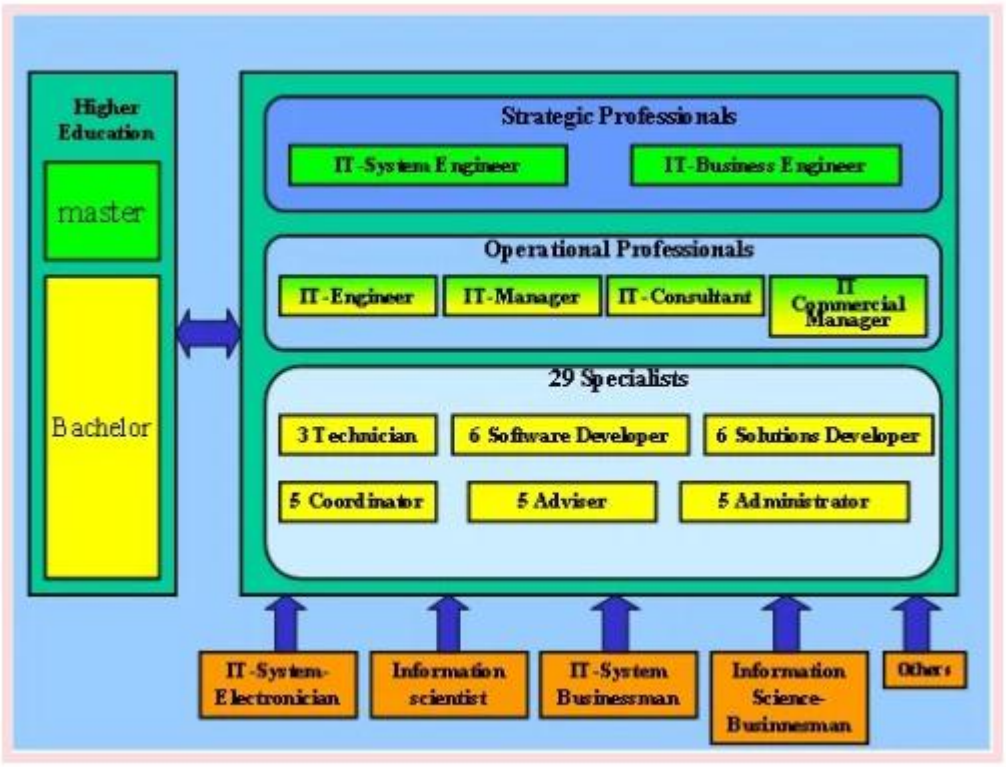
Bidang pekerjaan yang berperan dalam melakukan bimbingan, pendidikan dan pengarahan baik terhadap anak didik maupun pekerja level di bawahnya. Jenis pekerjaan ini juga memiliki 3 tingkatan seperti halnya pada programmer.

e. *Specialist*

Bidang 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



Gambar 5 :Lapisan Bidang IT

Secara umum, ada terdapat 3 lapisan bidang IT (gambar 3). Ketiga lapisan itu adalah:

1. Lapisan pertama (spesialis). Lapisan ini meliputi 6 golongan karakteristik profil, yaitu *software developer*, *technician*, *solution developer*, *coordinator*, *adviser* dan *administrator*. Lapisan ini memiliki 29 profil profesi secara keseluruhan.
2. Lapisan kedua. Lapisan ini terdiri dari 4 profil profesi, yaitu *IT Engineer*, *IT Manager*, *IT Consultan*t dan *IT Commercial Manager*.

3. Lapisan ketiga. Lapisan ini terdiri dari 2 profil profesi, yaitu *IT System Engineer* dan *IT Bussiness Engineer*.

- **Model British Company Society**

  Model British Computer Society (BCS) adalah suatu model yang komprehensif, tetap berlangsung dan mudah dipahami. T etapi bukanlah suatu sistem sertifikasi, tetapi suatu model untuk acuan program pengembangan profesi. Model Japan Information Technology Engineer Examination (JITEE) adalah komprehensif, tetapi tidak ada yang tertulis dalam bahasa Inggris. Berdasarkan kemungkinan yang tercocok pemetaan dilakukan terhadap model BCS, dan Japan IT Engineer Model.

  Untuk model BCS pekerjaan diklasifikasikan dalam tingkatan sebagai berikut :

  1. Unskilled Entry
  2. Standard Entry
  3. Initially Trainded Practitioner
  4. Trained Practitioner
  5. Fully Skilled Practitioner
  6. Experienced Practitioner/Manager
  7. Specialist Practitioner/Manager
  8. Senior Specialist/Manager
  9. Principal Specialist/Experienced Manager
  10. Senior Manager/Director

Setiap sel dari model BCS/ISM ditentukan berdasarkan :

a. Latar belakang akademik

b. Pengalaman dan tingkatan keahlian

c. Tugas dan atribut

d. Pelatihan yang dibutuhkan.

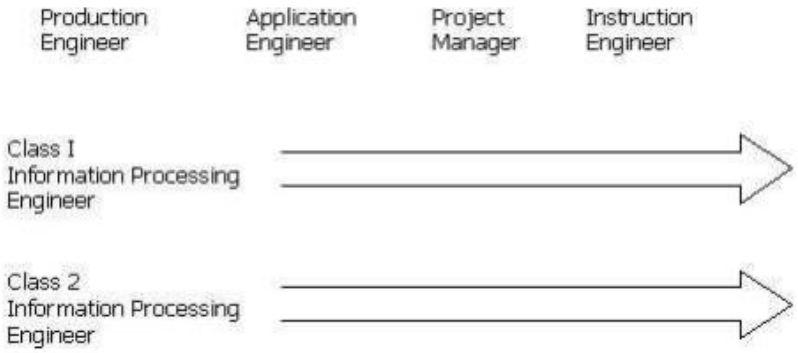
Berikut pemetaan gambar model BCS

	Programmer	System Analyst	Project Manager	Instructor	Specialist
9 Independent/ Managing 8 7	DLS 5	DLBA 2 DLS 5	DLM 8 DLM 7	ETT 6	
6 Moderately 5 Supervising 4 3	DLP 3	DLAD 4	DLM 6 DLM 5	ETT 5 ETT 4	
2 Supervised 1 0	DLP 1 DLP 2	DLAD 2 DLAD 3	DLM 4	ETT 2 ETT 3	

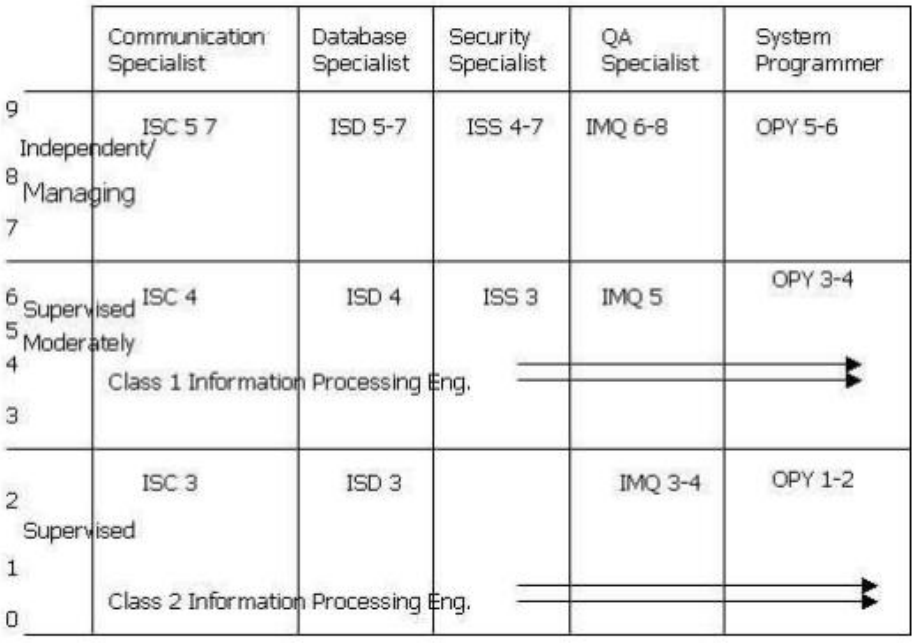
Gambar 6 :BCS Model

- **Model Japan ITEE Engineer**

Model JITEE mendefinisikan setiap cell berdasarkan Fungsi, Pengalaman, Pengetahuan, keahlian dan kemampuan.



Gambar III.6 Model JITEE



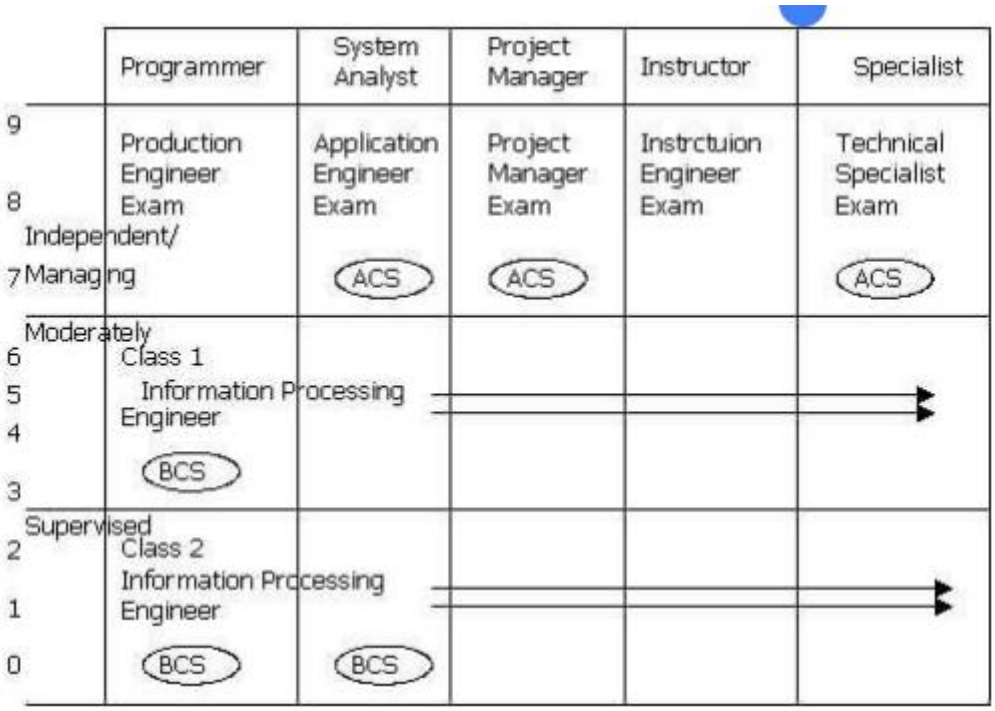
Gambar 7 : Pemetaan Spesialisasi JITEE

- **Model Sertifikasi**

  Sertifikasi berbeda dengan ujian, lisensi ataupun registrasi. Registrasi mungkin berguna untuk statistik, tetapi tidak praktis untuk diterapkan akan lebih bermanfaat dengan sertifikasi. Untuk sertifikasi, inisiatif harus lahir dari sektor industri d an untuk bidang teknologi informasi sebaiknya berfokus pada model SRIG-PS. Sertikasi pada model SRIG-PS berbeda dengan badan lain seperti IEEE. Sertifikasi pada model SRIG-PS adalah independen, obyektif, dan tugas yang regular bagi kepentingan profesional dalam satu atau lebih area di teknologi informasi. Sedangkan sertifik asi IEEE adalah suatu jaminan tertulis, yang merupakan suatu demonstrasi formal yang merupakan konfirmasi dan merupakan suatu sistem atau komponen dari suatu persyaratan tertentu dan diterima untuk keperluan operasi. Sertifikasi ini memiliki tujuan untuk membentuk tenaga praktisi TI yang berkualitas tinggi, serta standar kerja TI yang tinggi, juga pengembangan profesional yang berkesinambungan. Sedangkan bagi tenaga TI profesional tersebut sertifikasi ini merupa kan pengakuan akan pengetahuan yang kaya (bermanfaat bagi promosi, gaji), perencanaan karir, profesional development, dan meningkatkan international marketability. Ini sangat penting dalam kasus, ketika tenaga TI tersebut harus bekerja pada perusahaan m ultinasional. Perusahaan akan mengakui keahliannya apabila telah dapat menunjukkan sertifikat tersebut. Dan bagi masyarakat luas sertifikasi ini menjadikan mereka memiliki staf yang up to date dan berkualitas tinggi. Juga untuk memperoleh citra perusahaan yang baik, keuntungan yang kompetitif, merupakan alat ukur yang obyektif terhadap kemampuan staf, k ontraktor dan konsultan. Secara langsung dan tidak langsung akan meningkatkan produktifitas secara mikro maupun makro.

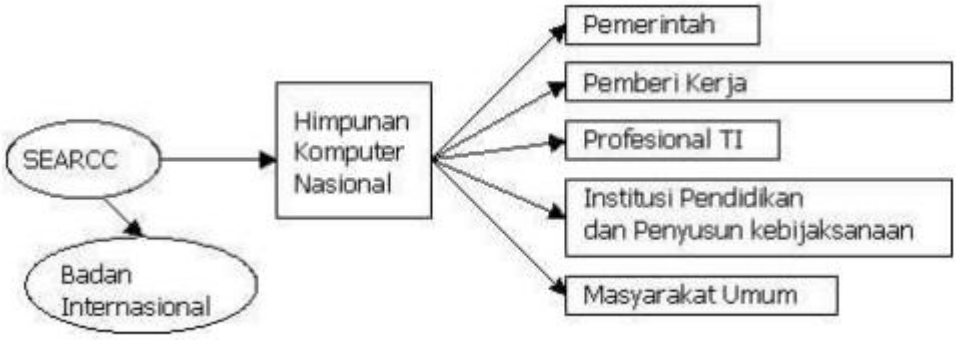
  Beberapa negara telah mengembangkan dan mempromosikan sistem sertifikasi yang khas bagi negara tersebut. Beberapa negara menerapkan dan membayar lisensi kepada sistem sertifikasi yang ada. Beberapa negara menbnggunakan tenaga ahli untuk melakukan uji an.

Untuk melakukan perbandingan terhadap sertifikasi yang dikembangkan oleh model SRIGPS dan sertifikasi yang telah ada maka digambarkan pada berikut:



Gambar 8 : Pemetaan sertifikasi SEARCC

- **Promosi Model SRIG**



Gambar 9 : Promosi Model SRIG-PS

Promosi ini memiliki berbagai sasaran, pada tiap sasaran tujuan yang ingin dicapai adalah berbeda-beda.

1. Pemerintah. Untuk memberi saran kepada pemerintah, dan pembuat kebijaksanaan dalam bidang TI dalam usaha pengembangan sumber daya manusia khususnya bidang TI.
2. Pemberi Kerja. Untuk membangkitkan kesadaran di antara para pemberi kerja tetang nilai-nilai dari standard profesional dalam meningkatkan kualitas profesional TI.
3. Profesional TI. Untuk mendorong agar profesional TI, dari negara anggota melihat nilai-nilai standar dalam profesi dan karir mereka.
4. Insitusi dan Penyusun kebijaksanaan Pendidikan. Untuk memberi saran pada pembentukan kurikulum agar dapat memenuhi kebutuhan dan standard profesional di regional ini dalam Teknologi Informasi.

5. Masyarakat Umum. Untuk menyadarkan umum bahwa Standard Profesional Regional adalah penting dalam menghasilkan produk dan jasa yang berkualitas.

Untuk mempromosikan model standardisasi dalam dunia TI ini, SEARCC memiliki berbagai perencanaan kampanye antara lain :

1. Publikasi dari Standard Profesional Regional diterbitkan di seluruh negara anggota
2. Presentasi secara formal di tiap negara anggota.
3. Membantu implementasi standard di negara-negara anggota
4. Memonitor pelaksanaan standard melalui Himpunan/Ikatan nasional
5. Melakukan evaluasi dan pengujian
6. Melakukan perbaikan secara terus menerus
7. Penggunaan INTERNET untuk menyebarkan informasi mengenai standard ini.

Untuk mengimplementasi promosi di Phase 2, SRIG-PS memperoleh dana bantuan yang akan digunakan untuk :

1. Biaya publikasi : disain, percetakan dan distribusi
2. Presentasi formal di negara anggota
3. Membantu implementasi standar di negara anggota
4. Pertemuan untuk mengkonsolidasi, memonitor, dan bertukar pengalaman

BAB IV
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 yangberlaku.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung denganinternet.
3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial yang cenderung lebih besar dibandingkan dengan kejahatankonvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan melintas batasnegara.
6. lasifikasi kejahatan komputer:
7. Kejahatan yang menyangkut data atau informasikomputer
8. Kejahatan yang menyangkut program atau softwarekomputer
9. Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengelolaan atauoperasinya
10. Tindakan yang mengganggu operasikomputer
11. Tindakan merusak peralatan komputer atau yang berhubungan dengan komputer atau sarana penunjangnya.
12. 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.

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 informasikeuangan. 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.

D. 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.

E. Cybercrime di Indonesia

Dalam dua dokumken konferensi PBB mengenai The Prevention of Crime and The Treatment of Offenders di Havana, Cuba pada tahun 1990, dan di Wina, Austria pada tahun 2000, ada dua istilah yangg dikenal yaitu : “cybercrime”, dan “computer related crime”. Dalam bac ground paper untuk lokakarya konfrensi PBB X/2000 di Wina, Austria, istilah cybercrime dibagi dalam dua kategori, yaitu pertama, cybercrime dalam arti sempit disebut computer crime, kedua cybercrime dalam arti luas disebut computer related crime.

Secara garis besar cybercrime dapat diartikan sebagai segala bentuk tidak kriminal atau perbuatan melanggar hukum yang memanfaatkan teknologi komputer berbasis pada kecanggihan perkembangan teknologi internet. Sedangkan penjahat cyber adalah orang yang melakukan tindakan ilegal dengan niat bersalah atau melakukan kejahatan dalam konteks kejahatan dunia maya (Rifauddin & Halida, 2018)

Cybercrime di Indonesia terjadi sejak tahun 1983. Saat itu terjadi pembobolan rekening bank Indonesia yang terjadi di New York. Pelakunya adalah karyawan bank tersebut yang melakukan tindak kejahatan pencurian rekening dengan menggunakan teknologi informasi. Kasus tersebut adalah kasus pertama yang menyebabkan kerugian langsung terhadap nasabah.

Cybercrime merupakan kejahatan baru yang muncul sebagai akibat dari berkembangnya Teknologi Informasi. Cybercrime melibatkan komputer dalam pelaksanaannya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional (Chintia et al., 2019).

Cybercrime dapat disimpulkan sebagai kegiatan atau perbuatan melawan hukum yang dilakukan dengan menggunakan perangkat komputer atau teknologi informasi sebagai alat untuk memperoleh keuntungan pelaku dan merugikan pihak korban.

Beberapa bentuk potensi cybercrime dalam kegiatan perbankan antara lain:

1. *Typo site,* pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan alamat situs asli. Pelaku menunggu kesempatan jika seseorang korban salah mengetikkan alamat dan masuk kesitus palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi user dan password korbannya, dan dapat dimanfaatkan untuk merugikan korban.
2. *Keylogger/keystroke logger:* Modus lainnya adalah keylogger. Hal ini sering terjadi pada tempat mengakses internet umum seperti di warnet. Program ini akan merekam karakter-karakter yang diketikkan oleh user dan berharap akan mendapatkan data penting seperti user ID maupun password. Semakin sering mengakses internet di tempat umum, semakin rentan pula terkena modus operandi yang dikenal dengan istilah keylogger atau keystroke recorder ini. Sebab komputer-komputer yang ada di banyak orang. Cara kerja dari modus ini sebenarnya sangat sedrhana, tetapi banyak para pengguna komputer ditempat umum yang lengah dan tidak sadar bahwa semua aktifitasnya dicatat oleh orang lain. Pelaku memasang program keylogger dikomputer-komputer umum, program keylogger ini akan merekam semua tombol kyboard yang ditekan oleh pengguna komputer berikutnya. Di lain waktu, pemasang keylogger akan mengambil hasil “jebakannya” dikomputer yang sama, dan dia berharap akan memperoleh informasi penting dari para korbannya, semisal user ID dan password.
3. *Sniffing:* usaha untuk mendapatkan user ID dan password dengan jalan mengamati paket data yang lewat pada jaringan komputer.

4. *Brute Force Attacking:* Usaha untuk mendapatkan password atau key dengan mencoba semua kombinasi yang mungkin.
5. *Web Deface:* System Exploitation dengan tujuan mengganti tampilan halaman muka satu situs.
6. *Email Spamming*: Mengirimkan junk email berupa iklan produk dan sejenisnya pada alamat email seseorang.
7. *Denial of Service:* Membanjiri data dalam jumlah sangat besar dengan maksud untuk melumpuhkan sistem sasaran.
8. Virus worm, trojan: Menyebarkan virus worm maupun trojan dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.

Seiring dengan perkembangan teknologi informasi di Indonesia banyak terjadi cybercrime seperti pembajakan program komputer, penghancuran sistem, penyebaran virus, penyebaran berita bohong, penipuan dengan menggunakan kartu kredit, pencurian data kartu kredit*(carding),* pembobolan bank *(banking fraud),* pornografi, pengrusakan terhadap sebagian atau keseluruhan sistem, prostitusi online, judi online, dan lain-lain.

Kasus-kasus lain yang banyak terungkap diantaranya adalahpenyebaran berita bohong (hoax), penyebaran gambar porno melalui internet *(cyber smuggling), page jacking (moustrapping), spam (junkmail), intercepting, cybersquatting, typosquatting*, dan lain-lain. Adapula yang termasuk ke dalam kejahatan terhadap sistem ataujaringan komputer diantaranya *adalah cracking, defacing, denial of service attack (Dos), distributed denial of service attack (Ddos), penyebaran virus (worm), dan pemasangan logic bomb (Widodo, 2009*) dalam (Ketaren, 2016).

Penggunaan Teknologi Informasi dan komunikasi sedikit banyaknya telah mengubah sikap dan perilaku masyarakat secara global. Perkembangan teknologi informasi dan komunikasi menyebabkan perubahan dalam tatanan kehidupan sosial masyarakat, pertumbuhan ekonomi, sosial politik, hubungan interaksi manusia, serta perubahan manusia dalam berinteraksi satu sama lain yang berlangsung dengan cepat.

Perkembangan teknologi informasi tumbuh pesat dengan meningkatnya populasi pengguna internet di seluruh dunia. Hal tersebut menimbulkan permasalahan baru yang dimanfaatkan oleh orang-orang yang tidak bertanggung jawab untuk melakukan kejahatan yang merugikan orang lain.

Berdasarkan data *We are Social x Hootsuite (*https://wearesocial.com/) tahun2020 terungkap bahwa pengguna internet di seluruh dunia telah mencapai angka 4,5 milyar orang. Angka ini menunjukkan bahwa pengguna internet telah mencapai lebih dari 60 persen penduduk dunia atau lebih dari setengah populasi penduduk bumi. Data menunjukkan bahwa 3.8 milyar pengguna internet mengakses dan menggunakan sosial media. Penelitian menunjukan bahwa pengguna internet rata-rata dunia menghabiskan waktu selama 6 jam 43 menit. Sebagian besar waktu tersebut digunakan untuk mengakses sosial media yaitu rata-rata 2 jam 24 menit setiap harinya. Jumlah pengguna sosial media yang berada di urutan pertama adalah Facebook dengan 2,449 milyar akun. Peringkat kedua adalah Youtube dengan jumlah akun mencapai 2 milyar akun. Di urutan ketiga adalah Instagram dengan 1 milyar akun. Urutan ke empat adalah Tiktok dengan 800 juta akun.

Seiring dengan perkembangan teknologi internet, menyebabkan munculnya kejahatan yang disebut dengan Cybercrime atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus Cybercrime di Indonesia, seperti pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, penyebaran berita bohong, penghancuran data, penipuan melalui email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer.

Di sisi lain perkembangan teknologi informasi membuat pelaku bisnis dan pengusaha dapat memasarkan produknya secara global melalui platform *ecommerce.* Para pelaku usaha dapat memasarkan produknya tanpa perlu memiliki toko atau tempat untuk menjual barangnya. Pembeli dapat langsung memesan produk kepada produsen secara langsung sehingga memangkas biaya promosi dan biaya lain-lainnya. Hal ini tentu saja berdampak besar terhadap penjualan bisnis perusahaan. Bagi konsumen transaksi digital saat ini memudahkan konsumen untuk memperoleh barang atau produk yang di inginkan tanpa harus keluar rumah. Proses pembayarannya pun mudah karena menggunakan uang elektronik, bank transfer ataupun kartu kredit. Hal ini memang memudahkan konsumen maupun pelaku usaha dalam melakukan transaksi bisnisnya. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan cybercrime, kejahatan ini juga tidak mengenal batas wilayah (borderless) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda

F. Contoh Kasus di Luar

Berikut beberapa contoh kasus cybercrime di luar:

1. Kasus Yahoo

   Pada tahun 2014, peretas berhasil mengakses data pengguna seperti alamat email, nomor telepon, tanggal lahir, encrypted passwords, serta pertanyaan keamanan dan jawabannya. Serangan ini membawa dampak pada 500 juta akun pengguna. Meskipun demikian, Yahoo meyakinkan penggunanya bahwa data perbankan tidak terpengaruh dan menyarankan kepada pengguna untuk segera mengubah password yang digunakan. Pada tahun 2012, sebanyak lebih dari 400.0000 password juga telah dicuri oleh peretas.

2. Kasus Ransomware Wannacry

   Dunia digemparkan dengan persebaran 'Ransomware' bernama Wanna Cry di dunia maya. Virus ini menyerang mulai dari Amerika sampai Indonesia. Virus ini menyerang sistem operasi Windows lama maupun terbaru. Jika komputer terkena virus ini maka komputer akan didiamkan dalam keadaan terkunci. Untuk membukanya korban diminta transfer uang kerekening si pembuat virus. Akibat virus ini Renault harus menutup beberapa pabrik perusahaan otomatif di Perancis karenan serangan ini.

3. Kasus facebook

   Facebook mendapat sorotan, sebanyak 87 juta penggua termasuk 1,1 juta penggguna Indonesia telah bocor ke Cambridge Analytica. Tidak hanya bocor ke Cambridge Analitica, data pengguna facebook juga bocor ke CubeYou. Indonesia berada di urutan ketiga setelah Amerika dengan kebocoran data 70,6 juta pengguna facebook dan Filipina dengan kebocoran data dengan jumlah 1,1 juta pengguna facebook. Adapun daftar negara lain yang terdaftar kebocoran data pengguna facebook yaitu Inggris, Meksiko, Canada, India, Brasil, Vietnam dan Australia dengan jumlah kebocoran data yang tidak sedikit

4. Kasus Malware DNSCharger kelompok Estonia

   Kelompok estonia diringkus oleh FBI dan perusahaan keamanan Trend Micro yaitu gerombolan penjahat *cyber* yang telah menginfeksi 4 juta komputer di 100 negara. Estonia melakukan kejahatan *cyber* sejak tahun 2007 dengan menyebarkan malware jenis DNSChanger. Dalam penyelidikan terungkap bahwa kejahatan *cyber* kelompok Estonia ini telah merugikan bukan saja individu, swasta, pemerintahan, tapi juga sampai ke lembaga seperti NASA, dan beberapa perusahaan besar lain yang namanya tidak ingin disebutkan

G. Contoh Kasus di Indonesia

Berikut contoh kasus cybercrime di Indonesia

1. 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.

2. 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)

3. 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

4. Seseorang yang berinisial SH membeli beberapa domain yang mirip dengan domain klikbca.com. Domain tersebut dibuat seolah-olah mirip dengan domain aslinya BCA sehingga menyebabkan nasabah memasukan data username dan passwordnya ke domain tersebut, akibatnya data pribadi nasabah dicuri oleh pelaku. Kasus tersebut termasuk kategori typosquatting dimana nama domain yang digunakan pelaku tidak diketahui oleh korban sehingga korban tidak menyadari bahwa datanya dicuri oleh pelaku.

5. Kasus peretasansitus presiden SBY

   Seseorang yang berinisial W meretas situs presiden Susilo Bambang Yudhoyono yang mengakibatkan situs presidensby.info tidak dapat di akses. Pelakunya meninggalkan jejak dengan menuliskan “jember hacker” di situs tersebut. Tidak berapa lama pelakunya ditemukan dari IP address yang berasal dai sebuah warnet di Jawa Timur.

6. Kasus Pencemaran Nama Baik Prita Mulyasari

   Prita Mulyasari adalah kasus yang terkait dengan UU ITE. Prita merupakan seorang ibu dua anak asal Tangerang. Prita menuliskan surat elektronik tentang kekecewaannya terhadap pelayanan kesehatan di salah satu rumah sakit. Tulisannya tersebar luas di internet dari milis ke milis. Pihak rumah sakit merasa dicemarkan nama baiknya dan kemudian melaporkan Prita ke pihak kepolisian. Pihak RS melayangkan dua gugatan, pidana dan perdata kepada Prita pada September 2008. Prita pun sempat dijatuhi vonis hukuman 6 bulan penjara juga denda lebih dari Rp 204 juta oleh Pengadilan Negeri (PN) Tangerang dan Pengadilan Tinggi Banten. Kasus ini viral di media sosial karena masyarakat dan media membicarakan kasus tersebut dalam waktu yang lama. Masyarakat bersimpati terhadap kejadian yang menimpa Prita dan kemudian ada gerakan koin cinta untuk Prita dimana banyak orang yang melakukan penggalangan dana dari koin-koin untuk membantu Prita membayar denda.

7. Kasus pornografi publik figur

   Seorang publik figur terkenal dilaporkan oleh warga masyarakat terkait dengan video pornografi yang diperankan oleh dirinya bersama beberapa wanita. Pelaku dijerat Pasal 27 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik atau ITE dan KUHP. Pelaku juga dijerat dengan UU Nomor 44 Tahun 2008 tentang

pornografi. Pelaku kemudian mendapatkan hukuman penjara 3 tahun 6 bulan dan denda 250 juta.

8. Kasus pencemaran nama baik musisi terkenal

   Musisi terkenal di Indonesia divonis hukuman penjara 1 tahun 6 bulan dengan dakwan melanggar Undang-Undang Informasi dan Transaksi Elektronik (ITE) karena cuitannya di sosial media yang dinilai menyebarkan kebencian dan permusuhan. Hakim menilai musis tersebut melanggar Pasal 45A Ayat 2 juncto Pasal 28 Ayat 2 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik juncto Pasal 55 Ayat 1 KUHP.

9. Kasus Peretasan Situs KPU

   Salah seorang pelaku berinisial D melakukan XSS atau *cross site scripting* dan SQL *injection* terhadap situs KPU tahun 2004. Pelaku melakukan SQL injection dan mengubah nama-nama partai peserta pemili tahun 2004 dengan nama-nama yang aneh. Akibatnya pelaku dijerat hukuman penjara.

10. Kasus serangan RansomwareWannaCry

    Tahun 2017 Ransomware WannaCry menyerang banyak negara dan melakukan pengrusakan terhadap sistem informasi yang berjalan di organisasi. Di Indonesia ransomware yang menyerang dua rumah sakit terkenal di Jakarta. Jenis serangan tersebut adalah malicious software atau malware yang menyerang komputer korban dengan cara mengunci komputer atau mengenkripsi semua data yang ada sehingga tidak bisa diakses kembali. Pelaku meminta tebusan sejumlah uang agar dapat mengembalikan sistem yang dikunci tersebut.

11. Kasus peretasan dan pembobolan data transaksi di ecommerce

    Salah satu ecommerce yang terkenal di Indonesia mengalami peretasan dan pencurian data. Akibatnya banyak user yang mendapatkan tagihan transaksi pembelanjaan dengan

menggunakan data kartu kredit yang tersimpan dalam akun ecommerce tersebut. Metode yang digunakan adalah Cross site scripting, modus phising dengan inject script terhadap web eccomerce tersebut sehingga user tidak sadar terjadi identity thieft atau pencurian username dan password. Hal tersebut mengakibatkan kerugian besar hingga mencapai angka milyaran.

12. Kasus skimming dana nasabah perbankan

    Sejak tahun 2017 salah satu bank pelat merah mengalami pencurian data nasabah. Pelakunya adalah orang asing dan orang Indonesia. Modus yang dilakukan pelaku adalah dengan memasang alat skimming yaitu alat untuk merekam data nasabah dari atm yang digunakan korban untuk bertransaksi. Korban yang tidak menyadari dirugikan karena uang tabungannya habis di bobol pelaku dengan cara melakukan pencurian data nasabah melalui alat skimming. Akibatnya pelaku dijerat hukuman penjara dan denda.

13. Kasus Judi Online

    Awal tahun 2020 seorang warga negara Indonesia ditangkap polisi karena terlibat tindakan judi online. Pelaku dijerat dengan undang-undangPasal 55 ayat (1) KUHP dan/atau Pasal 56 KUHP jo Pasal 303 KUHP dan/atau Pasal 27 ayat 2 UU ITE.

H. Penerapan UU ITE

Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE) disahkan pada tanggal 21 April 2008 dan menjadi cyber law pertama di Indonesia.

Pada 27 Oktober 2016 rapat paripurna Dewan Perwakilan Rakyat mengesahkan UU Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008. Pasal yang diubah adalah Pasal 27 ayat (1) dan (3), Pasal 28 ayat (2), dan Pasal 31 ayat (3).

Berikut rincian pada Undang-Undang tentang Informatika dan Transaksi Elektronik tersebut: Menghindari multitafsir ketentuan larangan mendistribusikan, mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik bermuatan penghinaan dan/ atau pencemaran nama baik pada ketentuan Pasal 27 Ayat (3), dilakukan 3 (tiga) perubahan sebagai berikut:

a. Menambahkan penjelasan atas istilah "mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik";

b. Menegaskan bahwa ketentuan tersebut adalah delik aduan bukan delik umum; dan

c. Menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP.Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) disampaikan kepada DPR RI sebelum disahkan. UU ITE diundangkan pada 21 April 2008 dan menjadi *cyber law* pertama di Indonesia.

Menurunkan ancaman pidana pada 2 (dua) ketentuan sebagai berikut:

1. Ancaman pidana penghinaan dan/atau pencemaran nama baik diturunkan dari pidana penjara paling lama 6 (enam) tahun menjadi paling lama 4 (tahun) dan/atau denda dari paling banyak Rp1 miliar menjadi paling banyak Rp750 juta;

2. Ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana penjara paling lama 12 (dua belas) tahun menjadi paling lama 4 (empat) tahun dan/atau denda dari paling banyak Rp2 miliar menjadi paling banyak Rp750 juta.

Melaksanakan putusan Mahkamah Konstitusi terhadap 2 (dua) ketentuan sebagai berikut:

1. Mengubah ketentuan Pasal 31 ayat (4) yang semula mengamanatkan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam Undang Undang;

2. Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hokum yang sah.

Melakukan sinkronisasi ketentuan hokum acara pada Pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, sebagai berikut:

1. Penggeledahan dan/atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, disesuaikan kembali dengan ketentuan KUHAP;
2. Penangkapan penahanan yang semula harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1×24 jam, disesuaikan kembali dengan ketentuan KUHAP.

Memperkuat peran Penyidik Pegawai Negeri Sipil dalam Undang-Undang Tentang Informasi dan Transaksi Elektronik pada ketentuan Pasal 43 ayat (5):

1. Kewenangan membatasi atau memutuskan akses terkait dengan tindak pidana teknologi informasi;
2. Kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana teknologi informasi.

Menambahkan ketentuan mengenai “right to be forgotten” atau “hak untuk dilupakan” pada ketentuan Pasal 26, sebagai berikut:

1. Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan;
2. Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan.

Memperkuat peran Pemerintah dalam memberikan perlindungan dari segala jenis gangguan akibat penyalahgunaan informasi dan transaksi elektronik dengan menyisipkan kewenangan tambahan pada ketentuan Pasal 40:

1. Pemerintah wajib melakukan pencegahan penyebarluasan Informas Elektronik yang memiliki muatan yang dilarang;
2. Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik yang memiliki muatan yang melanggar hukum.

Untuk mengantisipasi cybercrime, pemerintah dalam hal ini mengeluarkan aturan yang dituangkan dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya disebut Undang-Undang ITE.

Kebijakan hukum tersebut tertuang dalam UU ITE Pasal 45 sampai dengan Pasal 52 juncto Pasal 27 sampai dengan Pasal 37. Isi dari Pasal 27 sampai dengan Pasal 37 UU ITE.

Berikut ini adalah beberapa isi kutipan pasal 27 – 37, yaitu:

Pasal 27: (1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan. (2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian. (3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/ atau pencemaran nama baik. (4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat

diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 28: (1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan (2) Menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. (3) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29: Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31: (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. (3)

Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang_undang. (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32: (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak. (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33. (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian,

pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Pasal 37 Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia

Manfaat UU ITE

Beberapa manfaat dari UU. No 11 Tahun 2008 tentang (ITE), diantaranya:

a. Menjamin kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik.
b. Mendorong pertumbuhan ekonomi Indonesia.
c. Sebagai salah satu upaya mencegah terjadinya kejahatan berbasis teknologi informasi.
d. Melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi.

Pengaruh UU ITE

Dengan adanya UU ITE ini, maka mempengaruhi hal-hal berikut:

a. Transaksi dan sistem elektronik beserta perangkat pendukungnyamendapat perlindungan hukum. Masyarakat harus memaksimalkanmanfaat potensi ekonomi digital dan kesempatan untuk menjadi penyelenggara Sertifikasi Elektronik dan Lembaga Sertifikasi Keandalan.

b. E-tourism mendapat perlindungan hukum. Masyarakat harus memaksimalkan potensi pariwisata indonesia dengan mempermudah layanan menggunakan ICT.

c. Trafik internet Indonesia benar-benar dimanfaatkan untuk kemajuan bangsa. Masyarakat harus memaksimalkan potensi akses internet indonesia dengan konten sehat dan sesuai konteks budaya Indonesia.

d. Produk ekspor indonesia dapat diterima tepat waktu sama dengan produk negara kompetitor. Masyarakat harus memaksimalkan manfaat potensikreatif bangsa untuk bersaing dengan bangsa lain

I. Pelaksanaan UU ITE

Kemudahan dalam mengakses berita dan informasi memungkinkan orang yang tidak bertanggung jawab menyebarkan berita bohong atau yang sering disebut hoax. Hoax dianggap hal biasa karena diperoleh dengan mudah dan disebarluaskan melalui sosial media. Pemerintah dalam hal ini memiliki peran untuk melakukan controlling terhadap hoax tyang mungkin beredar di masyarkat.

Selain Hoax, ada lagi *finansial technology* ilegal yang melakukan transaksi dan kegiatan bisnis merugikan masyarakat. Fintech ini beroperasi tanpa ijin Otoritas Jasa Keuangan (OJK) dan tanpa ada jaminan dari Lembaga Penjamin Simpan Pinjam (LPS). Fintech ini beroperasi secara

ilegal, memberikan dana pinjaman mudah kepada masyarakat dengan bunga pengembalian yang sangat tinggi.

Berdasarkan data keminfo:

1. Kementerian Kominfo sejak 2016 juga merupakan anggota Satuan Tugas (Satgas) Waspada Investasi yang dibentuk oleh Otoritas Jasa Keuangan. Hadirnya Satgas ini bertujuan untuk melindungi konsumen atau masyarakat Indonesia dari maraknya fintech ilegal.
2. Tak hanya itu, Kementerian Kominfo di tahun 2017 juga meluncurkan portal cekrekening.id yang bertujuan untuk membantu masyarakat mendapatkan informasi rekening bank yang diduga terindikasi tindak pidana.
3. Melalui keminfo, masyarakat dapat melaporkan sekaligus melakukan cek rekening yang terindikasi tindakan penipuan apabila menerima permintaan transfer atau pembayaran uang dari pihak lain. Rekening yang dapat dilaporkan dalam situs ini adalah rekening terkait Tindak Pidana adalah penipuan, investasi palsu, narkotika dan obat terlarang, terorisme, dan kejahatan lainnya.
4. Kementerian Komunikasi dan Informatika terus mengimbau masyarakat untuk hanya menggunakan layanan yang sudah terdaftar di Otoritas Jasa Keuangan, dan tetap waspada dalam menggunakan layanan situs maupun aplikasi fintech.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) mencabut PP 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PP tersebut disahkan oleh Presiden Joko Widodo pada 4 Oktober 2019 dan diundangkan pada 10 Oktober 2019.

Peraturan Pemerintah tentang PSTE merupakan pengaturan lebih lanjut beberapa ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU 11 Tahun 2018 tentang ITE, yang dibentuk untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis.

Beberapa ketentuan yang diperlukan pengaturan lebih lanjut, yaitu:

- Kewajiban bagi setiap Penyelenggara Sistem Elektronik untuk menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan;
- Peran pemerintah dalam memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik, melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum, dan mencegah penyebarluasan dan penggunaan informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

Dalam penyelenggaraan sistem elektronik, setiap PSE memiliki kewajiban sebagai berikut:

- Menyelenggarakan sistem elektronik secara andal, aman dan bertanggung jawab (Pasal 3);
- Tidak memuat dan/atau memfasilitasi penyebaran informasi/dokumen elektronik yang dilarang UU (Pasal 5);

- Melakukan pendaftaran sistem elektronik (Pasal 6);
- Melaksanakan prinsip pelindungan data pribadi (Pasal 14);
- Menghapus informasi/dokumen elektronik yang tidak relevan (Pasal 15);
- Melakukan pengelolaan, pemrosesan, dan penyimpanan sistem/data elektronik di Indonesia oleh PSE Lingkup Publik (Pasal 20);
- Memberi akses dalam rangka pengawasan dan penegakan hukum oleh PSE Lingkup Privat (Pasal 21).

BAB 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

Dalam era perkembangan dan pemanfaatan teknologi informasi saat ini, menyebabkan perubahan sosial, ekonomi, budaya dan juga perubahan perilaku masyarakat secara global. Perkembangan dan pemanfaatan teknologi oleh masyarakat juga memunculkan masalah baru, yaitu munculnya kejahatan melalui jaringan internet yang dikenal dengan istilah Cybercrime. Untuk mengatasi kejahatan cybercrime ini dibutuhkan penanganan yang tepat mengingat jika untuk pembuktian kejahatan dalam dunia maya akan cukup menyulitkan penegak hukum untuk pembuktian kasus dan penegakan hukumnya.

Cyber law merupakan hukum baru yang di dalamnya memiliki berbagai aspek hukum yang sifatnya multidisiplin yang dapat juga diartikan sebagai hukum telekomunikasi multimedia dan informatika (telematika). Dimana dari pengertian tersebut menunjukkan sifat konvergentif dari communication, computing, content, dan comunity sehingga cyber law membahas dari teknologi dan informasi secara konvergensi. Definisi Hukum Telematika, atau yang dikenal dengan cyber law, adalah keseluruhan asas-asas, norma atau kaidah lembaga-lembaga, institusi-institusi dan proses yang mengatur kegiatan virtual yang dilaksanakan dengan menggunakan teknologi informasi dan komunikasi (TIK) (Ramli, 2016).

Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya) yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet.

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.

C. Ruang Lingkup Cyberlaw

Berikut ini adalah ruang lingkup cyberlaw menurut Jonatahan Rosenoer (Bahri, 2020)

- **Hak Cipta (Copy Right)**

  Hak cipta melindungi pemilik karya, agar karya yang diciptakan agar tidak diambil, digunakan, dan dieksploitasi oleh orang lain tanpa izin. [1] Pemilik hak cipta memiliki hak eksklusif untuk memperbanyak karya ciptaannya, menyiapkan karya turunan berdasarkan karya sebelumnya, menjual salinan hak ciptanya atau transfer kepemilikan hakcipta kepada orang lain, untuk melakukan dan menampilkan karya yang diciptakan secara publik, dan untuk memberi wewenang kepada orang lain untuk melakukannya (Rosenoer, 1997).

  Karya yang dimaksud dapat berupa buku, desain, novel, artikel ilmiah, hasil penelitian, program aplikasi, puisi, gambar,lagu, terjemahan, logo, dan karya lain hak cipta.

- **Hak Merk (Trade Mark)**

  Tujuan dari trade mark adalah untuk mengidentifikasi dan membedakan sumber barang atau jasa. Trade mark melindungi kata-kata, simbol, slogan, desain, karakter, kemasan, suara, bau, warna, serta konfigurasi produk, syang digunakan dalam perdagangan. Pada dasarnya, undang-undang merk dagang melindungi dari kebingungan di pasar akibat dari penggunaan kata-kata atau simbol yang serupa (Rosenoer, 1997)

- **Pencemaran Nama Baik (Defamation)**

  Pencemaran nama baik didefinisikan sebagai serangan terhadap reputasi dan nama baik seseorang. Yang tergolong pencemaran nama baik seperti pernyataan palsu baik secara

lisan atau tertulis yang menghadapkan seseorang pada kebencian, penghinaan, atau ejekan, atau yang menyebabkan seseorang dijauhi atau dihindari, atau yang memiliki kecenderungan untuk menyerang kehormatan orang lain (Rosenoer, 1997).

- **Fitnah, Penistaan, Penghinaan (Hate Speech)**

  Merupakan tindakan komunikasi yang dilakukan baik oleh individu atau kelompok kepada individu atau kelompok yang lain dalam bentuk provokasi, hasutan, ataupun hinaan terkait berbagai aspek seperti ras, warna kulit, gender, cacat, orientasi seksual, kewarganegaraan, agama dan lain-lain. Dalam arti hukum, Ujaran Kebencian (Hate Speech) adalah perkataan, perilaku, perkataan, tulisan, ataupun pertunjukan yang dilarang karena dapat memicu terjadinya tindakan kekerasan dan sikap prasangka entah dari pihak pelaku pernyataan tersebut ataupun korban dari tindakan tersebut (Syafyahya, 2018)

- **Serangan Terhadap Fasilitas Komputer (Hacking, Viruses, Illegal Access)**

  Hacking terkait dengan kegiatan untuk mencari kelemahan dari sistem keamanan komputer, baik itu dari sisi software maupun hardware. Adalah aktivitas yang dilakukan oleh seorang hacker untuk masuk kedalam sebuah sistem (komputer, program aplikasi, dll) yang kemudian membuat perubahan di dalamnya (Winarno, Zaki, & Community, 2015).

  Aktivitas hacking menuai pro dan kontra dari berbagai pihak. Pihak yang pro karena melihat dari sisi positif aktivitas ini di mana dapat melihat kelemahan sistem yang dibangun dari serangan pihak luar untuk kemudian diantipasi penanganannya sehingga sistem ‘kebal’ dari serangan pihak luar. Sedangkan pihak yang kontra berpendapat bahwa aktivitas ini merugikan karena pelaku masuk ke dalam sistem tanpa izin dan dapat melakukan apapun yang dapat berakibat fatal terhadap sistem.

- **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.**

Ruang lingkup Cyber Law di Indonesia adalah (Napitupulu, 2017):

a. Hukum Publik :

   Juridiksi, Etika Kegiatan Online, Perlindungan Konsumen, Anti Monopoli, Persaingan Sehat, Perpajakan, Regulatory Body, Data Protection dan Cyber Crimes.

b. Hukum Privat :

   HAKI, ECommerce, Cyber Contract, Domain Name, Insurance.

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):

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.

12. 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 dan tujuan dari UU ITE itu sendiri terdapat dalam **Pasal 3** UU ITE, yaitu (Suharyo, 2010)

a. Asas Kepastian Hukum

   Berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan

b. Asas Manfaat

   Berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat

c. Asas kehati-hatian

   Berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik

d. Asas iktikad baik

   Berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut

e. Asas kebebasan memilih teknologi atau netral teknologi

Berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang

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.

i. 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.

j. 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.

k. 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.

l. 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.

Pasal 23

- Pasal 23 ayat 1 membolehkan setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat untuk memiliki Nama Domain berdasarkan prinsip pendaftar pertama.
- Namun, pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain. Sehingga, setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak untuk mengajukan gugatan pembatalan Nama Domain itu.
- Dalam hal terjadi perselisihan pengelolaan Nama Domain oleh masyarakat. Untuk Pengelola Nama Domain yang berada di luar wilayah Indonesia dan Nama Domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan Perundang-undangan

Pasal 24

Pengelola Nama Domain adalah Pemerintah dan/atau masyarakat , Pemerintah berhak mengambil alih sementara pengelolaan Nama Domain yang diperselisihkan.

Pasal 25

Hak Cipta

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Pasal 26

penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan kecuali ditentukan lain oleh Peraturan Perundang-undangan . Setiap Orang yang dilanggar haknya dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

pasal 38-39

Penyelesaian Sengketa

Dalam hal, diatur di dalam, yaitu siapapun atau setiap Orang dan atau masyarakat dapat mengajukan gugatan secara perwakilan dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian, , sesuai dengan ketentuan Peraturan Perundang-undangan.

Untuk Gugatan perdata dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan, selain penyelesaian gugatan perdata, para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.

pasal 40-41

Peran Pemerintah dan Masyarakat

Pemerintah :

1. Memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan.
2. Melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.
3. Menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi(Instansi atau institusi harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data dan juga sesuai dengan keperluan perlindungan data yang dimilikinya.

Masyarakat :

Dapat berperan meningkatkan pemanfaatan Teknologi Informasi melalui penggunaan dan Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik sesuai dengan ketentuan Undang-Undang ini, dan dapat diselenggarakan melalui lembaga yang dibentuk oleh masyarakat yang dapat memiliki fungsi konsultasi dan mediasi.

pasal 42-44

Penyidikan terhadap tindak pidana dan alat bukti

- Penyidikan dilakukan dengan :
  a. memperhatikan perlindungan terhadap privasi,
  b. berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini,
  c. Memperhatikan kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.

- Dan untuk melakukan penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat serta penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Penyidik :

- Pejabat Polisi Negara Republik Indonesia,
- Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

pasal 43

Wewenang Penyidik

a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini;
b. memanggil setiap Orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini;
c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini;
d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini;
e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini;

f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang-Undang ini;
g. melakukan penyegelan dan penyitaan terhadap alat dan atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan;
h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau
i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.
j. dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.
k. penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.
l. dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.

pasal 44

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

pasal 27-52

perbuatan-perbuatan yang dilarang disertai dengan sanksinya

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)

Pasal 45

SANKSI

- **Pasa; 45 Ayat 1** , Dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

  Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) tentang Asusila, Perjudian, Penghinaan, Pemerasan , yaitu : Setiap Orang dengan sengaja dan tanpa hak (pasal 27 Ayat 1) : mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan dan/atau pencemaran nama baik, dan pemerasan dan/atau pengancaman.

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) tentang Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan , yaitu Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik dan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau

kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

a. **Pasal 45 Ayat 2**, Dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)
b. **Pasal 45 Ayat 3**, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 29** tentang Ancaman Kekerasan dan Menakut-nakuti , yaitu Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi

  Pasal 46 Ayat 1, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 30 ayat (1)** tentang Akses Komputer Pihak Lain Tanpa Izin, Cracking , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

  Pasal 46 Ayat 2, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 30 ayat (2)** tentang Akses Komputer Pihak Lain Tanpa Izin, Cracking , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Pasal 46 Ayat 3, Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) tentang Akses Komputer Pihak Lain Tanpa Izin, Cracking , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 30 ayat (3)** tentang Akses Komputer Pihak Lain Tanpa Izin, Cracking , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

  Pasal 47, Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 31 ayat (1)** atau ayat (2) tentang Penyadapan, Perubahan, Penghilangan Informasi , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain dan melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

  Pasal 48 ayat 1, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 32 ayat (1)** tentang Pemindahan, Perusakan dan Membuka Informasi Rahasia , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah,

menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Pasal 48 ayat 2, dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 32 ayat (2)** tentang Pemindahan, Perusakan dan Membuka Informasi Rahasia , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

  Pasal 48 ayat 3, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 32 ayat (3)** tentang Pemindahan, Perusakan dan Membuka Informasi Rahasia , yaitu Terhadap perbuatan Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya

  Pasal 49, Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).
- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 33** tentang Virus, Membuat Sistem Tidak Bekerja , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 50, Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal **34 ayat (1)** , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
  a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
  b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Pasal 51 ayat 1, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 35** tentang Menjadikan Seolah Dokumen Otentik , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 51 ayat 2, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam **Pasal 36** , yaitu Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Pasal 52 ayat 1, dikenakan pemberatan sepertiga dari pidana pokok, dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak

Pasal 52 ayat 2, Dipidana dengan pidana pokok ditambah sepertiga, dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik

Pasal 52 ayat 3, Diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga, dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan .

Pasal 52 ayat 4, Dipidana dengan pidana pokok ditambah dua pertiga, dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi.

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

Pengaturan cybercrime yang mengelompokan berbagai perbuatan ke dalam 2 klasifikasi besar, kemudian dibagi lagi dalam beberapa kelompok berdasarkan pasal-pasal di atas, dipedomani oleh pembuat UU ITE. Lebih jelasnya pengaturan cybercrime dalam UU ITE adalah sebagai berikut (Suharyo, 2010)

1. **Indecent Materials/ Illegal Content (Konten Ilegal).**

   Setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, pencemaran nama baik serta pemerasan, pengancaman serta yang menimbulkan rasa kebencian berdasarkan atas SARA serta yang berisi ancaman kekerasan (Pasal 27, 28, dan 29 UU ITE);

2. **Illegal Acces (Akses Ilegal).**

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau Sistem Elektronik milik orang lain dengan cara apapun untuk memperoleh Informasi elektronik serta melanggar, menerobos, melampaui atau menjebol sistem pengamanan (Pasal 30 UU ITE);

3. **Illegal Interception (Penyadapan Ilegal).**

   Setiap orang dengan sengaja dan tanpa hak melakukan intersepsi atas Informasi Elektronik dan/ atau Dokumen Elektronik dalam suatu Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/ atau penghentian Informasi Elektronik dan/ atau Dokumen Elektronik yang sedang ditransmisikan (Pasal 31 UU ITE);

4. **Data Interference (Gangguan Data).**

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan,

menyembunyikan, atau mentransfer suatu Informasi Elektronik milik orang lain atau milik publik kepada Sistem Elektronik orang lain yang tidak berhak, sehingga mengakibatkan terbukanya suatu Informasi Elektronik dan/ atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. (Pasal 32 UU ITE);

5. **System Interference (Gangguan Sistem).**

   Setiap orang dengan sengaja dan tanpa hak melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/ atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya (Pasal 33 UU ITE);

6. **Misuse of Devices (Penyalahgunaan Perangkat).**

   Setiap orang dengan sengaja dan tanpa hak memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan yang dilarang dan sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu, yang ditujukan agar sistem elektronik menjadi dapat akses dengan tujuan memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);

7. **Computer Related Fraud and Forgery (Penipuan dan Pemalsuan yang berkaitan dengan Komputer).**

   Setiap orang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan Informasi Elektronik dan/ atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (Pasal 35 UU ITE).

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. Kemudian pada tanggal 27 Oktober 2016 dalam sidang paripurna DPR RI disahkan RUU tentang perubahan UU no.11/2008.

Berikut tujuh point revisi dalam UUITE menurut Rudiantara yaitu :

1. Menambahkan sejumlah penjelasan untuk menghindari multitafsir terhadap „ketentuan penghinaan/pencemaran nama baik“ pada pasal 27 ayat 3.
2. Menurunkan ancaman pidana pencemaran nama baik dari paling lama 6 tahun menjadi 4 tahun dan denda dari Rp 1 miliar mejadi Rp 750 juta. Juga menurunkan ancaman pidana ancaman kekerasan Pasal 29 dari paling lama 12 tahun penjara menjadi 4 tahun dan denda dari Rp 2 miliar menjadi 750 juta.
3. Melaksanakan putusan MK atas pasal 31 ayat 4 yang mengamanatkan pengaturan tatacara intersepsi ke dalam UU. Juga menambahkan penjelasan Pasal 5 terkait keberadaan informasi elektronik sebagai alat bukti hukum.
4. Sinkronisasi hukum acara penggeledahan, penyitaan, penangkapan dan penahanan dengan hukum acara KUHAP.
5. Memperkuat peran PPNS UUITE untuk memutuskan akses terkait tindak pidana TIK.
6. Menambahkan ketentuan „right to be forgotten“: kewajiban menghapus konten yang tidak relevan bagi penyelenggara sistem elektronik. Pelaksanaan „right to be forgotten“ dilakukan atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
7. Memperkuat peran pemerintah untuk mencegah penyebarluasan konten negatif di Internet.

Empat hal yang berubah dari UUITE setelah mengalami revisi ditahun 2016 yakni :

1. **Penurunan hukum dan tidak ada penahanan**

   Menurunkan ancaman hukuman untuk para terdakwa. Untuk kasus pencemaran nama baik, hukuman penjara diturunkan dari 6 tahun menjadi empat tahun, hukumam dendapun diturunkan dari Rp 1 miliar menjadi Rp 750 juta.

   Adapun untuk kasus ancaman kekerasan di dunia maya, hukuman penjara yang semula 12 tahun menjadi hanya empat tahun. Selain itu hukuman dendapun turun dari Rp 2 miliar menjadi Rp 750 juta.

   Berdasarkan perubahan ini, kasus pencemaran nama baik dan ancaman kekerasandi Internet, kini termasuk ke dalam kategori tindak pidana ringan dengan ancaman penjara kurang dari lima tahun menurut pasal KUHAP pasal 21. Ini artinya, sang tersangka tidak boleh ditahan selama proses penyidikan.

2. **Hak untuk dilupakan (Right to be Forgotten)**

   Semua berita yang ada di Internet, baik itu fakta maupun berita bohong, tidak akan hilang kecuali apabila berita tersebut dihapus oleh penyedia layanan yang terkait. Oleh karena itu, pada pasal 26 UUITE kini menambahkan aturan tentang hak untuk dilupakan (riht to be forgotten).

   Dengan aturan baru ini, seseorang yang telah menyelesaikan sebuah masalah di masa lau atau tidak terbukti bersalah oleh pengadilan, berhak untuk mengajukan penghapusan terkait informasi yang salah yang telah beredar di internet.

3. **Penghapusan informasi yang melanggar Undang-Undang**

   Pada pasal 40 UUITE, terdapat penambahan ayat baru yang menyatakan bahwa Pemerintah berhak menghapus dokumen elektronik yang menyebarkan informasi pornografi, SARA, terorisme, hingga pencemaran nama baik. Apabila ada perbedaan mengenai suatu konten yang dipublikasikan melalui media apak melanggar undang-undang atau tidak, Pemerintah akan mengikuti mekanisme di Dewan Pers untuk menyelesaikan masalah tersebut. Jika situs yang menyediakan informasi tak baik tersebut tidak berbadan hukum, Pemerintah pun punya kewenangan untuk memblokir situs tersebut.

4. **Penyadapan harus dengan izin kepolisian atau kejaksaan**

   Dokumen elektronik hasil penyadapan merupakan alat bukti yang sah, asalkan dilakukan atas permintaan kepolisian atau kejasaan. Hal ini tercantum dalam pasal 5 UUITE

Dalam KUHP dapat ditentukan mengenai tindak pidana yang terkait dengan teknologi informasi bisa disebutkan, antara lain (Supanto, 2016)

a. **Pasal 362 KUHP**

   Untuk kasus Carding yang pelakunya mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di internet untuk melakukan transaksi di E-Commerce.

b. **Pasal 378 KUHP**

   Untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan.

c. **Pasal 335 KUHP**

   Dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail.

d. **Pasal 331 KUHP**

   Dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan e-mail kepada temanteman korban tentang suatu cerita yang tidak benar atau mengirimkan e-mail secara berantai melalui mailling list (millis) tentang berita yang tidak benar.

e. **Pasal 303 KUHP**

Dapat dikenakan untuk menjerat permainan judi yang dilakukan secara on-line di internet dengan penyelenggara dari Indonesia.

f. **Pasal 282 KUHP**

Dapat dikenakan untuk penyebaran pornografi maupunwebsiteporno yang banyak beredar dan mudah diakses di internet

g. **Pasal 282 dan 311 KUHP**

Dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang vulgar di internet.

Dalam UU ITE dengan menentukan adanya Ketentuan Pidana berarti menentukan adanya perbuatan yang dilarang, dan yang oleh karena itu diancam dengan sanksi pidana. Ini tidak lain sebagai perumusan tindak pidana dibidang informasi dan transaksi elektronik. Dengan mengkaji pasalpasal dalam UU ITE dapat dikelompok-kelompokkan perbuatan yang dilarang berkaitan dengan tindak pidana di bidang informasi dan transaksi elektronik tersebut. Pengelompokan tersebut sebagai berikut (Supanto, 2016)

4. **Kelompok I (Pasal 45)**

Sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, muatan perjudian, penghinaan dan/atau pencemaran nama baik, pemerasan dan/atau pengancaman; menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik, menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan

antargolongan (SARA); berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

5. **Kelompok II (Pasal 46)**

Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun bertujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik; melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

6. **Kelompok III (Pasal 47)**

Sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, dan baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

7. **Kelompok IV (Pasal 48, 49)**

Sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik; memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak; mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public, mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya; dan tindakan apa pun yang berakibat

terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

8. Kelompok V (Pasal 50)

Sengaja dan tanpa hak atau melawan hukum memproduksi, menjual,mengadakanuntukdigunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. Perangkat keras a t a u perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

b. Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

9. Kelompok VI (Pasal 51)

1. Sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

2. Sengaja dan tanpa hak/melawan hukum mendistribusikan dan/ atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

3. Sengaja dan tanpa hak/melawan hukum mendistribusikan dan/ atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
4. Sengaja dan tanpa hak/melawan hukum mendistribusikan dan/ atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
5. Sengaja dan tanpa hak/melawan hukum mendistribusikan dan/ atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
6. Sengaja dan tanpa hak/melawan hukum menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
7. Sengaja dan tanpa hak/ melawan hukum menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/ atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).
8. Sengaja dan tanpa hak /melawan hukum mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
9. Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
10. Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengantujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

11. Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

12. Sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/ atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

13. Sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/ atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan

14. Sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

15. Sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

16. Sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public, yang mengakibatkan terbukanya suatu Informasi Elektronik dan/ atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

17. Sengaja dan tanpa hak atau melawan hukum melakukan tindakanapapunyangberakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

18. Sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

10. Kelompok VII (Pasal 52)

1. Sengajadantanpahakmendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

2. Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau Sistem Elektronik milik Orang lain dengan cara apa pun ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik.

3. Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/ atau Dokumen Elektronik ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik.

4. Sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik.

5. Sengaja dan tanpa hak atau melawan hukumdengancaraapapunmengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau DokumenElektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik.

6. Sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik.

7. Sengaja dan tanpa hak atau melawan hukumdengancaraapapunmengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik yang mengakibatkan terbukanya suatu Informasi

Elektronik dan/atau Dokumen Elektronik yang bersifatrahasiamenjadidapatdiakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

8. Sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan SistemElektronikmenjaditidakbekerja sebagaimana mestinya ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik.
9. Sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
    a. Perangkat keras atau perangkat lunak Komputer yang dirancang atausecarakhususdikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
    b. Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

11. Kelompok VIII (Pasal 52)

1. Sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

3. Sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

4. Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau Sistem Elektronik milik Orang lain dengan cara apa pun ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintahdan/ataubadanstrategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritaspenerbangan.

5. Sengajadantanpahakataumelawan hukum mengakses Komputer dan/ atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik Pemerintahdan/ataubadanstrategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan

6. Sengajadantanpahakataumelawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan.

7. Sengajadan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain ditujukan terhadap Komputer

dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan.

8. Sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/ atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintahdan/ataubadan strategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan.

9. sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan.

10. Sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik

Pemerintahdan/ataubadanstrategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritaspenerbangan.

11. Sengajadantanpahakataumelawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya, ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan.

12. Sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya, ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan.

13. Sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki, ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik Pemerintahdan/ataubadan strategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan:

a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

14. Sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik, ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional,otoritas penerbangan

15. sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/ atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik, ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembagapertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan.

16. Sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain

17. Sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

18. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai denganPasal37dilakukanolehkorporasi dipidana dengan pidana pokok ditambah dua pertiga.

E. Modus Kejahatan Cyber

Berikut ini adalah beberapa modus yang biasa digunakan oleh pelaku kejahatan dalam melakukan tindak kejahatan cybercrime (Ketaren, 2016) :

1. Unauthorized Access

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Probing dan port merupakan contoh kejahatan ini.

2. Illegal Contents

Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

3. Penyebaran Virus Secara Sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4. **Data Forgery**

Kejahatan jenis 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.

5. **Cyber Espionage, Sabotage, and Extortion**

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. **Cyberstalking**

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

7. **Carding**

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8. **Hacking dan Cracker**

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

9. **Cybersquatting and Typosquatting**

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

10. **Hijacking**

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).

11. **Infringements of Privacy**

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. 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

materilmaupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakittersembunyi dan sebagainya.

12. **Offense against Intellectual Property**

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah 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.

13. **Defacing**

Defacing merupakan bagian dari kegiatan hacking web atau program application, yang menfokuskan target operasi pada perubahan tampilan dan/atau konfigurasi fisik dari web atau program aplikasi tanpa melalui source code program tersebut. Sedangkan deface itu sendiri adalah hasil akhir dari kegiatan cracking dan sejenisnya, tekniknya adalah dengan mebaca source codenya (ini khusus untuk konteks web hacking), kemudian mengganti image (misalnya), editing html tag dkk, dan lain-lain. Tindakan defacing ada yang sematamata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang untuk mencuri data dan dijual kepada pihak lain.

14. **Phising**

Phising merupakan kegiatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya. Phising biasanya dilakukan melalui e-mail spoofing atau pesan instan, dan sering mengarahkan pengguna untuk memasukkan rincian di sebuah website palsu yang tampilan dan nuansa yang hampir sama dengan yang aslinya.

15. **Spamming**

Spamming merupakan kegiatan mengirim email palsu dengan memanfaatkan server email yang memiliki “smtp open relay” atau spamming bisa juga diartikan dengan pengiriman informasi atau iklan suatu produk yang tidak pada tempatnya dan hal ini sangat mengganggu bagi yang dikirim. Yang paling banyak adalah pengiriman e-mail dapat hadiah, lotere, Kemudian korban diminta nomor rekeningnya, dan mengirim uang/dana sebagai pemancing, tentunya dalam mata uang dolar AS, dan belakangan tak ada kabarnya lagi.

16. **Snooping**

Snooping adalah suatu pemantauan elektronik terhadap jaringan digital untuk mengetahui password atau data lainnya. Ada beragam teknik snooping atau juga dikenal sebagai eavesdropping, yakni: shoulder surfing (pengamatan langsung terhadap display monitor seseorang untuk memperoleh akses), dumpster diving (mengakses untuk memperoleh password dan data lainnya), digital sniffing (pengamatan elektronik terhadap jaringan untuk mengungkap password atau data lainnya).

17. **Sniffing**

Sniffing adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer.

18. **Spoofing**

Spoofing adalah teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dimana penyerang berhubungan dengan pengguna dengan berpurapura memalsukan bahwa mereka adalah host yang dapat dipercaya “hal ini biasanya dilakukan oleh seorang hacker atau cracker”.

19. **Pharming**

Pharming adalah situs palsu di internet, merupakan suatu metode untuk mengarahkan komputer pengguna dari situs yang mereka percayai kepada sebuah situs yang mirip. Pengguna sendiri secara sederhana tidak mengetahui kalau dia sudah berada dalam perangkap, karena alamat situsnya masih sama dengan yang sebenarnya.

20. **Malware**

Malware adalah program komputer yang mencari kelemahan dari suatu software. Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. Malware terdiri dari berbagai macam, yaitu: virus, worm, trojan horse, adware, browser hijacker, dll.

F. 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.

BAB 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 (Pajar Pahrudin) :

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 (Pahrudin, 2017):

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 contoh etika yang telah ditetapkan oleh IETF (Pahrudin, 2017)

1. Netiket One to One Communication

Adalah kondisi dimana komunikasi terjadi antar individu “face to face“ dalam sebuah dialog. Contoh komunikasi via email. Hal-hal yang dilarang :

a. Jangan terlalu banyak mengutip
b. Hati-hati ketika membalas (reply) pesan. Jika harus mengutip jawaban seseorang, hapus bagian yang tidak diperlukan dan jawab hanya pada bagian-bagian yang relevan saja
c. Perlakukan email secara pribadi
d. Jika ada seseorang yang mengirimkan informasi secara pribadi, jangan mengirimnya ke dalam sebuah forum seperti mailing list
e. Hati-hati dalam menggunakan huruf kapital
f. Pesan yang menggunakan huruf kapital secara berlebihan sangat tidak enak untuk dilihat dan dibaca. Gunakan huruf kapital sewajarnya. Misalnya untuk menunjuk pada awal kalimat atau menunjukk kepada sesuatu yang khusus
g. Jangan membicarakan orang lain
h. Jangan menggunakan email untuk membicarakan orang lain apalagi membicarakan kejelekan orang lain
i. Jangan menggunakan CC (carbon copy)
j. Jangan mencantumkan nama pada carbon copy (CC) jika ingin mengirimkan email ke sejumlah orang lain, misalnya di mailing list

k. Jangan gunakan format HTML
l. Jika ingin menggunakan format HTML ketika mengirim email, pastikan program email teman anda dapat memahami kode HTML.
m. Jawablah secara masuk akal
n. Jawablah setiap pesan email yang masuk sesuai dengan kebutuhan dan pesan email

2. Netiket Pada One To Many Communication

Konsep komunikasi dimana satu orang dapat berkomunikasi kepada beberapa orang sekaligus. Contohnya alah pada mailing list dan net news.

Beberapa hal-hal tentang netiket untuk berkomunikasi bagi pengguna (user) mailing list atau Netnews (Suryana, 2014)

1. Biasakan untuk membaca terlebih dahulu data diskusi pada mailing list sebelum anda memutuskan untuk melakukan posting pertama kali pada mailing list kurang lebih satu atau dua bulan
2. Jika ada perilaku anggota sistem yang tidak baik, jangan menyalahkan moderator atau pengurus sistem
3. Selalu berfikir dan berhati-hatilah dengan kata-kata yang akan ditulis atau yang akan di post pada mailing list
4. Membaca berita dan posting data, kedua-duanya sama-sama mengambil sistem daya sistem
5. Jika ingin menulis artikel atau tulisan lainnya, pastikan jika artike atau tulisan tersebut ringkas dan to the point
6. Biasakan untuk membuat subject line yang mengikuti aturan atau konvensi yang disepakati dalam kelompok komunikasi tersebut
7. Tidak boleh mengirimkan artikel yang berbau spoffing (pemalsuan), dan forgeries (lelucon), kecuali mailing list yang memang bernuansa humor.

8. Beberapa mailing list menyambut atau memperbolehkan posting teks iklan
9. Letakkan signature atau tanda tangan di setiap teks yang di-posting
10. Jika terjadi perselisihan, salah paham atau perdebatan secara pribadi dengan peserta lainnya, sebaiknya dilakukan melalui email pribadi masing-masing (email to email)
11. Tidak diperbolehkan mengirimkan teks yang berbau seksual dan rasialis karena hal tersebut tidak etis mengingat anggota yang berada pada komunitas tersebut memiliki budaya lifestyle dan keyakinan yang berbeda-beda

3. Information Services

Pada perkembangan internet, diberikan fasilitas dan berbagai layanan baru yang disebut layanan informasi (information service). Berbagai jenis layanan ini antara lain seperti Gropher, Wais, Word Wide Web (WWW), Multi-User Dimensions (MUDs), Multi-User Dimensions which are object Oriented (MOOs)

Beberapa hal-hal tentang netiket yang harus diperhatikan pada Information services :

1. Bahwa semua jasa adalah kepunyaan object
2. Jika mendapat kesalahan terhadap layanan tersebut, lakukan pengecekan pertama kali terhadap kondisi lokal sistem
3. Pemakaian perlu mengetahui bagaimana file layanan tersebut bekerja pada sistem lokal yang dimilikinya
4. Pemakaian information service harus menggunakan pikiran yang terbuka bahwa di dalam internet terhubung berjuta-juta orang dengan kultur yang mungkin berbeda dengan kultur masyarakat di mana pengguna berada
5. Tidak menggunakan FTP (File Transfer Protocol) orang lain untuk menyimpan materi kita agar orang lain bisa mengambilnya

D. Tips Aman Berinternet

1. Harus Selalu Waspada Dan Hati-Hati Terhadap Link Mencurigakan

Dalam menggunakan internet pengguna disarankan untuk tidak merespon segala jenis tautan baik itu link, mapun pesan yang mencurigakan apalagi yang meminta informasi pribadi seperti nama ibu kandung, nama lengkap, no kartu atm dan jenis informasi pribadi lainnya. Hal ini dilakukan agar data pribadi kita tidak di salah gunakan oleh pihak yang tidak bertanggung jawab.

Jika memang diperlukan mengisi informasi pribadi, sebaiknya langsung melalui aplikasi atau situs terpercaya yang memang membutuhkan login masuk ke dalam akun pribadi kita. Jangan mudah untuk meng-klik sebuah link yang mencurigakan, karena bisa jadi link itu berisi halaman login palsu buatan hacker. Pastikan link yang kita klik merupakan sebuah situs resmi. Yang perlu di ingat adalah, sebuah situs dan layanan resmi tidak akan pernah mengirim pesan kepada penggunanya untuk meminta mengirim sandi atau informasi keuangan via email.

2. Berfikir Sebelum Melakukan Koneksi Ke Sebuah Situs

Jaringan internet memungkinkan kita untuk dapat terhubung ke situs manapun sehingga dapat menimbulkan efek positif maupun negatif. Anda harus berhati-hati, jangan dengan mudah untuk membuka situs internet yang tidak anda kenal, karena situs yang anda buka bisa jadi merubpakan situs ilegal yang sengaja dibuat untuk mengambil data pribadi ketika anda masuk kedalam situs tersebut. Hindari situs seperti survey online dan belanja online yang tidak terpercaya, karena resiko pengambilan data pribadi sangat besar

3. 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:

a. Agar Data Pribadi (Personal) dihapus (delete) atau diremajakan (up to date);
b. 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
c. 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:

a. 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).
b. 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.
c. DCO menjamin ketepatan, akurasi data konsumen, tidak kadaluwarsa, up to date terus diperbarui, sesuai tujuan penyimpanan data yang disetujui oleh konsumen.

b. DCO menjamin Lokasi & format penyimpanan atau database disetujui konsumen dan UU yang berlaku.
c. DCO menjaga integritas (tidak rusak dan hilang) data dan kerahasian (confidentiality) data subjek dengan enkripsi, password dll.

4. 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 terverifikasi, tidak anonim dan jelas. Certificate Authority (CA) adalah pihak ketiga yang membuat, memverifikasi publik & private key (kunci privat) untuk menjaga otentikasi pemiliknya.

5. Menggunakan sistem verifikasi 2 langkah

Verifikasi 2 langkah digunakan untuk mengamankan dan menambahkan pengamanan ekstra ke akun, sehingga bisa meminimalkan peluang akses yang tidak sah yang dilakukan oleh pihak yang tidak bertanggung jawab. Sistem keamanan ini biasanya digunakan pada sistem yang menggunakan transaksi keuangan ataupun pembayaran secara online seperti sistem perbankan dan sistem e-commerce.

6. 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:

a. 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.
b. 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.
c. Menemani anak-anak ketika sedang mengakses Internet atau letakan laptop atau perangkat lainnya di tempat yang terjangkau dari pengawasan orang tua.
b. 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.

c. Memberi batas waktu bermain Internet kepada anak-anak, untuk mencegah anakanak kecanduan bermain Internet.

7. Menghindari & menangkal spaM, Malware, ransoMware, virus & spyware

Ada beberapa hal yang dapat kita lakukan dalam upaya untuk Menghindari & menangkal spaM, Malware, ransoMware, virus & spyware

a. Rajin Update Sistem

   Pastikan kita untuk segera mungkin mengupdate software terbaru ketika kita menerima notifikasi untuk meng-update software. 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. 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.

b. Backup dokumen, foto atau berkas penting lainnya

   Backup dokumen, foto atau berkas penting lainnyake 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.

c. Jangan klik link web atau download file yang tidak dikenal.

   Hal ini dikarenakan 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

d. Berhati-hati gunakan wfi public.

   Terutama jika anda ingin melalukan transaksi keuangan, perbankan, ecommerce, credit cards serta aplikasi yang kritis dan strategis karena bisa jadi jaringan ini terenkripsi sehingga siapapun yang berada dijaringan tersebut dapat memantau segala aktivitas kita di internet termasuk situs apa saja yang kita kunjung. Jika diperlukan untuk memasukkan informasi pribadi, pastikan koneksi ke dalam situs tersebut aman. Sebagai contoh jika kita menggunakan browser seperti chrome, maka tanda bahwa situs yang kita kunjungi aman adalah adanya gambar ikon berupa gembok yang berwarna abu-abu pada kotak URL

e. Tidak gunakan perangkat pribadi di tempat bekerja, untuk memproses pekerjaan perusahaan.

   Hal ini disebabkan adanya risiko besar yang berpotensi mengancam sistem keamanan perusahaan-perusahaan karena pekerja yang menggunakan perangkat pribadi mungkin saja tidak mengetahui dan tidak mematuhi standar kelaikan TI yang telah ditetapkan perusahaan terkait penggunaan perangkat pribadi untuk bekerja. Kondisi tersebut tentu saja dapat berpotensi membukakan pintu lebar terhadap masuknya upaya-upaya serangan dan peretasan data, sekaligus meningkatkan risiko terhadap bisnis perusahaan (Ananda Widhia Putri)

8. Cara penjagaan berlapis serangan cracker dari Internet dan dalam Sistem

Ada beberapa cara penjagaan berlapis yang dapat dilakukan sebagai upaya menjaga keamanan dari serangan hacker dari internet dan dalam sistem, yaitu :

a. 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.

b. Memasang dan memperbaharui Anti virus, Anti Spam, Anti Malware

   Anti virus, Anti Spam, Anti Malware dan sensor konten di Server dan disetiap PC serta peralatan Anti Insider Threat yang merupakan pertahanan berlapis (defence in depth) bagi sebuah korporasi dan enterprise perlu diperbaharui agar serangan malware yang dapat menggangu sistem dapat dicegah sebelum terjadi.

c. Mengatur akun privillage.

   Membuat akun yang memiliki limited akses sangat diperlukan untuk menghindari serangan malware. Karena jika kita sedang menggunakan akun administrator dan ada malware yang masuk, maka malware tersebut dengan leluasa dapat menjalankan aktivitas kejahatannya

d. Memperbaharui Sistem Operasi yang digunakan

   Pembaharuan sistem operasi dilakukan karena biasanya pengembang sistem operasi menawarakan pengembangan tingkat keamanan yang lebih tinggi pada sistem operasi versi terbaru dibandingkan dengan sistem operasi versi sebelumnya.

9. Gunakan Kata Sandi Yang Kuat Dan Mengganti Secara Berkala

Agar aman dalam berinternet, sebaiknya pengguna jangan menggunakan kata sandi yang sama untuk akun yang berbeda. Untuk membuat kata sandi yang kuat, pengguna dapat menggunakan gabungan huruf, angka dan juga tanda baca agar kata sandi yang kita buat sulit ditebak oleh hacker. Selain itu kita juga perlu mengganti kata sandi secara berkala. Tambahan informasi tambahan untuk pemulihan akun jika kita keluar dari akun dan membutuhkan akses kembali

10. 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
b. Prinsip keadilan
c. 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
b. Tantangan pergaulan internasional
c. Tantangan pengembangan sikap dan tanggung jawab pribadi
d. Tantangan pengembangan sumber daya manusia

F. STUDI KASUS CYBERCRIME

Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan yang disebut dengan Cybercrime atau kejahatan melalui jaringan Internet. Adanya Cybercrime telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya pada jaringan internet.

Cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk didalamnya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit (carding), confidence fraud, penipuan identitas, pornografi anak, dan lain-lain (nunuk sulisrudatin)

Berikut ini adalah beberapa contoh kasus Kejahatan cyber yang pernah terjadi di Indonesia :

Kasus 1 : **Pencurian Kartu Kredit (Carding) (Sulisrudatin, 2018)**

Hal ini adalah salah satu jenis Cybercrime yang terjadi di Bandung sekitar Tahun 2003. Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet. Kejahatan seperti ini masuk ke dalam pelanggaran Pasal 378 KUHP tentang penipuan, Pasal 363 tentang Pencurian dan Pasal 263 tentang Pemalsuan Identitas. Prosesnya adalah, pelaku carding memperoleh data kartu kredit korban secara tidak sah (illegal interception) dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko online (forgery). Modus ini dapat terjadi kemungkinan akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesan barang di toko online. Kejahatan kartu kredit yang paling banyak terjadi adalah pencurian indentitas dan Card Not Present (CNP). Dengan jumlah kasus pencurian identitas sebanyak 402 kasus dan CNP 458 kasus dengan nilai masing masing Rp 1,14 miliar dan Rp 545 juta yang dialami 18 penerbit. Salah satu kasus pencurian data kartu kredit yang berhasil diungkap oleh pihak kepolisian yaitu tertangkapnya bandit penipuan kartu kredit, berinisial BA (37) dan AL (37). Direktur Kriminal Umum Polda Metro Jaya Kombes Pol Khrisna Murti mengatakan, kedua pelaku berhasil menggasak uang dari bank swasta lewat kartu kredit korban sebanyak ratusan juta rupiah. Sedangkan pihak bank selaku korban mengalami kerugian Rp600 juta untuk periode Januari hingga Mei 2015. Atas perbuatannya, para tersangka dikenakan Pasal 379 dan Pasal 362 KUHP dengan ancaman hukuman penjara paling lama empat dan lima tahun. Modus operandi kedua pelaku, yaitu dengan membeli daftar nasabah yang berisi data pemegang kartu kredit salah satu bank swasta dari pihak marketing. Mereka beralasan menawarkan asuransi jiwa, yang dilakukan pelaku BA. Setelah berhasil mendapatkan daftar data pribadi pemegang kartu kredit, tersangka BA menghubungi nomor telepon pengguna kartu kredit yang berada di dalam data tersebut dan mengaku dari credit card pusat bank swasta. Kemudian kepada para korban, BA menjelaskan

dan menggunting kartu kredit korban dengan modus akan menggantinya dengan kartu kredit baru dengan limit yang lebih besar tanpa biaya administrasi. Kemudian salah satu pelaku, yakni AL berperan sebagai kurir untuk mengambil kartu kredit korban berikut fotokopi KTP dengan alasan untuk menyesuaikan data dan memberikan tanda terima dengan logo salah satu bank atas nama pemilik kartu kredit. Pelaku BA membuat KTP palsu dengan data identitas fotokopi KTP korban yang akan dipergunakan pada saat melakukan transaksi di toko untuk membeli barang barang mewah.

Kasus 2 : **Penyebaran Virus Dengan Sengaja (Anto, 2018)**

Ini adalah salah satu jenis kasus cyber crime yang terjadi pada bulan Juli 2009, Twitter (salah satu jejaring social yang sedang naik pamor di masyakarat belakangan ini) kembali menjadi media infeksi modifikasi New Koobface, worm yang mampu membajak akun Twitter dan menular melalui postingannya, dan menjangkiti semua follower. Semua kasus ini hanya sebagian dari sekian banyak kasus penyebaran malware di seantero jejaring social. Twitter tak kalah jadi target, pada Agustus 2009 diserang oleh penjahat cyber yang mengiklankan video erotis. Ketika pengguna mengkliknya, maka otomatis mendownload Trojan-Downloader.Win32.Banload.sco. Modus serangannya adalah selain menginfeksi virus, akun yang bersangkutan bahkan si pemiliknya terkena imbas. Karena si pelaku mampu mencuri nama dan password pengguna, lalu menyebarkan pesan palsu yang mampu merugikan orang lain, seperti permintaan transfer uang . Untuk penyelesaian kasus ini, Tim keamanan dari Twitter sudah membuang infeksi tersebut. Tapi perihal hukuman yang diberikan kepada penyebar virusnya belum ada kepastian hukum.

Kasus 3: **Cybersquatting (Anto, 2018)**

Adalah mendaftar, menjual atau menggunakan nama domain dengan maksud mengambil keuntungan dari merek dagang atau nama orang lain. Umumnya 6 mengacu pada praktek membeli nama domain yang menggunakan nama-nama bisnis yang sudah ada atau nama orang orang terkenal dengan maksud untuk menjual nama untuk keuntungan bagi bisnis mereka. Contoh kasus cybersquatting, Carlos Slim, orang terkaya di dunia itu pun kurang sigap dalam mengelola brandingnya di internet, sampai domainnya diserobot orang lain. Beruntung kasusnya bisa digolongkan cybersquat sehingga domain carlosslim.com bisa diambil alih. Modusnya memperdagangkan popularitas perusahaan dan keyword Carlos Slim dengan cara menjual iklan Google kepada para pesaingnya. Penyelesaian kasus ini adalah dengan menggunakan prosedur Anticybersquatting Consumer Protection Act (ACPA), memberi hak untuk pemilik merek dagang untuk menuntut sebuah cybersquatter di pengadilan federal dan mentransfer nama domain kembali ke pemilik merek dagang. Dalam beberapa kasus, cybersquatter harus membayar ganti rugi uang

Kasus 4 : **Perjudian Online (Anto, 2018)**

Pada kasus ini pelaku menggunakan sarana internet untuk melakukan perjudian. Contohnya seperti yang terjadi di Semarang, Desember 2006. Para pelaku melakukan praktiknya dengan menggunakan system member yang semua anggotanya mendaftar ke admin situs itu, atau menghubungi HP ke 0811XXXXXX dan 024-356XXXX. Mereka melakukan transaki online lewat internet dan HP untuk mempertaruhkan pertarungan bola Liga Inggris, Liga Italia dan Liga Jerman yang ditayangkan di televisi. Untuk setiap petaruh yang berhasil menebak skor dan memasang uang Rp 100 ribu bisa mendapatkan uang Rp 100 ribu, atau bisa lebih. Modus para pelaku bermain judi online adalah untuk mendapatkan uang dengan cara instan. Dan sanksi menjerat para pelaku yakni dikenakan pasal 303 tentang perjudian dan UU 7/1974 pasal 8 yang ancamannya lebih dari 5 tahun. Dalam kasus ini telah melanggar UU ITE BAB VII Pasal 27 Ayat 2 yang berbunyi

“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian”.

Salah satu contoh kasus yang terjadi adalah pencurian dokumen terjadi saat utusan khusus Presiden Susilo Bambang Yudhoyono yang dipimpin Menko Perekonomian Hatta Rajasa berkunjung di Korea Selatan. Kunjungan tersebut antara lain, guna melakukan pembicaraan kerja sama jangka pendek dan jangka panjang di bidang pertahanan. Delegasi Indonesia beranggota 50 orang berkunjung ke Seoul untuk membicarakan kerja sama ekonomi, termasuk kemungkinan pembelian jet tempur latih supersonik T-50 Golden Eagle buatan Korsel dan sistem persenjataan lain seperti pesawat latih jet supersonik, tank tempur utama K2 Black Panther dan rudal portabel permukaan ke udara. Ini disebabkan karena Korea dalam persaingan sengit dengan Yak-130, jet latih Rusia. Sedangkan anggota DPR yang membidangi Pertahanan (Komisi I) menyatakan, berdasar informasi dari Kemhan, data yang diduga dicuri merupakan rencana kerja sama pembuatan 50 unit pesawat tempur di PT Dirgantara Indonesia (DI). Pihak PT DI membenarkan sedang ada kerja sama dengan Korsel dalam pembuatan pesawat tempur KFX (Korea Fighter Experiment). Pesawat KFX lebih canggih daripada F16. Modus dari kejahatan tersebut adalah mencuri data atau data theft, yaitu kegiatan memperoleh data komputer secara tidak sah, baik digunakan sendiri ataupun untuk diberikan kepada orang lain. Indentity Theft merupakan salah satu jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan. Kejahatan ini juga sering diikuti dengan kejahatan data leakage. Perbuatan melakukan pencurian dara sampai saat ini tidak ada diatur secara khusus

Kasus 5 : **Kejahatan Yang Berhubungan Dengan Nama Domain (Alfian, 2017)**

Dunia perbankan melalui internet (e-banking) Indonesia dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang hacker dan jurnalis. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan internet banking Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain wwwklik- bca.com, kilkbca.com, clikbca.com, klickca.com, dan klikbac.com. Isi situs-situs plesetan ini nyaris sama. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (user id) dan nomor identitas personal dapat diketahuinya. Diperkirakan, 130 nasabah BCA tercuri datanya. Menurut pengakuan Steven pada situs bagi para webmaster di Indonesia, www.webmaster.or.id tujuan membuat situs plesetan adalah agar publik berhatihati dan tidak ceroboh saat melakukan pengetikan alamat situs (typo site), bukan untuk mengeruk keuntungan. Nasabah yang tertipu akan login ke dalam website palsu dan mulai mengisi informasi penting mengenai data pribadi, seperti nomor kartu kredit, PIN, nomor rekening, password, tanggal lahir, atau nama ibu kandung. Si korban merasa telah mengunjungi website asli bank yang ia gunakan yang tidak lain website palsu. Data pribadi tadi telah dimiliki oleh pelaku phising dan akan digunakanannya untuk mengakses rekening atau kartu kredit korban. Korban yang tertipu baru akan menyadari penipuan saat ia menerima surat pernyataan dari bank atau penerbit kartu kreditnya Persoalan tidak berhenti di situ. Pasalnya, banyak nasabah BCA yang merasa kehilangan uangnya untuk transaksi yang tidak dilakukan. Ditengarai, para nasabah itu kebobolan karena menggunakan fasilitas Internet banking lewat situs atau alamat lain yang membuka link ke Klik BCA, sehingga memungkinkan user ID dan PIN pengguna diketahui

Kejahatan yang berhubungan dengan nama domain seperti kasus yang terjadi pada nasabah bank BCA di atas adalah dengan membuat “domain plesetan”, yaitu domain yang mirip dengan nama domain orang lain. .Istilah yang digunakan saat ini adalah typosquatting. Jadi, jika publik

tidak benar mngetik nama asli domain-nya, maka mereka akan masuk ke situs plesetan ini. Hal ini menyebabkan identitas pengguna (user_id) dan nomor identitas personal dapat diketahui.

Modus dari kegiatan kejahatan ini adalah penipuan dan termasuk penyalahgunaan user_ID dan password oleh seorang yang tidak punya hak. Motif dari kejahatan ini termasuk ke dalam cybercrime sebagai tindakan murni kejahatan. Hal ini dikarenakan para penyerang dengan sengaja membuat sebuah situs dengan membuat nama domainnya sama dengan suatu perusahaan atau merek dagang. Kejahatan kasus cybercrime ini dapat termasuk jenis cybersquatting, typosquatting, cybercrime uncauthorized access dan hacking-cracking. Sasaran dari kasus kejahatan ini adalah cybercrime menyerang individu (against person).

Kasus 6 : **Terjadinya Perubahan Dalam Website KPU**

Pada tanggal 17 April 2004, Dani Hermansyah melakukan deface dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam www.kpu.go.ig . Hal ini mengakibatkan keprcayaan masyarakat terhadap Pemilu yang sedang berlangsung pada saat itu menjadi berkurang. Dengan berubahnya nama partai di dalam website, maka bukan tidak mungkin angka-angka jumlah pemilih yang masuk di sana menjadi tidak aman dan bisa diubah.

Modus dari kejahatan ini adalah mengubah tampilan dan informasi website. Motif dari kejahatan ini termasuk ke dalam cybercrime sebagai tindakan murni kejahatan. Hal ini dikarenakan para penyerang dengan sengaja mengubah tampilan dan informasi dari website. Kejahatan kasus cybercrime ini dapat termasuk jenis hacking dan cracking, data frogery, dan bisa juga cyber terorism. Sasaran dari kasus kejahatan ini adalah cybercrime menyerang hak milik (against property) dan bisa juga cybercrime menyerang pemerintah (against government).

Kasus 7 : **Kasus Penyebaran Video Pornografi (Ketaren, 2016)**

Pada tahun 2008, Di Indonesia kasus pornografi kasusnya Ariel-Luna-Cut Tari. Kasus video porno Ariel "PeterPan" dengan Luna Maya dan Cut Tari, video tersebut di unggah di internet oleh seorang yang berinisial 'RJ'. Pada kasus tersebut, modus sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Penyelesaian kasus ini pun dengan jalur hukum, penunggah dan orang yang terkait dalam video tersebut pun turut diseret pasal-pasal sebagai berikut, Pasal 29 UURI No. 44 th 2008 tentang Pornografi Pasal 56, dengan hukuman minimal 6 bulan sampai 12 tahun. Atau dengan denda minimal Rp 250 juta hingga Rp 6 milyar. Dan atau Pasal 282 ayat 1 KUHP

Kasus 8 : **Pencemaran Nama Baik (Ketaren, 2016)**

Prita Mulyasari, Digugat dan dilaporkan ke Polisi oleh Rumah Sakit Omni Internasional atas tuduhan Pencemaran nama baik lewat millis. Kasus ini bermula dari surat elektronik yang dibuat oleh Prita yang berisi pengalamannya saat dirawat di unit gawat darurat Omni Internasional. Prita Mulyasari dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp.1 miliar

Kasus 9 : **Pencemaran Nama Baik (Ketaren, 2016)**

Narliswandi Piliang, wartawan yang kerap menulis disitus Presstalk.com , 14 Juli 2008 lalu di laporkan oleh Anggota DPR Alvin Lie ke Polda Metro Jaya. Kasus Tersebut bermula dari tulisan Narliswandi Piliang yang berjudul "Hoyak Tabuik Adaro dan Soekanto", yang berisikan PAN meminta uang sebesar Rp 2 Triliun kepada Adaro agar DPR tidak lakukan hak angket yang akan menghambat IPO Adaro. Narliswandi Piliang dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp. 1 miliar

Kasus 10 : **Pencemaran Nama Baik (Ketaren, 2016)**

Agus Hamonangan, adalah moderator milis FPK. Diperiksa sebagai saksi perkara pencemaran nama baik di Markas Kepolisian Daerah Metro Jaya. Pelapor kasus tersebut adalah Anggota DPR Fraksi Partai Amanat Nasional, Alvin Lie, terkait pemuatan tulisan berjudul "Hoyak Tabuik Adaro dan Soekanto", karya Narliswandi Piliang. Agus Hamonangan dikenakan pasal Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp 1 miliar

Kasus 11 : **Pencemaran Nama Baik (Ketaren, 2016)**

EJA (38) inisial, atas dugaan pencemaran nama baik dan penyebaran berita bohong melalui sistem elektronik. EJA dijadikan sebagai tersangka karena mengirimkan e-mail kepada kliennya soal lima bank yang dilanda kesulitan likuiditas, EJA telah resmi ditahan. Informasi EJA itu katanya dikhawatirkan akan menyebabkan rush atau kekacauan. Dikatakan bahwa EJA mendengar rumor soal sejumlah bank kesulitan likuidasi dari para broker secara verbal. EJA lalu menginformasikan hal itu kepada para kliennya melalui e-mail dengan domain perusahaannya. Informasi inilah yang lalu tersebar luas. EJA dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp. 1 miliar

Kasus 12 :

Julian Assange, adalah seorang jurnalis yang berasal dari Australia yang dikenal sebagai pendiri dan juru bicara WikiLeaks. Hal ini dilakukannya karena dia yakin bahwa pertukaran informasi akan mengakhiri pemerintahan yang tidak sah. WikiLeaks memiliki server utama di Swedia. Julian Assange menyusup ke dalam sistem keamanan dan mempublikasikannya. Polisi

Internasional bekerja sama untuk menangkap Julian Assange untuk mempertanggunjawabkan perbuatannya atas kebocoran informasi rahasia milik negara. (Ketaren, 2016)

Kasus 13 (Ketaren, 2016) :

Edward Joseph Snowden, adalah mantan kontraktor teknik Amerika Serikat dan karyawan Central Intelligence Agency (CIA) yang menjadi kontraktor untuk National Security Agency (NSA) sebelum membocorkan informasi program mata – mata rahasia NSA kepada pers. Snowden membocorkan informasi rahasia menyangkut program – program NSA yang sangat rahasia seperti PRISM kepada The Guardian dan The Washington Post. Skandal Snowden membuat hubungan Amerika dan negara di Eropa seperti Prancis dan Jerman menjadi terganggu. Dari skandal Snowden ini juga akhirnya terkuak bahwa Australia selama ini menyadap telepon Presiden Indonesia, Susilo Bambang Yudhoyono serta beberapa jajaran staffnya yang membuat hubungan diplomatik Indonesia dan Australia menjadi terganggu. Saat ini Edward Snowden berada dalam perlindungan negara Rusia.

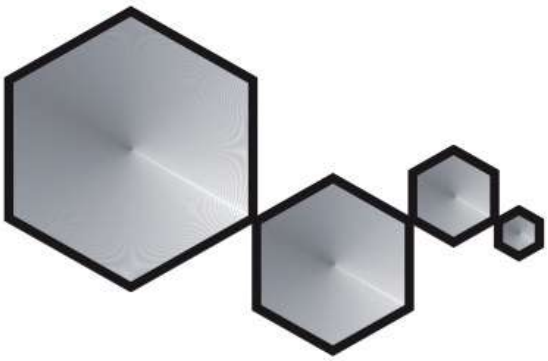
Kasus 14 : Penyebaran Virus Dengan Sengaja (Anto, 2018)

Ini adalah salah satu jenis kasus cyber crime yang terjadi pada bulan Juli 2009, Twitter (salah satu jejaring social yang sedang naik pamor di masyakarat belakangan ini) kembali menjadi media infeksi modifikasi New Koobface, worm yang mampu membajak akun Twitter dan menular melalui postingannya, dan menjangkiti semua follower. Semua kasus ini hanya sebagian dari sekian banyak kasus penyebaran malware di seantero jejaring social. Twitter tak kalah jadi target, pada Agustus 2009 diserang oleh penjahat cyber yang mengiklankan video erotis. Ketika pengguna mengkliknya, maka otomatis mendownload Trojan-Downloader.Win32.Banload.sco. Modus serangannya adalah selain menginfeksi virus, akun yang bersangkutan bahkan si pemiliknya terkena imbas. Karena si pelaku mampu mencuri nama dan password pengguna, lalu menyebarkan pesan palsu yang mampu merugikan orang lain,

seperti permintaan transfer uang . Untuk penyelesaian kasus ini, Tim keamanan dari Twitter sudah membuang infeksi tersebut. Tapi perihal hukuman yang diberikan kepada penyebar virusnya belum ada kepastian hukum

Kasus 15 : DoS (Denial Of Service) (Anto, 2018)

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan. Pada kasus Hacking ini biasanya modus seorang hacker adalah untuk menipu atau mengacak-acak data sehingga pemilik tersebut tidak dapat mengakses web miliknya. Untuk kasus ini Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya



DAFTAR PUSTAKA

Anoname, http://en.wikipedia.org

Anoname, UU RI No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, Penerbit DepKomInfo, Jakarta, 2008

Antonius Atosokhi Gea, S.Th. MM, Antonina Panca Yuni Wulandari S.Sos, Relasi dengan Dunia Character Building IV, Elex Media Komputindo, Jakarta, 2006

Bahri, I. S. (2020). Cyber Crime Dalam Sorotan Hukum Pidana. Bahasa Rakyat.

BSSN Book, Tip Singkat & Praktis di Dunia Siber, 2018.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati S.Kom., M.Sc.Eng, N. A. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. Journal of Information Engineering and Educational Technology, 2(2), 65. https://doi.org/10.26740/jieet.v2n2.p65-69

DRS. Abdul Wahid, S.H, MA, Mohammad Labib, SH, Kejahatan Mayantara (Cyber Crime), PT. Refika Aditama, Bandung, 2005

Drs. Dikdik M. Arief Mansur, SH, MH, Elisatris Gultom, SH. MH, Cyber Law (Aspek Hukum Teknologi Informasi), PT. Refika Aditama, Bandung, 2005

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. Times, 5(2), 35–42. http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126

Kode Etik Telematika

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. Teknologi Informasi Dan Komunikasi, 100–113.

Prof. Abdulkadir Muhammad, S.H, Etika Profesi Hukum, Penerbit PT. Citra Aditya Bakti, Bandung, 2001

Rifauddin, M., & Halida, A. N. (2018). Waspada Cybercrime dan Informasi Hoax pada Media Sosial Facebook. Khizanah Al-Hikmah/: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan, 6(2), 98. https://doi.org/10.24252/kah.v6i2a2

Ramli, A. M. (2016). Pengertian dan Lingkup Hukum Telematika. In Pengertian dan Ruang Lingkup Telematika (Vol. 2, pp. 1–2). Jakarta.

Rosenoer, J. (1997). Cyber Law/: THE LAW OF THE INTERNET. New York: Springer.

Sitompul, Josua, S.H, IMM, Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana, PT. Tata nusa, Jakarta, 2012

Suhariyanto, Budi, S.H, M.H, Tindak Pidana Teknologi Informasi (cybercrime), RajaGrafindo Persada, Depok, 2012

Suharyo. (2010). Laporan Penelitian Penerapan Bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus-Kasus Cybercrime. Jakarta. https://doi.org/10.1017/CBO9781107415324.004

Sumadi, H. (2016). Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia. Jurnal Wawasan Yuridika, 33(2), 175. https://doi.org/10.25072/jwy.v33i2.102

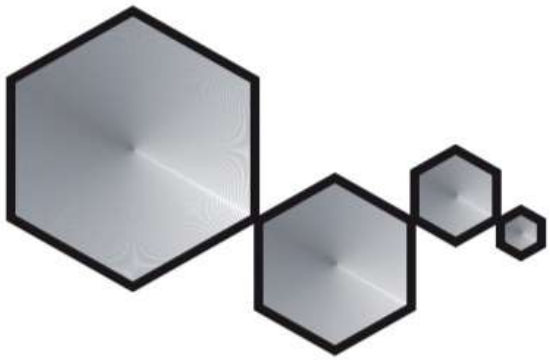
Supanto. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy. Yustisia Jurnal Hukum, 5(1). https://doi.org/10.20961/yustisia.v5i1.8718

Syafyahya, L. (2018). Makalah Kongres Kbi 2018 Ujaran Kebencian Dalam Bahasa Indonesia/: Kajian Bentuk Dan Makna. Kongres Bahasa Indonesia. Retrieved from http://repositori.kemdikbud.go.id/10234/1/UJARAN KEBENCIAN DALAM BAHASA INDONESIA.pdf

Teguh Wahyono, Etika Komputer dan Tanggung Jawab Profesional di Bidang Teknologi Informasi, Andi Publisher, Jakarta, 2006

Winarno, E., Zaki, A., & Community, S. (2015). Belajar Hacking Dari Nol Untuk Pemula. Jakarta: Gramedia.

-oo0oo-



GLOSARIUM

Cracker adalah sisi gelap dari *Hacker* dan memiliki ketertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer.

Cybercrime adalah kejahatan komputer atau penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau penyembuanyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.

Database administrator adalah pekerjaan yang membutuhkan keahlian untuk mendesain, mengimplementasikan, memelihara dan mengelola database.

EDP Operator adalah orang yang bertugas untuk mengoperasikan program-program yang berhubungan dengan electronic data processing dalam lingkungan sebuah perusahaan atau organisasilainnya.

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

Hardware engineering adalah pekerjaan yang mengharuskan memiliki keahlian dalam mengembangkan pengembangan perangkat keras yang akan digunakan untuk implementasi sistem informasi.

Instructor (Instruktur) adalah 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.

IT support adalah pekerjaan yang membutuhkan keahlian dalam mengatasi masalah umum yang terjadi pada komputer seperti install software, perbaikan hardware, perbaikan jaringan komputer, perbaikan komunikasi jaringan komputer di antara user, pemeliharaan rutin dan sederhana dari sebuah sistem informasi.

Networking Engineer adalah orang yang berkecimpung dalam bidang teknis jaringan komputer dari maintenance sampai pada troubleshooting-nya

Network architecture adalah pekerjaan yang membutuhkan keahlian dalam mendesain skema jaringan komputer, merancang stopologi jaringan komputer, menghubungkan skema satu komputer dengan komputer lain, memahami fungsi dan perangkat jaringan, membangun dan melakukan pengujian terhadapn jaringan komunikasinya.

Programmer merupakan orang yang bertugas mengimplementasikan rancangan sistem analis yaitu membuat program (baik aplikasi maupun sistem operasi) sesuai sistem yang dianalisa sebelumnya.

Project Manager (Manajer Proyek) adalah 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.

System analyst adalah pekerjaan yang membutuhkab keahlian untuk menganalisa kebutuhan sistem dan user.

Software engineering adalah pekerjaan yang mengharuskan memiliki keterampilan dalam pengembangan sistem informasi dimulai dari tahapn perencanaan, analisa, desain, implementasi hingga pegujian dan pemeliharaan.

Specialist adalah 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.

Techcnical engineer atau sering disebut teknisi adalah orang yang harus memiliki keterampilan dan penguasaan teknik yang terkait dengan cabang teknik tertentu, dengan adanya pemahaman yang praktis serta mempunyai konsep teknik fundamental umum.

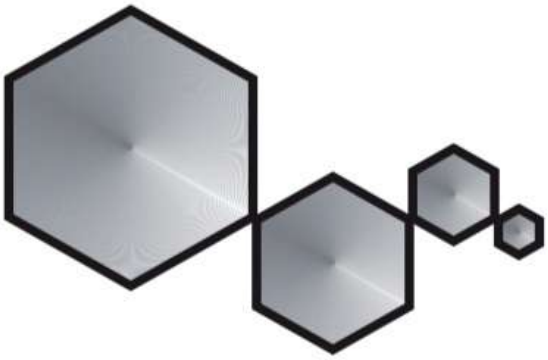
Web designer adalah orang yang melakukan kegiatan perecanaan, termasuk studi kelayakan, analisis dan desain terhadap suatu proyek pembuatan aplikasi berbasisweb.

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

Web administrator adalah pekerjaan yang membutuhkan keahlian teknis terhadap operasional sebuah situs atau website, bertanggung jawab terhadap pengelolaan situs atau website serta melakukan pemeliharaan terhadap jalannya sebuah situs atau website.

Web developer adalah pekerjaan yang membutuhkan keterampilan dalam pengembangan sebuah situs website. Web developer harus mampu merancang kebutuhan sistem dalam pembuatan situs website, dan membuat dapat diaksesnya halaman website dengan menggunakan jaringan komputer. Web developer harus mampu mengembangan sebuah situs website dan menampilkan situs website sehingga dapat diakses oleh user, serta melakukan pemeliharaan sistemnya.

-oo0oo-



TENTANG PENULIS

Susi Susilowati, M.Kom, lahir di Jakarta, menyelesaikan pendidikan S1 Ilmu Komputer di Universitas Gunadarma dan S2 di STMIK Nusa Mandiri Jakarta. Penulis telah melaksanakan sertifikasi kompetensi BNSP dalam bidang programmer. Sejak tahun 2010 penulis aktif mengajar sebagai dosen tetap pada Universitas Bina Sarana Informatika dan sudah memperoleh sertifikasi dosen sejak tahun 2016. Penulis berkontribusi aktif dalam penulisan jurnal ilmiah nasional dan internasional pada bidang sistem informasi dan yang lainnya.

Enok Tuti Alawiah, M.Kom, lahir di Ciamis Jawa Barat, menyelesaikan pendidikan S1 Ilmu Komputer di Universitas Pakuan Bogor dan S2 di STMIK Nusa Mandiri Jakarta. Penulis telah melaksanakan sertifikasi kompetensi BNSP dalam bidang programmer. Sejak tahun 2010 penulis aktif mengajar sebagai dosen tetap pada Universitas Bina Sarana Informatika dan sudah memperoleh sertifikasi dosen sejak tahun 2019. Penulis berkontribusi aktif dalam penulisan jurnal ilmiah nasional dan internasional pada bidang sistem informasi dan yang lainnya.

Dewi Ayu Nur Wulandari, M.Kom Dosen Universitas Bina Sarana Informatika Kampus Kota Bogor. Lulusan Program Magister Ilmu Komputer (S2) di STMIK Nusa Mandiri. Aktif sebagai dosen dan juga sebagai pembicara

seminar dan workshop. Pemenang kategori presenter terbaik di KNIT 2016 dan pemenang kategori paper terbaik di KNIST 2017. Pemenang hibah penelitian dari DIKTI tahun 2017.

-oo0oo-

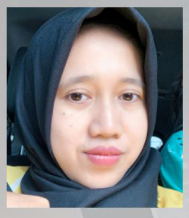
Etika Profesi Teknologi Informasi dan Komunikasi

Buku ini ditulis berdasarkan pengalaman dan pengetahuan penulis sebagai pengampu matakuliah Etika Profesi TIK. Buku Etika Profesi TIK ini disusun dengan tujuan untuk memudahkan mahasiswa, praktisi dan pemakai lainnya untuk memahami Etika Profesi TIK.

Inti dari Etika Profesi TIK adalah bagaimana setiap insan manusia yang menggunakan ilmu pengetahuan dan teknologi harus memahami dan mendalami aturan-aturan atau etika yang terkait dengan ilmu pengetahuan dan teknologi itu sendiri serta menjunjung tinggi etika dan profesionalisme di bidang TIK.

Topik-topik bahasan dalam buku ini yang dirangkai secara sederhana, komprehensif dan sistematis agar lebih mudah dipahami oleh siapapun yang ingin mempelajari Etika Profesi TIK.

Susi Susilowati, M.Kom, lahir di Jakarta, menyelesaikan pendidikan S1 Ilmu Komputer di Universitas Gunadarma dan S2 di STMIK Nusa Mandiri Jakarta. Penulis telah melaksanakan sertifikasi kompetensi BNSP dalam bidang programmer. Sejak tahun 2010 penulis aktif mengajar sebagai dosen tetap pada Universitas Bina Sarana Informatika dan sudah memperoleh sertifikasi dosen sejak tahun 2016. Penulis berkontribusi aktif dalam penulisan jurnal ilmiah nasional dan internasional pada bidang sistem informasi dan yang lainnya.



Enok Tuti Alawiah, M.Kom, lahir di Ciamis Jawa Barat, menyelesaikan pendidikan S1 Ilmu Komputer di Universitas Pakuan Bogor dan S2 di STMIK Nusa Mandiri Jakarta. Penulis telah melaksanakan sertifikasi kompetensi BNSP dalam bidang programmer. Sejak tahun 2010 penulis aktif mengajar sebagai dosen tetap pada Universitas Bina Sarana Informatika dan sudah memperoleh sertifikasi dosen sejak tahun 2019. Penulis berkontribusi aktif dalam penulisan jurnal ilmiah nasional dan internasional pada bidang sistem informasi dan yang lainnya.

Dewi Ayu Nur Wulandari, M.Kom Dosen Universitas Bina Sarana Informatika Kampus Kota Bogor. Lulusan Program Magister Ilmu Komputer (S2) di STMIK Nusa Mandiri. Aktif sebagai dosen dan juga sebagai pembicara seminar dan workshop. Pemenang kategori presenter terbaik di KNIT 2016 dan pemenang kategori paper terbaik di KNIST 2017. Pemenang hibah penelitian dari DIKTI tahun 2017.

Buku ini diterbitkan atas kerjasama dengan
Universitas Bina Sarana Informatika

eISBN: 978-623-6433-07-2

Susi Susilowati; Enok Tuti Alawiyah; Dewi Ayu Nur Wulandari

Etika Profesi Teknologi Informasi dan Komunikasi