

ETIKA

PROFESI

Dalam Bidang Teknologi Informasi



YAYASAN PRIMA AGUS TEKNIK

Vivi Kumalasari S., S.E, M.Si, Ak.

ETIKA PROFESI

Dalam Bidang Teknologi Informasi



Vivi Kumalasari S., S.E, M.Si, Ak.



YAYASAN PRIMA AGUS TEKNIK

PENERBIT :

YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ETIKA PROFESI

Dalam Bidang Teknologi Informasi

Oleh :
Vivi Kumalasari S., S.E, M.Si, Ak.



YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ETIKA PROFESI, Dalam Bidang Teknologi Informasi

Penulis :

Vivi Kumalasari S., S.E, M.Si, Ak.

ISBN : 9 78 623 6141 08 3

Editor :

Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :

Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :

Irdha Yudianto

Penebit :

Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Redaksi :

Jl. Majapahit no 605 Semarang

Telp. (024) 6723456

Fax. 024-6710144

Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :

Universitas STEKOM

Jl. Majapahit no 605 Semarang

Telp. (024) 6723456

Fax. 024-6710144

Email : info@stekom.ac.id

Hak cipta dilindungi undang-undang

Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa ijin tertulis dari penerbit

Kata Pengantar

Assalamualaikum Wr.Wb

Puji Syukur ke hadirat Allah SWT karena berkat rahmat dan hidayah-Nya, Penulis dapat menyelesaikan pembuatan buku ini. Materi yang terkandung dalam buku ini dibuat dengan sesederhana mungkin sehingga pembaca mudah untuk mempelajari dan mempraktekannya. Setelah mempelajari materi ini pembaca diharapkan dapat memahami dan menerapkan tentang etika yang berkaitan dengan profesi di bidang Teknologi Informasi. Penulis menyadari buku ini masih jauh dari sempurna dan mungkin juga banyak terdapat kesalahan. Untuk itu penulis sangat mengharapkan adanya saran dari semua pihak untuk dapat lebih menyempurnakan buku ini.

Sebelum mengakhiri kata pengantar ini, izinkanlah penulis mengucapkan terima kasih pada pihak-pihak yang memungkinkan diterbitkannya buku ini, yaitu semua staf Universitas STEKOM Semarang serta teman teman tercinta di lingkungan Universitas STEKOM Semarang.

Wassalamualaikum Wr.Wb

Penulis

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI	ii
BAB I TINJAUAN UMUM ETIKA	1
1.1 Definisi Etika	1
1.2 Pendekatan Etika	6
1.3 Kode Etik dan Tanggung Jawab Profesi	10
1.3.1 Kode Etik	10
1.3.2 Kode Etik Profesi	12
1.3.3 Pengertian Tanggung Jawab Profesi	14
BAB II PEKERJAAN DAN PROFESI.....	17
2.1 Pekerjaan dan Profesi.....	17
2.2 Profesi Kerja di Bidang Teknologi Informasi	21
2.3 Kompetensi Kerja di Bidang Teknologi Informasi	25
2.4 Sertifikasi di Bidang Teknologi Informasi.....	29
2.5 Lembaga dan Organisasi Profesi Teknologi Informasi	31
BAB III SEJARAH ETIKA DI BIDANG KOMPUTER	34
3.1 Konsep Etika di Bidang Komputer.....	34
3.2 Sejarah Etika di Bidang Komputer	36
3.3 Kode Etik Profesi di Bidang Teknologi Informasi	40
3.4 Tanggung Jawab Profesi IT.....	43
3.5 Pelanggaran Etika Profesi IT.....	44
BAB IV ETIKA DI DUNIA MAYA	49
4.1 Perkembangan Penggunaan Internet Masa Kini.....	49
4.2 Cyber Law dan UU ITE.....	52
4.2.1 Cyber Law	52
4.2.2 UU ITE... ..	55
4.3 Etika Menggunakan Internet menurut UU ITE	58
4.4 Etika di Dunia Maya menurut UU ITE	60
Bab V CYBER CRIME	63
5.1 Definisi Cyber Crime.....	63
5.2 Jenis-Jenis Cyber Crime.....	65
5.3 Bagaimana Mencegah Terjadinya Cyber Crime	72
DAFTAR PUSTAKA	75

BAB 1

TINJAUAN UMUM ETIKA

1.1 Definisi Etika

Konsep tentang etika di mulai pada abad ke lima sebelum Masehi. Berbagai mazhab di Yunani; yang ditandai dengan kehadiran tokoh Socrates, dimana Socrates mengatakan bahwa kebaikan itu adalah pengetahuan. Kemudian Plato, menurut Plato, baik itu apabila ia dikuasai oleh akal budi dan buruk itu apabila dikuasai oleh hawa nafsu. Sejarah tentang etika sudah sering digambarkan dan sempat mengisi beberapa buku tebal. Bahkan banyak gejala menunjukkan bahwa di semakin majunya peradaban manusia, minat terhadap etika tidak berkurang tapi justru bertambah. Hal ini dikarenakan kehidupan kita lebih kompleks daripada generasi- generasi sebelumnya dimana kita menghadapi berbagai masalah moral yang baru dan berat. Masalah-masalah itu ditimbulkan karena perkembangan pesat di bidang ilmu pengetahuan dan teknologi, tapi juga karena perubahan sosio-budaya yang mendalam dan pada waktu yang bersamaan berlangsung di mana-mana dalam kehidupan masyarakat modern.

Asal kata etika adalah “ethikos” yang merupakan bahasa Yunani. Merujuk serapan bahasa Yunani tersebut, arti dari etika adalah sesuatu hal yang timbul dari kebiasaan. Sedangkan menurut KBBI (Kamus Besar Bahasa Indonesia), etika adalah ilmu tentang apa yang baik dan apa yang buruk dan tentang hak dan kewajiban moral (akhlak).

Munculnya etika adalah pada saat manusia merefleksikan unsur etis ke dalam pendapat yang spontan. Kebutuhan akan adanya refleksi tersebut bisa dirasakan karena pendapat etis dapat berbeda dengan pendapat orang lain. Itulah mengapa manusia pada akhirnya membutuhkan etika, di mana tujuannya untuk mencari tahu apa yang harus dilakukan oleh manusia.

Secara lebih mendetail, etika adalah sesuatu dimana dan bagaimana cabang utama filsafat yang mempelajari nilai atau kualitas standar moral dan penilaian. Etika meliputi analisis dan penerapan konsep seperti benar, salah, baik, buruk, dan tanggung jawab. Tokoh *St. John dari Damaskus (abad ke-7 Masehi)* menempatkan etika dalam studi ilmu filsafat praktis. Sebagai sebuah bidang ilmu, objek etika adalah perilaku manusia. Namun, tidak seperti ilmu-ilmu lain yang meneliti perilaku manusia, etika memiliki sudut pandang normatif. Hal ini merupakan sudut pandang etika yang menilai tindakan manusia yang baik dan buruk. Secara umum, etika terbagi menjadi tiga bagian utama, yaitu meta-

etika (konsep etika), etika normatif (studi penentuan nilai etika), dan penerapan etika (studi tentang penggunaan nilai-nilai etika).

Berikut ini adalah pengertian etika menurut para ahli:

• *Menurut K. Bertens*

Etika adalah nilai-nilai dan norma-norma moral, yang menjadi pegangan bagi seseorang atau suatu kelompok dalam mengatur perilaku.

• *Menurut W. J. S. Poerwadarminto*

Etika merupakan studi tentang prinsip-prinsip moralitas (moral).

• *Menurut Prof. DR. Franz Magnis Suseno*

Etika adalah ilmu yang mencari orientasi atau ilmu yang memberikan arah dan pijakan dalam tindakan manusia.

• *Menurut Ramali dan Pamuncak*

Etika adalah pengetahuan tentang perilaku yang benar dalam profesi.

• *Menurut H. A. Mustafa*

Etika adalah ilmu yang menyelidiki, yang baik dan yang buruk untuk mengamati tindakan manusia sejauh bisa diketahui oleh pikiran.

Ciri-Ciri Etika

Terdapat beberapa karakteristik etika yang dapat membedakannya dengan norma-norma lainnya. Adapun ciri-ciri etika adalah sebagai berikut:

- Etika tetap berlaku walaupun tidak ada orang lain yang menyaksikannya.
- Etika sifatnya itu absolut atau mutlak.
- Didalam etika terdapat cara pandang dari sisi batiniah manusia itu.
- Etika sangat terkait dengan perbuatan serta perilaku pada manusia itu sendiri.

Fungsi Etika

1. Tempat untuk mendapatkan orientasi kritis yang berhadapan dengan berbagai suatu moralitas yang membingungkan.
2. Untuk menunjukkan suatu keterampilan intelektual yakni suatu keterampilan untuk berargumentasi secara rasional dan kritis.
3. Untuk Orientasi etis ini diperlukan dalam mengambil suatu sikap yang wajar dalam suasana pluralisme.

Manfaat Etika

1. Dapat menolong suatu pendirian dalam beragam suatu pandangan dan moral.
2. Dapat membedakan yang mana yang tidak boleh dirubah dan yang mana yang boleh dirubah.
3. Dapat menyelesaikan masalah-masalah moralitas ataupun suatu sosial lainnya yang membingungkan suatu masyarakat dengan suatu pemikiran yang sistematis dan kritis.
4. Dapat menggunakan suatu nalar sebagai dasar pijak bukan dengan suatu perasaan yang bikin merugikan banyak orang. Yaitu Berpikir dan bekerja secara sistematis dan teratur (step by step).
5. Dapat menyelidiki suatu masalah sampai ke akar-akarnya bukan karena sekedar ingin tahu tanpa memperdulikannya.

Macam – Macam Etika

1. Etika Filosofis

Secara harafiah, etika filosofis dapat dianggap sebagai etika yang berasal dari aktivitas berfilsafat atau berpikir yang dilakukan oleh manusia. Oleh karena itu, etika adalah bagian dari filsafat; dimana etika lahir dari filsafat dan ketika berbicara etika tidak dapat dipisahkan dari filsafat itu sendiri. Oleh karena itu, jika kita ingin mengetahui unsur-unsur etika maka kita harus bertanya juga tentang unsur-unsur filsafat.

2. Etika Teologis

Ada dua hal yang perlu diperhatikan berkaitan dengan etika teologis. Pertama, etika teologis tidak terbatas pada agama tertentu, akan tetapi setiap agama dapat memiliki etika teologisnya masing-masing. Kedua, etika teologis merupakan bagian dari etika secara umum, karena banyak unsur di dalamnya yang merupakan bagian dari etika secara umum, dan dapat dipahami seperti memahami etika secara umum.

Perbedaan Etika Dan Etiket

Etiket adalah suatu sikap seperti sopan santun atau aturan lainnya yang mengatur hubungan antara kelompok manusia yang beradab dalam pergaulan.

Tabel 1. Perbedaan Etika dan Etiket

Etika	Etiket
Etika adalah niat, perbuatan boleh atau tidak sesuai pertimbangan niat baik atau buruk sebagai akibatnya.	Etiket adalah cara melakukan perbuatan benar sesuai yang diharapkan
Etika adalah nurani (bathiniyah), sikap etis dan baik yang timbul dari kesadaran diri.	Etiket adalah formalitas (lahiriah), sikap yg tampak sopan dan santun
Etika bersifat absolut, pujian untuk kebaikan sanksi bagi kesalahan.	Etiket bersifat relatif, dianggap tidak sopan pada kebudayaan tertentu
Etika berlakunya tidak tergantung pada ada / tidaknya orang lain yang hadir	Etiket hanya berlaku jika ada orang lain yang hadir dan jika tidak ada orang lain maka etiket itu tidak berlaku di tempat lain.

Contoh Perbedaan Etika dan Etiket

Etiket :

1. Menyangkut cara perbuatan suatu dilakukan, misal ; memberi dan menerima dengan tangan kanan.
2. Berlaku dalam pergaulan, tidak ada orang lain tidak ada etiket
3. bersifat relatif

Etika :

1. Tidak terbatas cara namun norma tentang pelaku itu sendiri, misal ; dengan tangan kanan / kiri bila digunakan untuk mencuri tetap salah.
2. Tidak tergantung pada ada atau tidak adanya orang lain

Persamaan Akhlak, Etika dan Moral

1. Akhlak, etika, dan moral mengacu kepada ajaran atau gambaran tentang perbuatan, tingkah laku, sifat, dan perangai yang baik. Akhlak adalah sifat yang tertanam dalam jiwa yang menimbulkan perbuatan-perbuatan dengan gampang dan mudah tanpa memerlukan pertimbangan dan pemikiran. Sementara moral adalah suatu tindakan yang sesuai dengan ukuran tindakan yang umum diterima oleh kesatuan sosial atau lingkungan tertentu.
2. Akhlak, etika, dan moral merupakan prinsip atau aturan hidup manusia untuk mengukur martabat dan harkat kemanusiaannya. Sebaliknya, semakin rendah kualitas

akhlak, etika, moral seseorang atau sekelompok orang, maka semakin rendah pula kualitas kemanusiaannya.

3. Akhlak, etika, dan moral seseorang atau sekelompok orang tidak semata-mata merupakan faktor keturunan yang bersifat tetap, statis, dan konstan, tetapi merupakan potensi positif yang dimiliki setiap orang. Untuk pengembangan dan aktualisasi potensi positif tersebut diperlukan pendidikan, pembiasaan, dan keteladanan, serta dukungan lingkungan, mulai dari lingkungan keluarga, sekolah, dan masyarakat secara terus-menerus, berkesinambungan, dan dengan tingkat konsistensi yang tinggi.

Perbedaan Akhlak, Etika dan Moral

Berdasarkan Tolak Ukur

- ❖ Akhlak tolak ukurnya Al-qur'an dan As Sunnah
- ❖ Etika tolak ukurnya pikiran atau akal
- ❖ Moral tolak ukurnya norma hidup yang ada di masyarakat berupa adat atau aturan tertentu.

Berdasarkan Sifat

- ❖ Etika bersifat teori
- ❖ Akhlak dan Moral bersifat praktis

1.2 Pendekatan Etika

1. Egoisme

Rachels (2004) memperkenalkan dua konsep yang berhubungan dengan egoisme, yaitu egoisme psikologis dan egoisme etis. Egoisme psikologis adalah suatu teori yang menjelaskan bahwa semua tindakan manusia dimotivasi oleh kepentingan berkebutuhan diri. Egoisme etis adalah tindakan yang dilandasi oleh kepentingan diri sendiri. Yang membedakan tindakan berkebutuhan diri (egoisme psikologis) dengan tindakan untuk kepentingan diri (egoisme etis) adalah pada akibatnya terhadap orang lain. Tindakan berkebutuhan diri ditandai dengan ciri mengabaikan atau merugikan kepentingan orang lain, sedangkan tindakan mementingkan diri tidak selalu merugikan kepentingan orang lain.

2. Utilitarianisme

Utilitarianisme berasal dari kata Latin "*utilis*", kemudian menjadi kata Inggris "*utility*" yang berarti bermanfaat (Bertens, 2000). Menurut teori ini, suatu tindakan dapat dikatakan baik jika membawa manfaat bagi sebanyak mungkin anggota masyarakat, atau dengan istilah yang sangat terkenal "*the greatest happiness of the greatest numbers*". Perbedaan paham utilitarianisme dengan paham egoisme etis terletak pada siapa yang memperoleh manfaat. Egoisme etis melihat dari sudut pandang kepentingan individu, sedangkan paham utilitarianisme melihat dari sudut kepentingan orang banyak (kepentingan bersama, kepentingan masyarakat). Paham utilitarianisme dapat diringkas sebagai berikut :

- a. Tindakan harus dinilai benar atau salah hanya dari konsekuensinya (akibat, tujuan atau hasilnya).
- b. Dalam mengukur akibat dari suatu tindakan, satu-satunya parameter yang penting adalah jumlah kebahagiaan atau jumlah ketidakbahagiaan.
- c. Kesejahteraan setiap orang sama pentingnya.

3. Deontologi

Istilah deontologi berasal dari kata Yunani "*deon*" yang berarti kewajiban. Paham deontologi mengatakan bahwa etis tidaknya suatu tindakan tidak ada kaitannya sama sekali dengan tujuan, konsekuensi atau akibat dari tindakan tersebut. Konsekuensi suatu tindakan tidak boleh menjadi pertimbangan untuk menilai etis atau tidaknya suatu tindakan. Suatu perbuatan tidak pernah menjadi baik karena hasilnya baik. Hasil baik tidak pernah menjadi alasan untuk membenarkan suatu tindakan, melainkan hanya kisah terkenal Robinhood yang merampok kekayaan orang-orang kaya dan hasilnya dibagikan kepada rakyat miskin.

4. Teori Hak

Dalam pemikiran moral dewasa ini barangkali teori hak ini adalah pendekatan yang paling banyak dipakai untuk mengevaluasi baik buruknya suatu perbuatan atau perilaku. Sebetulnya teori hak merupakan suatu aspek dari teori deontologi, karena hak berkaitan dengan kewajiban. Malah bisa dikatakan, hak dan kewajiban bagaikan dua sisi dari uang logam yang sama. Dalam teori etika dulu diberi tekanan terbesar pada kewajiban, tapi sekarang kita mengalami keadaan sebaliknya, karena sekarang segi hak paling banyak ditonjolkan. Walaupun teori hak ini sebetulnya berakar dalam deontologi, namun sekarang ia mendapat suatu identitas tersendiri dan karena itu pantas dibahas tersendiri pula. Hak didasarkan atas martabat manusia dan martabat semua manusia itu sama. Karena itu teori hak sangat cocok dengan suasana pemikiran demokratis. Teori hak sekarang begitu populer, karena dinilai cocok dengan penghargaan terhadap individu yang memiliki harkat tersendiri. Karena itu manusia individual siapapun tidak pernah boleh dikorbankan demi tercapainya suatu tujuan yang lain.

Menurut perumusan termasyur dari Immanuel Kant : yang sudah kita kenal sebagai orang yang meletakkan dasar filosofis untuk deontologi, manusia merupakan suatu tujuan pada dirinya (*an end in itself*). Karena itu manusia selalu harus dihormati sebagai suatu tujuan sendiri dan tidak pernah boleh diperlakukan semata-mata sebagai sarana demi tercapainya suatu tujuan lain.

5. Teori Keutamaan (*Virtue Theory*)

Dalam teori-teori yang dibahas sebelumnya, baik buruknya perilaku manusia dipastikan berdasarkan suatu prinsip atau norma. Dalam konteks utilitarisme, suatu perbuatan adalah baik, jika membawa kesenangan sebesar-besarnya bagi jumlah orang terbanyak. Dalam rangka deontologi, suatu perbuatan adalah baik, jika sesuai dengan prinsip “jangan mencuri”, misalnya. Menurut teori hak, perbuatan adalah baik, jika sesuai dengan hak manusia. Teori-teori ini semua didasarkan atas prinsip (*rule-based*).

Disamping teori-teori ini, mungkin lagi suatu pendekatan lain yang tidak menyoroti perbuatan, tetapi memfokuskan pada seluruh manusia sebagai pelaku moral. Teori tipe terakhir ini adalah teori keutamaan (*virtue*) yang memandang sikap atau akhlak seseorang. Dalam etika dewasa ini terdapat minat khusus untuk teori keutamaan sebagai reaksi atas teori-teori etika sebelumnya yang terlalu berat sebelah dalam mengukur perbuatan dengan prinsip atau norma. Namun demikian, dalam sejarah etika teori keutamaan tidak merupakan sesuatu yang baru. Sebaliknya, teori ini mempunyai suatu tradisi lama yang sudah dimulai pada waktu filsafat Yunani kuno.

Keutamaan bisa didefinisikan sebagai berikut : disposisi watak yang telah diperoleh seseorang dan memungkinkan dia untuk bertingkah laku baik secara moral. Kebijaksanaan, misalnya, merupakan suatu keutamaan yang membuat seseorang mengambil keputusan tepat dalam setiap situasi. Keadilan adalah keutamaan lain yang membuat seseorang selalu memberikan kepada sesama apa yang menjadi haknya. Kerendahan hati adalah keutamaan yang membuat seseorang tidak menonjolkan diri, sekalipun situasi mengizinkan. Suka bekerja keras adalah keutamaan yang membuat seseorang mengatasi kecenderungan spontan untuk bermalas-malasan. Ada banyak keutamaan semacam ini. Seseorang adalah orang yang baik jika memiliki keutamaan. Hidup yang baik adalah hidup menurut keutamaan (*virtuous life*).

Menurut pemikir Yunani (Aristoteles), hidup etis hanya mungkin dalam polis. Manusia adalah “makhluk politik”, dalam arti tidak bisa dilepaskan dari polis atau komunitasnya. Dalam etika bisnis, teori keutamaan belum banyak dimanfaatkan. Solomon membedakan keutamaan untuk pelaku bisnis individual dan keutamaan pada taraf perusahaan. Di samping itu ia berbicara lagi tentang keadilan sebagai keutamaan paling mendasar di bidang bisnis. Diantara keutamaan yang harus menandai pebisnis perorangan bisa disebut : kejujuran, fairness, kepercayaan dan keuletan. Keempat keutamaan ini berkaitan erat satu sama lain dan kadang-kadang malah ada tumpang tindih di antaranya. Kejujuran secara umum diakui sebagai keutamaan pertama dan paling penting yang harus dimiliki pelaku bisnis. Kejujuran menuntut adanya keterbukaan dan kebenaran. Jika mitra bisnis ingin bertanya, pebisnis yang jujur selalu bersedia memberi keterangan. Tetapi suasana keterbukaan itu tidak berarti si pebisnis harus membuka segala kartunya. Sambil berbisnis, sering kita terlibat dalam negosiasi kadang-kadang malah negosiasi yang cukup keras dan posisi sesungguhnya atau titik tolak kita tidak perlu ditelanjangi bagi mitra bisnis. Garis perbatasan antara kejujuran dan ketidakjujuran tidak selalu bisa ditarik dengan tajam.

Ketiga keutamaan lain bisa dibicarakan dengan lebih singkat. Keutamaan kedua adalah *fairness*. *Fairness* adalah kesediaan untuk memberikan apa yang wajar kepada semua orang dan dengan “wajar” dimaksudkan apa yang bisa disetujui oleh semua pihak yang terlibat dalam suatu transaksi. Kasus *insider trading* adalah contoh mengenai cara berbisnis yang tidak fair. Dengan *insider trading* dimaksudkan menjual atau membeli saham berdasarkan informasi “dari dalam” yang tidak tersedia bagi umum. Kepercayaan (*trust*) juga merupakan keutamaan yang penting dalam konteks bisnis. Kepercayaan harus ditempatkan dalam relasi timbal balik. Ada beberapa cara

untuk mengamankan kepercayaan. Salah satu cara adalah memberi garansi atau jaminan. Cara-cara itu bisa menunjang kepercayaan antara pebisnis, tetapi hal itu hanya ada gunanya bila akhirnya kepercayaan melekat pada si pebisnis itu sendiri.

6. Teori Etika Teonom

Sebagaimana dianut oleh semua penganut agama di dunia bahwa ada tujuan akhir yang ingin dicapai umat manusia selain tujuan yang bersifat duniawi, yaitu untuk memperoleh kebahagiaan surgawi. Teori etika teonom dilandasi oleh filsafat Kristen, yang mengatakan bahwa karakter moral manusia ditentukan secara hakiki oleh kesesuaian hubungannya dengan kehendak Allah. Perilaku manusia secara moral dianggap baik jika sepadan dengan kehendak Allah, dan perilaku manusia dianggap tidak baik bila tidak mengikuti aturan/perintah Allah sebagaimana dituangkan dalam kitab suci. Teori Teonom adalah salah satu aliran moral yang meletakkan dasar moralnya pada perintah Allah secara mutlak. Menurut aliran ini Perintah Allah mutlak dijalankan oleh semua orang tanpa pengecualian. Dalam tradisi agama abrahamic ini, Allah sendiri menawarkan suatu hukum yang sifatnya harus ditaati. Pada dasarnya Tuhan tidak memaksa manusia untuk menerima hukum-hukum yang Ia tawarkan, karena manusia diciptakan secara bebas tetapi secara mendasar, teori ini mengajarkan bahwa benar secara moral apabila sesuai dengan perintah Allah, salah secara moral apabila tidak sesuai Allah, dan sifatnya wajib atau mengikat bila diperintahkan Allah.

Sebagaimana teori etika yang memperkenalkan konsep kewajiban tak bersyarat diperlukan untuk mencapai tujuan tertinggi yang bersifat mutlak. Kelemahan teori etika Kant terletak pada pengabaian adanya tujuan mutlak, tujuan tertinggi yang harus dicapai umat manusia, walaupun ia memperkenalkan etika kewajiban mutlak. Moralitas dikatakan bersifat mutlak hanya bila moralitas itu dikatakan dengan tujuan tertinggi umat manusia. Segala sesuatu yang bersifat mutlak tidak dapat diperdebatkan dengan pendekatan rasional karena semua yang bersifat mutlak melampaui tingkat kecerdasan rasional yang dimiliki manusia.

Etika ini terdiri dari dua macam, yaitu Etika Teonom Murni dan Etika Hukum Kodrat. Etika teonom murni mengajarkan bahwa tindakan dikatakan benar (baik) bila sesuai dengan kehendak Allah, dan dikatakan salah (buruk) apabila tidak sesuai dengan kehendak-Nya. Menurut teori ini Allah sama sekali bebas dalam menentukan apa yang harus kita anggap buruk. Tugas manusia dalam hal ini adalah menerima apa yang diajarkan Allah terhadapnya jangan sampai berpikir sendiri karena pikirannya tidak berdaya. Sedangkan etika hukum kodrat mengatakan bahwa baik dan buruk

ditentukan oleh Allah semata-mata. Sesuatu dikatakan benar jika sesuai dengan tujuan manusia atau sesuai dengan kodrat manusia. Thomas Aquinas, salah seorang tokoh teori ini mengatakan bahwa Allah menciptakan manusia karena Allah menghendaki agar manusia ada. Dikatakan bahwa kodrat manusia mencerminkan kehendak Allah Sang Pencipta. Karena itu manusia tinggal bertindak sesuai dengan kodratnya yang baik baginya. Dengan demikian, ia sekaligus memenuhi kehendak Allah.

1.3 Kode Etik dan Tanggung Jawab Profesi

1.3.1 Kode Etik

Kode etik merupakan suatu sistem norma, nilai serta aturan profesional secara tertulis yang dengan tegas menyatakan hal baik dan juga benar, serta apa yang tidak benar dan juga tidak baik bagi profesional. Secara singkat, pengertian kode etik adalah suatu pola aturan, tata cara, tanda, pedoman etis di dalam melakukan suatu kegiatan ataupun suatu pekerjaan. Kode etik berhubungan dengan perilaku seseorang. Pengertian kode etik lainnya adalah suatu aturan yang tertulis, secara sistematis dengan sengaja dibuat, berdasarkan prinsip-prinsip moral yang ada serta ketika dibutuhkan bisa difungsikan sebagai alat yang dapat digunakan menghakimi berbagai macam dari tindakan yang pada umumnya dinilai menyimpang dari kode etik yang ada. Berikut ini terdapat beberapa kode etik menurut para ahli, terdiri atas:

1. Menurut pasal 43 Undang-Undang Nomor 20 Tahun 2003 bahwa kode etik berisi norma dan etika yang mengikat perilaku guru dalam pelaksanaan tugas keprofesionalan.
2. Menurut Sonny Keraf, kode etik merupakan kaidah moral yang berlaku khusus untuk orang-orang profesional dibidang tersebut.
3. Menurut Kode Etik Guru Indonesia (hasil Kongres PGRI Ke-XX tahun 2008), Kode Etik Guru Indonesia adalah norma dan asas dan diterima oleh guru-guru Indonesia, sebagai pedoman sikap dan perilaku dalam melaksanakan tugas profesi sebagai pendidik, anggota masyarakat dan warga negara.
4. Menurut Prof. Dr. R. Soebekti, S.H. dalam tulisannya yang berjudul “Etika Bentuan Hukum”, kode etik suatu profesi berupa norma-norma yang harus diindahkan oleh orang-orang yang menjalankan tugas profesi tersebut.

Dalam pembentukannya, kode etik tentu memiliki tujuan didalamnya yaitu:

1. Agar profesional dapat memberikan jasa dengan sebaik-baiknya kepada para pemakai ataupun para nasabahnya.
2. Sebagai pelindung dari perbuatan yang tidak profesional.

Ketaatan dari tenaga profesional terhadap kode etik yang ada merupakan sebuah ketaatan yang naluriah. Penyelewengan/penyimpangan terhadap norma yang ditetapkan dan diterima oleh sekelompok profesi, yang mengarahkan atau memberi petunjuk kepada anggotanya bagaimana seharusnya berbuat dan sekaligus menjamin mutu profesi itu dimata masyarakat dinamakan pelanggaran terhadap kode etik profesi. Kode etik bagi sebuah profesi adalah sumpah jabatan yang juga diucapkan oleh para pejabat Negara. Kode etik dan sumpah adalah janji yang harus dipegang teguh. Artinya, tidak ada toleransi terhadap siapa pun yang melanggarnya. Berdasarkan pengertian kode etik, dibutuhkan sanksi keras terhadap pelanggar sumpah dan kode etik profesi. Bahkan, apabila memenuhi unsur adanya tindakan pidana atau perdata, selayaknya para pelanggar sumpah dan kode etik itu harus diseret ke pengadilan. Kita memang harus memiliki keberanian untuk lebih bersikap tegas terhadap penyalahgunaan profesi .

Kita pun tidak boleh bersikap diskrimatif dan tebang pilih dalam menegakkan hukum di Indonesia. Kode etik disusun oleh organisasi profesi sehingga masing-masing profesi memiliki kode etik tersendiri. Misalnya kode etik dokter, guru, pustakawan, pengacara, Pelanggaran kode etik tidak diadili oleh pengadilan karena melanggar kode etik tidak selalu berarti melanggar hukum. Kode etik dan sumpah jabatan harus ditegakkan dengan sungguh-sungguh. Profesi apa pun sesungguhnya tidak memiliki kekebalan di bidang hukum. Kita harus mengakhiri praktik-praktik curang dan penuh manipulatif dari sebagian elite masyarakat. Ini penting dilakukan, kalau Indonesia ingin menjadi sebuah Negara dan Bangsa yang bermartabat. Pelanggaran kode etik profesi merupakan pelanggaran yang dilakukan oleh sekelompok profesi yang tidak mencerminkan atau memberi petunjuk kepada anggotanya bagaimana seharusnya berbuat dan sekaligus menjamin mutu profesi itu dimata masyarakat.

Berapa penelitian yang telah dilakukan menyebutkan bahwa, ada pun yang menjadi penyebab mengapa terjadi pelanggaran kode etik yaitu;

1. tidak berjalannya kontrol dan pengawasan dari masyarakat
2. organisasi profesi tidak di lengkapi dengan sarana dan mekanisme bagi masyarakat untuk menyampaikan keluhan

3. rendahnya pengetahuan masyarakat mengenai substansi kode etik profesi, karena buruknya pelayanan sosialisasi dari pihak profesi sendiri
4. belum terbentuknya kultur dan kesadaran dari para pengemban profesi untuk menjaga martabat luhur profesinya
5. tidak adanya kesadaran etis dan moralitas diantara para pengemban profesi untuk menjaga martabat luhur profesinya

Secara umum, ada 2 jenis sanksi yang mungkin diberikan kepada pelanggar kode etik profesi adalah:

- a. Jika kode etik yang dilanggar masih dalam pelanggaran moral, maka sanksi yang diberikan adalah sanksi moral, berupa celaan dari kelompok atau pihak-pihak terkait.
- b. Jika kode etik yang dilanggar telah melewati batas norma moral dan sosial, maka sanksi yang mungkin diberikan adalah sanksi hukum.

1.3.2 Kode Etik Profesi

Etika profesi atau kode etik profesi merupakan acuan perilaku individu atau perusahaan dan dianggap sebagai perilaku yang diikuti oleh peserta dalam kegiatan profesional. Tenaga profesional memiliki pengetahuan dan keahlian khusus, dan secara khusus telah merumuskan kode etik untuk mengelola cara menggunakan pengetahuan dan keterampilan tersebut, terutama pada masalah etika. Biasanya hal ini terkait dengan kemampuan para profesional untuk membuat penilaian dan keputusan. Penilaian dan keputusan ini tidak dapat dilakukan oleh orang biasa tanpa pengetahuan dan keahlian khusus tersebut. Salah satu contoh paling awal dari etika profesional adalah Sumpah Hipokrates, yang masih diikuti oleh para dokter sampai sekarang.

Kode etik profesi muncul dalam bentuk norma, dan setiap anggota profesi harus berpegang pada norma tersebut dalam menjalankan tugas profesional dan kehidupan sosialnya. Norma-norma ini berisi petunjuk tentang bagaimana anggota industri menjalankan profesinya dan larangannya, yaitu peraturan tentang hal-hal yang tidak boleh mereka lakukan atau lakukan, tidak hanya untuk menjalankan tugas profesionalnya, tetapi juga melibatkan perilaku anggota. Secara umum, mereka semua adalah profesional dalam komunikasi sehari-hari di masyarakat. Dalam berkarir, seseorang perlu memiliki landasan yang perlu diperhatikan, antara lain:

- ❖ *Prinsip tanggung jawab.* Profesional harus bisa bertanggung jawab atas dampak profesinya, terutama yang ada di sekitar mereka.
- ❖ *Prinsip keadilan.* Menuntut seseorang untuk dapat menjalankan profesinya tanpa merugikan orang lain, terutama yang berkaitan dengan profesinya.
- ❖ *Prinsip otonomi.* Didasarkan pada kebutuhan untuk memberikan kebebasan penuh kepada para profesional untuk menjalankan profesinya.
- ❖ *Prinsip integritas moral.* Profesional juga harus membuat komitmen pribadi untuk melindungi kepentingan profesional, pribadi dan sosial mereka.

Fungsi dan Tujuan Kode Etik Profesi

Kode etik pada dasarnya memiliki rangkap fungsi, yaitu sebagai pelindung dan pengembangan profesi. Fungsi ini sama dengan yang dikemukakan oleh Gibson dan Michel (1945-449) yang menjadikan kode etik sebagai kode untuk menjalankan tugas profesional, dan menjadikan masyarakat sebagai kode jabatan. Pada dasarnya tujuan dibentuk atau dirumuskannya kode etik profesi adalah untuk kepentingan anggota dan organisasi profesi. Secara umum, tujuan pembentukan kode etik adalah sebagai berikut:

1. Menjaga martabat profesional

Dalam hal ini yang harus dilindungi adalah “citra” orang luar atau masyarakat sehingga “orang luar” itu memandang rendah atau “memandang rendah” profesinya. Oleh karena itu, setiap kode etik profesi akan melarang segala bentuk fitnah profesi terhadap dunia luar. Dari perspektif ini, kode etik juga memiliki namanya atau disebut “kode kehormatan.”

2. Menjaga kesejahteraan anggota

Artinya kesejahteraan berupa kesehatan materi dan mental atau mental. Mengenai kesejahteraan material anggota profesional, kode etik biasanya melarang anggota melakukan perilaku yang merugikan kesejahteraan anggotanya. Misalnya dengan menetapkan remunerasi minimal bagi pelaku industri untuk menjalankan tugasnya, sehingga siapapun yang tarifnya di bawah remunerasi minimum dianggap tercela karena tidak pantas dan tidak menguntungkan sesama pekerjaannya.

Sejauh menyangkut kesehatan mental atau mental anggota profesional, kode etik biasanya mengarahkan anggotanya untuk menjalankan tugas profesionalnya. Selain itu, kode etik juga memberikan batasan kepada anggotanya agar tidak melakukan perilaku yang dianggap tercela oleh masyarakat. Kode Etik juga menetapkan

peraturan yang dirancang untuk membatasi perilaku yang tidak pantas atau tidak jujur pada interaksi anggota industri dengan anggota industri lainnya.

3. Tingkatkan layanan profesional

Dalam hal ini, kode etik juga memuat tujuan pengabdian tertentu, sehingga para profesional dapat dengan mudah memahami tanggung jawab dan tanggung jawab pelayanannya saat menjalankan tugas profesionalnya. Oleh karena itu, Kode Etik menetapkan aturan yang harus diterapkan oleh para profesional dalam menjalankan tugasnya.

4. Tingkatkan kualitas profesional

Dalam rangka meningkatkan kualitas profesional, kode etik juga memuat rekomendasi yang relevan, sehingga anggota profesional senantiasa berupaya untuk meningkatkan kualitas anggotanya sesuai bidang pelayanannya.

Selain itu, kode etik juga mengatur bagaimana menjaga dan meningkatkan kualitas organisasi profesi. Dari uraian di atas, terlihat jelas bahwa tujuan penyusunan kode etik profesi adalah untuk menjaga harkat dan martabat profesi, menjaga dan memelihara kesejahteraan anggota, meningkatkan tingkat pelayanan anggota dan meningkatkan etika profesi. Kualitas profesional dan organisasi profesional yang sempurna.

1.3.3 Pengertian Tanggung Jawab Profesi

Etika mengacu pada suatu sistem atau kode perilaku berdasarkan kewajiban moral yang menunjukkan bagaimana seorang individu berperilaku dalam masyarakat. Rasa terhadap etika mengarahkan individu untuk menilai lebih dari kepentingan diri sendiri dan untuk mengakui maupun menghormati kepentingan orang lain. Perilaku etika juga merupakan fondasi profesionalisme modern. Profesionalisme didefinisikan secara luas, mengacu pada perilaku, tujuan, atau kualitas yang membentuk karakter atau memberi ciri suatu profesi atau orang-orang profesional. Seluruh profesi menyusun aturan atau kode perilaku yang mendefinisikan perilaku etika profesional bagi anggota profesi tersebut. Aturan ini disusun sedemikian rupa sehingga pengguna jasa profesional mengetahui apa yang diharapkan saat mereka memberi jasa tersebut; anggota profesi mengetahui perilaku apa yang dapat diterima; dan profesi dapat menggunakan aturan tersebut untuk mengawasi tindakan anggotanya dan menerapkan *liability* dalam hubungan dengan jasa profesional yang diberikan. Tanggung jawab profesional berdasarkan hukum *legal liability*, diartikan sebagai tanggung jawab

hukum pemberi jasa pengembalian profesi atas jasa yang diberikannya kepada kliennya atau tanggung jawab hukum pengembalian profesi terhadap pihak ketiga. Seorang profesional itu dalam memberikan pelayanannya bertanggung jawab kepada diri sendiri dan kepada masyarakat. Bertanggung jawab kepada diri sendiri artinya dalam bekerja karena integritas moral, intelektual, dan profesional sebagai bagian dari kehidupannya.

Profesional selalu memperhatikan cita-cita luhur profesi sesuai dengan tuntutan kewajiban hati nuraninya. Bertanggung jawab kepada masyarakat artinya kesediaan memberikan pelayanan sebaik mungkin sesuai dengan profesinya, tanpa membedakan antara pelayanan bayaran dan pelayanan cuma-cuma serta menghasilkan layanan yang bermutu yang berdampak positif bagi masyarakat. Pelayanan yang diberikan tidak semata-mata bermotif mencari keuntungan, melainkan juga pengabdian kepada sesama manusia. Bertanggung jawab juga berarti menanggung segala resiko yang timbul akibat pelayanannya itu. Kelalaian dalam melaksanakan profesi menimbulkan dampak yang membahayakan atau merugikan diri sendiri dan orang lain.

Prinsip-prinsip yang menjadi tanggung jawab seorang Profesional, meliputi:

1. Prinsip 1 – *Holistic* (Keseluruhan)

Profesional 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.

Contoh : Seorang Dokter memberikan resep obat yang tepat sesuai dengan dosis yang dianjurkan, demi kesembuhan pasien.

2. Prinsip 2 – *Optimal* (Terbaik)

Profesional selalu memberikan jasa/prakteknya yang terbaik bagi perusahaan.

Contoh : Seorang Dokter selalu mengusahakan semaksimal mungkin untuk kesembuhan pasiennya.

3. Prinsip 3 - *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 berkualitas daripada sebelumnya.

Contoh : Seorang Dokter tetap harus tetap melanjutkan jenjang pendidikannya tanpa mengenal waktu dan usia, guna menambah ilmu pengetahuan serta wawasan agar dapat di implementasikan pada pekerjaannya.

4. Prinsip 4 – Integrity (Kejujuran)

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

Contoh : Seorang Dokter harus jujur terhadap situasi dan kondisi apa pun kepada pasien mau pun pihak keluarga.

5. Prinsip 5 – 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.

Contoh : Seorang Dokter diwajibkan cekatan dalam menangani pasien serta bisa cepat dan tepat dalam mengambil keputusan.

6. Prinsip 6 – Team Work (Kerjasama)

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

Contoh : Seorang Dokter harus bisa bekerja sama dengan dokter lainnya dalam menangani masalah penyakit pada pasien.

7. Prinsip 7 – Innovation (Inovasi)

Profesional selalu berpikir ataupun belajar untuk mengembangkan kreativitasnya agar dapat mengemukakan ide-ide baru sehingga mampu menciptakan peluang peluang yang baru atas jasa/praktek yang diberikannya.

Contoh : Seorang Dokter harus bisa menciptakan ide-ide/gagasan baru dalam menanganin dan mengobati jenis-jenis penyakit yang terbaru.

8. Prinsip 8 – Communication (Komunikasi)

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

Contoh : Seorang Dokter harus bisa menjelaskan kepada pasien secara jelas tentang informasi baik dari jenis penyakit dan juga penanganan yang tepat .

Kedelapan prinsip tersebut dapat disingkat menjadi “HOLISTIC”, yaitu: *Holistic, Optimal, Life long learner, Integrity, Sharp, Team work, Innovation, dan Communication*

BAB 2

PEKERJAAN DAN PROFESI

2.1 Pekerjaan dan Profesi

Masih banyak orang yang tidak memahami dengan baik tentang perbedaan profesi dan pekerjaan. Banyak yang menganggap keduanya merupakan hal yang sama, padahal jika dijabarkan dengan cermat keduanya memiliki perbedaan. Kedua aktivitas tersebut memang dilakukan untuk mendapatkan penghasilan guna bertahan hidup, namun terdapat beberapa unsur yang membuatnya berbeda.

Pekerjaan mengacu pada jenis kegiatan ekonomi yang diusahakan oleh seseorang secara teratur untuk mendapatkan uang. Ketika seseorang melibatkan atau menduduki dirinya sendiri, sebagian besar waktu, dalam aktivitas ekonomi apa pun, aktivitas itu dikenal sebagai pekerjaannya. Contoh : Pengemudi, pemilik toko, pegawai pemerintah, pegawai, akuntan, dll. Suatu pekerjaan tidak selalu membutuhkan sekolah khusus dalam aliran tertentu. Kedua jenis pekerjaan fisik atau mental termasuk dalam pekerjaan. Atau dengan kata lain, pekerjaan adalah kegiatan yang dilakukan oleh orang tersebut untuk mencari nafkah. Ini bisa berupa bisnis, profesi, atau pekerjaan yang dilakukan seseorang untuk menghasilkan uang. Banyak yang berpikir bahwa pekerjaan dan profesi adalah sinonim, tetapi kenyataannya mereka berbeda.

Profesi berasal dari kata bahasa Inggris *profesion* , bahasa latin *professus* yang berartikan mampu atau ahli dalam suatu pekerjaan suatu profesi ialah suatu pekerjaan yang menuntut pendidikan tinggi, biasanya meliputi pekerjaan mental yang ditunjang oleh kepribadian serta sikap profesional. Profesi adalah kegiatan yang membutuhkan pelatihan khusus, pengetahuan, kualifikasi, dan keterampilan. Ini menyiratkan keanggotaan badan profesional, dan sertifikat praktik. Individu yang melakukan profesi memberikan layanan yang dipersonalisasi disebut profesional, yang dipandu oleh kode perilaku tertentu, yang dibentuk oleh badan terkait. Profesi diatur oleh badan atau undang-undang profesional. Untuk disebut sebagai seorang profesional, seseorang harus melanjutkan studi yang lebih tinggi dan memenuhi syarat ujian yang dilakukan oleh badan pengatur. Biasanya, seorang profesional dikatakan ahli di bidangnya. Kode etik dikembangkan oleh badan profesional yang harus diikuti oleh para profesional, untuk memastikan keseragaman dalam pekerjaan mereka. Contoh : Dokter, Insinyur, Pengacara, *Chartered Accountant*, dll. Garis demarkasi antara pekerjaan dan profesi tipis dan kabur. Ketika seorang profesional dibayar untuk keterampilan atau bakatnya, itu dikenal sebagai pekerjaan.

Tabel 2 Perbandingan Pekerjaan dan Profesi

Dasar untuk Perbandingan	Pekerjaan	Profesi
Berarti	Pekerjaan mengacu pada aktivitas rutin yang dilakukan seseorang untuk mendapatkan roti dan mentega.	Profesi adalah pekerjaan atau panggilan yang membutuhkan tingkat pengetahuan dan keahlian tinggi dalam bidang tertentu.
Kode etik	Tidak	Ya
Latihan	Tidak perlu	Wajib
Diatur oleh undang-undang	Tidak	Ya
Dasar pembayaran	Menghasilkan	Keterampilan dan Pengetahuan
Pendidikan yang lebih tinggi	Tidak	Ya
Tingkat kemandirian	Tidak ada independensi.	Seorang profesional sepenuhnya independen.
Tanggung jawab	Tidak	Ya
Penghargaan dan Status	Rendah	Sangat tinggi

Terdapat beberapa karakteristik khusus yang membedakan profesi dengan pekerjaan

a. Ujian kompetensi

Sebelum memiliki profesi, terdapat persyaratan khusus yang harus dipenuhi, yaitu lulus dalam uji kompetensi. Melalui tes tersebut, bisa disimpulkan apakah orang tersebut telah mampu menjalankan profesi dalam bidang tertentu atau tidak.

b. Kode etik

Profesi memiliki kode etik yang harus dipatuhi oleh semua orang yang menjalankannya, jika melanggar maka akan dikenakan sanksi yang sesuai dengan ketentuan.

c. Ketrampilan

Profesi memiliki pengetahuan teoritis dan juga ekstensif yang harus dipahami dengan baik sehingga mampu diterapkan dengan tepat. Untuk dapat menguasainya tentu dibutuhkan pelatihan serta pemahaman khusus dengan cara praktik. Tak heran jika seorang profesi harus berpendidikan tinggi.

d. Kebanyakan memberikan layanan publik

Biasanya profesi akan memberikan pelayanan kepada publik, contohnya adalah dokter yang berkontribusi khusus dalam kesehatan masyarakat secara luas. Penghasilan serta profesi dokter akan terus bertahan selama publik mempercayainya.

e. Lisensi

Untuk mendapatkan profesi, Anda harus memiliki lisensi resmi atau sertifikat yang menyatakan tentang keahlian khusus yang dimiliki.

f. Pelatihan khusus

Selain harus lulus ujian, Anda juga harus mengikuti pelatihan khusus untuk bisa mendapatkan profesi. Ini merupakan persyaratan mutlak yang harus dipenuhi oleh setiap orang yang ingin memiliki profesi. Dengan adanya pelatihan khusus, maka Anda bisa mendapatkan pendalaman materi dan juga pengalaman yang akan berguna untuk mengembangkan keterampilan yang dipelajari.

g. Otonomi kerja

Profesi bekerja secara profesional sehingga biasanya akan mengandalkan pengetahuan teoritis untuk melakukan sesuatu. Dengan begitu seseorang bisa lebih berfokus pada ilmu yang dikuasainya dan tidak mudah terganggu dengan lingkungan luar.

h. Asosiasi profesional

Dalam profesi, biasanya terdapat organisasi atau perkumpulan yang dikelola khusus untuk dapat meningkatkan status para anggotanya. Untuk bergabung dalam organisasi tersebut, Anda harus memiliki keterampilan yang sesuai dan memenuhi syarat.

Profesi dan Profesional

Profesional adalah seseorang yang menawarkan jasa atau layanan sesuai dengan protokol dan peraturan dalam bidang yang dijalannya dan menerima gaji sebagai upah atas jasanya. Seseorang yang merupakan ahli dalam suatu bidang juga bisa disebut “profesional” dalam bidangnya walaupun bukan merupakan anggota sebuah organisasi yang didirikan dengan sah. Orang yang profesional menurut Kahlil Gibran adalah orang yang mencintai profesinya. Dengan mencintai profesinya, orang akan terpacu untuk terus mengembangkan kemampuan yang mendukung profesi tersebut. Seorang profesional harus memiliki sikap seperti: komitmen, tanggung jawab, berpikir sistematis, penguasaan materi, dan menjadi bagian dari masyarakat profesional. Secara teoritis menurut Gilley dan Egglan (1989), standar pengertian profesional dapat didekati dengan empat perspektif pendekatan, yaitu:

a. Pendekatan berorientasi filosofis

Pendekatan orientasi filosofi ini melihat tiga hal pokok yang dapat digunakan untuk mengetahui tingkat profesionalisme sebagai berikut:

1. Pendekatan Lambang Profesional

Lambang profesional yang dimaksud antara lain seperti sertifikat, lisensi, dan

akreditasi. Sertifikasi merupakan lambang bagi individu yang profesional dalam bidang tertentu. Misalnya, seseorang yang ahli dalam menjalankan suatu program komputer tertentu berhasil melalui ujian lembaga sertifikasi tersebut sehingga akan mendapatkan sertifikat berstandar internasional. Adapun lisensi dan akreditasi merupakan lambang profesional untuk produk ataupun institusi. Sebagai contoh, lembaga pendidikan yang telah dianggap profesional oleh umum adalah lembaga pendidikan yang telah memiliki status terakreditasi, dan lain-lain. Akan tetapi, penggunaan lambang ini kurang diminati karena berkaitan dengan aturan-aturan formal.

2. Pendekatan Sikap Individu

Pendekatan ini melihat bahwa layanan individu pemegang profesi diakui oleh umum dan bermanfaat bagi penggunanya. Sikap individu tersebut antara lain adalah kebebasan personal, pelayanan umum, pengembangan sikap individual dan aturan-aturan yang bersifat pribadi. Orang akan melihat bahwa individu yang profesional adalah individu yang memberikan layanan yang memuaskan dan bermanfaat bagi pengguna jasa profesi tersebut.

3. Pendekatan Electic

Pendekatan ini melihat bahwa proses profesional dianggap sebagai kesatuan dari kemampuan, hasil kesepakatan dan standar tertentu. Hal ini berarti bahwa pandangan individu tidak akan lebih baik dari pandangan kolektif yang disepakati bersama. Pendekatan electic ini merupakan pendekatan yang menggunakan prosedur, teknik, metode dan konsep dari berbagai sumber, sistem, dan pemikiran akademis. Dengan kesatuan item-item tersebut di atas, masyarakat akan melihat kualitas profesionalisme yang dimiliki oleh seseorang individu ataupun yang mewakili institusi.

b. Pendekatan berorientasi perkembangan

Orientasi perkembangan menekankan pada enam langkah dalam proses berikut:

1. Berkumpulnya individu-individu yang memiliki minat yang sama terhadap suatu profesi.
2. Melakukan identifikasi dan adopsi terhadap ilmu pengetahuan tertentu untuk mendukung profesi yang dijalannya. Hal ini tentu saja disesuaikan dengan latar belakang akademis para pelaku profesi tersebut.
3. Setelah individu-individu yang memiliki minat yang sama berkumpul, selanjutnya para praktisi akan terorganisasi secara formal pada suatu lembaga yang diakui oleh pemerintah dan masyarakat sebagai sebuah organisasi profesi.

4. Membuat kesepakatan mengenai persyaratan profesi berdasarkan pengalaman atau kualifikasi tertentu. Hal ini sesuai dengan hakikat sebuah profesi, yang mengharuskan pelakunya memiliki pengetahuan tertentu yang diperoleh melalui pendidikan formal dan atau ketrampilan tertentu yang didapat melalui pengalaman kerja pada orang yang terlebih dahulu menguasai ketrampilan tersebut.
5. Menentukan kode etik profesi yang menjadi aturan main dalam menjalankan sebuah profesi yang harus ditaati oleh semua anggota profesi yang bersangkutan.
6. Revisi persyaratan berdasarkan kualifikasi tertentu seperti syarat akademis dan pengalaman melakukan pekerjaan di lapangan. Hal ini berkembang sesuai tuntutan tingkat pelayanan yang diberikan kepada para pengguna jasa profesi tersebut.

c. Pendekatan berorientasi karakteristik

Orientasi ini melihat bahwa proses profesional juga dapat ditinjau dari karakteristik profesi/pekerjaan. Ada delapan karakteristik pengembangan proses profesional yang saling terkait, yaitu: kode etik profesi yang merupakan aturan main dalam menjalankan sebuah profesi, pengetahuan yang terorganisir yang mendukung pelaksanaan sebuah profesi, keahlian dan kompetensi yang bersifat khusus, tingkat pendidikan minimal dari sebuah profesi, sertifikasi keahlian yang harus dimiliki sebagai salah satu lambang profesional, proses tertentu sebelum memangku profesi untuk bisa memikul tugas dan tanggung jawab dengan baik. Proses tersebut misalnya adalah riwayat pekerjaan, pendidikan atau ujian yang dilakukan sebelum memangku sebuah profesi, adanya kesempatan untuk menyebarluaskan dan bertukar ide diantara anggota, dan adanya tindakan disiplin dan batasan tertentu jika terjadi malapraktik dan pelanggaran kode etik profesi.

d. Pendekatan berorientasi non-tradisional

Pendekatan orientasi non-tradisional menyatakan bahwa seseorang dengan bidang 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, dan sebagainya.

2.2 Profesi Kerja di Bidang Teknologi Informasi

Mungkin kita mengetahui bahwa tidak semua pekerjaan yang ada di dunia ini merupakan sebuah profesi, dimana sebuah pekerjaan akan menjadi sebuah profesi ketika di pekerjaan tersebut seorang pekerja menuangkan keahlian khusus yang hanya

dimiliki orang tertentu saja, maka sebelum mengetahui apakah pekerjaan yang dijalankan merupakan sebuah profesi harus diuji terlebih dahulu, begitu pula dengan bidang teknologi informasi, karena tidak semua orang yang bekerja dan bersentuhan dengan dunia teknologi informasi dapat dikatakan sebagai profesi kerja bidang teknologi informasi.

Contoh sebuah pekerjaan yang bersentuhan dengan bidang TI tapi bukan merupakan profesi adalah operator komputer (menggunakan komputer hanya untuk urusan administrasi), saat ini kalau hanya menjadi operator komputer saja tidak perlu menggunakan orang yang mahir dibidang komputer, karena setiap individu sudah sangat terbiasa menggunakan komputer, dan bisa menjadi operator komputer, tentu hal ini berbeda dengan beberapa bidang pekerjaan yang membutuhkan *skill* dan kemampuan tinggi didunia teknologi informasi, misalnya *software developer*, atau *software engenieer* yang mana kedua profesi ini membutuhkan pengetahuan khusus di bidang teknologi informasi untuk menjalankan profesinya.

Jenis profesi di bidang teknologi informasi sangatlah beragam, hal ini dikarenakan bidang teknologi informasi selalu berkembang seiring dengan perkembangan zaman, semakin berkembang dunia teknologi informasi maka semakin beragam pula profesi di bidang teknologi informasi bahkan ada pula yang menyebutkan bahwa profesi berkembang menyesuaikan dengan skala bisnis dan kebutuhan pasar. Berikut ini adalah penggolongan pekerjaan bidang teknologi informasi yang berkembang saat ini yaitu :

a. Pekerja yang bergelut dengan perangkat lunak (*Software*)

Pekerja yang bergelut dengan perangkat lunak akan terbagi menjadi beberapa bagian, misalnya, merancang sistem operasi, basis data (*database*), ataupun dalam pengembangan aplikasi, contoh pekerja professional yang ada pada kategori ini yaitu :

1. *System Analyst* adalah professional bidang IT yang pekerjaannya menganalisa sistem yang akan diimplementasikan, mulai dari menganalisa sistem yang ada, tentang kelebihan dan kekurangannya, hingga studi kelayakan dan desain sistem yang akan dikembangkan. Analisis Sistem ini memegang peranan yang sangat penting di dalam suatu proses pengembangan sistem. Seorang analis sistem harus mampu mempunyai setidaknya sebanyak 4 macam keahlian, seperti :

- a. Analisis
 - b. Teknis
 - c. Manajerial
 - d. Interpersonal (mampu berkomunikasi dengan orang lain)
2. *Web designer* adalah professional bidang IT yang pekerjaannya melakukan kegiatan perencanaan, termasuk studi kelayakan, analisis dan desain terhadap suatu proyek pembuatan aplikasi berbasis web.
 3. *Programmer* adalah professional bidang IT yang pekerjaannya mengimplementasikan rancangan sistem analisis yaitu membuat program (baik aplikasi maupun sistem operasi) sesuai sistem yang dianalisa sebelumnya. 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. Sementara itu, Programmer sistem, menulis suatu program yang memang 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.
 4. *Web Programmer* memiliki tugas untuk mengimplementasikan rancangan *web designer*, dengan membuat program berbasis web sesuai dengan desain yang dirancang. Seorang Web Programmer akan mencoba untuk membangun sebuah website dengan melalui bahasa pemrograman seperti Ruby on Rails, PHP, .NET, Java dengan program Sublim, JS, dan lain sebagainya.
- b. Pekerja yang bergelut di dunia perangkat keras (*hardware*)
- Dalam dunia komputer, selain mengenal perangkat lunak tentunya dikenal pula perangkat keras, maka dari itu ada pula profesi yang berkaitan dengan perangkat keras diantaranya yaitu:
1. *Technical engineer*, yang kerap dipanggil teknisi yaitu professional IT yang berkecimpung dalam bidang teknik baik mengenai pemeliharaan maupun perbaikan perangkat sistem komputer. Seorang teknisi bekerja dalam *quality control* yang mana mereka akan mencoba untuk memeriksa setiap peralatan, melakukan ujicoba dan mengumpulkan suatu data. Sementara itu, apabila dalam bidang manufaktur itu sendiri, mereka bisa membantu merancang dan mengembangkan suatu teknologi baru.

2. *Networking Engineer*, merupakan professional IT yang berkecimpung dibidang teknis jaringan komputer dari *maintenance* sampai pada *troubleshooting*-nya. Jenis pekerjaan ini sendiri meliputi :

- a. Monitoring jaringan (memantau)
- b. Menguji jaringan
- c. Menginstal dan menerapkan program keamanan jaringan
- d. Mengevaluasi implementasi jaringan

Orang yang berkecimpung dalam pekerjaan yang seperti ini biasanya memiliki sertifikat seperti Cisco.

c. Pekerja yang bergelut dengan dunia sistem operasi (*operating system*)

Dimana pekerja jenis ini merupakan pekerja profesional yang mengurus operasional sistem operasi, adapun beberapa contoh profesinya yaitu:

1. *MIS Director* merupakan professional IT yang memiliki wewenang tertinggi dalam sebuah rantai sistem informasi. Dengan posisinya ia melakukan manajemen terhadap sistem tersebut secara keseluruhan baik *hardware*, *software* maupun sumberdaya manusianya.
2. *EDP Operator* adalah professional IT yang bertugas mengoperasikan program-program yang berhubungan dengan *electronic data processing* di perusahaan atau organisasi lainnya. 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.
3. *System Administrator* merupakan professional IT yang 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. 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.

d. Pekerja yang bergelut dengan dunia sektor industri teknologi informasi

1. *IT Business Development* dengan jenis pekerjaan yang diidentifikasi oleh pengelompokan kerja diberbagai sektor industri teknologi informasi. *Business Development* bertanggung jawab dalam menyusun target dan strategi jangka panjang organisasi, membangun hubungan dengan pelanggan, mengidentifikasi

peluang bisnis, melakukan negosiasi bisnis, serta memonitor perkembangan pasar.

2.3 Kompetensi Kerja di Bidang Teknologi Informasi

Beberapa profesi yang disebutkan dan diklasifikasikan di atas tentunya memiliki kemampuan dan keahlian yang sangat tinggi untuk memenuhi kebutuhan profesinya, dimana kemampuan ini didapat tidak hanya dari bangku perkuliahan saja melainkan juga dari pengalaman dan pembelajaran yang matang, dan untuk mendukung profesi yang melekat pada dirinya maka dari itu seorang pekerja profesional bidang teknologi informasi wajib memiliki kompetensi yang mumpuni, adapun beberapa kompetensi yang wajib dimiliki seseorang yang memiliki profesi bidang teknologi informasi adalah sebagai berikut :

a. **Kompetensi Pendukung Solusi Teknologi Informasi**

Kompetensi ini merupakan salah satu kompetensi yang wajib dimiliki seseorang yang berprofesi di bidang teknologi informasi, dimana setiap orang yang tidak mengerti bidang TI ataupun memiliki masalah di bidang TI dapat bertanya, ataupun meminta bantuan kepada orang yang memiliki profesi bidang IT, contohnya misalnya terdapat perusahaan ataupun perorangan yang membutuhkan sebuah aplikasi untuk memecahkan masalah yang terdapat dikantornya, maka seseorang yang memiliki kemampuan bidang TI misalnya programmer dapat memberikan solusi, yaitu dengan membuat sebuah aplikasi komputer yang mampu memberikan solusi kepada perusahaan tersebut, begitu pula dengan permasalahan permasalahan umum yang terkait dengan bidang teknologi informasi, misalnya instalasi OS, perakitan komputer, konfigurasi jaringan, ataupun hanya sekedar membersihkan virus, intinya adalah setiap orang yang bergelut ataupun memiliki profesi bidang TI wajib bisa memberikan solusi kepada masyarakat yang memiliki permasalahan permasalahan dibidang teknologi informasi.

b. **Ketrampilan Pengguna Teknologi Informasi**

Selain memberikan pendukung solusi seorang yang memiliki profesi ataupun kemampuan dibidang teknologi informasi wajib pula memiliki kompetensi menggunakan perangkat perangkat teknologi informasi, misalnya pengetahuan pengetahuan mengenai perangkat keras, memahami organisasi arsitektur jaringan, memahami penggunaan alat alat teknologi informasi, baik perangkat perangkat komputer standar, maupun perangkat jaringan yang sangat banyak jenisnya,

minimal bisa mengoperasikannya, begitu pula dengan perangkat perangkat telekomunikasi, banyak orang yang bisa menggunakan perangkat telekomunikasi, namun hanya orang yang memiliki pengetahuan dunia teknologi informasi yang tinggi yang dapat mengetahui secara lebih detail dan keseluruhan mengenai perangkat telekomunikasi tersebut, dan yang terbaru saat ini adalah muncul bisnis diinternet, bisnis internet sangat berkembang pesat saat ini, tentunya siapa yang wajib menguasainya? Yang wajib adalah orang yang faham benar dengan dunia teknologi informasi, yaitu mereka yang memiliki profesi di dunia teknologi informasi.

c. Pengetahuan bidang Teknologi Informasi

Selain bisa memberikan solusi, dan dapat mempergunakan perangkat perangkat teknologi informasi, seseorang yang berprofesi didunia teknologi informasi wajib selalu *mengupgrade* pengetahuannya, hal ini dikarenakan teknologi informasi adalah bidang ilmu yang sangat berkembang, dan perkembangannya sangatlah pesat, untuk orang yang berprofesi dibidang teknologi informasi apabila tidak menambah dan mengikuti perkembangan baru maka akan sangat ketinggalan, dan tentunya dengan menambah pengetahuan bidang teknologi informasi maka akan mendukung dua keterampilan yang telah dijelaskan sebelumnya.

Model SEARCC (South East Asia Regional Computer Confederation)

SEARCC merupakan sebuah forum atau badan yang beranggotakan Profesional IT yang terdiri dari 13 negara, dimana forum ini didirikan pada di Singapura oleh 6 ikatan komputer dari Hongkong, Indonesia, Malaysia, Filipina, Singapura dan Thailand. Indonesia sebagai anggota SEARCC telah aktif turut serta dalam berbagai kegiatan yang dilaksanakan oleh forum tersebut, salah satunya adalah SRIG-PS (*Spesial Regional Interest Group on Professional Standardisation*) yang mencoba untuk merumuskan standarisasi pekerjaan dalam dunia teknologi informasi, dimana dalam kegiatan ini dibuatlah sebuah model yang mengatur tentang profesi IT, dan disebut dengan model SEARCC. Model ini merupakan model 2 dimensi yang mempertimbangkan jenis pekerjaan dan tingkat keahlian maupun tingkat pengetahuan yang dibutuhkan. Beberapa kriteria yang menjadi pertimbangan dalam model ini adalah sebagai berikut:

1. *Cross Country, Cross – Enterprise Applicability*

Ini berarti bahwa pekerjaan yang diidentifikasi tersebut harus relevan atau sesuai dengan kondisi di setiap Negara atau pada region tersebut, serta memiliki pemahaman atas setiap fungsi pekerjaan

2. *Function Oriented* bukan *title oriented*

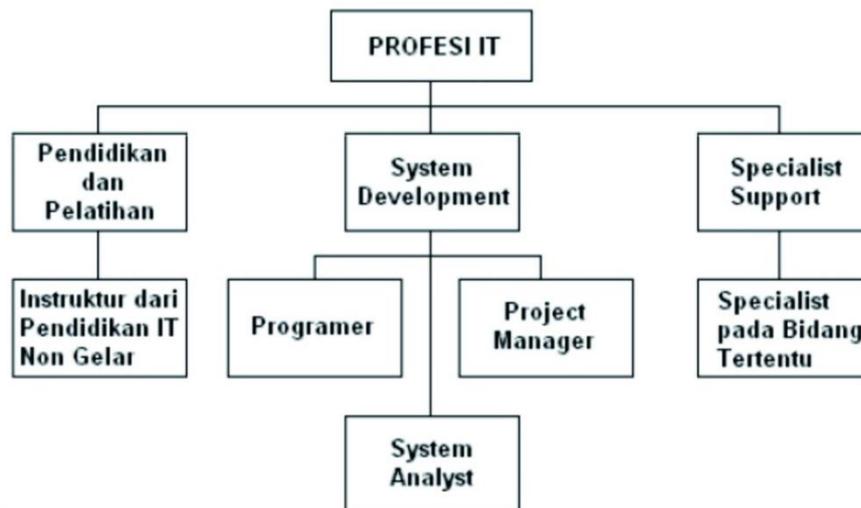
Klasifikasi pekerjaan yang diberikan dapat berorientasi pada fungsi, yang berarti bahwa gelar atau title saja berbeda, tapi yang penting adalah fungsi yang diberikan pada pekerjaan tersebut sama, gelar atau title dapat berbeda berbeda.

3. *Testable / certifiable*

Fungsi yang didefinisikan ini bisa diuji atau diukur

4. *Applicable*

Fungsi yang didefinisikan harus dapat diterapkan pada region masing masing



Gambar 1. Model SEARCC Pembagian Kerja di bidang Teknologi Informasi

Adapun penjelasan dari masing masing jenis pekerjaan atau profesinya adalah sebagai berikut:

a. Instruktur Dari Pendidikan IT Non Gelar

Merupakan seorang pengajar atau intruktur yang memiliki kompetensi dan tanggung jawab proses belajar mengajar atau melatih dibidang teknologi informasi, yang mana seorang instruktur IT harus memiliki kombinasi kemampuan menguasai pengetahuan tentang software dan hardware yang menjadi tanggung jawabnya, contoh dari profesi bidang ini adalah guru guru kursus, yang mana guru guru ini khusus mengajarkan teknologi informasi kepada peserta didiknya, dan guru inipun wajib memiliki kemampuan yang mumpuni

dibidang teknologi informasi.

b. *System Developer*

System developer atau yang biasa disebut dengan pengembang sistem biasanya merupakan sebuah tim, namun tidak menutup kemungkinan juga dikerjakan oleh satu orang, dan dari bidang keahlian ini terbagi lagi menjadi beberapa keahlian yaitu:

1. *Programmer*

Programmer adalah sebutan untuk seorang pengembang perangkat lunak (*software*) yang mana tugasnya adalah menulis kode kode program dan menciptakan sebuah perangkat lunak, istilah programmer sendiri mengacu pada suatu spesialis area *computer programming*. Praktisi programming biasanya dikenal pula dengan istilah analis programmer, insinyur perangkat lunakm ilmuwan komputer, atau analis perangkat lunak, beberapa bahasa pemrograman yang biasanya dikuasi oleh seorang programmer adalah (Java, C++, PHP dll).

2. *System Analyst*

Seperti yang kita ketahui diatas seorang *programmer* adalah orang yang menulis kode- kode program, namun sebelum kode itu ditulis tentunya dibutuhkan seseorang yang memahami alur dari aplikasi yang akan dibuat, menganalisa sistem yang sedang berjalan dan merancangnya dalam bentuk bentuk desain, disinilah peran dari seorang sistem analis.

3. *Project Manager*

Manager proyek harus memiliki suatu kombinasi keterampilan yang mencakup suatu kemampuan untuk menembus suatu pertanyaan dan mendeteksi asumsi, seorang manager proyek biasanya telah memiliki sertifikasi yang berkaitan dengan profesinya, seperti *Certifies Project Manager (CPM)* dan *Project Management Professional (PMP)* untuk mendukung profesinya.

c. *Specialist Support*

1. Spesialisasi Bidang Sistem Operasi dan *Networking*

System engineering yaitu adalah orang yang melakukan perencanaan sebuah perencanaan, mulai dari menciptakan dan melaksanakan proses untuk memastikan bahwa perencanaan tersebut berkualitas tinggi, terpercaya, efisiensi biaya dan terjadwa. Lalu ada pula *System Administrator* (admin,

administrator, sysadmin, site admin) yaitu profesi yang memiliki tugas untuk 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.

2. Spesialisasi dalam pengembangan aplikasi dan database

Dari sisi ini ada dua profesi yaitu *Application developer*, seperti yang sudah kita bahas pada bagian sebelumnya, dan adapula *database administrator* atau administrasi basis data yaitu orang yang bertanggung jawab terhadap keseluruhan basis data yang ada di dalam sebuah organisasi, mulai dari merancang, mengimplementasikan, merawat hingga memperbaiki kesalahan yang ada di dalam basis data.

3. Spesialisasi dalam audit dan keamanan sistem informasi

Ada dua profesi pada bidang ini yaitu *information system audit* dan *information security manager*.

2.4 Sertifikasi di Bidang Teknologi Informasi

Isu sertifikasi menjadi sangat hangat dibicarakan oleh berbagai kalangan khususnya pihak-pihak yang terlibat dalam proses pembinaan profesi baik pendidikan, kesehatan, keuangan, pemerintahan dan kemasyarakatan. Isu sertifikasi menjadi salah satu cara yang digunakan dalam membangun struktur karir profesional dan pengembangan kualitas atau mutu. Seperti sertifikasi untuk ISO 31000 untuk Risk Management Standard, ISO 26000 untuk Social Responsibility, Standar “Chain Of Custody”, Standar ISO 9001, Standar ISO 14001, Standar *Sustainable Forest Management* dan masih banyak lagi.

Badan Nasional Sertifikasi Profesi (BNSP)

Badan Nasional Sertifikasi Profesi (BNSP) dibentuk berdasarkan Peraturan Pemerintah Nomor 23 tahun 2004 atas perintah UU Nomor 13 tahun 2003, tentang Badan Nasional Sertifikasi Profesi, utamanya pasal 4 Ayat 1) : Guna terlaksananya tugas sertifikasi kompetensi kerja sebagaimana dimaksud dalam Pasal 3, BNSP dapat memberikan lisensi kepada lembaga sertifikasi profesi yang memenuhi persyaratan yang ditetapkan untuk melaksanakan sertifikasi kompetensi kerja. Ayat 2): *Ketentuan mengenai persyaratan dan tata cara pemberian lisensi lembaga sertifikasi profesi sebagaimana dimaksud dalam ayat 1) ditetapkan lebih lanjut oleh BNSP*. BNSP merupakan badan independen yang bertanggung jawab kepada Presiden yang memiliki

kewenangan sebagai otoritas sertifikasi personil dan bertugas melaksanakan sertifikasi kompetensi profesi bagi tenaga kerja. Pembentukan BNSP merupakan bagian integral dari pengembangan paradigma baru dalam sistem penyiapan tenaga kerja yang berkualitas.

Sertifikasi Bidang Teknologi Informasi

a. Sertifikasi Microsoft

Pada kategori nonteknis terdapat dua tingkatan sertifikasi, yaitu MOS (Microsoft Office Specialist) dan MOS Expert. Pemegang MOS menunjukkan bahwa dia memiliki keahlian atau keterampilan dalam menggunakan salah satu atau beberapa aplikasi yang tergabung ke dalam paket MicrosoftOffice, misalnya Word, Excel, atau PowerPoint. Sementara pemegang MOS Expert menunjukkan bahwa seseorang benar-benar menguasai secara mendalam salah satu atau beberapa aplikasi yang tergabung pada Microsoft Office.

Untuk kategori teknis, ada beberapa bidang yang dicakup oleh sertifikasi Microsoft, yaitu Mobility, Cloud Platform & Infrastructure, Productivity, Data Management & Analysis, dan App Builder. Meskipun mencakup bidang yang luas, pada dasarnya hanya ada empat macam sertifikasi untuk kategori teknis, yaitu MTA, MCSA, MCSE, dan MCSD.

b. Sertifikasi Cisco

Sertifikasi yang disediakan oleh Cisco meliputi delapan bidang, yaitu Routing and Switching, Design, Network Security, Service Provider, Service Provider Operations, Storage Networking, Voice, dan Wireless. Sementara tingkatannya meliputi empat tingkat, yakni Entry, Associate, Professional, serta Expert and Architect. Adapun nama-nama sertifikasi yang disediakan oleh Cisco adalah CCENT, CCNA, CCDA, dan CCNP R&S.

c. Sertifikasi CompTIA

Sertifikasi CompTIA ini dikeluarkan oleh sebuah lembaga independen. CompTIA menawarkan setidaknya empat tingkatan sertifikasi. Sertifikasi tingkat pertama atau tingkat dasar adalah CompTIA IT Fundamentals yang menyatakan bahwa pemegangnya memahami konsep, literasi, dan terminologi dasar TI. Sertifikasi tingkat kedua atau tingkat profesional adalah CompTIA A+. Pemegang sertifikasi ini memiliki kompetensi sebagai teknisi komputer yang memahami berbagai teknologi dan sistem operasi. Selain A+, ada lagi beberapa

sertifikasi tingkat kedua yang disediakan oleh CompTIA, yaitu Cloud Essentials dan Cloud+ yang menyatakan keahlian di bidang *cloud*, Cybersecurity Analyst (CSA+) yang menyatakan keahlian terhadap keamanan jaringan, Network+ dan Security+ yang masih berhubungan dengan jaringan, Linux+ yang menyatakan keahlian terhadap sistem operasi GNU/Linux, serta Server+ yang menunjukkan keahlian terhadap perangkat keras dan sistem operasi yang berhubungan dengan server.

Sertifikasi tingkat ketiga atau tingkat master adalah CASP (CompTIA Advanced Security Practitioner) yang merupakan sertifikasi lanjutan untuk Network+. Yang terakhir adalah sertifikasi spesial, yaitu sertifikasi yang berhubungan dengan bidang teknologi tertentu secara spesifik. Sertifikasi yang tersedia pada kategori ini adalah Certified Document Imaging Architect (CDIA+) yang menyatakan kompetensi terhadap manajemen dokumen dan pencitraan dokumen (*document imaging*), Certified Technical Trainer (CTT+) yang menyatakan kompetensi terhadap kemampuan memberikan pelatihan di bidang TI, dan Healthcare IT Technician yang menyatakan kompetensi terhadap teknisi peralatan TI di industri kesehatan.

d. Beberapa Sertifikasi Lain

1. RHCE (Red Hat Certified Engineer), sesuai namanya, sertifikasi ini dikeluarkan oleh Red Hat, salah satu distribusi Linux terkemuka. Sertifikasi ini memilikitingkatan menengah ke atas dan mencakup topik jaringan, khususnya dalam hal keamanan, menggunakan Red Hat sebagai perangkat utama.
2. Sertifikasi Java yang dikeluarkan oleh Oracle. Sertifikasi tersebut menyatakan kompetensiterhadap kemampuan pemrograman menggunakan bahasa Java.
3. Mikrotik Certified Network Associate (MTCNA) dan Mikrotik Certified Wireless Engineer (MTCWE). Kedua sertifikasi ini menyatakan kompetensi terhadap kemampuan penanganan jaringan. Sertifikasi ini mirip seperti yang dikeluarkan oleh Cisco, hanya saja vendornya adalah Mikrotik.

2.5 Lembaga dan Organisasi Profesi Teknologi Informasi

Organisasi profesi merupakan organisasi yang anggotanya adalah para praktisi yang menetapkan diri mereka sebagai profesi dan bergabung bersama untuk melaksanakan fungsi-fungsi sosial yang tidak dapat mereka laksanakan dalam kapasitas mereka sebagai individu. Contoh dari organisasi profesi diantaranya:

1. **ACM (*Association for Computing Machinery*)**

Organisasi ini adalah serikat ilmiah dan pendidikan computer yang didirikan pada tahun 1947. Anggotanya pernah sebanyak 78 ribu yang terdiri dari para profesional dan para pelajar yang tertarik dengan teknologi computer. Kantor pusatnya ada di kota New York Amerika Serikat. Secara umum ACM mensponsori konferensi yang bertujuan untuk memperkenalkan inovasi baru dalam bidang tertentu. ACM pernah mensponsori pertandingan catur antara Garry Kasparov dan computer IBM Deep Blue.

2. **IEEE (*Institute of Electrical and Electronics Engineers*)**

Merupakan organisasi internasional yang anggotanya adalah para insinyur dengan tujuan untuk mengembangkan teknologi. Peran dari organisasi ini adalah mengembangkan standar-standar dan ikut serta dalam usaha mempercepat teknologi-teknologi baru dalam aspek dalam bidang industry dan engineering yang meliputi telekomunikasi, jaringan computer, kerlistrikan, antariksa dan elektronika. IEEE di Indonesia dikenal dengan IEEE Indonesia Section yang berada pada IEEE Region 10 (Asia Pasifik). IEEE Indonesia Section memiliki beberapa chapter, diantaranya:

- a. *Communication Society Chapter*
- b. *Circuits and Systems Society Chapter*
- c. *Engineering in Medicine and Biology Chapter*
- d. *Joint Chapter of Education Society, Electron Devices Society, Power Electronics Society, Signal Processing Society.*
- e. *Joint Chapter MTT/AP-S*

3. ***South East Asia Regional Computer Confederation (SEARCC)***

Merupakan himpunan profesional IT di Asia Tenggara. Dibentuk pada bulan Februari tahun 1978 di Negara Singapore, oleh enam ikatan computer dari Negara Hong Kong, Indonesia, Malaysia, Philipina, Singapore dan Thailand. SEARCC mengadakan konferensi dua kali dalam setahun di tiap anggotanya secara bergilir. Salah satu kegiatannya adalah SRIG-PS (*Special Regional Interest Group on Profesional Standardisation*) yang merumuskan standarisasi pekerjaan di dalam Organisasi Profesi di bidang IT.

4. **IPKIN (*Ikatan Profesi Komputer dan Informatika Indonesia*)**

Sebagai organisasi nirlaba independent yang beranggotakan para profesional dalam bidang Komputer dan Informatika, IPKIN bertujuan untuk meningkatkan

pemanfaatan dan pengembangan teknologi Komputer dan Informatika di Indonesia guna menunjang Pembangunan Nasional.

5. **APJII (Asosiasi Penyelenggara Jasa Internet Indonesia)**

Organisasi ini bertugas untuk melakukan beberapa program kunci yang dinilai strategis untuk pengembangan jaringan internet di Indonesia. Program-program tersebut adalah:

- a. Tarif Jasa Internet
- b. Pembentukan Indonesia-Network Information Center (ID-NIC)
- c. Pembentukan Indonesia Internet Exchange (IIX)
- d. Negosiasi Tarif Infrastruktur Jasa Telekomunikasi
- e. Usulan Jumlah dan Jenis Provider

BAB 3

SEJARAH ETIKA DI BIDANG KOMPUTER

3.1 Konsep Etika di Bidang Komputer

Jumlah interaksi manusia dengan komputer yang terus meningkat dari waktu ke waktu membuat etika komputer menjadi suatu peraturan dasar yang harus dipahami oleh masyarakat luas. Etika komputer sendiri ini bertujuan untuk mencegah kejahatan-kejahatan terutama di dunia maya seperti pencurian data, pembajakan software, dan lainnya. Di dalam artikel *“What Is Computer Ethics?”* yang ditulis pada tahun 1985, James Moor memberikan suatu definisi etika komputer yang lebih luas dan meliputi banyak hal dibandingkan tokoh lainnya. Sejak tahun 1985, definisi etika komputer Moor telah menjadi hal yang paling berpengaruh. Dia mendefinisikan etika komputer sebagai analisis mengenai sifat dan dampak sosial teknologi komputer, serta formulasi dan justifikasi kebijakan untuk menggunakan etika tersebut secara etis. Lebih lanjut, Moor menjelaskan sebagai berikut:

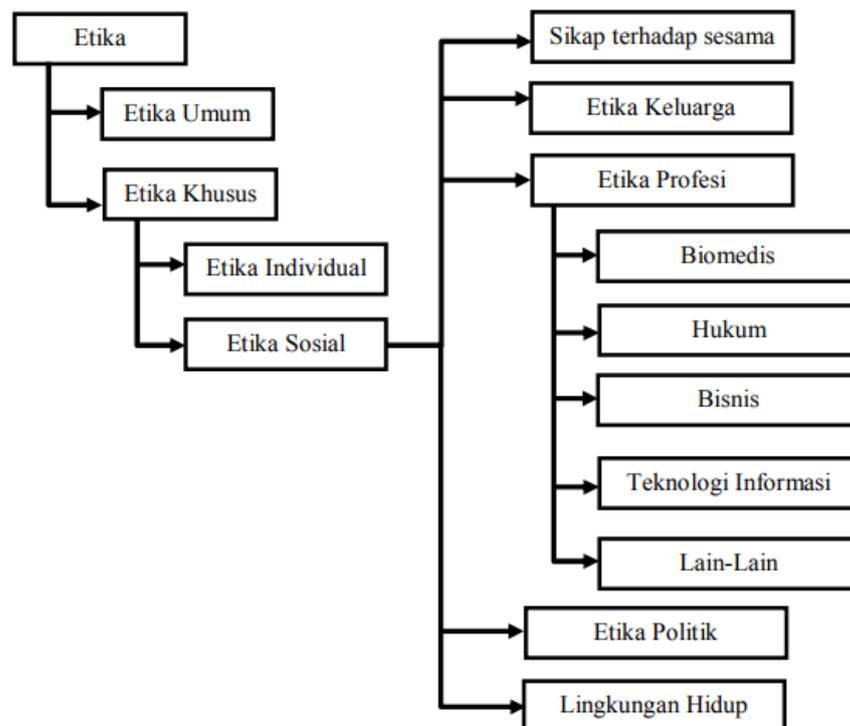
- a. Masalah khusus yang timbul di dalam etika komputer adalah disebabkan karena adanya suatu kekosongan kebijakan tentang bagaimana teknologi komputer harus digunakan.
- b. Komputer melengkapi kita dengan kemampuan baru dan pada saatnya memberikan kita banyak pilihan baru untuk bertindak.
- c. Tugas pokok dari etika komputer adalah untuk menentukan apa yang perlu kita lakukan dalam suatu kasus, yaitu: merumuskan kebijakan untuk memandu/ menuntun tindakan kita dalam memanfaatkan teknologi komputer.
- d. Satu kesulitan yang muncul adalah karena kekosongan kebijakan, maka suatu masalah di dalam etika komputer yang mungkin kelihatan sangat jelas pada awalnya, juga memperlihatkan cerminan kecil dari sebuah konsep yang bercampur aduk.
- e. Apa yang diperlukan pada kasus tersebut adalah dibutuhkannya suatu analisa yang menyediakan suatu kerangka kerja konseptual untuk merumuskan suatu kebijakan.

Menurut Moor, perkembangan komputer akan terjadi dalam dua langkah. Langkah pertama adalah sebagai “pengenalan teknologi” di mana teknologi komputer *developed* dan *refined*. Ini telah terjadi sepanjang 40 tahun pertama setelah Perang Dunia Kedua (*Second World War*). Langkah yang kedua – dalam dunia yang terindustrialisasi terjadi “penyebaran teknologikal (*technological permeation*)” di mana teknologi dapat diintegrasikan ke dalam aktifitas manusia sehari-hari dan ke dalam institusi sosial, perubahan sangat berarti dari konsep pokok, seperti “uang”, “pendidikan”, “pekerjaan,” dan ” pemilihan umum yang adil”.

Mengapa etika komputer dibutuhkan? Hal ini berkaitan dengan beberapa alasan, yaitu:

- a. Kelenturan logika, yaitu kemampuan memprogram komputer untuk melakukan apapun yang kita inginkan.
- b. Faktor transformasi, yaitu komputer dapat mengubah secara drastis cara kita melakukan sesuatu.
- c. Faktor tak kasat mata, yaitu semua operasi internal komputer tersembunyi dari penglihatan.

Gambar 2. Struktur Etika



Isu-isu Pokok Etika Komputer

- a. Kejahatan Komputer

Adalah kejahatan yang dilakukan dengan komputer sebagai basis teknologinya. Contohnya adalah virus, spam, penyadapan, carding, *Denial of Services* (DoS)/melumpuhkan target.

- b. *Cyber ethics*

Implikasi dari INTERNET (Interconnection Networking), memungkinkan pengguna IT semakin meluas, tak terpetakan, tak teridentifikasi dalam dunia *anonymouse*. Dalam hal ini diperlukan adanya aturan tak tertulis, seperti Netiket dan Emoticon.

c. E-commerce

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

d. Pelanggaran HAKI

Hal ini berkaitan dengan masalah pengakuan hak atas kekayaan intelektual, seperti pembajakan, *cracking*, *illegal software*, dst.

e. Tanggungjawab profesi

Sebagai bentuk tanggungjawab moral, perlu diciptakan ruang bagi komunitas yang akan saling menghormati. Misalnya IPKIN (Ikatan Profesi Komputer & Informatika yang didirikan di tahun 1974).

3.2 Sejarah Etika di Bidang Komputer

Sejarah etika di bidang komputer diawali di era 1940 – 1950-an. Pada era ini munculnya etika komputer sebagai sebuah bidang studi dimulai dari pekerjaan profesor Norbet Wiener. Terdapat dua peristiwa penting yang terjadi pada tahun 1940-an, yaitu Perang Dunia II dan lahirnya teknologi komputer. Selama Perang Dunia II, Profesor Norbert Wiener mengembangkan sebuah meriam antipesawat yang mampu melumpuhkan setiap pesawat tempur yang melintas di sekitarnya. Pengembangan senjata tersebut memicu Wiener untuk memperhatikan aspek lain selain kemajuan ilmu pengetahuan dan teknologi yaitu etika. Dalam penelitiannya, Wiener meramalkan terjadinya revolusi sosial dari perkembangan teknologi informasi yang dituangkan dalam sebuah buku berjudul *Cybernetics: Control and Communication in the Animal and Machine*. Penelitian Wiener masih terus berlanjut hingga tahun 1950-an. Pada tahun 1950, Wiener menerbitkan sebuah buku yang monumental, berjudul “*The Human Use of Being*”. Bagian pokok yang mencakup dalam buku tersebut adalah: 1) Tujuan hidup manusia 2) Empat prinsip-prinsip hukum 3) Diskusi tentang masalah-masalah pokok dalam etika komputer 4) Contoh topik kunci tentang etika komputer. Meskipun Wiener tidak pernah menggunakan istilah etika komputer dalam setiap bukunya, konsep pemikirannya telah menghasilkan fondasi yang kuat dalam perkembangan etika komputer di masa mendatang. Dasar-dasar etika komputer yang diberikan Wiener berada jauh di depan waktunya, dan hampir diabaikan untuk beberapa dekade.

Kemudian pada era 1960-an, yaitu pada pertengahan tahun 1960, Donn Parker dari *SRI*

International Menlo Park California melakukan berbagai riset untuk menguji penggunaan komputer yang tidak sah dan tidak sesuai dengan profesionalisme di bidang komputer. Dalam perkembangannya, ia menerbitkan “*Rules of Ethics in Information Processing*” atau peraturan tentang dalam pengolahan informasi. Parker juga dikenal menjadi pelopor kode etik profesi bagi profesional di bidang komputer, yang ditandai dengan usahanya pada tahun 1968 ketika ditunjuk untuk memimpin perkembangan Kode Etik Profesional yang pertama dilakukan untuk *Association Computing Machinery (ACM)*.

Kecerdasan buatan atau *artificial intelligence* memicu perkembangan program-program komputer yang memungkinkan manusia berinteraksi secara langsung dengan komputer. Pada era 1970-an, Josephn Weizenbaum, ilmuwan komputer MIT di Boston, mengembangkan suatu program komputer yang disebut ELIZA. ELIZA yaitu tiruan dari “*Psychotherapist Rogerian*” yang melakukan wawancara dengan pasien. Weizenbaum dikejutkan oleh reaksi dari penemuan sederhananya itu, dimana beberapa dokter jiwa melihatnya sebagai bukti bahwa komputer akan segera melakukan otomatisasi psikoterapi. Perkembangan etika komputer di era 1970-an juga diwarnai dengan karya Walter Maner yang sudah mulai menggunakan istilah “*computer ethics*” untuk mengacu pada bidang pemeriksaan yang berhadapan dengan permasalahan etis yang diciptakan oleh pemakaian teknologi komputer waktu itu.

Selanjutnya pada era 1980-an sejumlah konsekuensi sosial dan teknologi informasi yang etis menjadi isu di Amerika dan Eropa. Pembahasan *computer-enabled crime* atau kejahatan komputer, masalah yang disebabkan karena kegagalan sistem komputer, invasi keleluasaan pribadi melalui *database komputer* dan perkara pengadilan mengenai kepemilikan perangkat lunak mewarnai perkembangan etika komputer di era ini. Kemudian, pada era ini, para tokoh menyimpulkan bahwa etika komputer menjadi suatu disiplin ilmu. Pada pertengahan tahun 1980-an, James Moor dari Dartmouth College menerbitkan artikel menarik yang berjudul “*What Is Computer Ethics?*” sebagai isu khusus pada Jurnal *Metaphilosophy*. Sepanjang tahun 1990, berbagai pelatihan baru di universitas, pusat riset, konferensi, jurnal, buku teks, dan artikel menunjukkan suatu keanekaragaman yang luas tentang topik di bidang etika komputer. Perkembangan yang cukup penting lainnya berasal dari Sommon Rogerson dari De Montfort University, yang mendirikan *Centre for Computing and Social Responsibility*. Berkat jasa dan kontribusi pemikiran yang brilian dari para ilmuwan di bidang etika komputer, dimulai dari Wiener, Parker, Weizenbaum, sampai Rogerson, akhirnya etika komputer menjadi salah satu bidang ilmu utama pada banyak pusat riset dari perguruan tinggi di dunia yang akan terus berkembang

mengikuti perkembangan komputer itu sendiri.

Bagaimana dengan perkembangan etika komputer di Indonesia? Indonesia merupakan salah satu negara pengguna komputer terbesar di dunia sehingga penerapan etika komputer dalam masyarakat sangat dibutuhkan. Indonesia menggunakan dasar pemikiran yang sama dengan negara-negara lain sesuai dengan sejarah etika komputer yang ada. Pengenalan teknologi komputer menjadi kurikulum wajib di sekolah-sekolah, mulai dari Sekolah Dasar (SD) hingga Sekolah Menengah Atas (SMA sederajat). Pelajar, mahasiswa dan karyawan dituntut untuk bisa mengoperasikan program-program komputer dasar seperti Microsoft Office. Tingginya penggunaan komputer di Indonesia memicu pelanggaran-pelanggaran dalam penggunaan internet. Survei *Business Software Alliance* (BSA) tahun 2001 menempatkan Indonesia di urutan ketiga sebagai negara dengan kasus pembajakan terbesar di dunia setelah Vietnam dan China. Besarnya tingkat pembajakan di Indonesia membuat pemerintah Republik Indonesia semakin gencar menindak pelaku kejahatan komputer berdasarkan Undang-Undang Hak Cipta No. 19 Tahun 2002 (penyempurnaan dari UUHC No. 6 Tahun 1982 dan UUHC No. 12 Tahun 1997). Upaya ini dilakukan oleh pemerintah RI untuk melindungi hasil karya orang lain dan menegakkan etika dalam penggunaan komputer di Indonesia.

Gambar 3. Tokoh-Tokoh Pelopor Etika Komputer



Berbagai Pandangan dalam Cakupan Etika Komputer

Melihat sejarah perkembangan komputer yang telah dibahas di atas, ketika memutuskan untuk menggunakan istilah “etika komputer” pada pertengahan tahun 70-an, Walter Maner menggambarkan bidang tersebut sebagai bidang ilmu yang menguji “permasalahan etis yang menjengkelkan, yang diciptakan oleh teknologi komputer”. Maner berpendapat bahwa beberapa permasalahan etis sebelumnya sudah ada, diperburuk oleh munculnya komputer yang menimbulkan permasalahan baru sebagai akibat penerapan teknologi informasi. Sementara Deborah Johnson (1985) dalam bukunya *Computer Ethics*, menggambarkan bidang ini sebagai satu studi tentang cara yang ditempuh oleh komputer memiliki standar moral baru, yang memaksa kita sebagai pengguna untuk menerapkan norma-norma baru pula di dalam dunia yang “belum dipetakan”.

James Moor mendefinisikan etika komputer didalam artikelnya “*What Is Computer Ethics*” yang ditulis pada tahun 1985. Dalam artikel tersebut, Moor mengartikan etika komputer sebagai bidang ilmu yang tidak terikat secara khusus dengan teori ahli filsafat mana pun dan kompatibel dengan pendekatan metodologis yang luas pada pemecahan masalah etis. Menurut Moor (1985), terlihat bahwa terdapat suatu masalah khas dalam etika komputer yang muncul karena adanya suatu kebijakan yang belum jelas tentang bagaimana teknologi komputer harus digunakan. Satu tugas etika komputer adalah menentukan apa yang perlu kita lakukan didalamnya. Dalam kasus ini adalah merumuskan kebijakan untuk memandu tindakan kita. Secara lebih lanjut, Moor mengatakan bahwa teknologi komputer itu sebenarnya memiliki sifat revolusioner karena memiliki “*logically malleable*”. Komputer disebut “*logically malleable*” karena bisa melakukan aktivitas apa pun dalam membantu tugas manusia. Hal ini terjadi karena komputer bekerja menggunakan suatu logika pemrograman tertentu yang bisa dibuat oleh programernya. Logika pemrograman tersebut terbubung dimana-mana sehingga potensi aplikasi teknologi

komputer tampak tiada habisnya. Komputer merupakan suatu alat yang universal. Tentu saja batas komputer adalah seberapa besar batas dari kreativitas manusia sendiri.

Menurut Moor, revolusi komputer sedang terjadi dalam dua langkah. Langkah yang pertama adalah “pengenalan teknologi” di mana teknologi komputer dapat dikembangkan dan disaring. Ini telah yang terjadi di Amerika sepanjang empat puluh tahun pertam setelah Perang Dunia yang kedua. Langkah yang kedua adalah “penyebaran teknologi” di mana teknologi mendapat integrasi ke dalam aktivitas manusia sehari-hari dan ke dalam institusi sosial, mengubah seluruh konsep pokok, seperti uang (Money), pendidikan (education), kerja (work) dan pemilihan yang adil (fair elections). Sekarang ini, pengertian yang diberikan Moor adalah salah satu pengertian terbaik yang ada menyangkut bidang etika komputer tersebut.

Pada tahun 1990, Donald Gotterbarn memelopori suatu pendekatan yang berbeda dalam melukiskan cakupan khusus bidang etika komputer. Dalam pandangan Gotterbarn, etika komputer harus dipandang sebagai suatu cabang etika profesional, yang terkait semata-mata dengan standar kode dan praktk yang dilakukan oleh para profesional di bidang komputasi :

“There is little attention paid to the domain of professional ethics -- the calues that guide the day-to-day activities of computing professionals in their role as professionals. By computing professional I mean anyone involved in the design and velopment of computer artifacts.. The ethical decisions made during the development of these artifacts have a direct relationship to many of the issues discussed under the broader concept of computer ethics...” (Gotterbarn, 1991).

Dengan kepeloporannya tersebut, Gotterbarn akhirnya dilibatkan dalam sejumlah aktivitas terkait dengan penelitian di bidang etika komputer.

3.3 Kode Etik Profesi di Bidang Teknologi Informasi

Dalam lingkup TI, kode etik profesinya memuat kajian ilmiah mengenai prinsip atau norma-norma dalam kaitan dengan hubungan antara professional atau developer TI dengan klien, antara para professional sendiri, antara organisasi profesi serta organisasi profesi dengan pemerintah. Salah satu bentuk hubungan seorang profesional dengan klien (pengguna jasa) misalnya pembuatan sebuah program aplikasi. Seorang

profesional tidak dapat membuat program semaunya, ada beberapa hal yang harus ia perhatikan seperti untuk apa program tersebut nantinya digunakan oleh kliennya atau user dapat menjamin keamanan (security) sistem kerja program aplikasi tersebut dari pihak-pihak yang dapat mengacaukan sistem kerjanya (misalnya: hacker, cracker, dll).

Kode etik profesi merupakan sarana untuk membantu para pelaksana sebagai seseorang yang professional supaya tidak dapat merusak etika profesi. Tiga hal pokok yang merupakan fungsi dari kode etik profesi:

- a. Kode etik profesi adalah pedoman bagi setiap anggota profesi tentang prinsip profesionalita. Sehingga pelaksana profesi dapat mengetahui suatu hal yang boleh dilakukan dan yang tidak boleh dilakukan.
- b. Kode etik profesi adalah control social bagi masyarakat atas profesi yang dijalankan. Artinya etika profesi dapat memberikan suatu pengetahuan kepada masyarakat agar juga dapat memahami arti pentingnya suatu profesi, sehingga memungkinkan pengontrolan terhadap para pelaksana di tempat kerja.
- c. Kode etik profesi mencegah campur tangan pihak luar organisasi profesi tentang hubungan etika dalam keanggotaan profesi. Artinya bahwa pelaksana profesi pada suatu instansi atau perusahaan yang lain tidak boleh mencampuri pelaksanaan profesi di lain instansi atau perusahaan.

Dalam lingkup Teknologi Informasi, kode etik profesi merupakan kajian ilmiah mengenai prinsip atau norma-norma dalam kaitan professional dengan klien, antara professional sendiri, antara organisasi profesi. Salah satu bentuknya adalah kode etik pada saat membuat sebuah program aplikasi. Sehingga seorang professional tidak dapat seenaknya membuat program, ada beberapa hal yang harus diperhatikan seperti jaminan keamanan data selama pembuatan program. Jika pada professional Teknologi Informasi melanggar kode etik, mereka dikenakan sanksi moral, sampai pada dikeluarkan dari pekerjaan

Kode Etik Pengguna Internet

Adapun kode etik yang diharapkan bagi para pengguna internet adalah:

1. Menghindari dan tidak mempublikasi informasi yang secara langsung berkaitan dengan masalah pornografi dan nudisme dalam segala bentuk.
2. Menghindari dan tidak mempublikasi informasi yang memiliki tendensi menyinggung secara langsung dan negatif masalah suku, agama dan ras (SARA), termasuk didalamnya usaha penghinaan, pelecehan, pendiskreditan, penyiksaan

serta segala bentuk pelanggaran hak atas perseorangan, kelompok/ lembaga/ institusi lain.

3. Menghindari dan tidak mempublikasikan informasi yang berisi instruksi untuk melakukan perbuatan melawan hukum (illegal) positif di Indonesia dan ketentuan internasional umumnya.
4. Tidak menampilkan segala bentuk eksploitasi terhadap anak-anak dibawah umur.
5. Tidak mempergunakan, mempublikasikan dan atau saling bertukar materi dan informasi yang memiliki korelasi terhadap kegiatan pirating, hacking dan cracking.
6. Bila mempergunakan script, program, tulisan, gambar / foto, animasi, suara atau bentuk materi dan informasi lainnya yang bukan hasil karya sendiri harus mencantumkan identitas sumber dan pemilik hak cipta bila ada dan bersedia untuk melakukan pencabutan bila ada yang mengajukan keberatan serta bertanggung jawab atas segala konsekuensi yang mungkin timbul karenanya. Tidak berusaha atau melakukan serangan teknis terhadap produk, sumberdaya (resource) dan peralatan yang dimiliki pihak lain.
7. Menghormati etika dan segala macam peraturan yang berlaku dimasyarakat internet umumnya dan bertanggungjawab sepenuhnya terhadap segala muatan/ isi situsnya.
8. Untuk kasus pelanggaran yang dilakukan oleh pengelola, anggota dapat melakukan teguran secara langsung.

Etika Programmer

Adapun kode etik yang diharapkan bagi para programmer adalah:

- a. Seorang programmer tidak boleh membuat atau mendistribusikan Malware.
- b. Seorang programmer tidak boleh menulis kode yang sulit diikuti dengan sengaja.
- c. Seorang programmer tidak boleh menulis dokumentasi yang dengan sengaja untuk membingungkan atau tidak akurat.
- d. Seorang programmer tidak boleh menggunakan ulang kode dengan hak cipta kecuali telah membeli atau meminta ijin.
- e. Tidak boleh mencari keuntungan tambahan dari proyek yang didanai oleh pihak kedua tanpa ijin.
- f. Tidak boleh mencuri software khususnya development tools.
- g. Tidak boleh menerima dana tambahan dari berbagai pihak eksternal dalam suatu proyek secara bersamaan kecuali mendapat ijin.
- h. Tidak boleh menulis kode yang dengan sengaja menjatuhkan kode programmer lain

untuk mengambil keuntungan dalam menaikkan status.

- i. Tidak boleh membeberkan data-data penting karyawan dalam perusahaan.
- j. Tidak boleh memberitahu masalah keuangan pada pekerja
- k. Tidak pernah mengambil keuntungan dari pekerjaan orang lain.
- l. Tidak boleh mempermalukan profesinya.
- m. Tidak boleh secara asal-asalan menyangkal adanya bug dalam aplikasi.
- n. Tidak boleh mengenalkan bug yang ada di dalam software yang nantinya programmer akan mendapatkan keuntungan dalam membetulkan bug.
- o. Terus mengikuti pada perkembangan ilmu komputer.

3.4 Tanggung Jawab Profesi IT

Ciri-ciri profesionalisme yang harus dimiliki oleh seorang IT berbeda dari bidang pekerjaan yang lainnya. Ciri-cirinya adalah sebagai berikut :

1. Memiliki kemampuan / keterampilan dalam menggunakan peralatan yang berhubungan dengan bidang pekerjaan IT Seorang IT harus mengetahui dan mempraktekkan pengetahuan IT-nya ke dalam pekerjaannya.
2. Punya ilmu dan pengalaman dalam menganalisa suatu software atau program.
3. Bekerja di bawah disiplin kerja
4. Mampu melakukan pendekatan disipliner
5. Mampu bekerja sama
6. Cepat tanggap terhadap masalah client.
7. Keterampilan yang berdasar pada pengetahuan teoretis. Profesional diasumsikan mempunyai pengetahuan teoretis yang ekstensif dan memiliki keterampilan yang berdasar pada pengetahuan tersebut dan bisa diterapkan dalam praktek.
8. Asosiasi profesional. Profesi biasanya memiliki badan yang diorganisasi oleh para anggotanya, yang dimaksudkan untuk meningkatkan status para anggotanya. Organisasi profesi tersebut biasanya memiliki persyaratan khusus untuk menjadi anggotanya.
9. Pendidikan yang ekstensif. Profesi yang prestisius biasanya memerlukan pendidikan yang lama dalam jenjang pendidikan tinggi.
10. Ujian kompetensi. Sebelum memasuki organisasi profesional, biasanya ada persyaratan untuk lulus dari suatu tes yang menguji terutama pengetahuan teoretis.
11. Pelatihan institutional. Selain ujian, juga biasanya dipersyaratkan untuk mengikuti pelatihan istitusional dimana calon profesional mendapatkan

pengalaman praktis sebelum menjadi anggota penuh organisasi. Peningkatan keterampilan melalui pengembangan profesional juga dipersyaratkan.

12. Lisensi. Profesi menetapkan syarat pendaftaran dan proses sertifikasi sehingga hanya mereka yang memiliki lisensi bisa dianggap bisa dipercaya.
13. Otonomi kerja. Profesional cenderung mengendalikan kerja dan pengetahuan teoretis mereka agar terhindar adanya intervensi dari luar.
14. Kode etik. Organisasi profesi biasanya memiliki kode etik bagi para anggotanya dan prosedur pendisiplinan bagi mereka yang melanggar aturan.
15. Mengatur diri. Organisasi profesi harus bisa mengatur organisasinya sendiri tanpa campur tangan pemerintah. Profesional diatur oleh mereka yang lebih senior, praktisi yang dihormati, atau mereka yang berkualifikasi paling tinggi.
16. Layanan publik dan altruisme. Diperolehnya penghasilan dari kerja profesinya dapat dipertahankan selama berkaitan dengan kebutuhan publik, seperti layanan dokter berkontribusi terhadap kesehatan masyarakat.
17. Status dan imbalan yang tinggi. Profesi yang paling sukses akan meraih status yang tinggi, prestise, dan imbalan yang layak bagi para anggotanya. Hal tersebut bisa dianggap sebagai pengakuan terhadap layanan yang mereka berikan bagi masyarakat.

3.5 Pelanggaran Etika Profesi IT

Faktor utama meningkatnya pelanggaran Kode Etik Profesi IT adalah makin merebaknya penggunaan Internet. Jaringan luas komputer tanpa disadari para pemiliknya disewakan kepada spammer (penyebar e-mail komersial), fraudster (pencipta situs tipuan), dan penyabot digital. Terminal – terminal jaringan telah terinfeksi virus komputer, yang mengubah komputer menjadi “zombi”. Contohnya di Bandung banyak warnet yang menjadi sarang kejahatan komputer. Faktor lain yang menjadi pemicu adalah makin banyaknya para “Intelektual yang tidak BERETIKA”. Faktor penyebab Pelanggaran kode etik profesi IT:

- a. Tidak berjalannya kontrol dan pengawasan dari masyarakat.
- b. Organisasi profesi tidak dilengkapi dengan sarana dan mekanisme bagi masyarakat untuk menyampaikan keluhan.
- c. Rendahnya pengetahuan masyarakat mengenai substansi kode etik profesi, karena buruknya upaya sosialisasi dari pihak profesi sendiri.
- d. Belum terbentuknya kultur dan kesadaran dari para pengemban profesi TI untuk menjaga martabat luhur profesinya.

- e. Tidak adanya kesadaran etis dan moralitas di antara para pengemban profesi TI

Beberapa bentuk pelanggaran etika profesi di bidang teknologi informasi, yaitu:

1. Kejahatan Komputer

Selain memberikan dampak positif, komputer juga mengundang tangan-tangan kriminal untuk beraksi. Hal ini memunculkan fenomena khas yang disebut *computer crime* atau kejahatan di dunia komputer. Kejahatan komputer merupakan kejahatan yang ditimbulkan karena penggunaan komputer secara ilegal” (Andi Hamzah 1989). Beberapa kejahatan didunia komputer diantaranya:

- a. ***Unauthorized Access to Computer System and Service***, adalah 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 melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.
- b. ***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 adalah 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.
- c. ***Data Forgery***, merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless 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.
- d. ***Cyber Espionage***, merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

- e. ***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. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.
- f. ***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.
- g. ***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 materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.
- h. ***Cracking***, adalah kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak system keamanan suatu system computer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identetik dengan perbuatan negative, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.
- i. ***Carding***, adalah kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan *card credit* orang lain sehingga dapat merugikan orang tersebut baik materil maupun *non materil*.

- j. **Denial of Service Attack**, adalah serangan tujuan ini adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna jasa internet yang sah. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs web dengan data sampah yang tidak perlu bagi orang yang dituju. Pemilik situs web menderita kerugian, karena untuk mengendalikan atau mengontrol kembali situs web tersebut dapat memakan waktu tidak sedikit yang menguras tenaga dan energi.
- k. **Hate sites**, Situs ini sering digunakan oleh *hackers* untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para “ekstrimis” untuk menyerang pihak-pihak yang tidak disenanginya. Penyerangan terhadap lawan atau *opponent* ini sering mengangkat pada isu-isu rasial, perang program dan promosi kebijakan ataupun suatu pandangan (isme) yang dianut oleh seseorang / kelompok, bangsa dan negara untuk bisa dibaca serta dipahami orang atau pihak lain sebagai “pesan” yang disampaikan.
- l. **Cyber Stalking** adalah segala bentuk kiriman *e-mail* yang tidak dikehendaki oleh user atau junk e-mail yang sering memakai folder serta tidak jarang dengan pemaksaan. Walaupun e-mail “sampah” ini tidak dikehendaki oleh para user.
- m. **Hacker dan Cracker**

Terminologi hacker muncul pada awal tahun 1960an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi computer dan mereka berlutut dengan sejumlah computer mainframe. Kata hacker pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang computer yang lebih baik ketimbang yang telah dirancang bersama. Menurut Mansfield, hacker didefinisikan sebagai seorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah system operasi dan kode computer pengamanan lainnya tetapi tidak melakukan tindakan perusakan 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 mekumpuhkan seluruh system computer.

Penggolongan Hacker dan Cracker:

- Recreational Hackers, kejahatan yang dilakukan oleh netter tingkat pemula untuk sekedar mencoba kekurangan handalan system sekuritas suatu perusahaan.

- Crackers/Criminal Minded hackers, pelaku memiliki motifasi untuk mendapat keuntungan financial, sabotase dan pengrusakan data, type kejahatan ini dapat dilakukan dengan banyuan orang dalam.
- Political Hackers, aktifis politis (hactivist) melakukan pengrusakan terhadap ratusan situs web untuk mengkampanyekan programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendiskreditkan lawannya.

n. ***Fraud***

Merupakan kejahatan manipulasi informasi dengan tujuan mengeruk keuntungan yang sebesar besarnya. Biasanya kejahatan yang dilakukan adalah memanipulasi informasi keuangan. Sebagai contoh adanya situs lelang fiktif.

o. ***Gambling***

Perjudian tidak hanya dilakukan secara konvensional, akan tetapi perjudian sudah marak didunia cyber yang berskala global. Dan kegiatan ini dapat diputar kembali dinegara yang merupakan “*tax heaven*” seperti cymán islands yang merupakan surga bagi *money laundering*.

Jenis jenis online gambling antara lain :

1. *Online Casinos*

Pada online casinos ini orang dapat bermain rolet, blackjack dll

2. *Online Poker*

Online poker biasanya menawarkan texas hold'em, Omaha dll

3. *Mobil gambling*

Merupakan perjudian dengan menggunakan wereless device, seperti PDAs, Wereless tabled PCs, berapa casini online dan poker onlinemenawarkan pilihan mobil. GPRS,GSM data, UMTS, I-Mode adalah semua teknologi lapisan data atas nama perjudian gesit tergantung , jenis perjudian di Indonesia yaitu SDSB.com, jenis perjudian olah raga terlengkap di Indonesia dan Asia Tenggara.

p. ***Pornography dan Paedophilia***

Pornography merupakan jenis kejahatan dengan menyajikan bentuk tubuh tanpa busana, erotis, dan kegiatan seksual lainnya dengan tujuan merusak moral. Paedophilia merupakan kejahatan penyimpangan seksual yang lebih condong kearah anak anak (*child phornography*).

BAB IV

ETIKA DI DUNIA MAYA

4.1 Perkembangan Penggunaan Internet Masa Kini

Jaringan internet sudah jadi bagian kehidupan manusia yang kini tak bisa dipisahkan. Sebelum canggih seperti saat ini, internet pun punya perjalanan sejarah. Ini sejarah internet yang perlu kamu tahu. Menurut KBBI, pengertian internet adalah jaringan komunikasi elektronik yang menghubungkan jaringan komputer dan fasilitas komputer yang terorganisasi di seluruh dunia melalui telepon atau satelit berinternet. Adanya koneksi internet memudahkan informasi apapun tersebar luas ke seluruh dunia dan membantu segala bentuk kegiatan manusia. Berikut ini beberapa poin penting sejarah internet dan perkembangannya yang mempengaruhi kehidupan manusia:

Tahun 1969

Pada Oktober 1969, proyek terciptanya kata 'Login' muncul, proyek ini dilakukan oleh para peneliti di Universitas California (UCLA), Los Angeles. Proyek tersebut memaparkan bagaimana proses pengiriman data dalam bentuk kode biner pada dua komputer, komputer pertama mengirimkan kata 'LOG' dan komputer kedua mengirimkan kata 'IN'. Keberhasilan proyek tersebut mencetuskan sejarah internet awal dalam proyek APRANET (Advanced Research Project Agency Network), jaringan komputer yang dibentuk oleh Departemen Pertahanan Amerika. Awalnya hanya sekitar 4 komputer yang terhubung pada institusi pendidikan ternama di Amerika antara lain Stanford Research Institute, University of California (UCLA), St. Barbara, dan University of Utah. Lalu, pada tahun 1970 berkembang sekitar 13 hingga pada tahun 1981, menjadi 231 komputer yang terhubung dalam jaringan ARPANET. Proyek ARPANET didesain untuk kebutuhan militer yang mana bisa mengendalikan serangan ancaman nuklir, meningkatkan taktik militer dan mengelola keputusan melalui komputer.

Tahun 1971

Jaringan APRANET, digunakan dalam pengiriman surat elektronik pertama, dicetuskan penggunaan simbol '@' dalam alamat surel. Faktanya simbol tersebut berfungsi untuk memisahkan nama pengguna dengan jaringan yang sedang digunakan. Ssejarah internet email dilakukan oleh Ratu Inggris pada tahun 1973 yang mencoba untuk mengirim email menggunakan jaringan APRANET. Dan, pada 1976, mahasiswa Imperial College London menguji coba jaringan internet. Dari sini, istilah internet mulai

dimunculkan.

Tahun 1983

Internet muncul di dunia pada tanggal 1 Januari 1983. TCP/IP (Transmission Control Protocol/Internet Protocol) mulai diimplementasikan pada sistem jaringan internet. Dari sinilah, para peneliti mulai untuk menghubungkan jaringan satu dengan jaringan lainnya yang berbeda hingga menjadi internet modern seperti saat ini.

Tahun 1990

Berners-Lee dan timnya yang bekerja di CERN (organisasi eropa untuk riset nuklir) menciptakan World Wide Web (www). Publik mulai menggunakan 'www' yang berfungsi untuk digunakan dalam menelusuri situs website. Robert Cailliau dari Belgia membantu mengembangkan usul Berners-Lee. Penemuan ini didasarkan pada dua pilar, yaitu: bahasa pemrograman HTML, yang memungkinkan keberadaan website, serta protokol pertukaran hypertext HTTP, yang memungkinkan pengguna meminta, dan menerima laman yang diinginkan. Hingga pada tahun 1993 keberadaan internet semakin tersebar berkat dirilisnya situs pencari pertama, Mosaic. Dan, mulailah bermunculan situs penyedia email bernama Yahoo dan perusahaan berbasis online seperti Amazon dan eBay pada 1994. Sedangkan, kemunculan Google terjadi pada tahun 1998, sampai saat ini masih bermunculan pula perusahaan atau situs online yang dibutuhkan bagi kehidupan manusia

Tahun 2000an

Tahun 2000an menjadi titik awal penggunaan jejaring sosial. Hal tersebut dibuktikan dengan munculnya Thefacebook.com oleh Mark Zuckerberg pada tahun 2003. Awalnya Facebook hanya untuk menghubungkan para mahasiswa Harvard. Kemudian, semakin berkembang menjadi salah satu top media sosial dengan pengguna sekitar 2,3 miliar orang. Di tahun yang sama, setengah penduduk Inggris telah mengakses internet. Pada tahun 2007, Perusahaan Apple mulai meluncurkan ponsel pintar, yaitu iPhone.

Tahun 2009

Anniversary atau hari jadi Internet ke-40 tahun.

Tahun 2010

Perkembangan Facebook mencapai 400 juta pengguna aktif pada tahun 2010. Sosial media baru bermunculan, yaitu Pinterest dan Instagram.

Tahun 2011

Twitter dan Facebook berkembang pesat di wilayah Timur Tengah (Arab Saudi, Bahrain, Irak, dan lain-lain).

Tahun 2012

Seperti dilansir *Live Science*, pemerintahan Presiden Barack Obama mengumumkan penentangannya terhadap kontroversi 'Stop Online Piracy Act' (SOPA) yang memberlakukan aturan baru bagi penyedia layanan internet untuk mengawasi konten dari hak cipta. Hal tersebut berarti pemerintahan Presiden Obama tidak akan mendukung undang-undang yang mengurangi kebebasan berekspresi karena hal tersebut akan merugikan perusahaan teknologi seperti Google dan Youtube yang bergantung pada konten yang dibuat pengguna, serta penggunaan yang adil di internet.

Tahun 2013

Seorang mantan karyawan CIA dan kontraktor National Security Agency (NSA), Edward Snowden mengungkapkan bahwa NSA telah memiliki program pemantauan yang mampu melihat komunikasi ribuan orang termasuk warga Amerika.

Tahun 2015

Instagram, aplikasi berbagi foto dan video telah mencapai 400 juta pengguna melebihi pengguna Twitter sebesar 316 juta di pertengahan tahun.

Tahun 2016

Perusahaan teknologi Google meluncurkan Google Assistant berupa program asisten pribadi yang diaktifkan melalui suara. Hal tersebut menandakan penggunaan internet dalam sistem komputer pintar. Google akhirnya bergabung bersama Alexa milik Amazon, Siri dari Apple dan Cortana dari Microsoft dalam hal ini.

Faktanya, sejarah internet melalui proses yang cukup panjang hingga seperti sekarang. Kini, perkembangan teknologi semakin maju juga dengan adanya jaringan internet yang bisa kita akses dengan mudah.

Tahun 2019-sekarang

Pada tahun 2020, Kementerian Komunikasi dan Informatika (Kemkominfo) menyatakan, pengguna internet di Indonesia hingga saat ini telah mencapai 175,5 juta orang. Dengan capaian tersebut, Indonesia mengalami kenaikan 25 juta atau 17 persen dibandingkan tahun sebelumnya pada 2019. Dari jumlah pengguna internet tersebut, 80 persen di antaranya adalah remaja berusia 15-19 tahun. Dari informasi tersebut, dapat kita simpulkan bahwa perkembangan teknologi saat ini bagaikan dua mata pisau yang perlu mendapatkan perhatian khusus dari semua elemen.

Tidak bisa dipungkiri bahwa di balik manfaat internet, juga menimbulkan banyak mudarat dan dampak yang mengkhawatirkan, mulai dari pornografi, kasus penipuan, dan

kekerasan yang semua bermula dari dunia maya. Semua permasalahan tersebut, harus mendapat penanganan serius agar dampak negatif dari internet dapat diminimalkan.

Salah satunya, pemerintah mencanangkan Program INSAN agar masyarakat mengetahui cara menggunakan internet, pemanfaatannya dan dampak yang ditimbulkan. Program ini bertujuan untuk mensosialisasikan penggunaan internet secara sehat dan aman melalui pembelajaran etika berinternet sehat dengan melibatkan seluruh komponen masyarakat. Sedangkan Program “Incakap (Internet Cerdas Kreatif dan Produktif)” yang merupakan penggantian nama dari program “INSAN (Internet Sehat dan Aman)” disosialisasikan untuk mengantisipasi dampak negatif internet di kalangan masyarakat, khususnya pemuda dan pelajar selaku pengguna internet tertinggi di Indonesia.

Kemudian selama dua tahun terakhir ini (2020-2021), terjadi pergeseran penggunaan internet di kawasan perkotaan akibat pandemi Covid-19. Dalam masa pandemi Covid-19 ada perubahan atau pergeseran konfigurasi pemanfaatan atau penggunaan internet. Sebelumnya konfigurasi pemanfaatan internet itu berada di kantor, kampus, sekolah dan tempat publik. Namun, saat ini konfigurasi penggunaan internet bergeser ke perumahan, tempat tinggal, dan pemukiman. Hal ini sebagai konsekuensi pelaksanaan imbauan pemerintah untuk bekerja dari rumah (WFH), belajar dari rumah (LFH) dan beribadah di rumah. Akibat dari WFH, penggunaan internet jumlahnya semakin meningkat di wilayah real estate, perumahan dan pemukiman. Kementerian Kominfo juga telah meminta kepada penyelenggara layanan telekomunikasi seluler dan penyedia jaringan internet untuk menambah kapasitas dan infrastruktur jaringan guna mendukung pelaksanaan bekerja dan belajar dari rumah.

4.2 Cyber Law

4.2.1 Cyber Law

Pengertian *Cyber Law*

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

Jonathan Rosenoer (1997) membagi ruang lingkup *Cyber Law* dalam beberapa hal diantaranya:

- a. *Copyright* (hak cipta),
- b. *Trademark* (hak merek),
- c. *Defamation* (pencemaran nama baik),
- d. *Hate Speech* (penistaan, penghinaan, fitnah),
- e. *Hacking, Viruses, Illegal Access*, (penyerangan terhadap komputer lain),
- f. *Regulation Internet Resource* (pengaturan sumber daya internet),
- g. *Privacy* (kenyamanan pribadi),
- h. *Duty Care* (kehati-hatian),
- i. *Criminal Liability* (kejahatan menggunakan IT),
- j. *Procedural Issues* (yuridiksi, pembuktian, penyelidikan, dll.),
- k. *Electronic Contract* (transaksi elektronik),
- l. *Pornography, Robbery* (pencurian lewat internet),
- m. *Consumer Protection* (perlindungan konsumen), dan
- n. *E-Commerce, E-Government* (pemanfaatan internet dalam keseharian).

Tujuan *Cyber Law*

Cyber Law sangat dibutuhkan karena kaitannya dengan upaya pencegahan tindak pidana, maupun penanganan tindak pidana. *Cyber Law* akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme. Dengan kata lain, *Cyber Law* diperlukan untuk menanggulangi kejahatan *Cyber*.

Alasan *Cyber Law* Penting Untuk Hukum Di Indonesia

Cyber Law penting diberlakukan sebagai hukum di Indonesia. Hal tersebut disebabkan oleh perkembangan zaman. Menurut pihak yang pro terhadap *Cyber Law*, sudah saatnya Indonesia memiliki *Cyber Law*, mengingat hukum-hukum tradisional tidak mampu mengantisipasi perkembangan dunia maya yang pesat.

Contoh Kasus Yang Berkaitan Dengan *Cyber Law*

Salah satu contoh kasus dalam kejahatan *cyber* adalah kasus yang dialami oleh Wakil Ketua MPR periode 2009-2014 Lukman Hakim Saifuddin, di mana *e-mail* beliau dibajak oleh seseorang untuk mendapatkan kepentingan dengan

sejumlah uang dengan mengirimkan surat kepada kontak-kontak yang ada di *e-mail* milik beliau.

Lukman Hakim Saifuddin memiliki hak sebagaimana diatur dalam Pasal 26 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU ITE”) yang mengatakan bahwa “setiap orang yang dilanggar haknya sebagaimana yang dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.”

Dengan hak yang telah disebutkan di atas, Lukman Hakim Saifuddin berhak untuk mengajukan gugatan yang berdasarkan pada Pasal 28 ayat (1) UU ITE yang berbunyi, “setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik”, di mana hal tersebut merupakan perbuatan yang dilarang.

Sejalan dengan itu, pelaku dapat dikenakan pidana sesuai ketentuan Pasal 45A UU ITE yang berbunyi, “Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Dalam kasus yang menimpa Lukman Hakim Saifuddin tersebut, pelaku kejahatan dunia maya yang membajak *e-mail* beliau juga dapat diterapkan dengan pelanggaran Pasal 378 KUHP tentang penipuan yang berbunyi, “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat (*hoedanigheid*) palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, mengerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun.”

Asas-asas Cyber Law

Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu :

- a) *Subjective territoriality*, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.
- b) *Objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
- c) *Nationality*, yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
- d) *Passive Nationality*, yang menekankan yurisdiksi berdasarkan kewarganegaraan korban.
- e) *Protective Principle*, yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah.
- f) *Universality*, Asas ini selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini disebut juga sebagai “universal interest jurisdiction”. Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (crimes against humanity), misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun di masa mendatang asas yurisdiksi universal ini mungkin dikembangkan untuk internet piracy, seperti computer, cracking, carding, hacking and viruses, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional.

4.2.2 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. UU ini merupakan hasil kombinasi dari dua Rancangan Undang-undang atau RUU yaitu (1) RUU Tindak Pidana Teknologi Informasi dari Universitas Padjajaran atas arahan dari Departemen Komunikasi dan Informasi dengan bekerja-sama dengan Institut Teknologi Bandung dan (2) RUU Informasi Elektronik dan Transaksi Elektronik dari Universitas Indonesia atas arahan dari

Departemen Perindustrian dan Perdagangan. Lalu kedua RUU tersebut digabung dan disinkronisasi kembali oleh tim yang dipimpin oleh Prof. Ahmad M Ramli SH sebagai utusan dari Presiden kala itu yaitu Susilo Bambang Yudhoyono (SBY) dan berhasil diberlakukan tertanggal sejak 21 April 2008 sebelum akhirnya diperbarui dengan Undang-undang No. 19 Tahun 2016 tentang Perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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:

1. 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.
2. Menurunkan ancaman pidana pada 2 (dua) ketentuan sebagai berikut:
 - a. 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;
 - b. 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.

3. Melaksanakan putusan Mahkamah Konstitusi terhadap 2 (dua) ketentuan sebagai berikut:
 - a. Mengubah ketentuan Pasal 31 ayat (4) yang semula mengamankan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam Undang Undang;
 - b. Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hukum yang sah.
4. Melakukan sinkronisasi ketentuan hukum acara pada Pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, sebagai berikut:
 - a. Penggeledahan dan/atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, disesuaikan kembali dengan ketentuan KUHAP;
 - b. Penangkapan penahanan yang semula harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1×24 jam, disesuaikan kembali dengan ketentuan KUHAP.
5. Memperkuat peran Penyidik Pegawai Negeri Sipil dalam Undang-Undang Tentang Informasi dan Transaksi Elektronik pada ketentuan Pasal 43 ayat (5):
 - a. Kewenangan membatasi atau memutuskan akses terkait dengan tindak pidana teknologi informasi;
 - b. Kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana teknologi informasi.
6. Menambahkan ketentuan mengenai “*right to be forgotten*” atau “hak untuk dilupakan” pada ketentuan Pasal 26, sebagai berikut:
 - a. Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan;
 - b. Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan.
7. Memperkuat peran Pemerintah dalam memberikan perlindungan dari segala jenis gangguan akibat penyalahgunaan informasi dan transaksi elektronik dengan menyisipkan kewenangan tambahan pada ketentuan Pasal 40:
 - a. Pemerintah wajib melakukan pencegahan penyebaran Informasi Elektronik yang memiliki muatan yang dilarang;

- b. Pemerintah berwenang melakukan keputusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan keputusan akses terhadap Informasi Elektronik yang memiliki muatan yang melanggar hukum.

4.3 Etika Menggunakan Internet Menurut UU ITE

Etika dalam berinternet biasa disebut dengan *cyber ethic* (etika cyber). Cyber ethics adalah suatu aturan tak tertulis yang dikenal di dunia IT. Suatu nilai-nilai yang disepakati bersama untuk dipatuhi dalam interaksi antar pengguna teknologi khususnya teknologi informasi. Tidak adanya batas yang jelas secara fisik serta luasnya penggunaan IT di berbagai bidang membuat setiap orang yang menggunakan teknologi informasi diharapkan mau mematuhi *cyber ethics* yang ada. *Cyber ethics* memunculkan peluang baru dalam bidang pendidikan, bisnis, layanan pemerintahan dengan adanya kehadiran internet. Sehingga memunculkan netiket/*netiquette* yaitu salah satu etika acuan dalam berkomunikasi menggunakan internet, berpedoman pada IETF (*the internet engineering task force*), yang menetapkan RFC (*netiquette guidelines dalam request for comment*).

Etika kehidupan berbangsa atau bernegara yang semula mudah sekali disosialisasikan karena orang berinteraksi secara langsung secara fisik, maka dalam dunia cyber upaya mensosialisasikan *cyber ethic* menjadi sulit sekali dilakukan karena jangkauan teritorinya sudah jauh lebih luas. Sebenarnya *cyber ethic* dapat ditelaah dan dimengerti oleh pengguna internet, jika disadari terdapat etika kehidupan normal yang berlaku. Manusia tentu tak ingin dirugikan dalam kehidupannya. Di dunia maya hal itu pun mungkin terjadi dan saat itulah terjadi pelanggaran *cyber ethic*, misalnya seseorang mengirim email yang berisi informasi-informasi penjualan suatu produk dan karena email itu takut ditolak maka subyek email diubah menjadi sepenggal kalimat menarik yang tak ada hubungan dengan isi email. Kontan saja si penerima merasa dirugikan, karena untuk membuka email ia memerlukan biaya koneksi ke internet, tidak seperti saat ia menerima surat pos biasa, ia tidak dikenakan biaya apapun. Kesalahan si pengirim adalah mengelabui email dengan subyek yang tidak tepat dan itulah salah satu pelanggaran etika dalam berinternet. Beberapa contoh etika dalam berinternet, yaitu:

1. Netiket pada *One to One Communications*

Yang dimaksud dengan *One to One Communications* adalah kondisi dimana komunikasi terjadi antar individu (*face to face*) dalam sebuah dialog. Sebagai contoh adalah komunikasi via elektronik mail. Dan dibawah ini merupakan beberapa hal netiket pada komunikasi dengan menggunakan email.

a. Jangan terlalu banyak mengutip.

Jika harus mengutip pesan seseorang dalam jawaban e-mail, usahakan menghapus bagian-bagian yang tidak perlu, dan hanya menjawab bagian yang relevan saja. Pesan yang terlalu panjang memakan file yang besar yang membuat loading semakin lama.

b. Perlakuan e-mail secara pribadi

Jika seseorang mengirim informasi atau gagasan kepada anda secara pribadi (*private message*), Anda tidak sepatutnya mengirim/menjawabnya kembali ke dalam forum umum, karena pada dasarnya email adalah pesan pribadi.

c. Hati-hati dalam penggunaan huruf capital

Karena penggunaan karakter huruf bisa dianalogikan dengan suasana hati si penulis. Huruf kapital mencerminkan penulis yang sedang emosi, marah atau berteriak. Tentu sangat tidak menyenangkan tatkala Anda dihadapkan dengan lawan bicara yang penuh dengan emosi bukan? Walau begitu, ada kalanya huruf kapital dapat digunakan untuk memberi penegasan maksud. Tapi yang harus dicatat, gunakanlah penegasan maksud ini secukupnya saja, satu-dua kata dan jangan sampai seluruh kalimat/paragraf.

d. Jangan membicarakan orang lain

Jangan membicarakan orang atau pihak lain, apalagi kejelekannya. Berhati-hatilah terhadap apa yang ditulis. E-mail mempunyai fasilitas yang bernama "Forward", yang mengijinkan si penerima untuk meneruskan pesan tersebut kepada orang lain.

e. Jangan menggunakan CC

Jika ingin mengirim email ke sejumlah orang (misalnya di mailing-list), jangan cantumkan nama-nama pada kolom CC, jika kita melakukan hal tersebut semua orang yang menerima email kita bisa melihat alamat-alamat email orang lain. Umumnya seseorang tidak suka jika alamat emailnya dibebaskan didepan umum. Selalu gunakan BCC (*Bind Carbon Copy*), dengan cara ini setiap orang hanya bisa melihat alamat emailnya sendiri.

Komite Etika Berinternet

Seolah menjadi penengah di tengah wacana revisi UU ITE, Kementerian Komunikasi dan Informatika pun membentuk Komite Etika Berinternet atau *Net Ethics Committee (NEC)* untuk menjaga ruang digital yang bersih, sehat, beretika dan produktif.

Komite ini diharapkan dapat merumuskan panduan praktis mengenai budaya dan etika menggunakan internet dan media sosial, yang berlandaskan asas kejujuran, penghargaan, kebajikan, kesantunan dan menghormati privasi, individu serta data pribadi orang lain. Panduan praktis itu diharapkan bisa mendorong peningkatan literasi digital masyarakat, yang berkaitan dengan kecakapan menggunakan instrumen digital dan kemampuan merespons arus informasi. Komite Etika Berinternet ini beranggotakan berbagai pemangku kepentingan yang berasal dari unsur, Kemkominfo, Kementerian dan Lembaga terkait, pegiat literasi digital, akademisi, tokoh masyarakat dan tokoh agama, kelompok kepemudaan, dunia usaha, serta pemangku kepentingan lain yang terkait.

Komite Etika Berinternet ini muncul setelah Indonesia berada di peringkat rendah di kawasan Asia Pasifik dalam tingkat peradaban ruang digital, menurut survei salah satu raksasa teknologi. Dalam survei tersebut, Indonesia berada di peringkat 29 dari 32 negara yang menjadi subjek studi. Skor peradaban ruang digital ini dipengaruhi oleh, antara lain, tingkat penyebaran hoaks, perundungan siber dan ujaran kebencian. Diharapkan dengan adanya arahan dari komite ini, maka ruang digital Indonesia menjadi bersih, sehat, beretika, sopan santun, produktif dan mampu memberikan rasa keadilan bagi masyarakat. Komite ini juga akan mendorong pelaksanaan panduan praktis terkait budaya serta etika berinternet dan bermedia sosial bersama dengan seluruh ekosistem *multi-stakeholders*.

4.4 Etika di Dunia Maya Menurut UU ITE

Sejak awal peradaban, manusia selalu termotivasi memperbaharui teknologi yang ada. Hal ini merupakan perkembangan yang hebat dan terus mengalami kemajuan. Dari semua kemajuan yang signifikan yang dibuat oleh manusia sampai saat ini, mungkin hal yang terpenting adalah perkembangan internet. Pemakai internet telah mengalami kemajuan yang sangat signifikan dalam beberapa tahun belakangan ini. Jumlah paket data yang mengalir lewat internet, telah mengalami peningkatan yang dramatis.

Dan sebagaimana dunia nyata, internet sebagai dunia maya juga banyak mengandung tangan-tangan usil, baik untuk mendapat keuntungan materi maupun sekedar iseng, dan untuk mengantisipasi hal tersebut maka perlu dibuatkan suatu aturan-aturan atau etika beraktifitas dalam dunia maya tersebut, Beberapa alasan mengenai pentingnya etika dalam dunia maya adalah sebagai berikut:

- a. Bahwa pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adatistiadat yang berbeda-beda. Bahkan dalam suatu negara

pun tentunya masing-masing pribadi memiliki sifat, cara berbicara, menulis, dan rasa humor yang berbeda.

- b. Pengguna internet merupakan orang-orang yang hidup dalam dunia *anonymous*, yang tidak mengharuskan pernyataan identitas asli dalam berinteraksi. Hal ini membuat kita tidak mengenal dalam arti kata yang sesungguhnya atau bahkan satu pengguna dunia maya mungkin tidak akan pernah bertatap muka dengan pengguna yang lain.
- c. Berbagai macam fasilitas yang diberikan dalam internet memungkinkan seseorang untuk bertindak tidak etis atau suka iseng dengan melakukan hal-hal yang tidak seharusnya dilakukan.
- d. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat dan memungkinkan masuknya “penghuni” baru di dunia maya tersebut. Mungkin saja penghuni baru tersebut tidak mengetahui bagaimana seharusnya bergaul dengan baik dan benar. Untuk itulah perlu diberikan pemahaman agar memahami etika berinternet.

Perkembangan teknologi komunikasi yang semakin pesat juga tersebut memberikan kemudahan untuk semua orang dalam mendapatkan informasi ataupun menyebarkannya melalui media sosial. Untuk menyeimbangi perkembangan tersebut, sudah seharusnya dalam praktik komunikasi sendi-sendi etika juga harus dijaga eksistensinya. Hal ini berkaitan dengan bagaimana para pengguna media sosial tersebut memanfaatkan kecanggihan ini untuk hal yang positif serta bertanggung jawab saat berkomunikasi secara daring. Berdasarkan hasil survei APJII 2019-2020 untuk pengguna internet, saat ini penetrasi di Indonesia berjumlah 73,7 persen dimana sebelumnya pada tahun 2018 mencapai 64,8 persen. Perkembangan pengguna internet tersebut juga meningkatkan pengguna aktif di media sosial karena sebagian besar pengguna internet di Indonesia akan mengakses media sosial.

Beberapa kasus hoaks dan pelanggaran etika sebenarnya sudah terjerat pada hukum UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan diseret ke pengadilan untuk diproses hanya saja belum bisa memberikan efek jera untuk publik. Padahal disini UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik memiliki wewenang yang kuat untuk mengatur publik terkait etika praktik komunikasi ketika di media sosial. Selain Undang-undang, pihak kepolisian juga mengambil alih untuk menertibkan masyarakatnya di dunia maya dengan program polisi virtual.

Direktorat Tindak Pidana Siber Bareskrim Polri mulai mengaktifkan polisi virtual pada Rabu 24 Februari 2021 untuk mengawasi aktivitas warganet di jejaring dunia maya. Polisi virtual adalah kegiatan pelacakan unggahan tulisan atau gambar yang berpotensi melakukan pelanggaran pidana. Fungsi polisi virtual adalah menegur masyarakat yang mengunggah aktivitas yang berpotensi melanggar UU ITE serta memberi edukasi kepada masyarakat terkait UU ITE.

Namun kenyataannya dari program polisi virtual ini malah mendapat kritik dan polemik dimasyarakat yaitu dengan adanya polisi virtual dianggap akan membuat orang ketakutan untuk berpendapat karena ancaman UU ITE, polisi virtual juga dianggap tidak menyelesaikan polemik karena ketika melakukan kritik terancam dijera UU ITE, serta adanya virtual police tidak serta merta bisa menjadi solusi untuk memperbaiki etika warganet di media sosial.

Melihat hal tersebut seharusnya masyarakat bisa lebih terbuka dengan program pemerintah karena hal tersebutlah yang bisa memperbaiki etika dalam praktik komunikasi diruang lingkup media sosial. Ketika ada hukum yang mengatur hal tersebutlah yang bisa menertibkan komunikasi yang ada di dunia maya agar teratur sehingga tidak merugikan siapapun. Apabila hal tersebut dibiarkan tanpa adanya hukum dan oknum kepolisian yang mengatur akan menyebabkan hoaks ada dimana-mana seperti kasus hoaks vaksin Sinovac dari hal tersebut akan merugikan negara karena apabila publik terhasut maka berkurang pula kepercayaan publik kepada program vaksin yang dilakukan oleh pemerintah, serta orang akan semena-mena dalam berpendapat tanpa memperhatikan etika dalam praktik komunikasinya.

Masalah etika dalam praktik komunikasi di media sosial yang terbilang bebas akan semakin berlanjut dan merugikan publik apabila masyarakat juga tidak terbuka dengan program pemerintah itu sendiri. Diperkirakan polemik ini terjadi karena masyarakat kurang mendapat informasi mengenai program polisi virtual tersebut dan mengenai hukum UU ITE, serta harapannya pemerintah dan pihak kepolisian bisa lebih memberikan edukasi mengenai program tersebut dan lebih memberikan perhatian yang lebih kepada publiknya dengan terus memataui perkembangan di media sosial karena ketika publik selalu diterpa dengan berita hoaks dan juga kebebasan mengemukakan pendapat tanpa adanya etika akan memberikan efek buruk untuk perkembangan negara itu sendiri.

BAB V

CYBER CRIME

5.1 Definisi *Cyber Crime*

Seiring dengan perkembangan zaman, manusia berhasil menemukan berbagai macam teknologi yang berguna untuk kehidupan sehari-hari. Telah banyak inovasi teknologi yang kini hadir di tengah masyarakat. Hal ini diciptakan semata-mata untuk memenuhi kebutuhan sehari-hari manusia. Hadirnya teknologi juga memiliki pengaruh besar dalam kehidupan sehari-hari manusia. Hampir dapat dipastikan setiap orang kini juga telah bergantung dengan teknologi. Pasalnya, setiap hari kita memerlukan teknologi untuk menjalani aktivitas sehari-hari. Salah satu perkembangan teknologi yang sangat membantu dalam memenuhi kebutuhan sehari-hari ialah internet. Adanya teknologi ini telah berhasil memudahkan manusia untuk mengetahui beragam informasi dan menghubungkan dengan manusia lainnya di berbagai belahan dunia. Meski begitu, tidak jarang ada oknum yang memanfaatkan perkembangan teknologi untuk melakukan tindak kejahatan atau yang biasa disebut dengan *cyber crime*.

Cyber crime adalah tindak kejahatan yang dilakukan secara online. Kejahatan ini tidak mengenal waktu dan tidak pilih-pilih target. Bisa terjadi pada individu atau perusahaan di mana pun berada. Menurut *Organization of European Community Development* (OECD), *cyber crime* adalah semua bentuk akses ilegal terhadap suatu transmisi data. Itu artinya, semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam suatu tindak kejahatan. *The Prevention of Crime and The Treatment of Offenders* di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal tentang *cyber crime*:

1. ***Cybercrime dalam arti sempit*** disebut *computer crime*, yaitu perilaku ilegal/melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses oleh komputer.
2. ***Cybercrime dalam arti luas*** disebut *computer related crime*, yaitu perilaku ilegal/melanggar yang berkaitan dengan sistem komputer atau jaringan. Dari beberapa pengertian di atas, *cyber crime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Tujuan *cyber crime* sendiri beragam. Bisa sekedar iseng, sampai kejahatan serius yang merugikan korbannya secara finansial.

Dalam praktiknya, *cyber crime* bisa dilakukan seorang diri atau melibatkan sekelompok orang. Para pelaku *cyber crime* tentu adalah orang yang sudah ahli dalam berbagai teknik *hacking*. Bahkan, tak jarang sebuah aksi *cyber crime* dilakukan dari berbagai tempat berbeda di waktu bersamaan. Banyak contoh aksi *cyber crime* yang masih terjadi. Anda tentu telah mendengar informasi bahwa beberapa waktu yang lalu kejahatan online ini menimpa salah satu e-commerce terbesar di Indonesia. Pelaku meretas server perusahaan tersebut, dan berhasil mencuri jutaan data pelanggan. Mulai nama, nomor handphone, hingga alamat. Semua data tersebut bisa saja diperjualbelikan demi keuntungan pelaku. Hal ini tentu menjadi pukulan bagi citra perusahaan sekaligus kerugian bagi para pelanggannya.

Metode Cyber Crime

1. *Sniffing*
2. *Destructive device*
3. *Password Cracker*
4. *Distributed Denial of Attacks (DDoS)*
5. *Spoofing*

Motif Cyber Crime

Motif pelaku kejahatan di dunia maya (*cyber crime*) pada umumnya dapat dikelompokkan menjadi dua kategori, yaitu:

1. **Motif intelektual**, yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi. Kejahatan dengan motif ini pada umumnya dilakukan oleh seseorang secara individual.
2. **Motif ekonomi, politik, dan kriminal**, yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain. Karena memiliki tujuan yang dapat berdampak besar, kejahatan dengan motif ini pada umumnya dilakukan oleh sebuah korporasi.

Faktor Penyebab Munculnya Cyber Crime

Jika dipandang dari sudut pandang yang lebih luas, latar belakang terjadinya kejahatan di dunia maya ini terbagi menjadi dua faktor penting, yaitu:

1. Faktor Teknis

Dengan adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan pihak yang satu lebih kuat daripada yang lain.

2. Faktor Sosial ekonomi

Cyber crime dapat dipandang sebagai produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan. Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Melihat kenyataan seperti itu, *cyber crime* berada dalam skenario besar dari kegiatan ekonomi dunia.

5.2 Jenis-Jenis *Cyber Crime*

1. *Identity Theft*

Sesuai namanya, *identity theft* adalah jenis *cyber crime* berupa aksi pencurian identitas. Pelaku *identity theft* akan melakukan teknik peretasan pada website korban. Mereka akan mengakses server website untuk mendapatkan informasi pribadi yang tersimpan. *Identity theft* akan cenderung menasar toko online, website membership dan jenis website lain yang menggunakan data pelanggan dalam proses layanannya.

Selain itu, *identity theft* juga dapat terjadi saat Anda mengakses situs abal-abal. Hal ini terjadi ketika Anda memberikan data pribadi padahal situs itu sebenarnya milik peretas. Contoh kasus yang kerap terjadi adalah pencurian identitas menggunakan sayembara online. Tergiuir iming-iming hadiah yang besar, korban mengisi data diri di sebuah website. Ternyata, undian sayembara tidak pernah ada. Namun, data diri korban sudah terlanjur dimiliki pelaku kejahatan.

2. *Carding*

Carding adalah jenis *cyber crime* yang berupa pembobolan kartu kredit. Pelaku kejahatan mencuri data informasi kartu kredit, dan menggunakannya untuk kepentingan pribadi. Bagaimana pelaku bisa melakukan *carding*? Ada banyak cara, bisa dengan phishing, memasang malware di toko online, atau membeli informasi dari gelap internet. Dampak dari *carding* cukup merugikan. Sebab, jika tidak cepat

disadari, pemilik kartu kredit harus membayar tagihan besar atas belanja yang tidak dilakukan. Kadang, dalam jumlah yang sangat besar.

3. Corporate Data Theft

Corporate data theft mirip dengan *identity theft*. Bedanya, jenis *cyber crime* ini menyangkut data perusahaan. Pelaku meretas situs perusahaan, kemudian mencuri data-data yang penting. Data perusahaan yang berhasil didapatkan bisa dimanfaatkan untuk kepentingan pribadi, misalnya untuk bisa mengaksesnya tanpa hak. Bisa juga, data tersebut dijual di pasar gelap dengan harga tinggi.

Bentuk kejahatan online ini pernah dialami oleh perusahaan-perusahaan besar. Salah satunya, Canva. Situs desain grafis ini berhasil diretas sehingga 139 juta data pelanggan terancam. Artinya, dalam satu aksi saja, pencuri bisa mendapatkan banyak data untuk digunakan melakukan tindak kejahatan.

4. Cyber Extortion

Istilah *cyber extortion* mungkin masih asing bagi Anda. Padahal, jenis *cyber crime* berupa pemerasan ini cukup sering terjadi. Kejahatan online ini bisa menimpa perusahaan atau pribadi. Modusnya, pelaku akan meminta uang sebagai tebusan atas data penting yang telah dicuri. Kasus *cyber extortion* yang marak saat ini adalah penggunaan *ransomware*. Malware ini masuk ke perangkat korban dan mengendalikan data di dalamnya. Pemilik tidak dapat mengakses data tersebut tanpa menggunakan sandi dari pelaku kejahatan. Sedangkan untuk mendapatkan sandi tersebut, harus ada uang tebusan yang dibayarkan terlebih dahulu. Banyak perusahaan terkenal di dunia yang menjadi korban kejahatan ini, seperti Nokia, Domino, dan Freedly. Bahkan, pada kasus Domino, peretas meminta tebusan 30.000 Euro agar data 650.000 pelanggan Domino tidak disebarluaskan.

5. Cyber Espionage

Cyber espionage adalah jenis *cyber crime* yang memata-matai target tertentu, seperti lawan politik, kompetitor suatu perusahaan atau bahkan pejabat negara lain. Pelaku menggunakan teknologi canggih untuk memata-matai secara online. *Cyber espionage* biasa dilakukan dengan memanfaatkan *spyware*. Dengan aplikasi yang ditanam di komputer korban, semua aktifitas dan data penting bisa diakses tanpa disadari. Sebagai contoh, kejahatan *cyber espionage* ini pernah menimpa Barack Obama. Saat itu *spyware* digunakan untuk mencuri data sensitif terkait kebijakan luar negeri Amerika.

Aksi Cyber Crime

Setelah mengetahui jenis-jenis *cyber crime*, apa saja aksi yang biasa dilakukan oleh pelaku *cyber crime*. Ini dia bentuk aksinya:

1. Serangan Malware

Malware adalah aksi *cyber crime* dengan menggunakan software yang menyusup ke perangkat korban. Aksi ini sering berhasil mencapai tujuan karena korban tidak tahu ada malware menyerang. Artinya, aksi kejahatan bisa dilakukan dengan leluasa.

Biasanya malware masuk melalui email, pesan di instant messaging atau saat akses ke website berbahaya. Tak jarang juga malware masuk melalui tema atau plugin WordPress yang diinstal ke sistem website Anda.

Saat berada di perangkat korban, malware bisa melakukan apapun sesuai program yang dijalankan. Misalnya, mencuri data, memata-matai perilaku online korban hingga menghapus data yang diinginkan.

2. Phishing

Phishing masih menjadi aksi *cyber crime* favorit hacker. Alasannya, kejahatan online ini terbukti masih efektif, terutama untuk pencurian identitas. Menurut sebuah laporan, aksi *cyber crime* 67% bermula dari phishing. Data yang menjadi tujuan phising berupa data pribadi (nama, usia, dan alamat), data akun (username dan password) dan data finansial (nomor kartu kredit dan kode sandi). Langkah phising kerap berhasil karena pelaku phising menyamar menjadi pihak yang berwenang atau lembaga resmi, sehingga korban tidak merasa curiga. Contoh kasus phising yang terkenal adalah penggunaan PayPal untuk aksi kejahatan. Bagaimana aksi tersebut dijalankan? Pelaku mengirimkan email kepada korban dengan berpura-pura sebagai pihak PayPal. Dalam isi email tersebut, pelaku menyatakan bahwa akun korban telah “dibatasi” sebagai akibat dari pelanggaran kebijakan.

Lewat email tersebut, pelaku meminta korban untuk memperbarui akun mereka. Sebuah tautan yang diberikan mengarahkan korban ke situs palsu. Nah, saat korban memasukkan data diri sesuai petunjuk, pelaku berhasil mendapatkan informasi yang diinginkan. Itulah kenapa kita harus lebih jeli dengan email yang Anda terima. Sebagai contoh, saat mendapat email dengan alamat panjang berisi perpaduan huruf dan angka. Selain itu, jangan asal mengklik link di dalam email. Jadi, Anda tidak mudah masuk ke perangkap pelaku phising.

3. Deface Website

Deface adalah upaya mengubah tampilan sebuah website tanpa hak. Aksi *cyber crime* ini pernah heboh di Indonesia karena menimpa website lembaga pemerintah, KPU. Dalam aksinya, pelaku yang menyerang situs resmi KPU Kabupaten Seluma membuat tampilan depannya berubah. Pelaku juga menuliskan bahwa situs tersebut telah berhasil diretas oleh suatu kelompok. Selain mengubah tampilan website, aksi *cyber crime* ini juga sering digunakan untuk mengarahkan korban ke situs lainnya. Sebagai contoh, aksi deface pada website Google di Romania. Meskipun aksi ini sendiri disangkal pihak Google, pengunjung saat itu tidak dapat mengakses situs **google.ro**. Dampak deface sangat serius, terutama bagi bisnis. Kredibilitas online Anda sangat dipertaruhkan. Alasannya, website Anda akan dianggap tidak memiliki perlindungan yang baik bagi pengunjung.

4. Serangan DDoS

DDoS attacks adalah aksi *cyber crime* dengan target serangan ke server. Caranya, dengan membuat traffic sebuah server terlalu tinggi sampai tidak bisa mengatasi permintaan akses dari pengguna. Aksi DDoS berupaya membuat server website down, sehingga pengunjung tidak bisa mengaksesnya. Bisa dibayangkan bagaimana jika hal ini terjadi pada toko online kita? Tentu sangat merugikan, ya?

Kenyataannya, DDoS sendiri merupakan salah satu serangan yang populer digunakan oleh hacker. Alasannya, teknik DDoS dianggap cukup sederhana untuk dijalankan. Seperti halnya deface, serangan DDoS sangat mengancam reputasi online yang dibangun. Kepercayaan konsumen terhadap sebuah bisnis yang mengalami down tentu akan terpengaruh.

Sayangnya, serangan DDoS memang bisa menimpa siapa saja, termasuk salah satu media terbesar di dunia, BBC. Saat itu, serangan yang terjadi mengakibatkan hampir semua layanan BBC lumpuh. Seluruh domain milik BBC tidak bisa diakses. Parahnya, layanan On-Demand dan radio juga ikut mati. Jadi, kerugian finansial akibat DDoS tersebut cukup serius.

5. Hacking

Hacking adalah istilah *cyber crime* yang cukup umum. Aksi ini dilakukan dengan cara mengakses sistem komputer korban tanpa hak. Pada dasarnya hacker akan menggunakan keterampilan yang dimiliki untuk melakukan berbagai aksi *cyber crime*. Mulai merusak sistem, mencuri data pribadi, hingga mengekspos data yang diperoleh ke publik. Aksi hacking tidak selamanya bertujuan mendapatkan

keuntungan finansial. Banyak juga hacker yang melakukannya sekedar untuk memamerkan keahlian yang dimiliki. Contoh aksi hacking yang kerap terjadi adalah pembobolan kata sandi. Langkah inilah yang menjadi titik awal hacker melakukan tindak kejahatan selanjutnya. Beberapa waktu yang lalu, dua media besar di Indonesia pernah menjadi korban hacking. Para hacker berhasil menembus sistem keamanan website media tersebut dan berhasil menghapus beberapa berita yang pernah dimuat.

6. Social Engineering

Sepanjang tahun 2019, tercatat sebanyak 2300 kasus *social engineering* yang dilaporkan kepada pihak berwajib. Mayoritas kasus yang dilaporkan berujung pada penipuan online. *Social engineering* adalah aksi *cyber crime* dengan cara memanipulasi korbannya. Pelaku biasanya melakukan aksi dengan secara langsung menghubungi korban. Lewat pendekatan yang dilakukan, tanpa sadar, korban memberikan informasi yang diinginkan pelaku.

Sebagai contoh, aksi *social engineering* ini kerap menimpa pengguna ojek online. Modus yang dijalankan adalah dengan menelpon korban dan menanyakan kode OTP (*One Time Password*). Kode ini cukup penting untuk dapat mengambil alih akun korban. Sebenarnya kode OTP yang berasal dari sistem ojek online bersifat rahasia. Namun, tak jarang korban mau memberikan informasi tersebut dengan teknik phishing. Nah, jika pelaku berhasil mengakses akun korban, dompet digital atau kartu kredit yang terhubung dengan akun tersebut bisa dimanfaatkan.

7. Exploit Kit

Saat ini pelaku *cyber crime* semakin cerdas dalam melakukan serangan. Salah satunya dengan menggunakan ‘senjata’ exploit kit yang mudah didapat. *Exploit kit* adalah program untuk menyerang komputer dengan sistem keamanan rendah. Tujuannya, menyusup ke komputer korban dan memanfaatkannya. Tercatat 50% serangan hacker menggabungkan metode serangan dengan menggunakan *exploit kit*. Penggunaan *exploit kit* ini biasanya dimulai dengan aksi phishing lewat link email, popup, ataupun iklan. Jika korban sudah berhasil dikelabui dengan mengakses link yang diberikan, *exploit kit* akan mulai menguasai perangkat korban.

Lalu, bagaimana cara kerja *exploit kit*? Pertama, pelaku akan berusaha agar exploit kits yang disiapkan bisa masuk ke komputer korban. Setelah itu, program akan mencari kelemahan sistem pada komputer tersebut. Jika menemukan celah, exploit kits akan memanfaatkannya untuk mendownload malware. Program inilah yang akan

digunakan pelaku untuk mengendalikan komputer korban. Karena *exploit kit* bekerja secara diam-diam, Anda mungkin akan sulit mengetahui saat diserang. Maka dari itu, Anda perlu rajin mengupdate perangkat dan jangan sembarangan membuka link.

8. Pembajakan

Pembajakan adalah aksi menggandakan karya orang lain demi keuntungan pribadi. Di dunia online, pembajakan juga merupakan *cyber crime* yang kerap terjadi. Mulai dari pembajakan software berbayar hingga buku elektronik. Salah satu aksi *cyber crime* terkenal dalam hal pembajakan dilakukan oleh KingdotCom. Dalam aksi itu, mereka menayangkan acara televisi secara ilegal di websitenya. Tindakan ini menyebabkan kerugian finansial bagi pemilik stasiun TV karena sepiunya penonton yang membayar tayangannya. Sementara itu, pelaku mendapatkan keuntungan hingga lebih dari \$175 juta. Di Indonesia, aksi *cyber crime* ini cukup masih meresahkan. Faktanya, pemakaian software bajakan di Indonesia mencapai 83% dan merupakan salah satu yang tertinggi di Asia Pasifik. Padahal, software bajakan bisa saja mengandung malware yang justru membahayakan.

9. Penipuan Online

Penipuan online atau online scam merupakan aksi *cyber crime* yang juga perlu Anda waspadai. Sebab, bentuk penipuan yang terjadi bisa bermacam-macam dan platformnya juga bisa apa saja. Bisa marketplace atau media sosial. Online scam sendiri tidak hanya terjadi pada individu sebagai targetnya. Sebab pelaku online scam bisa berupa website toko online palsu, perusahaan investasi yang menjanjikan keuntungan besar dalam waktu cepat. Bahkan, online scam bisa terjadi di lingkup negara hingga internasional. Contoh kasus online scam lain yang cukup terkenal adalah OneCoin, salah satu mata uang cryptocurrency. Meskipun awalnya tampak seperti mata uang digital yang aman, pengguna baru sadar bahwa OneCoin hanyalah scam. Apalagi ditambah dengan hilangnya founder mereka secara mendadak. Alhasil, pengguna dirugikan atas investasi yang dilakukan.

10. Spamming

Spamming adalah aksi *cyber crime* dengan menyebarkan email spam secara massal. Isi email spam pun beragam, contohnya penawaran produk yang tidak jelas. Menurut riset, tingkat spam email dalam sebulan bisa mencapai 85%. Hal ini tentu cukup mengkhawatirkan, terutama bagi Anda yang menggunakan email untuk bisnis. Bisa-bisa dengan banyaknya spam yang diterima, ruang penyimpanan penuh, dan email penting dari klien justru tidak bisa masuk. Apalagi, kegiatan spam email masih

bisa terjadi mengingat aksi pencurian data hacker juga terus muncul. Ditambah dengan kasus adanya penjualan data oleh pihak tidak bertanggung jawab.

Kerugian yang Ditimbulkan dari *Cyber Crime*?

Setiap tindak kejahatan di dunia maya tentu saja mengakibatkan kerugian yang dirasakan oleh korbannya. Inilah beberapa kerugiannya:

1. Reputasi Online Bisa Terancam

Kerugian yang ditimbulkan dari *cyber crime* adalah reputasi online bisa terancam. Apalagi jika kita menggunakan aktivitas online untuk berbisnis. Jika menjadi korban, bisa jadi bisnis online kita akan kehilangan kepercayaan pelanggan. Katakanlah, toko online kita terkena hacking. Pengunjung akan merasa tidak aman untuk mengunjungi situs kita, sehingga bisa jadi ia memutuskan untuk tidak lagi berbelanja dari toko kita. Hal ini sangat merugikan bagi kita.

2. Kehilangan Data Penting

Salah satu kerugian terbesar *cyber crime* adalah kehilangan data. Hal ini bisa terjadi baik pada akun pribadi maupun website yang menyimpan data pribadi pelanggan. *Cyber crime* selalu mencari celah agar dapat mencuri data penting dan menggunakannya untuk berbagai kepentingan. Salah satunya untuk tujuan pemerasan atau menjualnya di pasar gelap. Sebagai contoh, Blackbaud, salah satu pembuat perangkat lunak manajemen keuangan pernah menjadi korban pencurian data rahasia. Perusahaan ini melaporkan bahwa situs mereka telah diretas. Peretas berhasil mencuri data tentang siswa dan alumni dari 10 Universitas di Inggris, AS, dan Kanada. Dampaknya, pelaku dapat menyebarluaskan data pribadi siswa dan alumni. Mulai nama, hingga nomor jaminan sosial.

3. Kerusakan Software dan Sistem Komputer

Kerusakan software dan program juga bisa terjadi akibat ulah cyber crime. Salah satu yang membuat heboh adalah serangan Ransomware WannaCry yang menyerang berbagai website pemerintah. Saat itu, serangan yang terjadi menyebabkan banyak perangkat yang tidak bisa diakses. Aksi ini terutama terjadi pada sistem operasi yang rentan, baik yang sudah lawas maupun yang versi bajakan. Itulah kenapa penting bagi Anda untuk selalu memperhatikan keamanan sistem di komputer Anda. Salah satunya, dengan terus mengupdate antivirus dan versi sistem operasi yang digunakan.

4. Kehilangan Sejumlah Uang

Kerugian finansial juga menjadi dampak terbesar dari kegiatan *cyber crime*. Bentuk aksinya bisa bermacam-macam, mulai dari phishing hingga extortion. Tak hanya dialami oleh individu, maupun perusahaan, kehilangan sejumlah uang akibat tindakan *cyber crime* juga dialami oleh negara. Berdasarkan penelitian Frost & Sullivan yang diprakarsai Microsoft pada 2018, kejahatan siber di Indonesia bisa menyebabkan kerugian mencapai Rp 478,8 triliun atau 34,2 miliar dollar AS. Jumlah itu tergolong sangat fantastis.

5.3 Bagaimana Mencegah Terjadinya *Cyber Crime*

Berikut ini tips bagaimana mencegah terjadinya *cyber crime* :

1. Gunakan Hosting yang Aman

Bisa dikatakan inilah langkah penting sebagai upaya melindungi website kita. Layanan hosting dengan perlindungan keamanan khusus dapat membantu kita mencegah aksi *cyber crime*. Salah satunya adalah Niagahoster yang memiliki fitur Imunify360. Fitur ini mampu memberikan proteksi dari serangan malware. Beberapa diantaranya dengan adanya Proactive Defense untuk memblokir ancaman secara realtime dan Patch Management yang akan mengupdate server ke versi terbaru secara otomatis.

2. Rajin Update

Rajin melakukan update bisa menjadi cara terhindar dari *cyber crime*. Baik update pada sistem operasi maupun pada sistem manajemen di website kita. Sebagai contoh jika kita menggunakan Windows, kita akan selalu mendapat notifikasi adanya update. Jika memungkinkan, segera lakukan update yang direkomendasikan. Hal ini berlaku juga bagi pengguna MacOS maupun Linux. Selain itu, lakukan update pada WordPress setiap kali ada versi terbaru. Kita bisa melakukannya secara langsung melalui halaman dashboard WordPress atau menggunakan langkah manual. Selain meningkatkan keamanan, kita juga akan mendapatkan fitur terbaru yang lebih canggih. Tidak hanya itu, jangan lupa untuk selalu melakukan update tema, dan plugin website WordPress kita. Kita bisa melakukannya sekaligus atau bertahap sesuai dengan kemampuan server kita.

3. Pasang SSL

Apakah kita pernah memperhatikan icon gembok yang berada sebelum URL Website? Nah, itu adalah tanda bahwa website tersebut menggunakan SSL. Dengan melihat icon gembok tersebut, pengunjung situs kita akan lebih percaya dengan

website kita. Hal ini karena pengunjung meyakini bahwa website kita memang aman untuk dikunjungi, karena telah mengaktifkan SSL. Sebenarnya, alasan utama mengapa kita harus memasang SSL adalah karena sertifikat SSL menjamin keamanan yang berlapis. SSL menjamin bahwa setiap paket data yang ditukar antara website kita dengan pengunjung yang mengaktifkan SSL, akan dilindungi oleh teknik enkripsi paling mutakhir. Hal ini tentu saja dapat membuat kita terhindar dari tindakan pencurian data yang dilakukan oleh pihak tak diinginkan. Informasi apapun yang didapatkan tidak akan terbaca, karena teknik enkripsi tersebut.

4. Terapkan 2-Factor Authentication

Sebagian kita mungkin sudah mengenal 2FA. 2-Factor Authentication (2FA) adalah metode keamanan yang memungkinkan website melakukan verifikasi pengguna secara real-time dengan kode unik yang dibuat saat itu juga. 2FA ini merupakan metode populer yang sudah diterapkan oleh perusahaan ternama, seperti Google, Facebook, Yahoo, dan lain sebagainya. Metode 2FA ini mengharuskan pengguna tidak hanya memasukkan username dan password mereka. Namun, juga akan diminta memasukkan kode OTP (*one-time password*) yang dikirimkan melalui SMS atau e-mail.

5. Gunakan Password Unik

Apakah kita termasuk yang masih membuat password dengan menggunakan tanggal lahir? Sebaiknya kita harus mengubahnya mulai dari sekarang. Password seperti tanggal lahir, nomor telepon, dan nomor rumah adalah tipe-tipe password yang mudah ditebak. Hal ini dapat membuat hacker semakin cepat untuk meretas akun kita. Gunakan password dengan kombinasi angka, huruf, dan juga simbol. Kombinasi password digunakan untuk menghindari serangan *cyber crime*. Jika kita kesusahan mengingat password kombinasi yang dibuat, aplikasi semacam LastPass tentu bisa membantu kita menggunakan password unik.

6. Hati-Hati dalam Membuka Email

Email menjadi salah satu media pelaku *cyber crime* menjalankan aksinya. Pelaku mengirimkan email kepada korban dengan berpura-pura sebagai pihak berwenang. Ada banyak macam isi email yang digunakan untuk melakukan kejahatan online. Salah satunya dengan memberikan link yang mengarahkan korban untuk mengkliknya. Jika tidak hati-hati, kita bisa terperangkap dalam rencana jahat yang sudah dipersiapkan oleh pelaku melalui link tersebut. Bisa jadi akan mendownload aplikasi

yang disusupi malware. Jika sudah curiga, kita bisa melakukan verifikasi kepada perusahaannya langsung untuk memastikan apakah email tersebut kredibel atau tidak.

Cara Penanggulangan *Cyber Crime*

1. Membuat Undang-Undang

Cara paling elegan agar tindakan *cyber crime* tidak semakin merajalela adalah dengan membuat peraturan yang dimasukkan kedalam Undang-undang. Penegakan hukum nantinya bakal membuat para pelaku *cyber crime* berpikir panjang sebelum melakukan tindakan kriminal karena dasar hukumnya jelas. Di Indonesia, aturan mengenai *cyber crime* saat ini menginduk pada UU ITE. Namun, sayangnya pola penindakannya masih belum maksimal dan seringkali terkesan dipaksakan. Penegakan hukum di ranah dunia maya memang masih abu-abu karena dokumen elektronik sendiri belum bisa dijadikan sebagai barang bukti oleh KUHP.

2. Membentuk Lembaga Penanganan Khusus

Kita tentu tidak asing dengan Divisi Cyber Crime Mabes Polri. Saat ini kita memerlukan lembaga khusus seperti itu untuk menangkal dan menyelidiki potensi terjadinya tindak kejahatan di ranah digital. Beberapa negara tercatat sudah mulai menerapkan konsep ini dengan membentuk lembaga khusus yang menangani persoalan *cyber crime*, kendati demikian hal tersebut hanya akan efektif jika diterapkan oleh banyak negara, sehingga tidak ada celah bagi pelaku *cyber crime* dimanapun mereka berada.

3. Memperkuat Sistem

Pengamanan sistem menjadi benteng pertama yang bisa kita andalkan untuk menghindari potensi *cyber crime*. Untuk mengamankan sistem secara mandiri kita bisa menambahkan beberapa add ons seperti Sertifikat SSL pada website, antivirus komputer, hingga melakukan pengamanan fisik pada jaringan untuk memproteksi server. Terlepas dari itu, jika kita memiliki website bisnis, pastikan menggunakan layanan VPS Indonesia dari Qwords.com yang sudah dibekali berbagai teknologi masa kini. Alhasil, kejahatan *cyber crime* seperti malware atau defacing lebih bisa diminimalkan.

DAFTAR PUSTAKA

- Firmansyah, Yoki.2020. Modul Etika Profesi Teknologi Informasi dan Komunikasi. Universitas Bina Sarana Informatika
<http://robby.c.staff.gunadarma.ac.id/Downloads/files/53538/Tinjauan+Umum+etika.pdf>
<https://infokomputer.grid.id/read/12341780/beberapa-sertifikasi-teknologi-informasi-yang-paling-banyak-diburu?page=3>
<https://kominfo.go.id>
http://mertoyoso97.blogspot.com/p/blog-page_17.html
<https://wahjudinsumpeno.wordpress.com/2012/07/16/sertifikasi-profesi/>
<https://www.kompasiana.com/antoniuz2/5b8c843bab12ae21d70bd753/perkembangan-internet-di-dunia-dan-indonesia?page=all>
<https://www.liputan6.com/citizen6/read/2111028/7-keahlian-it-yang-banyak-dicari-hingga-saat-ini>
- Wahyono, Teguh. 2009. Etika Komputer dan Tanggung Jawab Profesional Bidang Teknologi Informasi. Yogyakarta:Andi