

## BAB II

### TINJAUAN MENGENAI PERKEMBANGAN TEKNOLOGI INFORMASI, SERTA REAKSI HUKUM TERHADAPNYA

Seperti yang telah diuraikan pada bab I bahwa penggunaan komputer telah meluas hampir menyentuh seluruh aspek kehidupan masyarakat, maka perlu dicari kesamaan pandangan mengenai apa yang dimaksud dengan komputer, cyber space (dunia maya) serta bagaimana bentuk respon hukum yang dimaksudkan pada penelitian ini.

#### 2.1. PERKEMBANGAN TEKNOLOGI INFORMASI

##### 2.1.1. PERKEMBANGAN KOMPUTER

Kata Komputer berasal dari bahasa latin yaitu *computer* yang berarti menghitung (*to compute*). Menurut *Computer Manual*, komputer adalah suatu alat elektronik yang mampu melakukan beberapa tugas sebagai berikut :<sup>29</sup>

- a. menerima input,
- b. memproses input a quo sesuai dengan programnya,
- c. menyimpan perintah-perintah dan hasil dari pengolahan input,
- d. menyediakan output dalam bentuk informasi.

*An American College Dictionary* terbitan tahun 1961 menerjemahkan kata komputer sebagai berikut :

- a. *One who computes*
- b. *An apparatus for carrying out mathematical operation by mechanical or electrical mean or both :an analog computer performs mathematical operations by transforming data receive and can perform only simpler, linear operation.*<sup>30</sup>

Terjemahan bebas penulis :

- a. Seseorang yang menghitung,

---

<sup>29</sup> Robert H. Blissmer, *Computer Manual : An Introduction to Computer System*, New York : John Wiley and Sons Inc, 1985, bab I.

<sup>30</sup> *The American College Dictionary*, New York, House Inc, 1961, halaman 249.

- b. Suatu perangkat untuk menyelesaikan operasi matematika secara mekanik atau elektrik atau kedua-duanya : suatu komputer analog menampilkan operasi matematika dengan mentransformasikan data penerima dan bisa menampilkan secara sederhana operasi linier.

Terjemahan tersebut diatas menunjukkan bahwa kata *computer* pada masa itu masih cenderung diartikan sebagai suatu alat untuk menjalankan operasi matematika (perhitungan) berdasarkan data-data yang diterima.

Istilah komputer dimana pada mulanya berarti “penghitung”, kemudian berkembang menjadi lebih luas karena istilah *calculator* khusus dipakai untuk mesin hitung, yang asal katanya *to calculate*. Istilah komputer yang semula dipakai untuk alat penghitung suara pemilihan presiden (voting) itu berkembang terus sesuai dengan perkembangan teknologi.<sup>31</sup>

Komputer dalam Pengertian “*The Proposed West Virginia Computer Crimes Act*” adalah :<sup>32</sup>

*“an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similar device.”*

Terjemahan bebas penulis :

“peralatan untuk memproses data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis, atau tipe-setter, sebuah kalkulator tangan atau peralatan serupa lainnya.

<sup>31</sup> Andi Hamzah, *Hukum Pidana yang Berkaitan dengan Komputer*, Jakarta : Sinar Grafika, 1993, halaman 1

<sup>32</sup> Ari Juliano Gema, *Cyber Crime : Sebuah Fenomena di Dunia Maya*, <http://www.theceli.com/dokumen/jurnal/aj/a002.shtml>, diakses tanggal 4 Januari 2008.

Berdasarkan definisi-definisi tersebut di atas, dapat disimpulkan menurut penulis bahwa secara umum pengertian mengenai komputer adalah sebagai seperangkat alat yang bekerjasama satu dengan lainnya untuk menerima data (*input*), mengolah data tersebut dan menyajikannya dalam bentuk hasil pengolahan (*output*) seperti yang diinginkan oleh pengolahnya.

Dalam ilmu komputer dikenal istilah *EDPS (Electronic Data Processing System)*. *EDPS* dapat diartikan sebagai sistem pengolahan data secara elektronik, sedangkan secara non elektronik misalnya menetik sebuah surat dengan mesin tik.<sup>33</sup>

*EDPS* dibagi dalam tiga kelompok :

- a. *Hardware*
- b. *Software*
- c. *Brainware*

*Hardware* adalah segala sesuatu yang berhubungan dengan komponen-komponen komputer itu sendiri. Lebih tepatnya adalah perangkat keras komputer itu sendiri.<sup>34</sup> Perangkat-perangkat keras komputer antara lain adalah monitor, CPU (*Central Processing Unit*), *keyboard*, *printer*, media penyimpanan data misalnya, *hard disk*, *floppy disk*, dan lain-lain.

*Software* atau dalam bahasa Indonesia berarti perangkat lunak, yaitu segala sesuatu yang berhubungan dengan program-program komputer.

*Software* terdiri dari :

- 1) *Operating System*
- 2) Semua paket komputer, misalnya *Word Star*, *Lotus*, *Clipper* dan lain-lain.
- 3) Semua bahasa pemrograman, misalnya BASIC, Pascal dan lain-lain.
- 4) Semua program-program *utility*
- 5) Semua jenis-jenis *game* dan lain-lain.<sup>35</sup>

<sup>33</sup> Mico Pardosi, *Pengenalan Komputer*, Surabaya : Indah, 1996, halaman 11.

<sup>34</sup> *Ibid*, halaman 12.

<sup>35</sup> *Ibid*, halaman 17.

*Brainware* adalah pemakai komputer, pengendali atau *user*. *Brainware* dibagi dalam tiga bagian :

- 1) Operator Komputer, orang yang merawat, menghidupkan dan memasukkan data-data ke dalam komputer
- 2) *Programmer*, orang yang membuat program komputer
- 3) Analis System, orang yang menganalisa suatu perusahaan apakah perusahaan tersebut sudah selayaknya dikomputerisasi atau belum.<sup>36</sup>

Ernest E Keet dalam bukunya *Preventing Piracy* memberikan pengertian tentang *Hardware* serta *Software* komputer sebagai berikut:

*Computer Hardware is in the tangible component of a computer system and Computer Software any or several literary works referred to in the definition of computer program, program description and supporting material.*<sup>37</sup>

Untuk mengoperasikan sebuah komputer maka dibutuhkan suatu program Komputer. Erness memberikan definisi tentang ketiga hal tersebut adalah sebagai berikut:

*A Computer Program is a set of instructions capable, when incorporated in a machine readable medium, of causing a machine having information processing capabilities to indicate, perform or achieve a particular function task or result.*

(Program Komputer adalah serangkaian instruksi-instruksi yang mempunyai kemampuan, ketika ditempatkan pada suatu mesin pembaca, sehingga menyebabkan suatu mesin tersebut mempunyai kemampuan untuk mengolah informasi untuk mengindikasikan, melaksanakan suatu fungsi khusus atau hasil khusus/-Terjemahan bebas oleh penulis)

*A Program description is a complete procedural representation in verbal, schematic or other form, in sufficient detail to determine a set of instruction constituting a corresponding computer program.*

<sup>36</sup> *Ibid*, halaman 16.

<sup>37</sup> Ernest E Keet, *Preventing Piracy*, Addison Wesley, San Juan, 1997, hal 6

(Diskripsi Program adalah Prosedur secara utuh yang ditampilkan dalam bentuk verbal, sematik atau bentuk lain, dalam bentuk yang memenuhi syarat untuk memutuskan serangkaian instruksi/-Terjemahan bebas oleh penulis).

*Supporting material is any material, other than a computer program or a program description, created for aiding the understanding or application of a computer program, for example, problem description and use instructions.* (Materi Penunjang, adalah setiap materi, lain daripada program komputer atau Deskripsi Program yang diciptakan untuk membantu memahami atau penerapan dari program komputer, sebagai contoh diskripsi masalah dan instruksi penggunaan/-Terjemahan bebas oleh penulis)<sup>38</sup>

Dari definisi diatas program komputer merupakan serangkaian instruksi-instruksi/ perintah yang memungkinkan mesin komputer untuk dapat melakukan sebuah pekerjaan untuk menghasilkan sesuatu yang diperintahkan kepadanya.

Suatu program komputer dibuat oleh Progamer dengan menggunakan bahasa program (*Programming Language*) yang terdiri atas Bahasa Tingkat Tinggi (*High Level Language*) seperti Basic, Fortran, RPG, Bahasa Tingkat Rendah (*Lower Level Language*) yang berisi tulisan alphanumeric (*alphanumeric Label*) dan Bahasa Tingkat Paling Rendah (*Lowest Level Language*) yang berisi bahasa binary yang menggunakan dua simbol yaitu 0 dan 1.<sup>39</sup>

Dengan demikian , komputer hanyalah sebuah alat elektronik, dan seperti alat yang lainnya komputer tersebut tidak dapat bekerja dengan sendirinya dan harus ada manusia yang mengoperasikan.

<sup>38</sup> Ibid, hal 7

<sup>39</sup> Michael B Metzger, *Business Law and The Regulatory Environment*, Irwin, Illinois, 1986, hal 1337

## 2.1.2. PERKEMBANGAN INTERNET DAN CYBERSPACE.

### 2.1.2.1. Sejarah dan Perkembangan Internet

Sejarah perkembangan internet dimulai sejak adanya kekhawatiran Amerika Serikat terhadap kemajuan Uni Soviet di bidang teknologi dalam perang dingin setelah usai perang dunia ke dua. Uni Soviet berhasil meluncurkan Sputnik, satelit bumi pertama pada tahun 1957. Kondisi tersebut kemudian mendorong Presiden Eisenhower untuk memerintahkan dibentuknya DARPA (*Defense Research Project Agency*) dengan tujuan merebut kembali supremasi Amerika Serikat di bidang teknologi. Salah satu keinginan utama yang ingin dicapai oleh militer Amerika Serikat pada masa itu adalah mendesentralisasikan komando dan informasi-informasi strategis sehingga sistem pertahanan Amerika Serikat tetap dapat bertahan dan berfungsi dengan baik di tengah-tengah gencarnya serangan yang diarahkan ke target-target militer utama AS. J.C.R. Licklider yang merupakan pemimpin pertama program riset DARPA pada 1962 menyampaikan usulan untuk membangun sebuah sistem komputer yang saling terhubung yang disebut dengan *Jaringan Galactica* yang sangat mirip dengan apa yang dewasa ini disebut dengan internet<sup>40</sup>.

Usaha yang dilakukan Amerika Serikat tersebut untuk mengamankan dan melindungi data-data dan sistem komunikasi yang telah dibangun agar tidak dapat dihancurkan ketika terjadi perang. ARPANET dibangun dengan sasaran untuk membuat suatu jaringan komputer yang tersebar untuk menghindari pemusatan informasi di satu titik yang dipandang rawan untuk dihancurkan apabila terjadi peperangan. Dengan cara ini diharapkan apabila satu bagian dari jaringan terputus, maka jalur yang melalui jaringan tersebut dapat secara otomatis dipindahkan ke saluran lainnya. Hal inilah yang merupakan titik awal perkembangan jaringan antar komputer.

Pada awal 1980-an, ARPANET terpecah menjadi dua jaringan, yaitu ARPANET dan Milnet (sebuah jaringan militer), akan tetapi

---

<sup>40</sup> Arsyad Sanusi, *Hukum Teknologi Dan Informasi* Jakarta, 2004, hal 94.

keduanya mempunyai hubungan sehingga dapat saling berkomunikasi antar jaringan. Jaringan interkoneksi ini disebut DARPA Internet, tapi kemudian disingkat menjadi Internet saja. Kemudian disusul dengan perkembangan teknologi yang memungkinkan dilakukannya transfer data melalui komputer. Pengiriman pesan antar komputer (yaitu dari UCLA ke Universitas Stanford) pertama kali berhasil dilakukan pada tahun 1969 oleh tim yang dipimpin oleh Dr. Kleinrock. Menurut banyak pihak, inilah titik awal lahirnya internet.<sup>41</sup>

Komputer dapat berkomunikasi satu sama lainnya dengan menggunakan suatu bahasa, maka untuk menciptakan sebuah bahasa yang dipahami maka diciptakan sebuah bahasa bersama atau protokol yang dimulai pada tahun tujuh puluhan. Dengan adanya bahasa yang sama tersebut maka jaringan-jaringan komputer yang berbeda dapat saling berkomunikasi satu sama lainnya sehingga lahirlah *internet*. Bahasa bersama inilah yang kita kenal sebagai *Transmission Control Protocol/Internet Protocol* (TCP/IP). Dengan demikian telah terdapat standar yang disepakati bersama sehingga semua jenis komputer yang menggunakan sistem yang berlainan dapat berkomunikasi dengan bahasa yang sama.

Permasalahan yang muncul pada saat internet mulai digunakan adalah bagaimana menemukan sebuah tempat atau situs yang dituju, kemudian pada tahun 1993 InterNIC didirikan untuk menjalankan layanan pendaftaran domain. Pemerintah Amerika Serikat (*White House*) juga mulai menggunakan Internet dan pemerintah Amerika Serikat telah meloloskan peraturan yang disebut *National Information Infrastructure Act*. Penggunaan internet secara komersial dimulai pada 1994 dipelopori oleh perusahaan Pizza Hut, dan Internet Banking pertama kali diaplikasikan oleh First Virtual. Setahun kemudian, CompuServe, America Online, dan Prodigy mulai memberikan layanan akses ke Internet bagi masyarakat umum.<sup>42</sup>

---

<sup>41</sup> Ibid hal 94.

<sup>42</sup> Graifhan Ramadhan, *Modul Pengenalan Internet*, [http://www.dhani.singcat.com/files/pengenalan\\_internet.pdf](http://www.dhani.singcat.com/files/pengenalan_internet.pdf), diakses tanggal 22 Januari 2008 halaman 4.

Indonesia tidak luput dari perkembangan internet. Indonesia mengalami percepatan perkembangan internet yang sangat tinggi serta memiliki jumlah pelanggan atau pengguna jaringan internet yang terus meningkat sejak paruh tahun 1990an. Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan melihat banyaknya perusahaan yang menjadi provider (penyedia) untuk pengguna jasa internet di Indonesia. Perusahaan-perusahaan yang memberikan jasa tersebut di Indonesia merupakan pihak yang berperanan sangat penting dalam kemajuan perkembangan cyber law di Indonesia dimana fungsi-fungsi yang mereka lakukan seperti :

- 1) Perjanjian aplikasi rekening pelanggan internet;
- 2) Perjanjian pembuatan desain home page komersial;
- 3) Perjanjian reseller penempatan data-data di internet server;
- 4) Penawaran-penawaran penjualan produk-produk komersial melalui internet;
- 5) Pemberian informasi yang di update setiap hari oleh home page komersial;
- 6) Pemberian pendapat atau polling online melalui internet<sup>43</sup>

Internet (*Inter-Network*) adalah sebutan untuk sekumpulan jaringan komputer yang menghubungkan situs akademik, pemerintahan, komersial, organisasi, maupun perorangan. Dalam definisi ini tampak bahwa internet mencakup juga terhadap jaringan yang biasa disebut dengan LAN (*Local Area Network*) dan WAN (*Wide Area Network*).<sup>44</sup>

<sup>43</sup> Danan Mursito, Raya Reinhardt, dan Sukma Wardhana, *Pendekatan Hukum untuk Keamanan Dunia Cyber Serta Urgensi Cyber Law Bagi Indonesia*, Jakarta : Program Studi Teknologi Informasi Magister Fakultas Hukum UI, 2005, halaman 4.

<sup>44</sup> Internet, [www.MyPersonalLibraryOnLine.com](http://www.MyPersonalLibraryOnLine.com), diakses tanggal 22 Januari 2008. LAN (Local Area Network) merupakan jaringan milik pribadi dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer, digunakan untuk menghubungkan komputer-komputer milik pribadi dalam satu kantor atau pabrik untuk memakai bersama sumber daya dan saling bertukar informasi. WAN (Wide Area Network) merupakan jaringan yang menghubungkan komputer satu dengan komputer lainnya yang mencakup daerah yang lebih luas antara satu kota ke kota lainnya, negara bahkan benua.

Menurut *The Federal Networking Council (FNC)* memberikan definisi mengenai internet dalam resolusinya tanggal 24 Oktober 1995. Definisi yang diberikan adalah sebagai berikut :<sup>45</sup>

*Internet refers to the global information system that :*

- a. is logically linked together by a globally unique address space based in the Internet Protocol (IP) or its subsequent extensions/follow ons;*
- b. is able to support communications using the Transmission Control Protocol / Internet Protocol (TCP/IP) suite or its sub-sequent extension/follow ons, and / or other Internet Protocol (IP) compatible protocols; and*
- c. Providers, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.*

Terjemahan bebasnya :

Internet berarti sistem informasi global yang:

- a. secara logika dihubungkan secara bersama-sama oleh suatu alamat ruang yang unik berdasarkan pada *Internet Protocol* atau perluasannya;
- b. bisa mendukung komunikasi menggunakan Protokol Transmisi Kendali / *Internet Protocol* (TCP / IP) sesuai atau perluasannya / mengikuti, dan atau protokol pengganti *Internet Protocol* lain; dan
- c. Penyedia, penggunaan atau buatan dapat diakses, baik di depan umum atau secara pribadi, lapisan jasa tingkat tinggi pada komunikasi, dan infrastruktur terkait yang diuraikan di sini.

Internet telah menyediakan akses untuk layanan telekomunikasi untuk pemakainya yang tersebar di seluruh dunia. Layanan internet tersebut meliputi komunikasi langsung (*email, chat*), diskusi (*Usenet News, email, milis*), sumber daya informasi yang terdistribusi (*World*

<sup>45</sup> Agus Rahardjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatana Berteknologi*, Bandung : PT. Citra Aditya Bakti, 2002, halaman 60.

*Wide Web, Gopher*), *remote login* dan lalu lintas file (Telnet, FTP), serta aneka layanan lainnya.

Internet telah mengubah konsep berpikir manusia mengenai jarak dan waktu secara drastis, karena dengan adanya internet seolah-olah dunia menjadi kecil dan tidak mempunyai batas. Dengan menggunakan internet seseorang dapat melakukan komunikasi untuk berbagai macam tujuan dengan orang lain di seluruh dunia tanpa terhambat oleh jarak dan waktu.

Seperti yang telah dijelaskan di sebelumnya bahwa jaringan yang membentuk internet bekerja berdasarkan suatu set protokol standar yang digunakan untuk berkomunikasi satu dengan lainnya. Protokol ini mengatur format data yang diijinkan, penanganan kesalahan (*error handling*), lalu lintas pesan, dan standar komunikasi lainnya. Protokol standar pada internet dikenal sebagai IP.<sup>46</sup> Protokol ini memiliki kemampuan untuk bekerja diatas segala jenis komputer, tanpa terpengaruh oleh perbedaan perangkat keras maupun sistem operasi yang digunakan. Sebuah sistem komputer yang terhubung secara langsung ke jaringan memiliki nama domain dan alamat IP dalam bentuk numerik dengan format tertentu sebagai pengenal. Internet juga memiliki *gateway* ke jaringan dan layanan yang berbasis protokol lainnya.<sup>47</sup>

#### 2.1.2.2. Cyberspace

Hubungan antara berbagai jaringan internet tersebut lama kelamaan menimbulkan sebuah ruang (*space*) baru. Ruang yang baru tersebut merupakan sebuah dunia yang memungkinkan kita melakukan segala aktifitas di dunia nyata dapat dilakukan di ruang tersebut. Orang dapat melakukan komunikasi tanpa batas sehingga dengan adanya komunikasi tersebut maka segala aktifitas dapat dilakukan, seperti

<sup>46</sup> *Internet Protocol (IP)* merupakan standar bagi komputer untuk berkomunikasi dengan komputer lainnya dalam suatu jaringan. Selain itu juga merupakan metode untuk saling terkoneksi pada jaringan komputer dan standar komunikasi antar komputer.

<sup>47</sup> Graifhan Ramadhan, *Modul Pengenalan Internet*, [http://www.dhani.singcat.com/files/pengenalan\\_internet.pdf](http://www.dhani.singcat.com/files/pengenalan_internet.pdf), diakses tanggal 22 Januari 2008.

transaksi bisnis, hingga aktifitas pemerintahan. Pada tahun 1984, *William Gibson* seorang penulis telah menulis sebuah novel yang berjudul *Neuromancer*. Penulis tersebut sebelumnya bukan merupakan seorang yang terkenal, namun berkat tulisannya yang bersifat fiksi ilmiah tersebut ia memperoleh penghargaan. Ketika muncul novel tersebut, *cyberspace* belum ditujukan kepada interaksi yang terjadi melalui jaringan komputer. Seperti yang dijelaskan dalam *Neuromancer*, *cyberspace* adalah sebuah konsensus/kesepakatan bersama mengenai halusinasi dimana dapat dirasakan dan terlihat seperti sebuah ruang yang nyata namun sebenarnya sebuah konstruksi yang dibuat menggunakan komputer yang menampilkan data abstrak.<sup>48</sup> Melalui novel karangan *William Gibson* tersebut istilah *cyberspace* mulai digunakan untuk menggambarkan ruang maya yang tercipta dengan adanya jaringan internet.

Ketika muncul novel tersebut, *cyberspace* belum ditujukan kepada interaksi yang terjadi melalui jaringan komputer. Istilah *cyberspace* tersebut ditujukan kepada adanya suatu ruang di internet. Pada tahun 1990 ketika Jhon Perry Barlow pertama kali mengaplikasikan istilah *cyberspace* untuk dunia yang terhubung atau online ke internet.

*Cyberspace* merupakan bentuk visualisasi spasial dari keseluruhan informasi yang ada di dalam sistem-sistem pemrosesan informasi global, yang terjadi melalui saluran-saluran yang diciptakan oleh jaringan-jaringan komunikasi yang ada pada saat ini maupun pada masa yang akan datang, sehingga memungkinkan beberapa orang user sekaligus untuk terlibat dan saling berinteraksi secara penuh, memungkinkan tersedianya input dan output dari dan ke semua orang yang berpartisipasi, memungkinkan dilakukannya simulasi realitas-realitas maya, memungkinkan dilakukannya pengendalian dan pengumpulan data dari jarak jauh melalui telepresence, dan

---

<sup>48</sup> Abu Bakar Munir, *Cyber Law, Policies and Challenges*, Malaysia, Butterworths Asia, 1999, halaman 1

memungkinkan terjadinya integrasi dan interkomunikasi total dengan berbagai produk dan lingkungan yang canggih yang ada di dunia riil.<sup>49</sup>

Cyberspace merupakan suatu dunia atau ruang maya yang didalamnya terdapat beberapa aktivitas sekaligus terjadi di dalam sebuah sistem komputer atau jaringan sistem komputer, yang memiliki suatu komunitas dan model interaksi tersendiri.

Seiring dengan perkembangan penggunaan komputer, cyberspace digunakan untuk menunjuk pada sebuah masyarakat virtual yang terbentuk melalui komunikasi yang terjalin dalam jaringan-jaringan komputer yang saling terhubung. Di dalam ruang cyberspace, kesepakatan-kesepakatan bisnis dapat dilakukan secara instan dari seluruh penjuru dunia, tanpa perlu lagi menggunakan pena, kertas dan bahkan tanpa perlu melakukan komunikasi tatap muka langsung. Transaksi-transaksi perbankan banyak memanfaatkan ruang cyberspace, orang-orang kini banyak yang mempergunakan kartu debit maupun kartu kredit untuk menggantikan mata uang konvensional dalam transaksi mereka.

Menurut M. Arsyad Sanusi, dalam bayang-bayang realisme cyberspace ini, waktu, jarak dan hambatan-hambatan fisik lainnya tidak lagi memiliki arti, batas-batas wilayah tradisional yang memisahkan negara-negara dengan batas-batas ruang fisik dan riil telah menjadi tidak jelas dan sulit ditemukan.

Seperti yang telah diungkapkan pada bab sebelumnya bahwa saat ini masyarakat dapat dikatakan sedang dalam masa peralihan dari “masyarakat industri” ke “masyarakat informasi”, sehingga informasi merupakan sesuatu yang sangat berharga yang kemudian mengakibatkan meningkatnya penggunaan teknologi informasi pada berbagai bidang. Salah satu wujud teknologi informasi adalah internet yang memungkinkan untuk berkomunikasi dua arah dalam bentuk yang lebih bervariasi dari sekedar suara dan gambar. Komunikasi dua arah tersebut

---

<sup>49</sup> Hillary Pearson, *Information in a Digital Age – The Challenge to Copyright*, dalam *The Computer and Security Report*, seperti dikutip oleh M. Arsyad Sanusi, op. cit, halaman 103

berguna untuk berbagai macam aktifitas masyarakat. Dengan adanya Internet memungkinkan terjadinya transaksi bisnis secara elektronik dimana para pihak tidak perlu bertatap muka dalam dimensi ruang dan waktu yang sama.

Peran penting internet secara umum adalah :

- 1) Distribusi seografis mencakup seluruh dunia, pada saat masuk dan berada dalam jaringan seseorang dapat berkomunikasi dengan siapapun di seluruh dunia;
- 2) Memerlihatkan arsitektur yang kuat, karena merupakan jaringan kerja dan tidak terdapat pusat kontrolnya;
- 3) Kecepatan beropersinya sesuai waktu yang sesungguhnya (*real time speed*);
- 4) Akses bersifat universal, siapapun dapat menghubungkan diri dengan jaringan internet;
- 5) Memberikan kebebasan berbicara, tidak ada larangan untuk berpendapat dan berbicara.<sup>50</sup>

Kelebihan sarana internet yang tidak mengenal batas geografis juga menjadikan internet sebagai sebuah sarana yang dapat menjangkau hampir semua aspek kehidupan manusia. Komunikasi menjadi sebuah kata kunci dalam perkembangan teknologi internet tersebut.

### 2.1.3. COMPUTER CRIME DAN CYBER CRIME

#### 2.1.3.1. COMPUTER CRIME

Seperti telah dijelaskan sebelumnya bahwa perkembangan teknologi sangat membantu kehidupan manusia dalam berbagai aspek. Namun perkembangan teknologi tersebut juga mempunyai dampak negatif.

Dengan adanya internet, selain mempermudah kehidupan manusia dalam dalam berbagai aspeknya, di sisi lain juga menjadi alat

<sup>50</sup> Hince IP Panjaitan et al., *Membangun Cyber Law Indonesia yang Demokratis*, (Jakarta : Indonesia Media Law and Policy Centre), 2005., halaman 95

untuk mempermudah melakukan perbuatan yang menyimpang. Seperti apa yang dikatakan oleh Jonathan Blumen :<sup>51</sup>

*“The Internet is ‘dangerous’ because it is a medium for the instantaneous and uncontrolled transmission of ideas”*

Terjemahan bebas penulis :

“Internet berbahaya karena ini merupakan media untuk penyampaian pemikiran secara cepat dan tidak terkendali”.

Karena sifatnya yang tidak terkendali tersebut maka terdapat kemungkinan ekses yang bergeser dari manfaat semula. Neill Barret juga telah memperingatkan bahwa :<sup>52</sup>

*“The Internet has been described by many as a ‘Bad Neighbourhood’, or as being a haven for pornography. This is certainly true : the Internet provides very many niches within which such immoral activity can be performed. It also supports criminal activity which is wholly amoral in nature”*

Terjemahan bebas penulis :

“Internet digambarkan sebagai ‘Tetangga yang Buruk’, atau tempat berlindungnya pornografi. Hal ini sepenuhnya benar : Internet memberikan banyak celah dimana aktivitas imoral ditampilkan. Ini juga mendukung aktivitas kriminal yang sepenuhnya merupakan perbuatan yang tidak bermoral”.

Pergeseran manfaat internet ini tidak lepas dari karakteristik yang dimiliki internet itu sendiri. Seperti yang dikatakan oleh *Robert Strang (Assistant US Attorney Southern Distric of New York)* bahwa kejahatan komputer merupakan salah satu kejahatan yang dapat dilakukan dengan hampir tanpa jejak yang dapat menunjukkan siapa pelakunya hingga merupakan salah satu daya tarik bagi pelaku yang berniat melakukannya.

Secara gramatikal kejahatan Komputer dalam bahasa Inggris disebut dengan istilah *Computer Crime*. Selain penggunaan istilah

<sup>51</sup>Jonathan Blumen, *Is Pornography Bad?*, 1995, [http://www.Spectacle.org/Is\\_Pornography\\_Bad.html](http://www.Spectacle.org/Is_Pornography_Bad.html), diakses tanggal 20 Pebruari 2008.

<sup>52</sup> Agus Raharjo, *Cyber crime di Indonesia (Prospek Pengaturan dan Penegakan Hukumnya)*, dalam *Cyber Crime Jurbal Studi Kepolisian*, Edisi 056, April-Juni 2003 halaman 20.

tersebut dalam beberapa literatur digunakan juga beberapa istilah untuk mendefinisikan kejahatan komputer yaitu antara lain, *Computer misuse*, *Computer fraud*, *Computer assisted crime*, *Computer related crime*, *computer misbruik* (Belanda), *computer criminaliteit* (Belanda).

Beberapa ahli telah mencoba mendefinisikan pengertian dari penyalahgunaan komputer, baik dalam suatu undang-undang ataupun rancangan undang-undang sehingga muncul berbagai definisi mengenai penyalahgunaan komputer atau tindak pidana dengan menggunakan sarana komputer. Adapun beberapa definisi tersebut sebagai berikut :<sup>53</sup>

Penyalahgunaan Komputer menurut Departemen Kehakiman Amerika didefinisikan sebagai berikut;

*"any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution. It has two main categories. First, computer as a tool of crime, such as found, an theaf property... Second, computer is the object of crime such sabotage, theaf or alteration data."*

Terjemahan bebasnya :

"semua tindakan tidak sah yang menggunakan pengetahuan teknologi komputer untuk sarana kejahatan, penyelidikan, atau penuntutan. Hal itu mempunyai dua kategori. Pertama, komputer sebagai alat kejahatan, seperti mulai melakukan pencurian harta benda, ... Kedua, komputer adalah obyek kejahatan seperti sabotase atau perubahan data pada komputer."

Dengan adanya definisi yang beragam tersebut dapat dikatakan hingga saat ini belum ada rumusan yang tepat mengenai kejahatan komputer. Beberapa pengertian dari kejahatan komputer yang dapat dikutip oleh penulis sebagai contoh keragaman dfinisi tersebut:

<sup>53</sup> U.S. Departement of Justice, H. Kadish Sanford, *Encyclopedia of Crime and Justice*, The Free Press Division of Macmillan, New York, 1983, hlm.218.

1. Munir Fuady memberikan definisi tentang kejahatan Komputer yaitu sebagai suatu kejahatan *white collar crime*<sup>54</sup> yang dilakukan oleh orang-orang yang mengerti komputer, baik karena kesalahannya ataupun karena kelalaiannya telah menggunakan teknologi komputer sebagai sarana untuk melakukan kejahatan, dengan merugikan kepentingan pihak lain, untuk menguntungkan dirinya sendiri ataupun orang lain berupa perolehan uang, barang, atau keuntungan lainnya.<sup>55</sup>
2. Menurut Jusuf Randi, kejahatan Komputer merupakan kejahatan dengan modus operandi baru yakni kejahatan menggunakan atau memperdaya komputer.<sup>56</sup>
3. Menurut IBM Inc Japan kejahatan komputer adalah:
  - a. *Crime using computer as a tool of theft , fraud, emblezzlement and so forth*
  - b. *Crime through computer system, such at tempering and elimination of the computer data and program.*
4. Kaspersen memberikan definisi *Any illegal act which directly interferences with the planned course of authomated data processing.*
5. Andi Hamzah memberikan pengertian kejahatan komputer sebagai kejahatan dibidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Dalam beberapa literatur, kejahatan Komputer diidentikan dengan Kejahatan Mayantara (*Cyber Crime*). Menurut Barda Nawawi Arief, sebagaimana dikutip oleh Abdul Wahid, Persatuan bangsa-bangsa (PBB) dalam Kongres PBB X tahun 2000 mengidentikan *Cyber Crime* sebagai

<sup>54</sup> Konsepsi tentang *White Colar Crime* pertama kali dipergunakan oleh Edwin H Sutherland pada Desember 1939. Sutherland dalam makalahnya membatasi White Colar Crime sebagai *a violatton criminal law by the person of upper social economic class in the course of his occupational activities*. Lihat Marjono Reksodiputro, *Pertanggungjawaban Pidana Korporasi Dalam Tindak Pidana Korporasi*, dalam *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Pusat Pelayanan Keadilan dan Pengabdian hukum Universitas Indonesia, Jakarta,1991, hal 65.

<sup>55</sup> Munir Fuady, *Kejahatan Komputer dan Internet*, Dalam Munir Fuady, *Bisnis otor: Anatomi Kejahatan Kerah Putih* ( Bandung: Citra Aditya:2004), hal 127.

<sup>56</sup> Al Wisnubroto, *Kebijakan Pidana Dalam Penanggulangan Penyalahgunaan Komputer* (Yogyakarta: Kanisius:1998), hal 22

*Computer Related Crime*, dimana mencakup keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya dan bentuk bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer. Pengertian *computer crime* menurut *Organization of European Community Development (OECD)* yang didefinisikan dalam kerangka computer abuse yakni;<sup>57</sup>

*"Any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmitting of data";*

Terjemahan bebas penulis :

*"Setiap perilaku yang melanggar / melawan hukum, etika atau tanpa kewenangan yang menyangkut pemrosesan data dan / atau pengiriman data."*

Selanjutnya *National Police Agency (NFA)* memberikan definisi kejahatan komputer yang sangat sederhana, yaitu *"computer crime is crime toward to computer"* yang berarti kejahatan komputer adalah kejahatan yang ditujukan kepada komputer, baik terhadap komputer itu ataupun dengan menggunakan komputer.<sup>58</sup> Menurut penulis, semua perumusan atau batasan yang diberikan mengenai kejahatan komputer (*computer crime*) atau penyalahgunaan komputer (*computer misuse*) tersebut secara umum dapat disimpulkan, yaitu perbuatan atau tindakan yang dilakukan dengan menggunakan komputer sebagai alat/sarana untuk melakukan tindak pidana atau komputer itu sendiri sebagai objek tindak pidana.

Menurut Agus Raharjo sebagaimana dikutip oleh Abdul Wahid, *Cyber Crime* sesungguhnya berbeda dengan *computer crime*. Menurut Nazura Abdul Manap membedakan *Computer Crime* dengan *Cyber Crime*, yaitu:

<sup>57</sup> Eddy Djunaedi Kamasudirdja, *Yurisprudensi Kejahatan Komputer*, CV Tanjung Agung Jakarta, 1993, hlm.3.

<sup>58</sup> Djoko Sarwoko, *Computer Crime sebagai Dimensi Baru Tindak Pidana Ekonomi*, *Varia Peradilan* No.21 Tahun II, Juni 1987, hlm. 150.

*Defined broadly, " computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a computer as tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who authorizedly transfers a costumer's money to dormont account for his own interest or a person without permission has obtained acces to other person's computer directly to download information, which in the first place, are confidential. The situation require direct acces by the hecker to the victim's computer. There is no internet line involved. Or only limited working used such as the local area network*

*Whereas cyber crime are crime committed virtually through internet online. This means that the crimes committed could extended to other countries, which is beyond the Malaysian jurisdiction. Anyway, it coueses no harm to refer computer crimes as cyber crime or vice versa since they have same imact in law.*

*Terjemahan bebasnya:*

Kejahatan komputer diartikan secara luas dapat melingkupi berbagai macam pelanggaran, aktivitas dan masalah-masalah komputer. Juga dikenal dengan melakukan kejahatan menggunakan komputer sebagai sarana dan melibatkan kontak langsung antara kriminalitas dan komputer. Sebagai contoh seorang pegawai bank yang tidak jujur yang mempunyai kewenangan untuk mentransfer dana milik nasabah ke rekening lain untuk nkepentingan dirinya sendiri atau orang yang tanpa ijin telah mendapatkan akses ke komputer milik orang lain untuk mengambil informasi yang dirahasiakan. Kondisi tersebut memerlukan akses langsung oleh seorang hacker dengan komputer milik korbannya. Tidak ada jaringan internet yang terlibat. Atau hanya terbatas dengan jaringan terbatas seperti LAN Sedangkan kejahatan cyber dilakukan secara virtual melalui jaringan internet. Ini berarti kejahatan dilakukan dapat diperluas kepada negara lain.

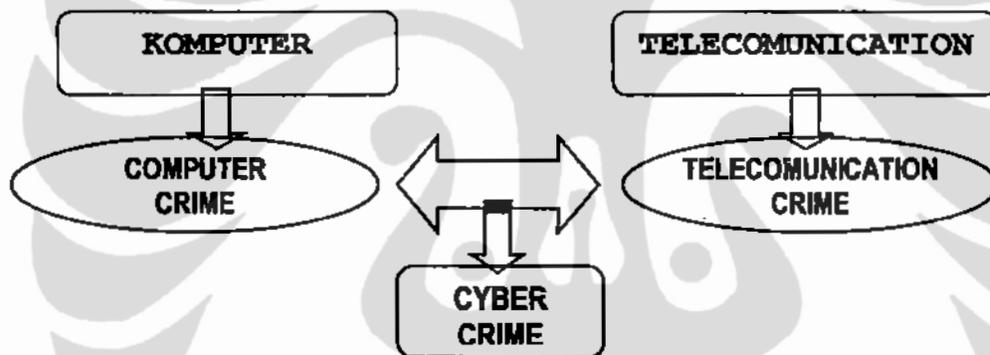
Tidak terbatasnya ruang dan waktu dalam melakukan aktivitas dengan menggunakan internet sebagai media, menyebabkan sulitnya suatu

aktivitas dalam dunia maya dideteksi dengan cara konvensional. Akibat yang ditimbulkan tidak sesederhana yang kita bayangkan, komputer yang dahulunya sebagai alat pengumpul dan menyimpan data saat ini dapat digunakan untuk melakukan kejahatan lama dalam kemasan baru. **Kejahatan yang menggunakan komputer dengan berbasis *internet* disebut dengan istilah *cyber crime*.**

### 2.1.3.2. CYBER CRIME

Seringkali *cyber crime* secara umum disamakan dengan *computer crime*, padahal keduanya adalah berbeda walaupun keduanya sama-sama kejahatan yang memanfaatkan kemajuan teknologi, untuk membedakan keduanya akan lebih mudah dengan memperhatikan bagan berikut:

#### Perbedaan *Computer Crime* dan *Cyber Crime*<sup>59</sup>



Sesuai dengan bagan di atas, dapat disimpulkan bahwa *computer crime* itu timbul akibat dari perkembangan teknologi komputer, dan *telecommunication crime* timbul karena kemajuan dalam bidang teknologi telekomunikasi sedangkan *cyber crime* merupakan hasil perpaduan antara kejahatan komputer (*computer crime*) dan kejahatan telekomunikasi (*telecommuni-cation crime*). Sehingga dapat dikatakan bahwa *computer crime* adalah kejahatan yang berhubungan dengan komputer tetapi tidak berhubungan dengan telekomunikasi, dan apabila *computer crime* tersebut telah menggunakan teknologi telekomunikasi (*media internet*) maka *computer crime* berubah menjadi *cyber crime*.

<sup>59</sup> Agus Rahardjo, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Op.Cit, hlm.228

Teknologi komputer adalah sebuah teknologi yang membawa manusia pada tingkat peradaban yang lebih tinggi, yang juga membawa dampak negatif berupa kejahatan komputer dan *cyber crime*.<sup>60</sup> Belum terdapat definisi baku mengenai cyber crime itu sendiri, akan tetapi akan disebutkan beberapa pengertian cyber crime yang lazim dipergunakan.

*The Oxford Reference Online* mendefinisikan cyber crime as crime committed over the Internet.<sup>61</sup>

Terjemahan penulis bahwa cyber crime adalah kejahatan yang dilakukan melalui internet.

*The Encyclopedia Britannica* memberikan pengertian *cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology*.<sup>62</sup>

Terjemahan bebasnya adalah bahwa cyber crime adalah kejahatan yang dilakukan oleh orang yang memiliki pengetahuan khusus atau keahlian dalam menggunakan teknologi komputer.

Menurut Roger Leroy Miller dan Gaylord A. Jentz "*a cyber crime is a crime that occurs in the virtual community of the internet, as opposed to the physical world*" Selanjutnya keduanya menyatakan "*the location of cyber crime - cyberspace - raises new issues in the investigation of crimes and the prosecution of perpetrators*."<sup>63</sup>

Terjemahan bebas penulis, cyber crime adalah kejahatan yang sebenarnya terjadi dalam komunitas internet, yang berlawanan dengan dunia nyata, penempatan kejahatan siber – dunia maya – memunculkan isu baru di dalam penyelidikan kejahatan dan penuntutan pelaku."

<sup>60</sup> Edmon Makarim, *Kompilasi Hukum Telematika*, Op.Cit, hlm. 218

<sup>61</sup> [www.crime-research.org/library/Cybercriminal.html](http://www.crime-research.org/library/Cybercriminal.html), diakses tanggal 20 Pebruari 2008

<sup>62</sup> [www.crime-research.org/library/Cybercriminal.html](http://www.crime-research.org/library/Cybercriminal.html), diakses tanggal 20 Pebruari 2008

<sup>63</sup> Roger Leroy dan Gayloid A. Jentz, *Law for E-Commerce*, Thompson Learning, United States, 2002. hlm.99

Cyber crime merupakan kejahatan yang relatif baru dan menimbulkan dampak yang sangat luas karena akibatnya tidak hanya dirasakan secara nasional namun juga internasional. Cyber crime dimasukkan dalam jenis kejahatan yang sifatnya internasional berdasarkan *United Nation Convention Against Transnasional Organized Crime (Palermo Convention)* November 2000 dan berdasarkan Deklarasi Asean tanggal 20 Desember 1997 di Manila.<sup>64</sup>

Cyber crime yang disampaikan oleh ITAC (*Information Technology Association of Canada*) pada "*International Information Industry Congress (IIC) 2000 Millenium Congress* di Quebec pada tanggal 19 September 2000, menyatakan bahwa :

*"Cyber crime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically enabled crime."*<sup>65</sup>

Terjemahan bebas penulis :

"Cyber crime merupakan ancaman yang nyata dan berkembang terhadap pembangunan ekonomi dan sosial di penjuru dunia. Teknologi Informasi menyentuh seluruh aspek kehidupan manusia dan dapat menimbulkan kejahatan secara elektronik".

Cyber crime menurut Muladi merupakan suatu istilah umum yang pengertiannya mencakup berbagai tindak pidana yang dapat ditemukan dalam KUHP atau perundang-undangan pidana lain yang menggunakan teknologi komputer sebagai suatu komponen sentral. Cybercrime berupa tindakan sengaja merusak property, masuk tanpa ijin, pencurian hak milik atas kekayaan intelektual, perbuatan cabul, pemalsuan, pornografi anak dan pencurian.<sup>66</sup>

<sup>64</sup> M.A. Erwin MAP, *Kejahatan Transnasional (Transnational Crime)*, Jakarta : Markas Besar Kepolisian Negara Republik Indonesia, Badan Reserse Kriminal, Desember 2002, halaman 34.

<sup>65</sup> ITAC, *IIC Common Views Paper On Cyber Crime*, IIC 2000 Millenium Congress, September 19th, 2000, sebagaimana dikutip oleh Barda Nawawi, *Masalah Cyber Crime (Tindak Pidana Mayantara)*, dalam *Perbandingan Hukum Pidana*, op. cit, halaman 252.

<sup>66</sup> Widyopramono Hadiwidjojo, *Cybercrime dan Pencegahannya*, dalam *Jurnal Hukum Teknologi : Tindak Pidana Telematika (Telematic Crime)*, Volume 2, Nomor 1, Agustus 2005, halaman 11.

Jenis-jenis *cyber crime* sangat banyak dan dengan cepat berkembang seiring dengan perkembangan teknologi, sehingga hukum seakan sangat tertinggal dalam mengikuti perkembangan jenis-jenis kejahatan tersebut. Namun sebenarnya hakekat dari kejahatan yang berhubungan dengan komputer (*cyber crime*) menurut John T. Soma secara umum dapat dikelompokkan menjadi beberapa jenis yaitu<sup>67</sup>:

- 1) *Misappropriation of computer time.*
- 2) *Theft of software (computer program, source codes, etc).*
- 3) *Theft of computer data or information generated or stored in computer.*
- 4) *Theft of services acquired by using the computer as tool.*
- 5) *Destruction or vandalism of computer hardware.*
- 6) *Destruction or interruption of computer processes causing confusion and delay.*
- 7) *Theft of trade secrets (often concurrent with the theft of software or programs).*
- 8) *Theft of money, financial instruments (negotiable instruments), and property.*

Terjemahan bebas penulis:

- 1) Ketidaktepatan/perbedaan waktu pada komputer.
- 2) Pencurian perangkat lunak (program komputer, sumber kode, dll).
- 3) Pencurian data komputer atau informasi yang melalui atau yang disimpan pada komputer.
- 4) Pencurian terhadap sebuah jasa dengan menggunakan komputer sebagai alat/sarana.
- 5) Perusakan atau vandalisme terhadap perangkat keras komputer.
- 6) Perusakan atau gangguan dari proses komputer yang menyebabkan kebingungan dan penundaan.
- 7) Pencurian rahasia perdagangan (sering disamakan dengan pencurian perangkat lunak atau program komputer).

---

<sup>67</sup> Soma, John T, op cit, hal 270

8) Pencurian uang, instrumen keuangan dan harta benda.

Dari beberapa hakekat kejahatan komputer diatas, metode untuk melakukannya beragam-macam dan berkembang seiring perkembangan teknologi sehingga menunjukkan kompleksitas dari metode-metode seperti yang akan kami sebutkan di bawah ini. Komunitas komputer menyebutkan beberapa modus operandi tertentu dan memberikan nama yang spesifik. Penyebutan tersebut dari beberapa sumber dapat disebutkan antara lain<sup>68</sup>:

**a. Data Leakage**

Istilah ini digunakan oleh Yusuf Randi dalam bukunya *Proteksi Terhadap Kriminalitas Dalam Bidang Komputer*. Data leakage atau berarti kebocoran Data dimana suatu tindakan pembocoran suatu data yang bersifat rahasia dilakukan oleh orang yang bekerja dan dipercaya untuk menjaga data yang ada dalam komputer tersebut, misalnya rahasia perusahaan dan rahasia negara. Cara yang sering digunakan adalah dengan menuliskan data rahasia tersebut ke dalam kode-kode tertentu sehingga data tersebut dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggungjawab.

**b. The Trojan Horse**

The Trojan Horse atau Kuda Troya merupakan suatu istilah yang telah diterima dalam dunia komputer untuk menjelaskan kejahatan komputer dengan cara memalsu data atau program, yaitu mengubah, menambah atau mengurangi data komputer.

Dalam modus ini komputer menjalankan dua fungsi yaitu selain menjalankan aktivitas yang telah ditentukan dalam standar perusahaan, tetapi komputer tersebut dengan program yang sama digunakan untuk tujuan menguntungkan diri si pelaku. Sebagai contoh seorang programer komputer disuatu bank diberikan tugas untuk membuat program penghitungan transaksi, karena ketrampilan

---

<sup>68</sup> John T Soma, *Computer Technology and The Law*, Denver, McGraw-Hill, Inc, 1983, Arsyad Sanusi, *Hukum Teknologi Dan Informasi*, Mizan, Jakarta:2004, Al Wisnubroto, *Kebijakan Pidana Dalam Penanggulangan Penyalahgunaan Komputer* (Yogyakarta: Kanisius:1998).

dan posisinya sebagai programmer, maka dia membuat program komputer yang digunakan untuk menghitung transaksi yang memungkinkan terjadinya penghitungan pengurangan bunga dari nasabah yang kemudian hasil pengurangannya tersebut dimasukkan ke rekening Programmer tersebut.

**c. *Data Diddling***

Istilah Data Diddling digunakan untuk menjelaskan suatu kejahatan komputer dengan cara pemalsuan data yaitu mengubah data yang sah dengan cara tidak sah dengan cara mengubah input dan output. Perbuatan ini biasanya dilakukan oleh mereka yang dipercaya memakai komputer disuatu tempat (perusahaan) memasukkan data palsu sehingga Output komputer akan tidak menampilkan hasil sebenarnya tetapi *output* tersebut akan menggambarkan sesuatu yang diinginkan oleh penjahat tersebut untuk maksud dan tujuan tertentu.

Contoh dari Data Diddling, seorang petugas komputer disuatu instansi pemerintah yang bertugas menginput nilai kredit pegawai untuk kenaikan pangkat, untuk membantu pegawai naik pangkat padahal sebetulnya nilainya masih kurang, petugas komputer tersebut menambahkan nilai kredit pegawai tersebut sehingga memenuhi persyaratan untuk kenaikan pangkat.

**d. *Joycomputing***

Istilah Joycomputing ini merupakan pendapat dari Nico Keyzer dalam suatu makalah di badan pembinaan Hukum Nasional Jakarta.<sup>69</sup> Pengertian dari Joycomputing adalah penggunaan komputer orang lain tanpa hak, baik karena ketiadaan kewenangan maupun karena melampaui kewenangan yang dimiliki. Misalnya seorang pegawai disuatu perusahaan dimana untuk menjalankan pekerjaan sehari-hari dia dibekali komputer oleh perusahaan untuk menjalankan tugas-tugas yang dibebankan oleh perusahaan kepadanya. Akan tetapi tanpa sepengetahuan atasan dan wewenang

---

<sup>69</sup> Al.Wisnubroto, *Op.Cit.* Hal 33

yang dimiliki dia menggunakan komputer tersebut bukan untuk mengerjakan tugas kantor melainkan untuk kepentingan pribadinya yang tidak ada hubungannya dengan tugas kantor. Dalam literatur lain seperti diungkapkan oleh R.A Brown joycomputing ini menggunakan istilah *Theft of Computer time and services*.<sup>70</sup>

**e. Hacking**

Merupakan suatu tindakan memperluas jaringan komputer secara tidak sah dengan jalan menyambungkannya dengan jaringan komputer yang sudah ada tanpa ijin dari pemilik jaringan tersebut. Dalam hacking ini terjadi penambahan terminal komputer baru yang dilakukan secara melawan hukum pada sistem jaringan komputer telah ada. Kejahatan Hacking sangat ditakuti karena data bisa hilang atau tercuri sehingga berpotensi akan adanya kerugian.

**f. Electromagnetic Pickup.**

Kejahatan komputer dengan model ini menggunakan bantuan alat-alat elektromagnetik yang dapat mempengaruhi komputer seperti yang diinginkan oleh pelakunya walaupun alat elektromagnetik tersebut tidak berhubungan secara fisik dengan komputer.

**g. Between The Lines Entry**

Istilah ini untuk menggambarkan suatu kejahatan komputer dengan cara menghubungkan suatu terminal komputer liar dengan line pribadi yang sah dan masuk ke dalam sistem komputer ketika user tidak aktif, tetapi masih menyalakan komputer. Atau dengan cara mengintersepsi dan membatalkan tanda Sign off pada terminal komputer yang sah, kemudian para pelaku kejahatan meneruskan bermain komputer tersebut.

**h. Logic Bomb**

Kejahatan Komputer *Logic Bom* ini menggunakan suatu program perusak yang ditanamkan dalam suatu program komputer

<sup>70</sup> Munir Fuady, *Kejahatan Komputer dan Internet*, Dalam Munir Fuady, *Bisnis Kotor: Anatomi Kejahatan Keras Putih* (Bandung: Citra Aditya:2004), hal 132

yang dibuat oleh seorang Programmer. Program ini pada suatu ketika akan merusak sistem komputer dan data-data yang ada. Biasanya Logic Bom ini korbannya adalah mereka yang menggunakan program komputer ilegal, dan Logic Bomb merupakan pengaman dari Software Developer untuk melindungi ciptaannya. Dalam dunia pertanian dikenal dengan Gen terminator, dimana untuk mencegah terjadinya pembiakan bibit dari hasil penanaman pengembang bibit memasukkan gen terminator agar supaya petani tidak dapat menggunakan hasil panennya untuk menjadi bibit penanaman selanjutnya.

**i. Trapdoor**

Program Trapdoor ini dipasang dalam komputer seperti pemasangan logic bomb atau kuda troja. Program ini bekerja untuk menghapuskan semua sistem pengaman pada komputer tersebut sehingga orang-orang dapat dengan bebas ke luar masuk dan mencuri data dalam komputer tersebut.

**j. Virus**

Virus adalah program pengacau komputer yang cara memasukkannya lewat disk, internet dan alat penyimpan lainnya. Virus komputer ini seperti halnya virus biologi yang berkembang dengan cepat manakala telah terinstal dalam komputer. Sebagai salah satu upaya mencegah virus maka dibuatlah program anti virus, akan tetapi nti virus ini sering terlambat hadirnya sehingga mana kala anti virus tertentu telah ada dilapangan dijumpai virus yang baru.

Disamping bentuk-bentuk diatas penulis akan memperkenalkan bentuk kejahatan komputer lain yang termasuk dalam kelompok pembajakan software komputer (*Software piracy*) adalah sebagai berikut:

**k. Counterfeiting**

*Counterfeiting* adalah duplikasi dan distribusi program komputer secara ilegal dan berskala besar yang dilakukan oleh suatu perusahaan penganda profesional. Pembajakan dengan modus

operandi *counterfeiting* dilakukan dengan alat rekam yang canggih, dimana modus operandinya adalah mengkopi satu program komputer asli (original) atau ilegal kedalam media perekam seperti disket, Compact Disk (CD) dalam jumlah yang banyak. Selanjutnya CD atau disket yang berisi program komputer tersebut dibuat sedemikian rupa sehingga menyerupai tampilan Program komputer asli. Hal tersebut dilakukan untuk mengelabui konsumen agar produk ilegal tersebut dianggap asli. Dalam membuat produknya, pembajak menggunakan teknologi tinggi sehingga produk yang dihasilkan sulit untuk dibedakan dengan yang asli.

Bentuk lain dari pembajakan ini adalah kompilasi dari berbagai judul program komputer yang dikemas dalam satu CD secara ilegal dan dipasarkan dengan nama yang berbeda.

#### 1. *End-User Copying*

Pembajakan Program Komputer dengan model End User Copying merupakan pengkopian program komputer yang dilakukan dengan menggunakan program komputer asli kedalam beberapa komputer tanpa lisensi.

Model pembajakan tersebut melanggar prinsip *end user License*, dimana pemilik program asli dilarang mengkopi programnya kedalam komputer lain selain komputernya sendiri.

Dalam setiap produk Program Komputer baik produk massal ataupun produk khusus (*mass Product and Tailor made*), pembeli diberikan suatu sertifikat yang disebut *End-User-Licensing Agreement (EULA)*. Dalam sertifikat tersebut dinyatakan bahwa produsen merupakan pemilik hak cipta atas program komputer yang dibeli dan pembeli hanya memiliki hak untuk menggunakannya saja. Pembeli tidak diperbolehkan untuk menggandakan, menyewakan, atau meminjamkannya tanpa persetujuan pemegang Hak Cipta.

Dalam sistem Hak Cipta Indonesia (UU No.19 Tahun 2003 Tentang Hak Cipta) pemilik program komputer dapat menggandakan (*back-up copy*) program komputernya hanya untuk kepentingan

sendiri. Program Komputer orisinal yang dibeli rusak dan tidak dapat membuat *back-up copy* maka pemilik dapat meminta produsen untuk mengkopir program komputer yang rusak tersebut dengan gratis.

Hal ini pelayanan yang harus diberikan oleh produsen. Dalam UU No. 8 tahun 1998 tentang perlindungan konsumen bahwa produsen harus menyediakan unit pelayanan pasca penjualan untuk kepentingan konsumen. Dalam industri program komputer, setiap produsen program komputer harus memiliki suatu unit jasa yang disebut *Supporting Services* yang bertujuan untuk memberi dukungan bagi optimalisasi penggunaan dan pemanfaatan oleh pembeli atas produk program komputer tersebut.<sup>71</sup>

m. ***Hard-Disk Loading***<sup>72</sup>

Pembajakan model hard-disk loading dilakukan dengan membuat memuat salinan program Komputer yang tidak sah (*illegal Copy*) ke Hard-disk komputer dengan cara menginstalkannya kedalam Hard-disk komputer.

n. ***Piracy of OEM Product***

Pembajakan model OEM (*Original Equipment Manufactures*) dilakukan oleh perusahaan pembuat komputer yang telah mempunyai hubungan (*perjanjian*) dengan pengembang Software untuk menginstal program-program kedalam hard drive dari komputer. Modus operandi yang dilakukan adalah penginstalan dengan menggunakan satu kopi program komputer yang legal kedalam komputer yang dibuat dimana perusahaan pembuat komputer tersebut menginstalkan program-program komputer kedalam hard drive beberapa komputer tanpa memberitahukan kepada perusahaan pembuat software.

o. ***Internet Piracy***<sup>73</sup>

<sup>71</sup> B.C Rikrik Rzkliyana SH, *Hakekat Kepemilikan, (Secara Hukum) Atas Sebuah Program Komputer*, Majalah CHIP edisi Mei 2000 hal 130-131

<sup>72</sup> Adrian Wicaksono, *Beberapa aspek Teknis dan Masalah Hak Cipta Yang Terkait dengan Software PC*, Makalah pada seminar Nasional Hak Cipta dalam Industri Perangkat Lunak Komputer dan Penggunaannya di Indonesia, Oktober, 1999, hal 4

Internet piracy merupakan pembajakan Program Komputer dengan menggunakan media internet, dimana pembajakan dilakukan dengan mendownload program Komputer dari situs-situs yang melakukan penjualan program Komputer. Program Komputer Yang dijual oleh situs-situs tersebut adalah ilegal.

p. **Adaptasi Program Komputer**<sup>74</sup>

Pembuatan adaptasi dari suatu Program komputer dibagi dalam dua kategori yaitu adaptasi yang diijinkan dan Adaptasi yang tidak diijinkan, Adaptasi yang diijinkan adalah suatu Adaptasi yang dibuat dalam hal menjalankan Program Komputer dan Adaptasi yang dilarang adalah pembuatan terjemahan (*translation*) atau aransemen/pengubahan (*Arrangement/alteration*) dari program tersebut.<sup>75</sup> Dengan mengacu pada *Copyright Act section 24 (4)* perbuatan yang termasuk dalam kategori Adaptasi adalah:

*...a version of the program in which it is converted into or out of a computer language or code or into a different computer language or code, otherwise than incidentally in the course of running the program.*

Adaptasi dilakukan dengan mengubah ke dalam bahasa atau kode yang sama atau bahasa komputer yang berbeda dan dilakukan diluar hal yang berhubungan dengan pelaksanaan suatu program komputer. Dari definisi diatas dapat dilihat tentang kemungkinan terjadinya suatu perkeyasaan ulang (*reverse engineering*) untuk suatu program dimana dapat dilakukan dengan bahasa pemograman yang sama atau berbeda.

<sup>73</sup> Justisiani Perdana Kusumah, *Pengalaman Dalam Mengajukan Gugatan Perkara Perdata Hak Cipta Program Komputer*, makalah pada sosialisasi UU tentang Hak Cipta; Arti Penting Perlindungan Hak Cipta bagi Karya film, musik dan Komputer Program, Medan, 26 Oktober 2001, hal 2

<sup>74</sup> David I Bainberge, *Computer And The Law*, Logman Group, London, 1989, hal 25

<sup>75</sup> David Bainbage, *Intellectual Property*, Thomas Pub, London, 1999, hal 125

## 2.2. REAKSI HUKUM TERHADAP PERKEMBANGAN TEKNOLOGI INFORMASI

### 2.2.1. Kebijakan Kriminalisasi Kejahatan Komputer.

Respon hukum terhadap perkembangan teknologi informasi merupakan sebuah proses aksi dan reaksi. Perkembangan teknologi mengikuti kebutuhan manusia namun apabila dalam perkembangannya menimbulkan masalah sehingga mengganggu ketertiban masyarakat yang sudah ada maka pada saat itulah hukum mulai bereaksi.

Perkembangan hukum selalu terjadi di belakang, yaitu dalam rangka merespon perkembangan-perkembangan sosial, ekonomi, dan teknologi di masyarakat yang kemudian berpengaruh atau mengubah masyarakat secara dramatis.

Henry Cheseman mengatakan bahwa :<sup>76</sup>

“Law cannot be written in advance to anticipate every dispute that could arise in the future. Therefore, general principles are developed to be applied by courts and jurise to individual disputes. This flexibility in law leads to some uncertainty in predicting results of lawsuits.”

Terjemahan bebasnya :

Hukum tidak dapat disusun mendahului dan untuk mengantisipasi setiap sengketa yang mungkin akan terjadi di masa yang akan datang. Oleh karena itu, maka pengadilan-pengadilan dan para juri mengembangkan prinsip-prinsip umum yang akan diterapkan pada sengketa-sengketa tertentu. Fleksibilitas seperti ini mengakibatkan terjadinya ketidakpastian di dalam memprediksikan hasil-hasil yang mungkin diperoleh dari gugatan-gugatan hukum).

---

<sup>76</sup> Henry R. Cheseman, *Contemporary Business and E-Commerce Law, Global, Digital and Ethical Environment*, seperti dikutip oleh M. ARSYAD SANUSI, HUKUM DAN TEKNOLOGI INFORMASI, 2005, TimKemasBuku, halaman 28

Dengan demikian hukum mengambil tempat dibelakang dari perkembangan-perkembangan teknologi tersebut. Yang menjadi masalah adalah bagaimana menentukan sebuah perbuatan patut untuk dikategorikan sebagai perbuatan pidana dan dapat dikenakan pidana? Setiap manusia mempunyai kepentingan-kepentingan yang satu sama lain berbeda-beda dan bahkan ada yang saling bertentangan, sehingga kemungkinan terjadinya konflik antara-kepentingan-kepentingan tersebut tidak terelakkan. Untuk menentukan kepentingan mana yang harus dilindungi terdapat bermacam-macam cara yang dapat digunakan untuk menilainya. Hal ini seperti yang disampaikan oleh Prof. Mr. Roeslan Saleh, bahwa dalam mencari kriteria positif bagi penentuan pidana kelompok-kelompok delik, kita memang dapat menunjukkan syarat-syarat tertentu bagi inkriminalisasi yang bagi delik-delik dari suatu kelompok tertentu itu adalah sama, tetapi pada akhirnya bagi tiap-tiap kelompok itu, dan bahkan *bagi tiap-tiap delik itu secara tersendiri-sendiri, keadaan-keadaan khusus memainkan peranan pula*. Tiap-tiap kriterium itu hanya mempunyai arti yang relatif<sup>77</sup>.

Teknologi Informasi saat ini telah mencapai tingkat perkembangan yang sangat cepat, sehingga memungkinkan terwujudnya information superhighways sebagai representasi dari Teknologi Informasi. Perkembangan tersebut mengakibatkan terjadinya perubahan pola-pola perdagangan dan perekonomian dunia sedemikian rupa, sehingga batas-batas politis dan geografis negara-negara menjadi tidak relevan atau tidak diperlukan lagi.<sup>78</sup>

Perubahan-perubahan sosial yang merupakan reaksi dari perkembangan teknologi salah satunya adalah perubahan yang terjadi di bidang hukum. Artinya perubahan yang terjadi di bidang hukum selalu terjadi menyusul perkembangan-perkembangan yang terjadi di bidang teknologi.

Oleh karena perkembangan teknologi sosial ini, menyebabkan hukum yang tertinggal sehingga diperlukan peran serta aktif dari hakim yang dapat

---

<sup>77</sup> Roeslan Saleh, Prof. Mr, op cit, hal 88.

<sup>78</sup> Henry R. Cheeseman, op cit, hal 28

berfungsi sebagai pembentuk hukum. Hukum disini diartikan sebagai putusan pengadilan yang dihasilkan oleh hakim sebagai respon dari suatu perbuatan melawan hukum yang sebelumnya belum diatur dalam hukum positif.

Karena sifatnya yang tidak mengenal batas-batas geografis maka isu kejahatan komputer tidak hanya menjadi masalah domestik tetapi menjadi persoalan seluruh negara-negara didunia. Dalam Konggres Persatuan bangsa-bangsa Tentang Pencegahan Kejahatan dan Pembinaan narapidana di Havana Kuba 7 Agustus – 7 september 1990 masalah Kejahatan Komputer mejadi salah satu isu penting yang dibicarakan. Dalam pembicaraan akhirnya menghasilkan resolusi antara lain menyatakan:

*Call upon Member States in view of work already done in the field of computer related crimes, to intensify their effort to more effectively combat computer abuses that deserve the application of criminal saction at national level, including the consideration, if necessary of following measures:*

- (a) *modernization of national criminal law and procedures including measures to:*
  - (i) *ensure that existing law offebces and law concerning investigative power and amissibility of evidence in judicial proceeding adequately apply and if necessary make appropriate changes*
  - (ii) *In the absence of laws that adequately apply, create offences and investigative and evedentiary procedures, where necessary to deal with novel and sophisticated form of criminal activity.*
  - (iii) *Provide for forfeiture or restitution of illegally acquired assets resulting from the commission of computer relted crime.<sup>79</sup>*

---

<sup>79</sup> United Nation, *Document A/CONF.144/L.11 Eighth United Nations Congress on The Prevention of Crime and The Treatment of Offender*, Havana-Cuba, September 1999, halaman 3  
Terjemahan bebasnya:

Respon hukum suatu negara atas sebuah perbuatan yang dianggap menyimpang tergantung pada sistem hukum yang dianut negara tersebut. Respon hukum terhadap suatu fenomena merupakan indikasi dari terjadinya pertemuan (konvergensi) antara fenomena tersebut dengan hukum<sup>80</sup>. Sehingga respon hukum pidana atas suatu kegiatan komputer terjadi karena terjadi pertemuan(konvergensi)antara kepentingan umum dengan kegiatan pengoperasian tertentu dari komputer yang mengakibatkan kepentingan umum tersebut terusik.

Pada negara-negara *Civil Law* respon yang dilakukan terhadap suatu fenomena yang mengusik keseimbangan yang telah ada pada masyarakat dengan pendekatan peraturan. Hal ini merupakan konsekuensi dari sistem hukum *Civil Law* yang mendasarkan pada hukum tertulis, sehingga untuk menangani suatu kasus dibutuhkan peraturan perundang-undangan. Pendekatan yang berbeda dilakukan oleh negara-negara *Common Law*, dimana hukum tertulis bukan satu-satunya sumber hukum bagi hakim untuk memutus suatu perkara, karena hakim dapat menggali hukum dari keadaan sosial serta melihat kembali pada yurisprudensi yang ada untuk diterapkan pada suatu kasus.

Disamping perbedaan dalam sistem hukum, pengaturan mengenai kejahatan komputer juga beragam antara satu negara dengan negara lainnya. Hal ini menurut Roeslan Saleh sebagaimana dikutip oleh AL. Wisnubroto karena adanya perbedaan pendekatan yang digunakan, adapun pendekatan tersebut antara lain sebagai berikut<sup>81</sup>:

---

Meminta negara anggota, dalam kerangka kerja yang telah dilakukan dalam kaitan kejahatan komputer, untuk mengintensifkan usaha mereka untuk secara lebih efektif memberantas kejahatan komputer yang terdapat saksi pidana dalam hukum nasionalnya, termasuk mempertimbangkan, jika diperlukan melakukan tindakan sebagai berikut:

- a) modernisasi hukum pidana nasional dan hukum acara termasuk tindakan untuk:
  - (i) memastikan bahwa hukum yang sedang berlaku dan hukum acaranya cukup untuk diterapkan dalam proses pengadilan, jika diperlukan buat perubahan yang tepat.
  - (ii) Dalam hal tidakadaan hukum yang cukup untuk diterapkan, ciptakan hukum pidana dan hukum acara, dimana jika diperlukan berkaitan dengan aktivitas kriminal yang baru dan canggih
  - (iii) Disediakkannya restitusi aset yang didapatkan dari kejahatan komputer tersebut.

<sup>80</sup> Arsyad Sanusi, *Hukum Teknologi Dan Informasi*, Mizan, Jakarta:2004, hal 239-240

<sup>81</sup> AL. Wisnubroto, *Op.Cit.*, hal 206

**a. *Property Approach,***

Pendekatan ini merupakan yang tertua dan paling banyak digunakan. Dalam pendekatan ini, kejahatan Komputer dilihat sebagai bagian dari delik terhadap harta kekayaan, sehingga isi inti dari catatan-catatan komputer diterjemahkan menurut nilai finansialnya. Disamping itu kepentingan-kepentingan yang dikaitkan dengan penggunaan komputer dimasukkan dalam property.

**b. *Forgery Approach***

Dalam pendekatan ini kejahatan komputer dilihat sebagai bagian dari delik-delik pemalsuan, dimana integritas dari keterangan-keterangan catatan komputer merupakan hal yang diperhatikan dalam suatu penyelesaian.

**c. *Information Approach***

Merupakan penyelesaian yang diarahkan pada sifat dipercayainya isi dan arti dari catatan- catatan komputer.

Pendekatan lain seperti diungkapkan oleh Muladi sebagaimana dikutip oleh Abdul Wahid adalah sebagai berikut:

**a. *Global Approach***

Yaitu suatu pendekatan yang menghendaki adanya peraturan baru yang bersifat umum terhadap kejahatan komputer yang mencakup berbagai bentuk perbuatan berupa manipulasi, perusakan, pencurian dan penggunaan komputer secara melawan hukum dan tanpa kewenangan.

**b. *Evolutionary approach***

Yaitu suatu pendekatan yang berusaha untuk mengadakan pembaharuan atau amandemen terhadap perumusan kejahatan-kejahatan tradisional dengan menambah perumusan kejahatan-kejahatan tradisional dengan menambah objek dan cara-cara melakukan kejahatan komputer dalam perumusannya. Dalam pendekatan ini berarti dilakukan modifikasi atau tambahan.

**c. *Compromise Approach***

Yaitu kompromi antara pendekatan global dengan pendekatan evolusioner yaitu dilakukan dengan mencantumkan komputer dalam kodifikasi hukum pidana.

Melihat pendekatan yang diungkapkan oleh para ahli diatas maka pada prinsipnya keduanya menggunakan hukum pidana untuk menyelesaikan masalah kejahatan komputer akan tetapi pendekatan yang dikemukakan oleh Roeslan Saleh adalah upaya maksimalisasi hukum pidana yang ada sedangkan pendekatan yang diungkapkan oleh Muladi lebih kepada pembuatan aturan baru yaitu diatur secara khusus, amandemen atau melakukan penambahan materi dalam kodifikasi hukum pidana.

Pendekatan lain seperti terjadi di Belanda yang dilakukan oleh Komisi Komputer Belanda (1985-1986). Dalam laporannya Komisi tersebut membedakan antara perlindungan untuk sarana dan perlindungan untuk data. Untuk masalah sarana hal-hal yang dijadikan tindak pidana meliputi (a) menghancurkan merusak, membuat tidak dapat dipakai ataupun menimbulkan gangguan, (b) berkenaan dengan memasuki secara melawan hukum sistem komputer. Untuk perlindungan data masalah yang dijadikan tindak pidana meliputi (a) membuat tidak dapat dipakainya atau menghapus atau membuat tidak dapat dimasuki data, (b) manipulasi data dan (c) pelanggaran terhadap perlindungan terhadap data yang dirahasiakan.<sup>82</sup> Atas keputusan tersebut Komisi Komputer Belanda menyarankan untuk melakukan revisi KUHP-nya dengan cara (1) membuat pasal baru, (2) menambah pasal yang ada dengan beberapa kata dan (3) merubah Pasal yang telah ada<sup>83</sup>

Jika suatu negara memikirkan kejahatan komputer akan dimasukkan dalam sebuah aturan hukum, D.K Piragoff sebagaimana dikutip oleh Mardjono Reksodiputro merekomendasikan langkah-langkah yang harus dilakukan yaitu<sup>84</sup>:

---

<sup>82</sup> Mardjono Reksodiputro, *Beberapa Catatan Tentang Penyalahgunaan Komputer Dalam Masyarakat*, Dalam Mardjono Reksodiputro, *Kemajuan pembangunan Ekonomi Dan Kejahatan: Buku Karangan Kesatu* (Pusat Pelayanan Keadilan dan Pengabdian Hukum: Jakarta, 1997), hal 11-12

<sup>83</sup> Mardjono Reksodiputro., *Loc.Cit*

<sup>84</sup> Mardjono Reksodiputro, *Ibid.*, hal 4-6

1. *determine what computer-related conduct the public industry, government and other interest groups are complaining about.*

(memutuskan apakah perbuatan berkaitan dengan komputer dari industri publik, pemerintahan dan kelompok lainnya)

2. *Examine the degree to which traditional laws apply to these computer abuse and the degree to which these abuses are merely traditional crimes committed in new ways. If the law does not apply, determine why. If the law applies question whether, on policy grounds it should apply.*

(Diuji tingkat aturan hukum tradisional diterapkan untuk penyalahgunaan komputer dan tingkat dimana penyalahgunaan tersebut semata-mata merupakan kejahatan tradisional yang dilakukan dengan cara baru. Jika hukum tidak dapat diterapkan, mengapa demikian. Jika hukum dapat diterapkan pertanyaannya apa yang menjadi dasar diterapkannya kebijakan tersebut).

3. *For computer abuses that are not fully covered by existing laws, the question arises as to whether and to what degree they should be prohibited by criminal laws, administrative law, civil law or not prohibited at all?*

(Untuk penyalahgunaan komputer yang tidak dapat dicakup secara penuh oleh hukum yang berlaku, pertanyaan yang muncul apakah perbuatan tersebut dilarang melalui hukum pidana, administrasi, hukum perdata atau tidak sama sekali?).

- d. *For each of these abuses, identify the social interest allegedly being violated.*

(Untuk setiap penyalahgunaan tersebut, identifikasi kepentingan masyarakat yang dilanggar).

- e. *A computer abuse may violate more than one interest, or many be conceptualized as violation of copyright, privacy or as a misappropriation of data or information. Identify all of these interest and means*

(Identifikasi semua hal yang berkaitan dengan penyalahgunaan komputer karena suatu penyalahgunaan komputer mungkin melanggar lebih dari satu aturan hukum seperti pelanggaran Hak Cipta, pemalsuan data atau informasi)

- f. *After identifying these interest, determine if the same or similiar abuses and interest in the non-computer environment are addressed by the law. (for example, is there an offence in the current law parrarel to the destruction of computer data) Converserly determine if an abuse and interest in the non computer environment has a parrarel in the computer environment an abuse thet is parrarel to an existent offences, such as destruction of property or interception of communication.*

(Setelah mengidentifikasi segala hal yang berkaitan, putuskan jika terdapat penyalahgunaan yang sama atau mendekati sama yang dilakukan tanpa komputer yang telah diatur dalam hukum yang ada).

- g. *If the answer to question 6 is in the affirmative, determine whether environment or should they be protected equally in the computer environment ( e.g theft of tangible property and misappropriation of information may not be equivalent; destruction of property and dstruction of data may be equivalent).*

(jika jawaban no 6 mendukung, putuskan apakah kondisi tersebut harus dilindungi secara sama dalam lingkungan komputer).

- h. *If the answer to question 6 is in negative, determine of it is justifiable to protect interest in the computer enviroment that are not protected in the non-computer environment ( e.g alteration or modification data).*

(Jika jawaban no. 6 adalah tidak, putuskan apakah dibenarkan untuk melindungi komputer yang tidak dilindungi dalam kondisi biasa ( tanpa ada komputer)

- i. *After identifying the abuses and the interest and how the current law applies if at all, determine whether the legislative or judicial application or extension of the law to the abuse would create unwarranted legal or social-economic effect.*

(Setelah mengidentifikasi penyalahgunaan dan kepentingan dan bagaimana hukum yang ada saat ini diterapkan, tetapkan apakah penerapan hukum atau perluasan dari hukum pada peyalahgunaan tersebut akan menciptakan ketidakpastian hukum atau efek sosial ekonomi).

10. *Determine what limit are necessary for the definition of the offence in order to distinguish criminal from non-criminal conduct and to prevent over- criminalization.*

(Tetapkan apakah diperlukan pembatasan untuk definisi dari kejahatan tersebut untuk membedakan perbuatan kriminal dengan yang bukan kriminal dan untuk mencegah kriminalisasi yang berlebihan)

Pendapat Piragoff tersebut pada intinya menggarapkan agar berhemat dalam menggunakan menetapkan perbuatan sebagai perbuatan pidana (kriminalisasi).Selanjutnya jika keputusan yang diambil nantinya adalah menggunakan hukum pidana untuk kejahatan komputer maka, Piragoff sebagaimana dikutip oleh mardjono Reksodiputro juga memberikan beberapa saran yang harus diperhatikan antara lain:<sup>85</sup>

1. *Be cognizant of the disticion between information and data both when assessing the applicability of laws and where creating new laws.*

---

<sup>85</sup> *Ibid*, hal 7-8

2. *ensure that data is protected in both its corporeal and incorporeal form, and also protected not just when it is in the computer but in other form as well such in the course of communication.*
3. *Does the proposed protection of data include unauthorized alteration as well as destruction?*
4. *Does the protection of data include interference with use as well as destruction of data?*
5. *Are the consequential effects of data interference upon tangible property or safety of life included?*
6. *Does surveillance and interception of computer communication include communication to, from and within a system and those to and from a person?*
7. *Are other processes of function of a computer system, in addition to communication of data, protected from surveillance and interception?*
8. *Is surveillance and interception covered in all of its possible forms or is only access (i.e. entry) to a system covered?*
9. *Theft of computer services or time may be different than unauthorized use of a computer system since the former usually includes some element of deprivation of use or money's worth. Criminalizing unauthorized use may require different or additional prerequisites of liability, or require additional safeguards to prevent over criminalization.*
10. *Are there traditional laws concerning unauthorized use or property? If yes can these be extended. If not is a special computer-use offence justifiable?*
11. *If an offence of unauthorized use is created, is it sufficiently limited to prevent over criminalization?*
12. *Are all types of computers covered by the law?*
13. *Be cognizant of the distinction between misappropriation of data and misappropriation of information.*

14. *Would traditional laws concerning theft of property adequately apply to the misappropriation of information? If so, would they apply without causing unwarranted legal or social-economic effect?*
15. *Is treatment of unauthorized acquisition, disclosure or use of information consistent between the computer and non computer environment?*
16. *Consider the creation of special offence or regulatory techniques to address the protection, distribution and use of various types of information. Universal solution, such as uniform concept of property may not be applicable. Policy considerations may vary depending on the nature of the information.*
17. *Ensure that appropriate mental requirement or other techniques are employed to distinguish criminal from noncriminal conduct, and to prevent over criminalization. These techniques and safeguard may vary depending on the nature of the abuse.*

Pendapat Piragof tersebut diatas merupakan sebuah pernyataan untuk berhati-hat menggunakan undang-undang hukum pidana. Jika memang mendesak untuk menciptakan aturan pidana baru maka perumusannya harus dibatasi dan disusun dalam kata dan kalimat yang tepat.

Selama belum terdapat aturan yang secara spesifik mengatur mengenai kejahatan komputer ini Indonesia mengikuti pendapat Piragoff dalam penanggulangan kejahatan komputer, yaitu menggunakan pendekatan operasional atau maksimalisasi hukum pidana yang ada untuk menjerat pelaku kejahatan komputer menggunakan peraturan yang telah ada.

Al. Wisnubroto dalam suatu penelitiannya mengungkapkan bahwa penanggulangan kejahatan komputer yang ada pada saat ini di Indonesia dititikberatkan pada kebijakan pidana yang bersifat aplikatif,

artinya dengan cara mengoperasionalkan ketentuan yang terdapat dalam perundang-undangan hukum pidana positif (KUHP) dan berbagai undang-undang lainnya yang memuat ketentuan pidana (undang-Undang Hak Cipta<sup>86</sup>, Undang-Undang Tindak Pidana Korupsi).<sup>87</sup>

Lebih lanjut menurut Al.Wisnubroto penggunaan ketentuan pidana yang ada dilihat dalam konteks tujuan akhir atau akibat dari perbuatan dan tidak jarang dalam penerapannya menggunakan interpretasi ekstensif dan melakukan analogi.<sup>88</sup> Pendapat Wisnubroto tersebut senada dengan apa yang disampaikan oleh Mardjono Reksodiputro bahwa kejahatan komputer yang terjadi merupakan kejahatan biasa dan bukan kejahatan baru dan masih dapat diselesaikan melalui KUHP yang sekarang berlaku.<sup>89</sup>

Seiring perkembangan waktu dan perkembangan teknologi maka masalah kejahatan komputer dimasukkan menjadi salah satu materi dalam Rancangan Kitab Undang-Undang Hukum Pidana Nasional. Pengaturan masalah kejahatan komputer secara khusus dalam R KUHP Nasional dilandasi pemikiran antisipatif dan proaktif atas fenomena kejahatan komputer yang semakin berkembang.<sup>90</sup>

### 2.2.2. Aspek-Aspek dalam Kriminalisasi Kejahatan Komputer

<sup>86</sup> Pasal 72 UU No.19 Tahun 2002

Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu Program Komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan atau denda paling banyak Rp.500.000.000 ( lima ratus juta rupiah).

<sup>87</sup> Al.Wisnubroto, *Op.Cit* hal 267

<sup>88</sup> *Ibid.*, hal 268

<sup>89</sup> Mardjono Reksodiputro, *Kejahatan Komputer: Suatu Catatan Sementara Dalam Rangka KUHP Nasional Yang Akan Datang*, dalam *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Pusat Pelayanan Keadilan dan Pengabdian hukum Universitas Indonesia, Jakarta,1991, hal 10.

Mardjono Reksodiputro membuat pendapat ini dengan menarik dari kasus Manipulasi bank di BRI Yogyakarta cabang Brigjen Katamso dan Transfer Fiktif BNI 1946 cabang New York. Respon lain seperti yang terjadi di Belanda, yaitu dibentuknya Komisi Kejahatan Komputer (1985-1986). Komisi ini menyarankan penyempurnaan *Wetboek Van Strafrecht* (WvS) dengan cara pertama, membuat pasal baru, kedua menambah pasal yang ada dengan beberapa kata, ketiga menambah pasal yang sudah ada.

<sup>90</sup> Dirjen Peraturan Perundang-Undangan Departemen Hukum dan HAM, *Rancangan Kitab Undang-Undang Hukum Pidana*,( Jakarta: 2004), hal 12.

KUHP yang berlaku saat ini merupakan peninggalan dari Belanda, mulai berlaku sejak 1918 yang merupakan pencerminan dari Wetboek van Strafrecht tahun 1886. Lebih dari seratus tahun sejak berlakunya Wetboek van Strafrecht Hindia Belanda, kemudian setelah kemerdekaan, dengan Undang-Undang No. 1 Tahun 1946 dinyatakan sebagai Kitab Undang-Undang Hukum Pidana Indonesia. Apabila dilihat dari usia dan perjalanan KUHP Indonesia sudah sewajarnya diadakan pembaharuan agar lebih sesuai dengan kondisi dan perkembangan jaman dan masyarakat Indonesia. Demikian pula jika dihubungkan dengan dasar-dasar falsafah suatu bangsa yang seharusnya melandasi undang-undang yang berlaku di negara tersebut.<sup>91</sup> Sehingga perlu adanya pembaharuan hukum pidana yang merupakan bagian dari hukum pembentukan hukum yang dijiwai dan bersumber pada Pancasila dan Undang-Undang Dasar 1945.<sup>92</sup>

-- Pembaharuan hukum pidana yang menyeluruh harus meliputi hukum pidana materiil, hukum pidana formil, dan hukum pelaksanaan pidana.<sup>93</sup> Ketiganya harus bersama-sama diperbaharui, karena apabila tidak maka akan timbul kesulitan dalam penerapannya dan tentu saja tujuan pembaharuan hukum tidak akan tercapai.

Negara Indonesia yang telah ratusan tahun dijajah oleh Belanda, mengakibatkan Indonesia menerapkan hukum yang diadopsi dari Belanda. Namun sesuai dengan perkembangan jaman, hukum nasional yang kini berlaku dirasa kurang mengakomodasi perubahan-perubahan yang terjadi karena perkembangan jaman ini. Sehingga perlu dilakukan pembaharuan hukum agar lebih sesuai dengan jiwa bangsa Indonesia dan tidak begitu tertinggal dengan perubahan-perubahan sosial dalam masyarakat.

KUHP yang berlaku saat ini merupakan peninggalan dari Belanda, mulai berlaku sejak 1918 yang merupakan pencerminan dari Wetboek van Strafrecht tahun 1886. Lebih dari seratus tahun sejak berlakunya Wetboek

---

<sup>91</sup> Roeslan Saleh, *Stelsel Pidana Indonesia*, Jakarta : Aksara Baru , 1987, halaman 3.

<sup>92</sup> Roeslan Saleh, *Perkembangan Pokok-Pokok Pemikiran dalam Konsep KUHP*, makalah disampaikan pada Penataran Nasional Hukum Pidana dan Kriminologi, Semarang, 3-15 Desember 1995, halaman 13.

<sup>93</sup> Sudarto, *Pembaharuan Hukum Pidana di Indonesia*, dalam *Simposium Pembaharuan Hukum Pidana Nasional*, Jakarta, Binacipta, 1986, halaman 26

van Strafrecht Hindia Belanda, kemudian setelah kemerdekaan, dengan Undang-Undang No. 1 Tahun 1946 dinyatakan sebagai Kitab Undang-Undang Hukum Pidana Indonesia. Apabila dilihat dari usia dan perjalanan KUHP Indonesia sudah sewajarnya diadakan pembaharuan agar lebih sesuai dengan kondisi dan perkembangan jaman dan masyarakat Indonesia. Demikian pula jika dihubungkan dengan dasar-dasar falsafah suatu bangsa yang seharusnya melandasi undang-undang yang berlaku di negara tersebut.<sup>94</sup> Sehingga perlu adanya pembaharuan hukum pidana yang merupakan bagian dari hukum pembentukan hukum yang dijiwai dan bersumber pada Pancasila dan Undang-Undang Dasar 1945.<sup>95</sup>

Untuk pengawasan terhadap perilaku orang dalam pemanfaatan teknologi informasi, diyakini hukum sangat berperan strategis. Bagaimanapun hukum memiliki fungsi dan peranan. Salah satu fungsi daripada hukum adalah sebagai sarana untuk melakukan pembaharuan yang ada di masyarakat. Pembaharuan yang dimaksud tentunya lebih dititikberatkan pada upaya peningkatan kesejahteraan. Oleh karena itu dalam konteks mengarahkan implikasi pemanfaatan teknologi informasi terhadap perubahan sosial yang harus digandeng dengan kondisi hukum yang memadai.

Kriminalisasi kejahatan komputer sebagai sebuah respon hukum terhadap ketidakseimbangan dalam masyarakat merupakan pilihan yang diambil Indonesia. Hal ini dapat dilihat pada RUU KUHP nasional dalam revisi terakhir dijumpai adanya beberapa pasal yang mengatur tentang kejahatan komputer.

Terhadap kriminalisasi tersebut perlu dilakukan kajian yaitu kepada siapa perlindungan yang akan diberikan serta apa yang perlu dilindungi. Seperti yang telah dijelaskan di atas bahwa dengan adanya dunia maya maka seluruh informasi dapat atau memungkinkan diakses. Teknologi informasi merupakan sebuah tuntutan dimana pada suatu saat

---

<sup>94</sup> Roeslan Saleh, *Stelsel Pidana Indonesia*, Jakarta : Aksara Baru , 1987, halaman 3.

<sup>95</sup> Roeslan Saleh, *Perkembangan Pokok-Pokok Pemikiran dalam Konsep KUHP*, makalah disampaikan pada Penataran Nasional Hukum Pidana dan Kriminologi, Semarang, 3-15 Desember 1995, halaman 13.

seluruh informai dan data akan disimpan dan ditransfer melalui jaringan komputer. Jika hal tersebut terjadi maka privasi menjadi hal yang perlu diperhatikan. Secara garis besar terdapat beberapa aspek privasi baik yang dilindungi oleh hukum maupun yang tidak. Seperti yang dikatakan oleh *Thomas J. Imedinghaff* yang dikutip oleh Edmon Makarim bahwa terdapat tiga aspek dari privasi yaitu<sup>96</sup>:

a. *Privacy of a Person's Persona*

Hak atas privacy ini didasarkan pada prinsip umum bahwa setiap orang mempunyai hak untuk dibiarkan sendiri (*the right to be let alone*). Pada umumnya ada empat jenis pelanggaran terhadap privacy atau pribadi seseorang, yaitu

- 1) Publikasi yang menempatkan seseorang pada tempat yang salah.
- 2) Penggunaan yang tidak tepat nama atau kesukaan seseorang untuk tujuan komersial.
- 3) Pembukaan fakta-fakta pribadi yang memalukan kepada publik.
- 4) Mengganggu kesunyian atau kesendirian seseorang.

b. *Privacy of Data About Person*

Hak privasi dapat juga mengikat pada informasi mengenai seseorang yang dikumpulkan dan digunakan oleh orang lain. Termasuk di dalamnya, sebagai contoh, informasi tentang kebiasaan seseorang, catatan medis, agama dan keanggotaan dalam partai politik, catatan pajak, data-data karyawan, catatan asuransi, catatan tindak pidana dan lain sebagainya. Penyalahgunaan informasi-informasi yang dikumpulkan atas anggota-anggota suatu organisasi/lembaga atau atas pelanggaran-pelanggaran dari suatu perusahaan termasuk dalam hak prvasi seseorang.

c. *Privacy of a Person's Communications*

Dalam situasi tertentu, hak atas privacy dapat juga mencakup komunikasi secara *online*. Dalam hal-hal tertentu, pengawasan dan penyingskapan isi dari komunikasi elektronik oleh orang lain bukan

<sup>96</sup> Edmon Makarim, *Pengantar Hukum Telematika, Suatu Kompilasi Kajian*, Jakarta, PT. Rajagrafindo Persada, 2005, hal 160.

oleh pengirim atau orang yang dikirim dapat merupakan pelanggaran dari privasi seseorang.

Data-data mengenai privasi seseorang saat ini banyak dikumpulkan oleh lembaga-lembaga pemerintah maupun organisasi-organisasi lainnya untuk berbagai keperluan. Pihak pemerintah mengumpulkan identitas dalam jumlah besar seperti kartu tanda penduduk sedangkan lembaga lain seperti perbankan mengumpulkan data-data mengenai nasabahnya. Dengan adanya teknologi informasi maka data-data tersebut siap dikomunikasikan baik kepada pihak yang berwenang menerima informasi maupun pihak-pihak lain yang tidak berwenang yang mungkin menyalahgunakan informasi tersebut.

Kriminalisasi terhadap sebuah perbuatan tidak terlepas dari hukum formil untuk membuktikan perbuatan tersebut.

### 2.2.3. **Peradilan Pidana Dalam Kasus Kejahatan Komputer**

Seiring dengan perkembangan teknologi khususnya teknologi informasi seperti yang telah dijelaskan di atas sangat mempengaruhi proses sosial dalam masyarakat yang juga sangat berpengaruh pada sistem peradilan pidananya. Sistem peradilan pidana harus mampu mengikuti perkembangan tersebut untuk mengatasi konflik-konflik yang muncul akibat penggunaan teknologi informasi dimana muncul berbagai modus kejahatan modern yang berkembang dengan sangat cepat.

Pembaharuan sistem peradilan pidana mencakup baik hukum materiil maupun hukum formil. Pada aspek hukum formil terdapat beberapa pokok permasalahan dalam penyelesaian kasus kejahatan komputer. Pada saat terjadi kejahatan komputer maka sesuai dengan sifatnya yang dapat dikendalikan dari suatu tempat yang jauh maka penyidik dalam menjalankan tugasnya akan berbenturan dengan permasalahan privacy.

Pada saat sebuah peristiwa yang diduga sebuah tindak pidana yang berhubungan dengan kejahatan komputer maka penyidik akan melakukan penyidikan dengan bukti yang bisa dianggap minim karena sifatnya yang dapat dikatakan tanpa jejak. Pada saat proses pengungkapannya yang

digunakan adalah hukum pidana formil sehingga dalam pembaharuan hukum pidana hukum pidana formil mempunyai peranan yang sangat besar.

Pada proses penyidikan kejahatan komputer di satu sisi penyidik harus menjaga hak-hak privasi seseorang dan disisi lain penyidik dalam mengungkap peristiwa tersebut kemungkinan harus menerobos hak-hak privasi seseorang mengingat sifat-sifat kejahatan komputer yang antara lain sedikit melibatkan kontak fisik serta dikendalikan dari tempat yang jauh.

Pada proses penyidikan tersebut penyidik akan mencari alat bukti untuk membuktikan perbuatan dan kesalahan orang tersebut. Dudeja memberikan definisi tentang bukti yaitu:

*information that tends to prove or disprove a fact in question. Evident may consist of dokumen, public record, affidavit or the testimony of witnesses. It also may be an object, such as a murder weapon*<sup>97</sup>

(Terjemahan bebas oleh penulis, informasi yang cenderung digunakan untuk membuktikan atau menyangkal suatu fakta yang dimaksud. Bukti dapat terdiri atas dokumen, data-data publik, pernyataan tertulis atau keterangan dari saksi. Juga bisa berupa objek seperti senjata.)

Dengan demikian bukti tidak terbatas berupa fisik tetapi juga non fisik. Untuk mencari dan mengumpulkan bukti penyidik mempunyai wewenang antara lain pertama memanggil orang untuk didengar dan diperiksa sebagai saksi dan tersangka yang kemudian dituangkan dalam bentuk berita acara pemeriksaan yang dikenal dengan Berita acara pemeriksaan (BAP) Saksi dan berita Acara pemeriksaan (BAP) Tersangka. Kedua, mendatangkan ahli yang memiliki keahlian khusus sebelum memberikan keterangan wajib memberikan sumpah atau janji dihadapan

<sup>97</sup> Dudeja, *Cyber Crime and The Law*, New Delhi, Commonwealth Publishers, 2002, hal 93.

penyidik. Keterangan ahli berupa Berita Acara Pemeriksaan Ahli dan laporan yang dibuat oleh ahli, ketiga melakukan pemeriksaan surat, keempat melakukan pengeledahan dan penyitaan barang bukti.

Berdasarkan bukti-bukti tersebut maka penyidik akan menentukan ada tidaknya suatu tindak pidana, jenis tindak pidana serta pelaku dari tindak pidana. Jika tidak terdapat cukup bukti maka penyidik menghentikan penyidikan.

Dengan demikian pada proses penyidikan peristiwa kejahatan komputer pembedaan antara *factual guilt* (bersalah berdasarkan fakta) dan *legal guilt* (bersalah berdasarkan hukum) sangat penting. Pada saat terjadi sebuah peristiwa pidana dalam lingkup kejahatan komputer penyidik tetap harus menjaga hak-hak privasi seseorang namun sebaliknya bukti-bukti kejahatan komputer tersebut hanya didapat dari tempat yang dapat dianggap sebagai privasi seseorang. Sehingga pada tahap ini penyidik akan melakukan proses hukum yang diperlukan seperti pengeledahan, penangkapan, penahanan dan lain-lain. Pada tahap ini seseorang akan ditempatkan pada posisi *factual guilt*. Pada proses ini seperti yang dikatakan oleh Herbert L. Packer bahwa seseorang yang ditempatkan posisinya sebagai tersangka dapat dikatakan sebagai *presumption of guilt*<sup>98</sup>. *Factual guilt* tersebut dapat menjadi *legal guilt* setelah melewati beberapa tahapan pada proses peradilan dan pengadilan menilai perbuatan tersebut salah berdasarkan hukum.

---

<sup>98</sup> Herbert L. Packer, *The Limits of The Criminal Sanction*, California, Stanford University Press hal. 176