

# **NASKAH AKADEMIK**

## **Rancangan Undang – Undang Tindak Pidana Di Bidang Teknologi Informasi**

Disiapkan Oleh:  
**Ir. Mas Wigrantoro Roes Setiyadi SE, MSi., MPP**



**Global Internet Policy Initiative – Indonesia**

bekerja sama dengan

**Cyber Policy Club**

dan

**Indonesia Media Law And Policy Center**

**November 2003**

## Daftar Isi

	Halaman
1. Pendahuluan	3
2. Definisi dan Ruang Lingkup Teknologi Informasi	8
3. Internet	14
4. Kejahatan Komputer, Internet, dan Teknologi Informasi	19
5. Perkembangan Hukum Pidana Teknologi Informasi	27
6. Alat Bukti Elektronik Dalam Hukum Pidana	35
7. Kejahatan Transnasional	39
8. Model Regulasi	42
9. Sanksi Pidana	47
10. Penyidikan	52
11. Daftar Referensi	55

## 1. Pendahuluan

Perkembangan Teknologi Informasi (TI) dalam kehidupan umat manusia abad ke 21 telah menandai suatu kemajuan baru yang tidak kalah penting dari penemuan molekul untuk pembuatan nuklir di masa Einstein. Banyak hal penting di abad 21 yang berkaitan dengan pemanfaatan TI dapat dijadikan sebagai tolok ukur kemajuan umat manusia. Keberhasilan penerbangan ulang – alik ke ruang angkasa oleh Amerika Serikat, Uni Sovyet dan China merupakan beberapa contoh keberhasilan TI dalam memfasilitasi teknologi ruang angkasa. Namun demikian keberhasilan dan sisi positif penggunaan TI bagi kemajuan peradaban umat manusia, di sisi lain juga menimbulkan eksese penyalahgunaannya untuk tujuan memperoleh keuntungan material secara tidak sah dan melawan hukum sehingga merugikan kepentingan individu, kelompok, dan Negara.

Kemajuan Teknologi Informasi di samping telah memberikan kemaslahatan terhadap masyarakat di sisi lain juga menimbulkan kekhawatiran karena adanya penggunaan yang menyimpang dari tujuan sebenarnya. Agar peluang kerugian yang ditimbulkan oleh adanya pemanfaatan Teknologi Informasi yang tidak semestinya sekecil mungkin, dibutuhkan perangkat peraturan dan perundangan yang membatasi sekaligus menghukum penggunaan Teknologi Informasi untuk kejahatan.

Kejahatan Teknologi Informasi (*cybercrime*) merupakan permasalahan yang harus ditangani secara serius karena dampak dari kejahatan ini sangat luas dan banyak merugikan perekonomian masyarakat karena apabila tidak ditanggulangi secara dini akan berkembang dan jika tidak terkendali dampaknya dapat sangat fatal bagi kehidupan bermasyarakat. Kendala utama dalam penyelidikan *cybercrime* antara lain *boderless* baik korbannya maupun tersangkanya sehingga perangkat hukum konvensional yang ada di Indonesia belum atau tidak bisa menjangkau secara efektif karena itu perlu diwujudkan hukum baru atau *cyberlaw*. Selain itu diperlukan peralatan *forensik computing* yang tepat guna pembuktian kejahatannya, serta menyiapkan penyidik Polri untuk dididik dan mampu menyidik *cybercrime* serta kerja sama dengan penegak hukum dengan yang ada di luar negeri.

Kejahatan dalam bidang Teknologi Informasi secara umum terdiri dari dua kelompok. Pertama, kejahatan biasa yang menggunakan Teknologi Informasi sebagai alat

bantunya. Dalam kejahatan ini, terjadi peningkatan modus dan operandi dari semula menggunakan peralatan biasa, sekarang telah memanfaatkan Teknologi Informasi. Dampak dari kejahatan biasa yang telah menggunakan Teknologi Informasi ternyata cukup serius, terutama bila dilihat dari jangkauan dan nilai kerugian yang ditimbulkan oleh kejahatan tersebut. Pencurian uang atau pembelian barang menggunakan kartu kredit curian melalui media Internet dapat menelan korban di wilayah hukum negara lain, suatu hal yang jarang terjadi dalam kejahatan konvensional. Kedua, kejahatan yang muncul setelah adanya Internet, di mana sistem komputer sebagai korbannya. Jenis kejahatan dalam kelompok ini makin bertambah seiring dengan kemajuan teknologi informasi itu sendiri. Salah satu contoh yang termasuk dalam kejahatan kelompok kedua adalah merusak situs Internet, pengiriman virus atau program – program komputer yang tujuannya merusak sistem kerja komputer tujuan.

Kesulitan yang banyak dihadapi dengan perangkat perundangan yang selama ini berlaku antara lain ada pada penindakan terhadap kejahatan jenis kedua, yang ternyata belum diatur dalam KUHP. Kesulitan berikutnya adalah pada pengumpulan dan penyajian barang bukti yang sah di pengadilan. Sistem hukum harus dapat mengakui catatan transaksi elektronik sebagai alat bukti yang sah di pengadilan. Pengaturan penindakan terhadap pelaku kejahatan di bidang Teknologi Informasi sangat penting, karena baik korban aktual maupun korban potensialnya sangat luas. Demikian pula jangkauannya, sangat luas dan memiliki peluang untuk dilakukan secara lintas negara, dan heterogen dengan kualitas dan persepsi yang berbeda. Substansinya-pun beragam, meliputi segala aspek kehidupan baik yang bersifat positif maupun negatif. Informasi muatannya ada yang masih berupa konsep, issue, data, fakta dan gagasan yang bersifat objektif dan dapat pula bersifat subjektif. Kepentingan yang terkait dapat berupa kepentingan negara, kepentingan publik, dan dapat pula kepentingan kelompok atau bahkan kepentingan pribadi.

Penelitian yang dilakukan *The American Bar Association* menunjukkan kerugian finansial yang diakibatkan *computer-related crime* 145-730 juta dolar AS per tahun. Tertangkapnya David Smith (pembuat virus Melissa), Enud Tanebaum, dan Vice Miscovic (pembobol sistem pertahanan komputer Pentagon) ternyata tidak membuat jera pembuat virus lainnya. Onel de Gusman, pembuat virus *Love Bug* ternyata menimbulkan

kerugian finansial bagi Amerika Serikat sebesar US\$ 8 miliar. Tim Lloyd pembuat *time-bomb software* menimbulkan kerugian 12 juta dolar AS. Hasil survei AC Nielsen menunjukkan, Indonesia menempati posisi keenam terbesar di dunia atau keempat di Asia dalam kejahatan Internet atau *cybercrime*.

*The Internet Fraud Complaint Center*, sebuah lembaga kerja sama antara FBI dan *National White Collar Crime Centre* menunjukkan, 63% *cybercrime* merupakan *fraud involving online auctions*. Yaitu sebuah kejahatan yang dilakukan dengan modus menawarkan lelang barang secara *online*. Namun setelah penawar mengirimkan uang secara *online*, barang tidak pernah dikirim. Ada tipe lain, yaitu *fraud involving online retail sales*, pelaku kejahatan menempatkan iklan barang dan jasa yang jenisnya mirip dengan barang dan jasa pada situs-situs lelang kredibel. Namun, setelah calon pembeli mengklik *banner* iklan tersebut, tanpa disadari dia akan dibawa ke situs lain. Cara lain adalah *payment card fraud*. Tipe kejahatan ini dilakukan dengan membayar transaksi *online* menggunakan nomor kartu kredit sah hasil curian.

Jika disepakati bahwa kejahatan Teknologi Informasi apapun bentuknya tergolong tindakan kejahatan yang harus dihukum, pertanyaan yang sering diajukan adalah apakah perundangan Indonesia sudah mengatur masalah tersebut? Ada dua kelompok pendapat dalam menjawab pertanyaan ini. Kelompok pertama berpendapat bahwa sampai hari ini belum ada perundangan yang mengatur masalah kriminalitas penggunaan Teknologi Informasi (*cybercrime*), dan oleh karenanya jika terjadi tindakan kriminal di dunia cyber sulit bagi aparat penegak hukum untuk menghukum pelakunya. Pendapat ini diperkuat dari kenyataan bahwa banyak kasus kriminal yang berkaitan dengan dunia cyber tidak dapat diselesaikan oleh sistem peradilan dengan tuntas karena aparat menghadapi kesulitan dalam melakukan penyidikan dan mencari pasal – pasal hukum yang dapat digunakan sebagai landasan tuntutan di pengadilan.

Kelompok kedua beranggapan bahwa tidak ada kekosongan hukum, oleh karenanya meski belum ada undang – undang yang secara khusus mengatur masalah *cybercrime*, namun demikian para penegak hukum dapat menggunakan ketentuan hukum yang sudah ada. Untuk melaksanakannya diperlukan keberanian hakim menggali dari undang – undang yang ada dan membuat ketetapan hukum (*yurispridensi*) sebagai landasan keputusan pengadilan. Kelompok kedua ini berpendapat bahwa mengingat

lamanya proses penyiapan suatu undang – undang, sementara demi keadilan, penanganan tindakan kejahatan Teknologi Informasi tidak dapat ditunda, maka akan lebih baik kiranya jika digali ketentuan hukum yang ada dan dianalisis apakah ketentuan hukum tersebut dapat digunakan sebagai landasan tuntutan dalam kejahatan Teknologi Informasi.

Pendapat dua kelompok di atas mendorong diajukannya tiga alternatif pendekatan dalam penyediaan perundang-undangan yang mengatur masalah kriminalitas Teknologi Informasi. *Alternatif pertama* adalah dibuat suatu Undang – Undang khusus yang mengatur masalah Tindak Pidana di Bidang Teknologi Informasi. Undang – undang ini bersifat *lex specialist* yang khusus mengatur masalah pidana pelanggaran pemanfaatan Teknologi Informasi, baik yang tergolong kejahatan konvensional menggunakan komputer sebagai alat, maupun kejahatan jenis baru yang muncul setelah adanya Internet dan menjadikan Teknologi Informasi sebagai sasaran kejahatan. *Alternatif kedua*, memasukkan materi kejahatan Teknologi Informasi ke dalam amandemen KUHP yang saat ini sedang digodok oleh Tim Departemen Kehakiman dan HAM. Sebagaimana diketahui KUHP belum mencakup jenis – jenis kejahatan Teknologi Informasi, khususnya yang muncul setelah adanya Internet. *Alternatif ketiga*, melakukan amandemen terhadap semua undang – undang yang diperkirakan akan berhubungan dengan pemanfaatan Teknologi Informasi, seperti misalnya Undang – undang Perpajakan, Perbankan, Asuransi, Kesehatan, Pendidikan Nasional, dan lain sebagainya. Amandemen terhadap berbagai undang – undang ini untuk menyesuaikan kemungkinan adanya pelanggaran terhadap klausa yang tergolong pidana dalam undang – undang tersebut yang dilakukan menggunakan Teknologi Informasi.

Dari kriteria efisiensi dan kepraktisan, alternatif ketiga sulit dilaksanakan. Jika katakanlah, terdapat seribu undang – undang, maka negara perlu menyediakan tenaga ahli untuk memeriksa satu persatu undang – undang tersebut, mengubah sesuai kebutuhan dan selanjutnya Dewan Perwakilan Rakyat (DPR) akan mengesahkan amandemen terhadap seribu undang - undang tersebut. Sebaliknya alternatif kedua dapat dilakukan sepanjang ada kemauan politik dari Pemerintah dan DPR. Permasalahannya proses perubahan KUHP sudah berjalan hampir selesai, sedangkan persoalan perlu- tidaknya kejahatan Teknologi Informasi dimasukkan ke dalam KUHP (baru) belum pernah secara

serius dibahas di forum nasional. Dengan demikian, alternatif pertama menjadi suatu hal yang disarankan, apalagi kajian mengenai hal ini sudah disiapkan oleh Lembaga Swadaya Masyarakat (LSM) Global Internet Policy Initiative (GIPI) - Indonesia dan Indonesia Media Law and Policy Center (IMPLC) yang tidak menambah beban anggaran bagi pemerintah.

Mengingat perhatian pemerintah masih terpusat pada pembuatan Undang – Undang Informasi dan Transaksi Elektronik (UU-ITE) yang juga penting karena merupakan salah satu perangkat hukum yang mengatur pemanfaatan Teknologi Informasi (cyberlaw), dan pentingnya Negara Republik Indonesia segera memiliki Undang – Undang Tindak Pidana di Bidang Teknologi Informasi ((TIPITI), maka kajian dan usulan yang dibuat oleh GIPI beserta komunitas telematika Indonesia ini diharapkan dapat menjadi inisiatif DPR. Sehingga dengan demikian keduanya (UU-ITE dan UU-TIPITI) akan saling melengkapi dalam memberi kepastian dan perlindungan hukum bagi pengguna Teknologi Informasi.

Selain dari pada itu, selain karena UU TIPITI ini dibuat berdasarkan asas keamanan, kepastian hukum, etika, manfaat, adil, dan merata, yang lebih utama adalah bahwa ia dibuat dengan tujuan untuk mendukung ketertiban pemanfaatan Teknologi Informasi yang digunakan oleh orang berkewarga-negaraan Indonesia, dan atau badan hukum yang berkedudukan di Indonesia, orang asing, atau badan hukum asing yang melakukan kegiatan atau transaksi dengan orang, atau badan hukum yang lahir dan berkedudukan di Indonesia, dengan tetap menjunjung tinggi hukum Indonesia dan hak asasi manusia, tidak diskriminatif baik berdasarkan suku, agama, ras maupun antar golongan.

## 2. Definisi dan Ruang Lingkup Teknologi Informasi

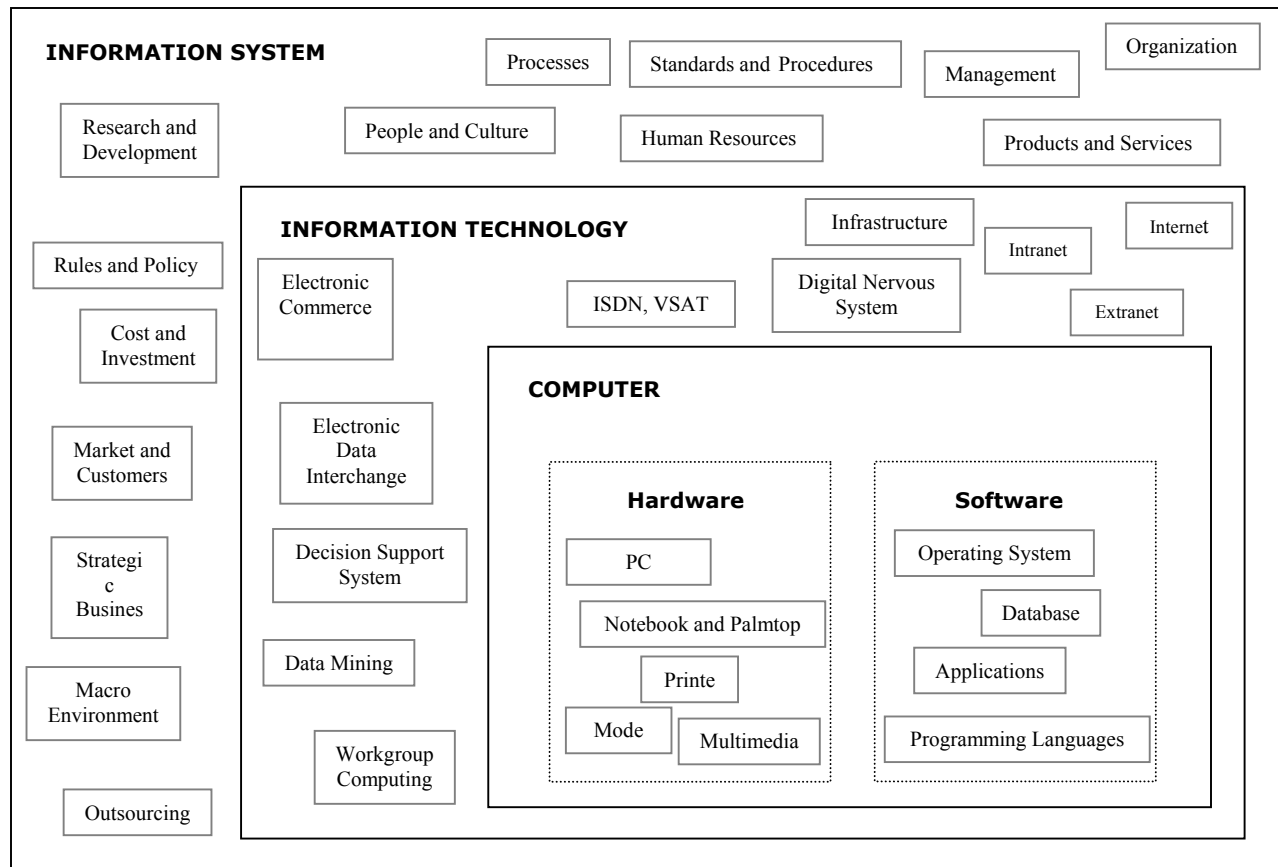
Turban, (1996) mendefinisikan Teknologi Informasi dengan ungkapan: *in its narrow definition, refers to the technological side of an information system. It includes hardware, databases, software networks and other devices.*

Sementara mengenai Sistem Informasi didefinisikan sebagai : *a collection of components that collects, processes, stores, analyzes, and disseminates information for a specific purpose.*

Beberapa referensi lain mendefinisikan Teknologi informasi sebagai suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi. Dalam perspektif lain, Teknologi Informasi menjadi mungkin dalam formatnya saat ini karena difasilitasi oleh komputer yang di dalamnya terdapat dua komponen pokok yaitu perangkat keras (*hardware*) dan perangkat lunak (*software*). Wujud hardware berupa antara lain namun tidak terbatas pada: personal komputer, komputer mini dan mainframe, notebook, palmtop, printer, modem, dan lain sebagainya. Adapun software antara lain terdiri dari kelompok: sistem operasi, data base, sistem aplikasi, dan bahasa pemrograman (*programming language*).

Kumpulan hardware dan software membentuk teknologi yang digunakan sebagai penyedia layanan kebutuhan sistem informasi, seperti misalnya: *electronic data interchange*, Internet, Intranet, Extranet, *Data Mining*, *Workgroup computing*, *Decision support system*, *electronic commerce*, ISDN, VSAT, dan lain sebagainya. Dengan demikian cakupan Teknologi Informasi menjadi cukup luas, tidak hanya komputer atau Internet saja, namun termasuk juga peralatan – peralatan elektronika digital lain yang berbasis komputasi baik yang digunakan secara *stand alone* maupun terhubung ke suatu jaringan.





Untuk mempermudah pemahaman terhadap ruang lingkup Teknologi Informasi yang perlu diatur dalam Undang-undang tentang Tindak Pidana Di Bidang Teknologi informasi ini, berikut diuraikan beberapa pengertian antara lain:

1. Teknologi Informasi adalah suatu teknik atau cara Elektronik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi.
2. Telekomunikasi adalah setiap pemancaran, pengiriman, dan atau penerimaan dari setiap informasi dalam bentuk tanda – tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya.
3. Data adalah fakta berupa angka, karakter, symbol, gambar, tanda-tanda, isyarat, tulisan, suara, bunyi yang merepresentasikan keadaan sebenarnya yang selanjutnya digunakan sebagai masukan suatu Sistem Informasi.
4. Data Elektronik adalah Data yang merupakan hasil luaran dari suatu Elektronik.

5. Elektronik adalah segala macam alat dan peralatan yang dibuat dan bekerja berdasarkan prinsip elektronika untuk memperoleh, mengolah, menyimpan dan atau menyampaikan informasi dalam format digital, dalam media elektromagnetik, optikal atau sejenisnya;
6. Informasi adalah Data hasil pengolahan Sistem Informasi yang bermanfaat bagi penggunaanya.
7. Informasi Elektronik adalah Data Elektronik hasil pengolahan Sistem Informasi yang bermanfaat bagi penggunaanya.
8. Sistem Informasi adalah tata cara pengelolaan Informasi menggunakan Teknologi Informasi
9. Komputer adalah Elektronik yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
10. Sistem Komputer adalah Komputer atau sekumpulan Komputer yang terhubung dengan Elektronik dan atau sekumpulan Komputer lainnya, menuruti perintah suatu program, melaksanakan pemrosesan Data dan menghasilkan Data Elektronik.
11. Jaringan Komputer adalah Komputer dan atau Sistem Komputer yang saling terhubung menggunakan media komunikasi, masing-masing memiliki otoritas untuk melaksanakan tugas berdasarkan program.
12. Internet adalah Jaringan Komputer global atau jaringan yang menghubungkan Jaringan Komputer di seluruh dunia dengan menggunakan protokol komunikasi Internet Protocol.
13. Intranet adalah Jaringan Komputer privat yang menggunakan protokol komunikasi Internet Protocol, dapat namun tidak selalu, terhubung ke Internet, dan hanya dapat digunakan dalam lingkungan terbatas.
14. Nama Domain adalah kode atau susunan karakter yang bersifat unik, menunjukkan lokasi tertentu dalam Internet, berhubungan dengan berkas elektronik (*file*) yang disimpan dalam alat penyimpan dalam Sistem Komputer, yang digunakan untuk menyimpan Informasi atau Data Elektronik lainnya yang berkaitan dengan pemilik atau pengelola Nama Domain.

15. Surat Elektronik adalah suatu jenis layanan yang memungkinkan pengguna Komputer untuk mengirim Data, Informasi, atau pesan melalui Internet atau Jaringan Komputer kepada pengguna Komputer lainnya.
16. Alamat Surat Elektronik adalah alamat Internet dari seseorang, perkumpulan, organisasi, atau badan usaha, untuk berkomunikasi melalui Internet atau komunikasi Elektronik lainnya.
17. Nomor Internet Protokol adalah tanda pengenal unik dalam bentuk sederetan angka menggunakan ketentuan baku untuk menandai setiap Elektronik yang terhubung ke Internet.
18. Situs Internet adalah suatu lokasi di dalam Internet yang digunakan untuk menempatkan Data Elektronik atau aplikasi Internet yang dapat diakses oleh pengguna Internet.
19. Sandi Akses (*password*) adalah angka, karakter, simbol lainnya atau kombinasi diantaranya yang merupakan kunci untuk dapat mengakses komputer, sistem komputer, jaringan komputer, Internet, atau media elektronik lainnya.
20. Privasi adalah hak individu untuk mengendalikan penggunaan informasi tentang identitas pribadi baik oleh dirinya sendiri atau oleh pihak lainnya.
21. Database adalah semua data yang terdapat dalam suatu organisasi terutama yang tersimpan dalam alat penyimpan sistem komputer yang dapat diakses menggunakan ketentuan-ketentuan tertentu.
22. Komunikasi Data adalah pengiriman dan penerimaan data dalam jaringan komputer.
23. Penyedia Layanan Teknologi Informasi adalah organisasi atau badan hukum yang memberikan layanan jasa di bidang teknologi informasi, meliputi namun tidak terbatas pada penyedia akses Internet, penyedia jasa pembangunan perangkat lunak komputer dan aplikasi Internet, penyedia jasa pemandu sistem informasi, serta penyedia jaringan telekomunikasi dan jasa telekomunikasi.
24. Penerima adalah seseorang yang menerima atau dimaksudkan untuk menerima data elektronik dari pengirim.
25. Pengirim adalah seseorang yang mengirim, meneruskan, menyimpan, atau menyalurkan setiap pesan elektronik atau menjadikan setiap pesan elektronik dapat dikirim, disimpan, atau disalurkan kepada orang lain.

26. Pelanggan adalah orang, badan usaha, badan hukum, atau instansi pemerintah yang menggunakan layanan teknologi informasi berdasarkan kontrak
27. Pemakai adalah orang, badan usaha, badan hukum, atau instansi pemerintah yang menggunakan layanan teknologi informasi yang tidak berdasarkan kontrak.
28. Pengguna adalah pelanggan dan pemakai.
29. Teknologi Enkripsi adalah penggunaan algoritma matematika untuk membuat data elektronik terkodekan sedemikian rupa sehingga hanya dapat dibaca oleh mereka yang memiliki kunci pembukanya.
30. Tanda Tangan Digital atau tandatangan elektronik adalah tanda jati diri berupa informasi elektronik yang berfungsi sebagai pengesahan oleh pengguna melalui metode elektronik atau prosedur yang telah ditentukan.
31. Transaksi Elektronik adalah setiap transaksi yang dilakukan oleh dua pihak atau lebih melalui jaringan komputer atau media elektronik lainnya, dengan menggunakan system informasi elektronik yang menimbulkan hak dan kewajiban kepada masing-masing pihak yang bertransaksi.
32. Perdagangan secara elektronik adalah setiap perdagangan baik barang ataupun jasa yang dilakukan melalui jaringan komputer atau media elektronik lainnya, dengan system informasi elektronik
33. Alat Pembayaran adalah uang atau semua jenis mekanisme pembayaran lainnya yang berfungsi untuk menggantikan uang
34. Kartu kredit adalah bagian dari alat pembayaran berupa kartu beridentitas unik yang diberikan oleh perusahaan penjamin pembayaran kepada perorangan atau perusahaan berdasarkan kontrak, yang digunakan oleh pengguna untuk melakukan transaksi elektronik dan atas penggunaan kartu kredit tersebut, pengguna kartu dinyatakan berhutang kepada perusahaan penjamin pembayaran selaku penerbit kartu kredit.
35. Kartu Debit adalah bagian dari alat pembayaran berupa kartu beridentitas unik yang diterbitkan oleh lembaga perbankan kepada nasabah tabungan pada bank bersangkutan berdasarkan kontrak, yang digunakan oleh pengguna untuk alat pembayaran dalam transaksi elektronik dan atas penggunaan kartu debit tersebut, maka tabungan yang dimiliki oleh pengguna, dipotong langsung oleh Bank.

36. Akses adalah perbuatan memasuki, memberikan instruksi atau melakukan komunikasi dengan fungsi logika, aritmatika, atau memori dari komputer, sistem komputer, atau jaringan komputer.
37. Intersepsi adalah tindakan seseorang, badan usaha atau badan hukum untuk melakukan pencegahan terhadap lalu lintas komunikasi data melalui media kawat, serat optik maupun gelombang elektromagnetik dalam suatu sistem komputer baik menggunakan sarana teknis atau non-teknis.
38. Alat bukti elektronik meliputi: perangkat keras sistem komputer atau jaringan komputer peralatan lain yang tersambung ke komputer, perangkat lunak yang dapat berupa sistem operasi, sistem data base, dan atau sistem aplikasi yang tersimpan atau terpasang dalam sistem komputer atau jaringan komputer.

### 3. Internet

Berawal dari kebutuhan untuk mengembangkan sekaligus melindungi dari bahaya senjata nuklir, pada tahun 1964 Departemen Pertahanan Amerika Serikat membangun jaringan komputer tanpa *central hub*, dan *switching station* (Cameron, 1994). Proyek yang diberi nama *Advanced Research Projects Agency* (ARPA) ini semula bertujuan untuk memperbaiki dan menyempurnakan kelemahan dari jaringan komputer yang sudah ada, ketika itu bila *central hub* tidak berfungsi maka seluruh jaringan akan berhenti (*down*). Dalam konteks pertahanan, jaringan komputer harus tetap berfungsi meskipun ada serangan bom nuklir menghancurkan fasilitas komputer.

Perkembangan berikutnya, pada tahun 1980, ketika mulai muncul *Personal Computer* (PC) timbul kebutuhan untuk menghubungkannya dalam jaringan komputer yang lebih besar untuk saling – tukar informasi. Universitas California Berkeley adalah lembaga yang pertama kali membangun jaringan kampus berprotokol *Transmission Control Protocol/Internet Protocol* (TCP/IP) dengan sistem operasi UNIX. Jaringan kampus ini kemudian berkembang dan mampu dihubungkan dengan jaringan lain milik *National Science Foundation* (NSF) membentuk NSFNET. Dengan dipakainya NSFNET oleh hampir semua perguruan tinggi di Amerika Serikat, maka mahasiswa dapat menggunakan Internet, walau dalam prakteknya masih terbatas pada departemen – departemen matematika, sains, dan *computer science*.

Pertumbuhan dan komersialisasi Internet mulai terlihat sejak tahun 1991 ketika dibentuknya Commercial Internet Exchange (CIX), suatu organisasi swasta yang terdiri dari 60 perusahaan *Internet Access Providers* bekerja sama membiayai pembangunan jaringan fisik yang dihubungkan dengan jaringan milik publik (*publicly-owned networks*), sehingga memungkinkan informasi komersial ditransmisikan melalui Internet. Mengalirnya informasi komersial melalui Internet membawa dampak yang signifikan dalam praktek bisnis. Melalui Internet kalangan bisnis dapat memasarkan produknya ke seluruh dunia tanpa harus terhambat oleh dimensi ruang dan waktu. Dengan kata lain, Internet mampu mengatasi hambatan perdagangan yang ditetapkan suatu negara terhadap mitra dagang asing (Thurow, 1999).

Perkembangan berikutnya, penggunaan Internet mendorong perubahan pada struktur organisasi perusahaan dari hirarkis kepada organisasi jaringan (*network organization*), trend perubahan ini selanjutnya memungkinkan munculnya semakin banyak perusahaan baru yang menggunakan Internet sebagai basis usaha, menggantikan pola bisnis tradisional (Tapscott, 1999). Perusahaan – perusahaan ini menciptakan nilai (*value*) yang diwujudkan dalam produk dan jasa yang dipasarkan melalui Internet.

Adanya Internet memungkinkan masyarakat untuk dapat berkomunikasi dalam bentuk yang lebih bervariasi; tidak seperti telepon yang hanya mampu menyampaikan suara, faksimili untuk text dan gambar, televisi untuk gambar dan suara namun tidak dapat dua arah; melalui Internet, suara, text , dan gambar ditransmisikan secara bersamaan dan terjadi komunikasi dua arah. Lebih lanjut, dampak dari kecanggihan Internet ini adalah dimungkinkannya melakukan transaksi dagang secara elektronik sehingga para pihak yang bertransaksi tidak perlu saling berhadapan dalam dimensi ruang dan waktu yang bersamaan.

Peran penting Internet secara umum adalah:

- a. Distribusi geografis mencakup seluruh dunia, pada saat masuk dan berada dalam jaringan seseorang dapat berkomunikasi dengan siapapun di seluruh dunia;
- b. Memperlihatkan arsitektur yang kuat, karena merupakan jaringan kerja dan tidak terdapat pusat kontrolnya;
- c. Kecepatan beroperasinya sesuai waktu yang sesungguhnya (*real time speed*);
- d. Akses bersifat universal, siapapun dapat menghubungkan diri dengan jaringan Internet;
- e. Memberikan kebebasan berbicara, tidak ada larangan untuk berpendapat dan berbicara.

### **Nama Domain**

Dalam Internet, setiap komputer terhubung ke jaringan memerlukan alamat (*address*) yang unik dalam bentuk IP address. Pada mulanya pengalamatan menggunakan kombinasi angka 32 digit, namun hal ini bukan merupakan hal yang mudah untuk diingat. Pada dasarnya komputer sudah mampu mengenali alamat dalam bentuk IP address, namun tidak demikian halnya dengan manusia, karena urutan angka yang membentuk

alamat sulit diingat. Untuk mengatasinya digunakanlah nama host (*host name*), sehingga mempermudah manusia mengoperasikan jaringan komputer.

Sebagai contoh, <http://www.yahoo.com> dan <http://204.71.200.72> adalah dua Universal Resource Locater (URL) yang identik. Teknik pengalamatan di awal munculnya Internet adalah menggunakan tabel. Masing – masing host/komputer menyimpan daftar kombinasi nama komputer dan IP address, pada file yang dinamakan HOSTS.TXT. File ini berisi nama dan IP address seluruh komputer yang terkoneksi ke Internet. Setiap kali ada perubahan atau penambahan host baru file ini diperbaharui dan dikirim ke seluruh anggota jaringan. Ketidak – praktis muncul ketika host/komputer yang terhubung ke Internet meningkat pesat mencapai puluhan ribu bahkan juta sambungan.

Pada tahun 1984 Paul Mockapertis mengusulkan sistem data base pengalamatan terdistribusi untuk menggantikan sistem pengalamatan sebelumnya yang menggunakan table alamat IP. Dengan sistem pemberian nama host yang terdistribusi ini masing – masing organisasi anggota jaringan hanya bertanggung jawab terhadap database yang berisi informasi jaringan miliknya saja. Sistem baru ini disebut *Domain Name System* (DNS) dan berlaku hingga sekarang. Selain untuk memetakan IP address dan Nama Host, DNS juga digunakan sebagai sarana bantu penyampaian *electronic mail* (e-mail).

### **World Wide Web**

Perkembangan Internet tidak akan menjadi demikian besar seperti sekarang bila tidak muncul aplikasi jaringan yang membentuk *World Wide Web* (www) yang diciptakan oleh Tim Bernes-Lee dari The European Particle Physics Laboratory (CERN) di Geneva, Swiss (Cameron, 1994). Berbeda dengan aplikasi sejenis yang muncul sebelumnya, www memberikan suatu cara untuk mengintegrasikan berbagai aplikasi pencari (*search engine*) ke dalam satu antarmuka (*interface*). www adalah suatu program *client/server* yang dapat diakses oleh aplikasi pengurut (*browser*).

Sebelum berkembangnya www, Internet umumnya hanya digunakan oleh kalangan akademisi dan riset. Pada tahun 1993 NCSA meluncurkan piranti lunak Mosaic, suatu browser www dengan kemampuan grafik yang dapat digunakan pada seluruh



sistem operasi komputer yang - waktu itu - banyak dipakai seperti: X, PC/Windows, dan Macintosh. Munculnya Mosaic semakin meningkatkan penggunaan Internet dan lalu lintas data melalui www, pada tahun yang sama mencapai 342,000% dibandingkan dengan pertumbuhan jenis browser lainnya seperti Gopher yang hanya mencapai 997% saja (Onno W. Purbo, 2001a). Dunia bisnis dan media pun serta merta mulai memperhatikan Internet karena perkembangan di atas. Hadirnya Mosaic ternyata menjadi titik belok perkembangan Internet dari yang semula hanya digunakan oleh kalangan akademisi dan riset menjadi digunakan oleh banyak orang untuk bisnis dan hiburan.

### **Website**

Web browser menggunakan konsep *Uniform Resource Locator* (URL) untuk mengakses layanan tertentu pada jaringan Internet. URL mengandung nama skema yang digunakan diikuti oleh tanda titik dua dan string yang pengertiannya bergantung pada skema yang digunakan. Contoh URL, misalnya: <http://www.yahoo.com/Arts/Humanities/> Layanan www saat ini merupakan layanan yang paling populer di antara seluruh jenis layanan jaringan komputer yang menggunakan protokol komunikasi *Transmission Control Protocol/Internet Protocol* (TCP/IP) termasuk Internet<sup>1</sup>. Server www diakses dengan menggunakan www browser seperti Netscape dan Internet Explorer dari Microsoft. Protokol yang digunakan untuk layanan www ini adalah *Hypertext Transfer Protocol* (HTTP).

### **Keamanan Jaringan**

Guna keperluan pengendalian keamanan informasi berbasis Internet sistem keamanan jaringan menjadi suatu keharusan untuk diperhatikan, karena jaringan komputer Internet yang sifatnya global dan publik pada dasarnya tidak aman (Onno W. Purbo, 2001b). Pada saat data terkirim dari suatu komputer ke komputer yang lain di dalam Internet, data itu akan melewati sejumlah komputer lain yang berarti akan memberi kesempatan kepada pengguna Internet lainnya untuk menyadap atau mengubah data tersebut. Data dikatakan aman dari penyadapan atau perusakan hanya apabila

---

<sup>1</sup> Dalam dunia komunikasi data komputer, diperlukan protokol untuk mengatur bagaimana sebuah komputer berkomunikasi dengan komputer lainnya. TCP/IP adalah sekelompok protokol yang mengatur komunikasi data komputer di Internet.

komputer tidak terhubung ke suatu jaringan (*stand alone*). Pembobolan sistem keamanan di Internet terjadi hampir tiap hari di seluruh dunia.

Masalah keamanan jaringan berhubungan pula dengan resiko. Resiko adalah suatu kemungkinan di mana penyusup berhasil mengakses komputer di dalam jaringan yang dilindungi. Apakah penyusup dapat membaca, menulis, atau mengeksekusi suatu file yang dapat mengakibatkan kerugian terhadap organisasi pemilik jaringan komputer tersebut? Apakah penyusup dapat merusak data yang penting? Seberapa besar hal – hal tersebut dapat menimbulkan kerugian terhadap pemilik jaringan komputer? Siapa saja yang dapat memperoleh akses terhadap suatu account, maka orang tersebut dapat menyamar sebagai pemilik *account*. Dengan kata lain, bila ada satu *account* aktif yang tidak aman dalam suatu sistem jaringan, maka seluruh jaringan komputer tersebut memiliki potensi resiko tidak aman.

#### 4. Kejahatan Komputer, Internet dan Teknologi Informasi

Meskipun belum ada kesepakatan mengenai definisi kejahatan Teknologi Informasi (cybercrime), namun ada kesamaan pengertian universal mengenai kejahatan komputer. Hal ini dapat dimengerti karena kehadiran komputer yang sudah mengglobal mendorong terjadinya universalisasi aksi dan akibat yang dirasakan dari kejahatan komputer tersebut (Mas Wigrantoro, 2002). Secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia cyber adalah:

*Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan [ada fasilitas komputer yang dimasuki atau digunakan tersebut.*

Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer.

Keragaman aktivitas kejahatan yang berkaitan dengan komputer atau jaringan komputer sangat besar dan telah menimbulkan perbendaharaan bahasa baru, misalnya *hacking, cracking, virus, time bomb, worm, troyan horse, logical bomb, spamming, hoax*, dan lain sebagainya. Masing – masing memiliki karakter berbeda dan implikasi yang diakibatkan oleh tindakannya-pun tidak sama. Secara umum, bentuk – bentuk aktivitas kejahatan komputer dapat dikelompokkan ke dalam dua golongan: **penipuan data** dan **penipuan program**. Dalam bentuk pertama, data yang tidak sah dimasukkan ke dalam sistem atau jaringan komputer, atau data yang sah dan seharusnya di-*entry* diubah sehingga menjadi tidak valid atau sah lagi. Fokus perhatian pada kasus pertama ini adalah adanya apemalsuan dan atau kerusakan data input dengan maksud untuk mengubah output. Bentuk kejahatan kedua, yang relatif lebih canggih dan lebih berbahaya adalah apabila seseorang mengubah program komputer, baik dilakukan langsung di tempat komputer tersebut berada maupun dilakukan secara *remote* melalui jaringan komunikasi data. Pada kasus ini penjahat melakukan penetrasi ke dalam sistem komputer dan selanjutnya mengubah susunan program dengan tujuan menghasilkan keluaran (*output*) yang berbeda dari seharusnya, meski program tersebut memperoleh masukan (*input*) yang benar.

Bainbridge (1993) dalam bukunya Komputer dan Hukum membagi beberapa macam kejahatan dengan menggunakan sarana komputer :

- a. Memasukkan instruksi yang tidak sah, yaitu seseorang memasukkan instruksi secara tidak sah sehingga menyebabkan sistem komputer melakukan transfer uang dari satu rekening ke rekening lain, tindakan ini dapat dilakukan oleh orang dalam atau dari luar bank yang berhasil memperoleh akses kepada sistem komputer tanpa ijin.
- b. Perubahan data input, yaitu data yang secara sah dimasukkan ke dalam komputer dengan sengaja diubah. Cara ini adalah suatu hal yang paling lazim digunakan karena mudah dilakukan dan sulit dilacak kecuali dengan pemeriksaan berkala.
- c. Perusakan data, hal ini terjadi terutama pada data output, misalnya laporan dalam bentuk hasil cetak komputer dirobek, tidak dicetak atau hasilnya diubah.
- d. Komputer sebagai pembantu kejahatan, misalnya seseorang dengan menggunakan komputer menelusuri rekening seseorang yang tidak aktif, kemudian melakukan penarikan dana dari rekening tersebut.
- e. Akses tidak sah terhadap sistem komputer atau yang dikenal dengan hacking. Tindakan hacking ini berkaitan dengan ketentuan rahasia bank, karena seseorang memiliki akses yang tidak sah terhadap sistem komputer bank, sudah tentu mengetahui catatan tentang keadaan keuangan nasabah dan hal-hal lain yang harus dirahasiakan menurut kelajiman dunia perbankan.

Dengan demikian pengamanan terhadap system jaringan komputer tidak saja dalam perhitungan keuangan secara otomatis yang sering dipakai dalam bidang perbankan, system pengupahan, transaksi lintas negara (salah satunya *electronic transfer*), namun yang tidak kalah penting untuk mendapat perhatian yaitu menyangkut pengamanan terhadap data itu sendiri dari perusakan data. Yang dimaksud dengan perusakan data disini adalah penghapusan atau perubahan data sehingga tidak dapat digunakan lagi, ataupun penggunaan data oleh pihak-pihak yang tidak berwenang. Beberapa orang membedakan istilah proteksi dan sekuriti. Usaha pengamanan data dari kerusakan yang tidak disengaja umumnya disebut sebagai proteksi, sedangkan usaha pengamanan dari perusakan yang disengaja disebut sebagai sekuriti.

Ancaman terhadap penggunaan Internet dapat datang dari jaringan Internet maupun dari lingkungan dalam (*internal*). Bernstein (et all, 1996) mengutip suatu hasil

penelitian yang menyatakan bahwa 80% hingga 95% bobolnya sistem keamanan komputer disebabkan dari lingkungan dalam perusahaan, hanya sebagian kecil saja gangguan sistem keamanan yang disebabkan oleh jaringan Internet. Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi investasi serta sumber daya di dalam jaringan komputer tersebut.

Sebagai efek dari makin banyaknya komputer yang terhubung ke Internet baik dalam suatu organisasi maupun intra organisasi, ancaman gangguan yang semula dapat dengan mudah dilokalisasi, sekarang menjadi lebih sulit karena dapat berpengaruh terhadap semua elemen jaringan. Beberapa jenis ancaman yang dapat diproteksi ketika komputer terhubung ke jaringan, dapat dikelompokkan menjadi katagori sebagai berikut:

1. **Menguping** (*eavesdropping*). Memantau seseorang atau sekelompok individu yang melakukan komunikasi data dan mencatat identitasnya untuk disalah-gunakan di kemudian hari. Seseorang menyadap *user ID* dan *password* yang tidak diacak yang dikirim melalui jaringan. Penyadap ilegal yang lebih canggih dapat mencuri semua isi pesan seperti e-mail, transaksi web, atau file yang di-*download*.
2. **Menyamar** (*masquerade*). Seorang user menggunakan identitas user lainnya. Pengacau membuat informasi yang sama dengan milik orang lain untuk memperoleh hak akses ke suatu jaringan.
3. **Pengulangan** (*reply*). Urutan kejadian atau perintah direkam dan dijalankan lagi pada kesempatan lain untuk memberi efek adanya akses tidak berijin. Jeleknya prosedur otentikasi dieksploitasi bersamaan dengan metoda penyamaran untuk mengalahkan sistem proteksi yang ada.
4. **Manipulasi data** (*data manipulation*). Integritas data dirusak selagi masih dalam media penyimpanan, atau selama ditransmisikan. Kurangnya pengawasan akses memungkinkan pengacau untuk masuk ke sistem dan memodifikasi data. Cara ini hampir sama dengan *reply* dan *masquerade* di mana pesan atau data yang terkirim disusupi dan dimodifikasi serta kemudian dikirim lagi ke alamat tujuan tanpa sepengetahuan pengirim dan penerima.
5. **Kesalahan penyampaian** (*misrouting*). Komunikasi untuk seorang user dialihkan ke user lain, yang dapat pula informasinya disusupi. *Misrouting* dapat digunakan

bersamaan dengan *masquerade*, manipulasi data, dan *reply*. Hal ini biasanya dapat terjadi pada jaringan yang tidak dirancang dengan baik.

6. **Pintu jebakan atau Kuda Troyan** (*trapdoor*). Rutin program yang dimasukkan secara legal ke dalam suatu sistem namun apabila dijalankan akan merusak sistem tersebut secara keseluruhan. Hal ini biasanya dapat terjadi karena prosedur pengelolaan sistem tidak menggunakan pengecekan *source-code* ketika suatu file di-*download* dari Internet.
7. **Virus** (*viruses*). Virus komputer adalah suatu rutin program yang menempel dan menjadi bagian dari rutin program lainnya serta dapat memperbanyak dirinya sendiri. Virus dapat merubah atau menghapus sistem arsip, serta merubah data. Virus menempatkan dirinya pada bootsector dan arsip data pada piranti penyimpanan (*hard disk*) sehingga setiap kali komputer dihidupkan secara otomatis virus akan aktif pula.
8. **Pengingkaran** (*repudiation*). Seseorang atau lebih yang masuk ke dalam jaringan dan melakukan transaksi namun menolak bahwa mereka telah masuk ke dalam sistem jaringan. Hal seperti ini merupakan ancaman terhadap kontrak atau transaksi keuangan secara elektronik melalui Internet.
9. **Penolakan Pelayanan** (*denial of service*). Pemasukan rutin program yang dapat menyebabkan semua akses ke dalam sistem atau aplikasi komputer terinterupsi atau ditolak. Hal ini dapat dilakukan dengan mengirim e-mail atau paket data dalam ukuran besar yang melebihi kapasitas jaringan atau sistem.

Bernstein (1996) menambahkan ada beberapa keadaan di Internet yang dapat terjadi sehubungan dengan lemahnya sistem keamanan antara lain:

1. Password seseorang dicuri ketika terhubung ke sistem jaringan dan ditiru atau digunakan oleh si pencuri.
2. Jalur komunikasi disadap dan rahasia perusahaan pun dicuri melalui jaringan komputer.
3. Sistem Informasi dimasuki (*penetrated*) oleh pengacau (*intruder*).
4. Server jaringan dikirim data dalam ukuran sangat besar (*e-mail bomb*) sehingga sistem macet.

Selain itu ada tindakan menyangkut masalah kemanan berhubungan dengan lingkungan hukum:

1. Kekayaan Intelektual (*intellectual property*) dibajak.
2. Hak cipta dan paten dilanggar dengan melakukan peniruan dan atau tidak membayar royalti
3. Terjadi pelanggaran terhadap ketentuan penggunaan teknologi tertentu.
4. Dokumen rahasia disiarkan melalui *mailing list* atau *bulletin boards*.
5. Pegawai menggunakan Internet untuk tindakan a-susila seperti pornografi.

Sistem keamanan yang berkaitan dengan masalah keuangan dan E-Commerce antara lain:

1. Data keuangan dapat dicuri atau dirubah oleh *intruder* atau *hacker*.
2. Dana atau kas disalah – gunakan oleh petugas yang memegangnya
3. Pemalsuan uang
4. Seseorang dapat berpura – pura sebagai orang lain dan melakukan transaksi keuangan atas nama orang lain tersebut.

Selain beberapa kelemahan di atas, ada permasalahan yang lebih serius terutama jika dikaitkan dengan “efek kompresi waktu” yang terjadi dalam Internet. Dengan kemampuan Internet untuk menghubungkan jaringan komputer di seluruh dunia, transaksi keuangan yang dilakukan secara online memiliki dampak yang cukup besar. Dengan hanya menekan satu tombol click saja kita dapat membuat transaksi antar – benua yang dapat bermuara pada keuntungan atau kerugian keuangan. Di satu sisi, kecepatan komunikasi elektronik memberi banyak kemudahan, namun di sisi lain hal ini mengurangi proses pengawasan secara manual yang pada beberapa keadaan masih diperlukan. Dalam membangun sistem keamanan dalam Internet dan atau E-Business fleksibilitas perlu diberi perhatian, tetapi tanpa mengurangi ketangguhan dari sistem keamanan tersebut.

Penggunaan komputer sebagai sarana dalam melakukan kejahatan dapat dikategorikan sebagai computer crime yaitu setiap tindakan melawan hukum dengan menggunakan komputer, baik melalui sistemnya maupun aplikasinya yang menimbulkan kerugian bagi seseorang atau badan hukum. Selain kejahatan konvensional yang menggunakan komputer, muncul pula kejahatan jenis baru yang menargetkan sistem komputer lain sebagai sasarannya. Kejahatan ini makin signifikan baik modus, jangkuan maupun jumlah korbannya seiring dengan makin tersebar-luasnya penggunaan Internet

untuk bertransaksi bisnis. Kejahatan jenis ini sering disebut cybercrime, yakni penggunaan Internet untuk merusak sistem komputer lain atau untuk tujuan penipuan, memperoleh akses yang seharusnya bukan menjadi haknya, penggunaan Internet untuk meng-copy data tanpa izin, maupun penggunaan Internet untuk menyebarkan virus komputer. Semua kasus tersebut di atas telah terjadi di Indonesia, namun hingga saat ini belum ada peraturan perundang – undangan yang mengaturnya khususnya yang mempidana kejahatan – kejahatan tersebut agar tidak ada pihak yang dirugikan dan perbuatan tersebut tidak dilakukan lagi.

Penggunaan Teknologi Informasi khususnya Internet yang memiliki dampak merugikan bagi orang lain adalah ketika terjadi gangguan terhadap privasi individu seperti penyebaran data pribadi melalui Internet, atau pengiriman dan penerimaan surat elektronik yang jumlahnya besar dan tidak berkaitan dengan si penerima sehingga menghambat masuknya e-mail lain yang diharapkan (*email bomb*), seseorang selalu mengintip pola penggunaan Internet orang lain (*cyber stalking*), dan lain sebagainya. Masalah gangguan terhadap privasi (*privacy breaches*) terkait dengan keselamatan dan keamanan data transaksi dari segala gangguan sadapan (*wiretapping*) atau intersepsi dan pencurian data dari pihak manapun karena hal ini terkait dengan prasyarat komunikasi data yang handal yakni *confidentiality*, *integrity*, dan *availability* data, sehingga perlu diatur dalam Undang – Undang Tindak Pidana Di Bidang Teknologi Informasi.

Selain masalah pelanggaran privasi, European Convention on Cybercrime (2001) menambahkan ada tiga jenis praktik kejahatan baru yang muncul dengan adanya Internet: *Offences against the confidentiality, integrity and availability of computer data and system; computer related offenses*; dan *offences related to infringement of copy right and related rights*. Kejahatan tipe pertama meliputi: akses ilegal (*illegal access*), intersepsi ilegal (*illegal interception*), interferensi data (*data interference*), interferensi sistem (*system interference*), dan penyalah-gunaan peralatan komputer (*misuse of device*). Kejahatan tipe kedua meliputi: *computer related forgery, computer related fraud, offences related to child pornography*. Sedangkan kejahatan tipe ketiga meliputi kejahatan terhadap Hak Kekayaan Intelektual. Selain jenis – jenis kejahatan sebagaimana diidentifikasi di atas, masih terdapat jenis tindak kejahatan lain yang muncul setelah



adanya Internet, antara lain *cyber-gambling*, *cyber-pornography*, *counterfeiting*, *defamation*, *hackers*, *drug cartel*, *cybersquatting*, dan *international money laundering*.

Dalam beberapa literatur, cybercrime sering diidentikkan sebagai *computer crime*. *The U.S. Department of Justice* memberikan pengertian computer crime sebagai:

“...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution”.

Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu “any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data”. Andi Hamzah dalam bukunya *Aspek-aspek Pidana di Bidang Komputer* (1989) mengartikannya sebagai “kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal”. Dari beberapa pengertian tersebut, computer crime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih (Wisnubroto, 1999).

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan Teknologi Informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:

1. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

3. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui Internet.

4. *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.

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. *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.

7. *Infringements of Privacy*

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

Pada dasarnya cybercrime meliputi semua tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*).

## 5. Perkembangan Hukum Pidana Teknologi Informasi

Kebijakan kriminal (*criminal policy*) mencakup pendekatan penal melalui sistem peradilan pidana, dan kriminalisasi (*criminalization*) yang mengatur ruang lingkup perbuatan yang bersifat melawan hukum (*actus rea*), pertanggung-jawaban pidana (*mens rea*), dan sanksi yang dapat dijatuhkan, baik berupa pidana (*punishment*) maupun tindakan (*treatment*). Dalam era demokratisasi, perumusan peraturan hukum harus mempertimbangkan secara komprehensif beragam dimensi persoalan. Semua aspirasi dan pelbagai kepentingan harus diseleraskan dan diserasikan. Salah satu hal yang penting untuk perlu menjadi pertimbangan adalah persoalan komunikasi massa yang menempati posisi strategis dalam kehidupan demokrasi dan akan bersentuhan secara langsung tidak hanya dengan persoalan supremasi hukum yang bersifat *top down* – misalnya kepentingan keamanan negara dan kesatuan nasional – tetapi juga sebaliknya *bottom up*, sebab masyarakat akan cenderung melemparkan pertanyaan kritis dan tidak begitu saja menerima produk suatu hukum (Muladi, 2003). Dalam konteks ini masyarakat akan mempersoalkan hak – hak warga seperti kebebasan berekspresi, kebebasan media, dan masalah – masalah HAM yang lain seperti persoalan privasi, hak untuk memperoleh informasi, dan lain sebagainya yang saat ini sangat diperhatikan dalam legislasi positif nasional. Di sinilah relevansi persoalan hak dan kewajiban menjadi penting. Dalam penegakan hukum keberadaan hak – hak harus dijaga keseimbangannya dengan efisiensi dan efektivitas penegakan hukum.

Seiring munculnya dan berkembangnya Teknologi Informasi dan mulai adanya kejahatan yang menggunakan Teknologi Informasi terjadi pula perkembangan perangkat hukum, khususnya yang mengatur perilaku penggunaan dan pidana bagi pelaku kejahatan di bidang Teknologi Informasi. Pada tahap pertama masyarakat menggunakan *soft law* dalam bentuk kode etik atau kode perilaku (*code of conduct*). Misalnya di Jepang (1996) dan di Singapura dalam bentuk *Internet Code of Conduct*. Namun demikian upaya semacam ini masih dipandang belum mencukupi terbukti dengan makin luasnya penyalah-gunaan TI dan Internet, sehingga kemudian dibuatlah hukum administratif yang bersifat *semi hard law* berupa *code of practice* seperti yang dirumuskan oleh the Australian Internet Industry Association, 1999. *Code of conduct*, kode etik, dan *code of*

*practice* tergolong kebijakan kriminal yang menggunakan sarana non-penal (*prevention without punishment*). Ketika kejahatan Teknologi Informasi sudah semakin canggih dan korbannya sudah makin banyak serta melibatkan kejahatan transnasional, sarana penegakan hukum yang dilakukan adalah dengan melakukan kriminalisasi berupa penerapan hard law berupa Undang – Undang, sebagaimana dilakukan oleh Singapura dengan membuat *Computer Misuse Act* (1993), dan Malaysia dalam bentuk *Computer Crimes Act* (1997).

Barda Nawawi Arief, dalam Mardjono (2002), mengusulkan agar dalam hal kriminalisasi, dibedakan antara (a) harmonisasi materi/substansi dan (b) harmonisasi kebijakan formulasi. Yang pertama adalah tentang apa yang akan dinamakan tindak pidana di bidang Teknologi Informasi, dan yang kedua apakah pengaturan hukuman pidana bagi kejahatan Teknologi Informasi tersebut akan berada di dalam atau di luar KUH Pidana. Untuk hal pertama, merujuk pada *Convention on Cyber Crime* dari Dewan Eropa (ditanda –tangani di Budapest, Hungaria pada tanggal 23 November 2001) dikategorikan delik sebagai berikut:

1. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer. Termasuk di sini:
  - a. mengakses sistem komputer tanpa hak (*illegal access*);
  - b. tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
  - c. tanpa hak merusak data (*data interference*);
  - d. tanpa hak mengganggu sistem (*system interference*);
  - e. menyalahgunakan perlengkapan (*misuse of devices*);
2. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer-*computer related offenses : forgery and fraud*);
3. Delik-delik yang bermuatan pornografi anak (*content-related offenses, child pornography*);
4. Delik-delik yang berhubungan dengan hak cipta (*offences related to infringements of copyright*).

Tentang kebijakan formulasi, dapat dilakukan dua pendekatan sebagai berikut:

- a. Menganggapnya sebagai kejahatan biasa (*ordinary crime*) yang dilakukan dengan komputer teknologi tinggi (*high-tech*) dan KUHP - dengan diamanemen - dapat dipergunakan untuk menanggulangnya;
- b. Menganggapnya sebagai kejahatan kategori baru (*new category of crime*) yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan biasa (misalnya masalah yurisdiksi, dan karena itu perlu diatur secara tersendiri di luar KUHP).

Mardjono lebih jauh berargumen bahwa Indonesia dapat menggunakan kedua pendekatan tersebut bersama-sama, sebagaimana Amerika Serikat mempergunakan kedua pendekatan tersebut bersama-sama, misalnya dengan mengamenden *Securities Act* 1933 (UU Pasar Modal) dan mengundang *Computer Fraud and Abuse Act*.

Sebaliknya di Belanda *Commissie Franken* dalam tahun 1987 dan Kaspersen menganjurkan pendekatan pertama dan hanya menyempurnakan *Wetboek van Strafrecht* (Kasperen, 1990). *Commissie Franken* merumuskan sembilan bentuk penyalahgunaan (*misbruikvormen*):

1. tanpa hak memasuki sistem komputer;
2. tanpa hak mengambil (*onderscheppen*) data komputer;
3. tanpa hak mengetahui (*kennisnemen*);
4. tanpa hak menyalin/mengkopi;
5. tanpa hak mengubah;
6. mengambil data;
7. tanpa hak mempergunakan peralatan;
8. sabotase sistem komputer;
9. mengganggu telekomunikasi (Kasperen : 315).

Perumusan *Commissie Franken* dibuat lebih dari 13 tahun yang lalu. Sementara ini cyber crime telah mengalami perkembangan yang menakutkan, karena itu perlu dipelajari bersama dengan saran-saran Konvensi Dewan Eropa 2000.

Namun demikian, dalam usaha kriminalisasi-primair (menyatakan sebagai delik perbuatan dalam *abstracto*) sebaiknya kita berpedoman pada 7 asas yang dikemukakan de Roos (1987), yaitu:

- a. masuk akal nya kerugian yang digambarkan;
- b. adanya toleransi yang didasarkan pada penghormatan atas kebebasan dan tanggungjawab individu;
- c. apakah kepentingan yang dilanggar masih dapat dilindungi dengan cara lain (asas subsidiaritas);
- d. ada keseimbangan antara kerugian, toleransi dan pidana yang diancamkan (asas proportionalitas);
- e. apakah kita dapat merumuskan dengan baik, sehingga kepentingan hukum yang akan dilindungi, tercermin dan jelas hubungannya dengan asas kesalahan – sendi utama hukum pidana;
- f. kemungkinan penegakannya secara praktis dan efektif (serta dampaknya pada prevensi umum).

Di dalam negeri, meskipun di dalam KUHP tidak ada pasal – pasal yang secara khusus mengatur kejahatan komputer dan atau Teknologi Informasi, namun demikian ada beberapa pasal yang dapat digunakan sebagai acuan. Tentu saja dalam menggunakannya diperlukan perluasan pengertian mengenai objek yang diatur [barang] dari yang semula rumah atau pekarangan (*property*) menjadi komputer atau sistem komputer.

KUHP Pasal 167 ayat (1) berbunyi:

*Barang siapa dengan melawan hukum masuk dengan paksa ke dalam, atau melawan hukum ada di dalam rumah atau tempat yang tertutup atau pekarangan yang tertutup, yang dipakai oleh orang lain dan tidak segera pergi dari tempat itu, atas permintaan orang yang berhak atau permintaan atas nama yang berhak, dipidana dengan pidana penjara selama – lamanya sembilan bulan atau denda sebanyak – banyaknya empat ribu lima ratus rupiah.*

Pasal ini sebetulnya untuk memidana pelaku kejahatan terhadap hak kebebasan dan ketenteraman rumah tangga. Perbuatan yang diancam hukuman dalam pasal ini adalah:

- a. dengan melawan hukum masuk ke rumah, ruangan tertutup dan sebagainya dengan paksa;
- b. dengan melawan hukum berada di rumah, ruangan tertutup dan sebagainya, serta tidak segera pergi dari tempat itu atas permintaan yang berhak atas rumah atau ruangan tersebut.

Masuk dengan demikian saja, belum dapat diartikan sebagai “masuk dengan paksa”. Yang dapat diartikan “masuk dengan paksa” ialah masuk dengan cara yang bertentangan dengan kehendak yang dinyatakan sebelumnya oleh yang berhak, misalnya: dengan perkataan, dengan perbuatan, dengan tulisan “dilarang masuk” atau tanda – tanda lain yang sama artinya dan dapat dipahami oleh orang di daerah sekitarnya. Yang dapat dianggap sebagai masuk dengan paksa adalah orang yang masuk dengan jalan membongkar, memanjat, memakai anak kunci palsu, perintah palsu, pakaian jabatan palsu atau orang yang bukan karena kekeliruan masuk ke tempat itu dan orang yang berada di tempat tersebut.

Relevansi pasal 167 ayat (1) KUHP ini dengan kejahatan Teknologi Informasi adalah adanya kesamaan konsepsi antara rumah dan pekarangan dengan komputer atau fasilitas sistem komputer atau jaringan komputer di mana semuanya memenuhi konsep “ruang” untuk menaruh barang milik atau properti. Jika rumah dan atau tempat tertutup digunakan untuk menyimpan harta benda, sistem komputer juga dipakai untuk menyimpan harta benda berupa program dan data yang perlu dilindungi. Oleh karena itu bila ada pihak yang masuk ke fasilitas sistem komputer dan atau jaringan komputer tanpa hak, apalagi tindakannya dengan melawan hukum seperti memalsu identitas, merusak password, dan atau kunci rahasia yang melindungi sistem komputer tersebut, maka tindakan ini dapat disetarakan dengan tindakan melawan hukum yang melanggar pasal 167 ayat (1) KUHP.

Selanjutnya dalam Pasal 191 bis, dinyatakan:

*Barang siapa dengan sengaja menghancurkan, merusakkan, atau membuat sampai tidak dapat dipakai lagi sesuatu bangunan listrik atau merintanginya atau bekerjanya listrik itu, atau menggagalkan atau merintanginya ikhtiar untuk menjaga keselamatan atau untuk memperbaiki bangunan listrik itu, dipidana:*

*ke-1. dengan pidana penjara selama – lamanya sembilan bulan atau denda sebanyak – banyaknya empat ribu lima ratus rupiah, jika terjadi halangan atau rintangan untuk memberi kekuatan listrik bagi keperluan umum;*

*ke-2. dengan pidana penjara selama – lamanya tujuh tahun, jika perbuatannya itu dapat mendatangkan bahaya umum untuk barang;*

*ke-3. dengan pidana penjara selama – lamanya sembilan tahun, jika perbuatannya itu dapat mendatangkan bahaya maut untuk orang;*

*ke-4. dengan pidana penjara selama – lamanya lima belas tahun, jika perbuatannya itu mendatangkan bahaya maut kepada orang dan perbuatannya itu berakibat matinya orang.*

Yang diancam hukuman dengan pasal ini ialah perbuatan dengan sengaja menghancurkan, merusakkan, atau membuat demikian rupa sehingga tidak dapat dipakai lagi sesuatu bangunan listrik atau merintanginya jalannya atau bekerjanya listrik itu, atau pula, menggagalkan atau merintanginya khtiar untuk menjaga keselamatan atau untuk memperbaiki bangunan listrik tersebut. Relevansi pasal ini dengan kejahatan dunia cyber adalah karena pada dasarnya sistem komputer merupakan bangunan rangkaian listrik yang saling terhubung dan melaksanakan fungsi – fungsi tertentu untuk memenuhi kepentingan manusia pada umumnya. Sehingga dengan demikian, tindakan menghancurkan, merusakkan atau membuat sampai tidak dapat dipakai lagi sesuatu fasilitas sistem komputer, terutama komputer yang dimiliki oleh lembaga publik: pemerintah, militer, perbankan, parlemen, polisi dan lain sebagainya, sama saja dengan merusak bangunan atau instalasi listrik sebagaimana dimaksud pada pasal 191 bis KUHP.

Untuk memperkuat acuan, dapat ditambahkan dengan Pasal 551 yang menyatakan bahwa:

*Barangsiapa, tanpa berhak, berjalan atau berkendara di atas tanah kepunyaan orang lain, oleh yang berhak dilarang dimasuki dan sudah diberi tanda larangan yang nyata bagi pelanggar, dipidana dengan pidana denda sebanyak – banyaknya dua ratus lima puluh rupiah.*

Jika hanya dilihat susunan kata per katanya saja, kesimpulan yang dapat ditarik hanyalah bahwa pasal ini melarang kepada orang yang berjalan atau berkendara di atas tanah orang lain yang nyata – nyata sudah diberi tanda larangan bahwa tanah itu tidak boleh dilalui. Namun demikian apabila dilakukan kajian perluasan konsepsi, tanah identik dengan ruang atau fasilitas sistem komputer karena memiliki kesamaan sifat yaitu properti. Berjalan atau berkendara di atas tanah tanpa ijin meski sudah ada larangan dapat disamakan sebagai akses kepada fasilitas komputer tanpa ijin. Penggunaan *user-id*,



*password* dan alat verifikasi lainnya dapat disamakan sebagai peringatan larangan masuk tanpa izin.

Di bidang telekomunikasi yang merupakan bagian dari Teknologi Informasi, ketentuan yang mengatur tindak pidana kejahatan telekomunikasi sudah diatur dalam Undang – Undang Nomor 36 tahun 1999, dalam pasal 22 berbunyi:

*Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:*

- f. akses ke jaringan telekomunikasi; dan atau*
- g. akses ke jasa telekomunikasi; dan atau*
- h. akses ke jaringan telekomunikasi khusus.*

Penekanan dari pasal ini adalah larangan terhadap akses tidak sah kepada jaringan dan jasa telekomunikasi. Pada kenyataannya dan sesuai dengan definisi telekomunikasi (pasal 1 UU 36/1999) tidak ada perbedaan lagi antara jaringan dan jasa telekomunikasi dengan jaringan dan jasa Teknologi Informasi, karena di dalamnya juga selalu terdapat sistem komputer. Oleh karena itu, tindakan mengakses sistem komputer dengan tidak sah dapat dikenai tuntutan pidana sesuai pasal 50 yang berbunyi:

*Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,- (enam ratus juta rupiah).*

Tiga pasal KUHP di atas dan dua pasal dari Undang – Undang Telekomunikasi belum lazim digunakan sebagai acuan bagi aparat penegak hukum untuk menjerat pelaku kejahatan komputer untuk kategori tindakan akses tidak sah. Salah satu persoalan yang menyulitkan digunakannya pasal – pasal tersebut di atas adalah pada pembuktian. Selain karena pada umumnya aparat penegak hukum belum memiliki pengetahuan dan ketrampilan yang memadai mengenai substansi bidang Teknologi Informasi, sehingga oleh karenanya timbul permasalahan tersendiri ketika mengumpulkan barang bukti, juga karena undang – undang yang adapun belum mengatur dan mengakui catatan elektronik sebagai alat bukti yang sah di pengadilan. Berangkat dari kenyataan ini, diperlukan keberanian luar biasa pada para polisi, jaksa dan hakim untuk menyidik, menuntut, dan memutus perkara cybercrime dengan menggunakan perangkat hukum yang sudah ada.

Dengan memperhatikan referensi yang ada, lingkup tindak pidana pemanfaatan Teknologi Informasi meliputi seluruh jenis kejahatan baik yang telah diatur maupun belum diatur dalam Kitab Undang – Undang Hukum Pidana (KUHP) dan yang terbukti dilakukan oleh siapa saja dengan memanfaatkan Teknologi Informasi. Penentuan ancaman dan hukuman terhadap pelaku kejahatan Teknologi Informasi berdasarkan bobot pemanfaatan Teknologi Informasi dalam kejahatan dimaksud dan besarnya ancaman hukuman. Semakin besar bobot pemanfaatan Teknologi Informasi dalam kejahatan dimaksud semakin besar peluang penggunaan Undang – Undang Tindak Pidana di Bidang Teknologi Informasi (UU-TIPITI) ini.

Yang tergolong pelanggaran sehingga perlu diatur dalam UU-TIPITI ini adalah:

- a. Barangsiapa memanfaatkan Teknologi Informasi dengan melawan hukum.
- b. Barangsiapa melakukan intersepsi dengan melawan hukum.
- c. Barangsiapa dengan sengaja dan melawan hukum merusak atau mengganggu data yang tersimpan dalam alat penyimpan data elektronik yang tersusun sebagai bagian dari sistem komputer.
- d. Barangsiapa dengan sengaja menghilangkan bukti – bukti elektronik yang dapat dijadikan alat bukti sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer.
- e. Barangsiapa dengan sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer, dan Internet.
- f. Barangsiapa memanfaatkan Teknologi Informasi untuk menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi.
- g. Barangsiapa memanfaatkan Teknologi Informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat – sifat pornografi.
- h. Barangsiapa memanfaatkan Teknologi Informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.
- i. Setiap badan hukum penyelenggara jasa akses Internet atau penyelenggara layanan Teknologi Informasi, baik untuk keperluan komersial maupun keperluan internal perusahaan, dengan sengaja tidak menyimpan atau tidak dapat menyediakan catatan transaksi elektronik sedikitnya untuk jangka waktu dua tahun.

## 6. Alat Bukti Elektronik Dalam Hukum Pidana

Pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu (Muladi, 2003). Hal ini disebabkan oleh luasnya kausa dan motif berkembangnya jenis kejahatan yang berbasis teknologi Informasi dewasa ini. Penggunaan transaksi elektronik yang tidak menggunakan kertas (*paperless transaction*) dalam sistem pembayaran menimbulkan permasalahan khususnya terkait dengan ketentuan pembuktian sebagaimana diatur dalam Pasal 184 Kitab Undang – undang Hukum Acara Pidana yang menetapkan alat bukti yang sah adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Sedangkan dalam Pasal 1866 Kitab Undang-undang Hukum Perdata disebutkan alat –alat bukti terdiri atas: bukti tulisan, bukti dengan saksi – saksi, persangkaan, pengakuan dan sumpah.

Berkenaan dengan hukum pembuktian dalam proses peradilan baik dalam perkara pidana maupun perdata, akibat kemajuan teknologi khususnya Teknologi Informasi, ada suatu persoalan mengenai bagaimana kedudukan produk teknologi , khususnya catatan elektronik, sebagai alat bukti. Sebagai contoh, penggunaan teleconference dalam persidangan oleh beberapa kalangan dipandang sebagai terobosan hukum atau penemuan hukum karena penggunaan teknologi ini belum diatur dalam KUHAP. Di dalam KUHAP telah nyata – nyata secara jelas menentukan keharusan kehadiran saksi dalam persidangan. Keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan di sidang pengadilan. Dalam hal penggunaan tele-videoconference kehadiran saksi di sidang pengadilan bukan secara fisik,namun secara virtual, hal inilah yang masih menimbulkan pro dan kontra apakah kehadiran secara virtual ini dapat disetarakan dengan kehadiran fisik.

Mengenai keabsahan transaksi dan kekuatan pembuktian, transaksi elektronik tidak memerlukan hard copy atau warkat kertas, namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti berupa nomer atau kode yang dapat disimpan/direkam di komputer atau dicetak. Permasalahannya muncul ketika terjadi sengketa, apakah bukti/kode nomor transaksi dapat digunakan sebagai alat bukti yang muat menurut hukum Indonesia, mengingat Indonesia belum memiliki ketentuan khusus

yang mengatur kegiatan dan transaksi elektronik melalui Internet. Sementara belum ada perundangan yang mengatur masalah ini, Sundari (2003) berpendapat bahwa sesuai Pasal 1338 Kitab Undang – Undang Hukum Perdata, perjanjian di antara bank dan nasabah mengikat kedua belah pihak dan berlaku seperti undang – undang bagi kedua belah pihak (*pacta sun servanda*), sehingga bukti/kode nomor transaksi yang dipegang oleh kedua belah pihak tersebut dapat diperlakukan sebagai alat bukti yang sah.

Pengakuan catatan transaksi elektronik sebagai alat bukti yang sah di pengadilan sudah dirintis oleh *United Nation Commission on International Trade* (UNCITRAL) yang mencantumkan dalam *e-commerce model law* ketentuan mengenai transaksi elektronik diakui sederajat dengan “tulisan” di atas kertas sehingga tidak dapat ditolak sebagai bukti pengadilan. Mengacu pada ketentuan UNCITRAL, ada peluang bagi Indonesia untuk menempatkan tanda tangan atau bukti elektronik sebagai alat bukti yang sah, sepanjang ditetapkan dalam Undang – Undang yang khusus mengatur soal transaksi elektronik.

Masalah pelik yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku kejahatan Teknologi Informasi yang mengusik rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku. Kendala yang klasik adalah sulitnya menghukum si pelaku mengingat belum lengkapnya ketentuan pidana yang mengatur tentang kejahatan komputer, Internet atau Teknologi Informasi. Masalah utama adalah belum diterimanya dokumen elektronik (misalnya file komputer) sebagai alat bukti oleh konsep yang dianut UU No 8/1981 (KUHP). Pasal 184 ayat (1) dari Undang undang ini secara definitive membatasi alat-alat bukti hanyalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa saja.

Satu fiksi hukum berikut ini cukup memberikan gambaran kendala tersebut : Seorang pegawai di sebuah instansi pertahanan pemerintah menyalin data-data rahasia yang tersimpan di dalam media penyimpan komputer ke dalam sebuah disket yang memang tersedia di tempat kerja tersebut. Ketika sedang menyerahkan disket yang berisi rahasia negara tersebut kepada pihak lawan, pegawai tersebut berhasil ditangkap oleh dinas Intelijen pemerintah. Studi terhadap masalah hukum yang muncul atas fiksi hukum di atas adalah sulitnya menjaring si pelaku atas sangkaan pembocoran rahasia negara. Kalaupun kasus dilanjutkan maka yang terjadi adalah sebuah kontroversial yaitu

sangkaan terhadap si pelaku sebagai penggelapan sebuah disket. Fiksi hukum di atas memang bukanlah contoh kejahatan komputer. Namun mengingat kejahatan komputer banyak berhubungan dengan data elektronik yang tersimpan di dalam disket, hard disk, CD ROM, dan sebagainya, akan sulit bagi Jaksa untuk mendakwa si pelaku mengingat tidak diakuinya dokumen elektronik sebagai alat bukti oleh KUHAP.

Mengingat kelemahan KUHAP tersebut, dalam menjalankan tugasnya penyidik harus dengan cerdas menggunakan definisi dokumen elektronik yang dapat diterima sebagai alat bukti. Pada dasarnya dalam praktik peradilan hakim sudah menerima dokumen elektronik sebagai alat bukti, meskipun hal ini mungkin dilakukan tanpa sadar. Dalam kasus-kasus pidana yang berhubungan dengan perbankan umumnya rekening Koran atau dokumen apapun yang berisikan data nasabah berikut laporan keuangannya dihadirkan sebagai alat bukti surat. Padahal yang dimaksud dengan rekening koran sebenarnya adalah cetakan (*print out*) laporan keuangan nasabah yang dalam bentuk aslinya berupa dokumen elektronik (*file komputer*).

Prosedur system perbankan modern saat ini seluruhnya menggunakan komputer sebagai petugas yang secara otomatis mendebet rekening nasabah (misalnya pengambilan lewat ATM atau pengambilan melalui cek dan giro), atau secara otomatis menambahkan bunga atas dana nasabah. Seluruh proses ini dicatat oleh komputer dan disimpan dalam bentuk file. Dengan demikian seluruh proses pembuktian kasus-kasus perbankan dalam kaitannya dengan dana nasabah sangatlah mustahil didasarkan pada dokumen yang aslinya berbentuk kertas. Kalaupun ada dokumen berbentuk kertas maka itu hanyalah cetakan file komputer pada bank yang bersangkutan. Dengan diterimanya rekening Koran tersebut sebagai alat bukti surat maka hal ini dapat menjadi dasar bagi penyidik untuk menggunakan cetakan file komputer sebagai alat bukti surat.

Doktrin tentang hal ini juga diberikan oleh Subekti (1995). Menurut Subekti pembuktian adalah upaya meyakinkan Hakim akan hubungan hukum yang sebenarnya antara para pihak dalam perkara, dalam hal ini antara bukti-bukti dengan tindak pidana yang didakwakan. Dalam mengkonstruksikan hubungan hukum ini, masing-masing pihak menggunakan alat bukti untuk membuktikan dalil-dalilnya dan meyakinkan hakim akan kebenaran dalil-dalil yang dikemukakan. Untuk itu hakim patut menerima dalil-dalil para

pihak (jaksa ataupun terdakwa) tanpa harus dikungkung oleh batasan alat-alat bukti sepanjang dalil tersebut memenuhi prinsip-prinsip logika.

Untuk memperjelas pendapat Subekti tersebut, ilustrasi dibawah ini mungkin akan memberikan pemahaman yang lebih memperluas cakrawala berpikir: Pernah dipersoalkan, apakah selain lima macam “alat bukti” yang disebutkan dalam pasal 1866 Kitab Undang-undang Hukum Perdata, Pasal 164 RIB (Kini oleh KUHAP diatur dalam Pasal 184 ayat (1) atau pasal 283 RDS, tidak terdapat lagi alat-alat bukti lainnya. Persoalan tersebut lazimnya dijawab, bahwa penyebutan alat-alat bukti dalam pasal-pasal tersebut tidak berarti melarang alat-alat bukti lainnya yang bukan tulisan. Pasal 1887 Kitab Undang-undang Hukum Perdata misalnya menyebutkan “tongkat berkelar” yang dapat dipakai untuk membuktikan penyerahan-penyerahan barang. Ada juga yang mengatakan bahwa bukti lain itu yang tidak berupa tulisan, kesaksian, pengakuan, atau sumpah, seyogyanya saja dianggap sebagai “persangkaan”, tetapi pendapat yang demikian itu tidak tepat. Kita juga tidak boleh melupakan bahwa undang-undang yang kita pakai sekarang ini dibuat seratus tahun yang lalu. Dengan kemajuan dalam berbagai bidang teknologi yang pesat dalam setengah abad yang lalu ini muncullah beberapa alat baru, seperti fotocopy, tape recorder, dan lain-lain yang dapat dipakai sebagai alat bukti.

## 7. Kejahatan Transnasional

Kemajuan Teknologi Informasi yang sedemikian pesat telah melahirkan Internet sebagai sebuah fenomena dalam kehidupan umat manusia. Internet, yang didefinisikan oleh The U.S. Supreme Court sebagai *international network of interconnected computers* (Reno v. ACLU, 1997), telah menghadirkan berbagai kemudahan bagi setiap orang, bukan saja untuk berkomunikasi, tetapi juga untuk melakukan banyak hal lainnya seperti transaksi bisnis. Pada perkembangannya, ternyata penggunaan Internet, selain berdampak positif juga membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti-sosial dan perilaku kejahatan yang selama ini dianggap tidak mungkin terjadi. Sebagaimana sebuah teori mengatakan, *crime is a product of society itself*, yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas suatu masyarakat, semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat itu.

Sebagaimana diketahui hukum positif di Indonesia masih bersifat *lex loci delicti* yang mencakup wilayah, barang bukti, tempat/fisik kejadian serta tindakan fisik yang terjadi. Padahal, kondisi pelanggaran yang mungkin terjadi di cyberspace dapat dikatakan sangat bertentangan dengan hukum positif yang ada tersebut. Mengingat sifat kejahatan Teknologi Informasi khususnya Internet cenderung bersifat lintas negara (*transborder crimes*) maka langkah kebijakan kriminal, baik yang berupa penal maupun non-penal memerlukan kerja sama internasional, apakah berupa *mutual assistance*, ekstradisi, maupun bentuk – bentuk kerjasama lainnya. Dalam beberapa kasus kejahatan transnasional seperti narkoba dan pencucian uang penggunaan Teknologi Informasi sangat mendukung keberhasilan kejahatan dimaksud, dan diakui lebih efisien dalam operasionalnya. Karena itu dibutuhkan langkah – langkah harmonisasi hukum antar bangsa sebagai bagian dari kerja sama internasional dalam kaitannya dengan *double criminality principle*.

Antisipasi terhadap perkembangan kejahatan transnasional menggunakan Teknologi Informasi melalui proses kriminalisasi telah dilakukan dengan berbagai konvensi internasional dan perundang – undangan nasional dengan tujuan untuk dapat mencegah dan memberantas kejahatan dimaksud secara efektif (Romli, 2003). Namun

perkembangan kejahatan transnasional tersebut juga bersentuhan dengan yuridiksi hukum dua negara atau lebih yang mengakibatkan semakin potensial menimbulkan konflik yurisdiksi hukum sehingga pada gilirannya semakin rumit penegakan hukum dalam kasus – kasus kejahatan transnasional dimaksud. Antisipasi sistem hukum pidana terhadap kejahatan transnasional melalui penggunaan Teknologi Informasi dapat dibedakan dalam tiga lingkup masalah, yaitu, pertama, masalah definisi kejahatan yang dilakukan melalui sarana Teknologi Informasi khususnya penggunaan komputer atau yang dikenal dengan *cybercrime*. Kedua, masalah berlakunya hukum pidana negara tertentu terhadap kejahatan transnasional melalui penggunaan Teknologi Informasi; dan Ketiga, mengenai masalah pembuktian hukum atas kasus – kasus kejahatan transnasional dimaksud.

Untuk menjamin adanya kemampuan menangani kejahatan transnasional, Undang - Undang Tindak Pidana di Bidang Teknologi Informasi ini berlaku terhadap setiap orang atau badan hukum yang melakukan tindak pidana di bidang Teknologi Informasi di wilayah negara Republik Indonesia dan atau negara lain yang mempunyai yurisdiksi dan menyatakan maksudnya untuk melakukan penuntutan terhadap pelaku tersebut. Negara lain mempunyai yuridiksi sebagaimana dimaksud dalam ayat (1), apabila :

- a. Kejahatan dilakukan oleh warga negara dari negara yang bersangkutan;
- b. Kejahatan dilakukan terhadap warga negara dari negara yang bersangkutan;
- c. Kejahatan tersebut juga dilakukan di negara yang bersangkutan;
- d. Kejahatan dilakukan terhadap suatu negara atau fasilitas pemerintah dari negara yang bersangkutan di luar negeri termasuk fasilitas kantor perwakilan atau tempat fasilitas pejabat diplomatik atau konsuler dari negara yang bersangkutan;
- e. Kejahatan dilakukan dalam pesawat udara yang dioperasikan oleh pemerintah negara yang bersangkutan; atau
- f. Kejahatan dilakukan dalam kapal yang berbendera negara tersebut atau pesawat udara yang terdaftar berdasarkan Undang-Undang negara yang bersangkutan pada saat kejahatan itu dilakukan.

Lebih jauh, Undang-Undang Tindak Pidana di Bidang Teknologi Informasi ini berlaku juga terhadap tindak pidana pemanfaatan teknologi informasi yang dilakukan :

- a. Terhadap warga negara Republik Indonesia yang berkedudukan di luar wilayah negara Republik Indonesia;



- b. Terhadap fasilitas negara Republik Indonesia di luar negeri, termasuk fasilitas pejabat diplomatik dan konsuler Republik Indonesia;
- c. Dalam kapal yang berbendera negara Republik Indonesia atau pesawat udara yang terdaftar berdasarkan undang-undang negara Republik Indonesia pada saat kejahatan itu dilakukan; atau
- d. Oleh setiap orang yang tidak memiliki kewarganegaraan dan bertempat tinggal di wilayah negara Republik Indonesia;

## 8. Model Regulasi

Pengaturan tentang kejahatan Teknologi Informasi (*cybercrime*) pada hakekatnya merupakan pengaturan aspek hukum pidana dari *cyberlaw*. Dapat dikatakan bahwa sampai saat ini belum ada definisi yang seragam tentang *cybercrime*, baik nasional maupun di aras global. Terlepas dari belum adanya kesepakatan mengenai definisi *cybercrime*, yang pasti berbagai negara maupun fora internasional telah berupaya memerangi kejahatan Teknologi Informasi tersebut dengan membuat resolusi, konvensi, ataupun perundang-undangan.

### **Perserikatan Bangsa - Bangsa**

Sidang Umum PBB pada tanggal 4 Desember 2000 menanda – tangani Resolusi 55/63 yang berisi tentang memerangi tindakan kriminal penyalah-gunaan Teknologi Informasi. Butir – butir Resolusi yang selanjutnya menandai dimulainya perhatian dunia terhadap masalah kejahatan Teknologi Informasi selengkapnya sebagai berikut:

- c. Setiap negara harus menjamin bahwa hukum dan praktik hukum tidak melindungi pelaku kejahatan Teknologi Informasi;
- d. Kerja sama penegakan hukum dalam investigasi dan prosecution kasus – kasus internasional kejahatan Teknologi Informasi harus dikoordinasikan di antara negara yang bersangkutan;
- e. Perlunya dilakukan pertukaran informasi antar – negara sehubungan dengan permasalahan yang dihadapi dalam memerangi kejahatan Teknologi Informasi;
- f. Personalia penegakan hukum harus dilatih dan dilengkapi dengan peralatan yang memadai untuk menghadapi kejahatan Teknologi Informasi;
- g. Sistem hukum harus melindungi kerahasiaan, integritas dan ketersediaan data dan sistem komputer dari kerusakan yang tidak semestinya dan menjamin bahwa tindakan kriminal berupa kejahatan teknologi Informasi memperoleh hukuman;
- h. Sistem hukum harus mengizinkan penjagaan dan akses yang cepat terhadap data elektronik yang berhubungan dengan dan atau digunakan dalam investigasi kejahatan Teknologi Informasi;

- i. Pemerintah perlu menjamin adanya kemampuan untuk pengumpulan dan pertukaran bukti atas terjadinya tindakan kejahatan teknologi Informasi untuk dapat segera dilakukan investigasi;
- j. Masyarakat perlu dibuat mengerti dan menyadari mengenai kebutuhan untuk mencegah dan memerangi tindakan kejahatan di bidang Teknologi Informasi;
- k. Untuk alasan praktis, Teknologi Informasi perlu dirancang untuk membantu mencegah dan mendeteksi akan adanya penyalah-gunaan yang menjurus kepada kejahatan, mencari pelakunya, dan mengumpulkan bukti;
- l. Perang melawan kejahatan penyalah-gunaan Teknologi Informasi memerlukan pengembangan solusi dengan memperhatikan proteksi kebebasan individu dan privasi serta pemeliharaan kapasitas Pemerintah untuk memerangi kejahatan penyalah – gunaan Teknologi Informasi tersebut.

Pada bagian akhir dari Resolusi ini, PBB mengajak semua negara anggotanya untuk memperhatikan dan melaksanakan langkah – langkah tersebut di atas dalam memerangi kejahatan Teknologi Informasi.

### **Asia Pacific Economy Cooperation (APEC)**

Menindak-lanjuti Resolusi PBB 55/63 tersebut di atas para pemimpin ekonomi yang tergabung dalam organisasi Kerja Sama Ekonomi Asia Pasifik (APEC) sepakat membentuk APEC Cybercrime Strategy yang bertujuan mengupayakan secara bersama keamanan Internet (*cybersecurity*) dan mencegah serta menghukum pelaku cybercrime. Selanjutnya diminta kepada para pemimpin anggota APEC agar membentuk unit – unit pengamanan yang bertugas memerangi kejahatan cybercrime, serta menunjuk personalia yang bertugas sebagai *point of contact* dalam kerja sama internasional memerangi cybercrime.

Selain menganjurkan dua hal tersebut di atas APEC juga melakukan identifikasi dan inventarisasi terhadap kesiapan masing – masing anggota dalam menyiapkan dan mengimplementasikan Undang – Undang Tindak Pidana di Bidang Teknologi Informasi (cybercrime law). Menurut versi APEC, ada tiga hal penting yang perlu terakomodasi dalam cybercrime law:

- a. Hukum normatif (*substantive laws*) yakni yang mengatur kriminalisasi kejahatan Teknologi Informasi;
- b. Hukum positif (*procedural laws*) yang menyediakan rujukan dan kewenangan bagi aparat penegak hukum dalam melakukan penyidikan dan prosecution terhadap pelaku kejahatan teknologi Informasi; serta
- c. Kebijakan publik atau produk hukum lain guna memfasilitasi kerja sama internasional dalam rangka upaya bersama memerangi cybercrime.

Lebih jauh, kepada anggotanya APEC juga memberikan panduan dalam membuat cybercrime law, khususnya yang mengatur tentang hukum normatif. Adapun kategori kejahatan yang perlu tercakup dalam cybercrime law tersebut antara lain:

1. Akses ilegal terhadap komputer atau jaringan komputer;
2. Intersepsi ilegal terhadap komunikasi elektronik;
3. Gangguan (*interference*) terhadap data komputer, seperti penghapusan atau membuat data tersebut rusak sehingga tidak dapat dipakai atau membuat data tidak dapat diakses oleh yang berhak;
4. Gangguan terhadap sistem komputer, seperti dengan sengaja mematikan komputer atau sistem komputer sehingga orang yang berhak tidak dapat menggunakannya;
5. Kejahatan yang berkaitan dengan penyalah-gunaan peralatan, seperti menggunakan *software tools* untuk memperoleh, secara ilegal, kode akses kepada komputer atau sistem komputer atau melakukan intersepsi terhadap jaringan komunikasi data (Internet);
6. Kejahatan berkenaan dengan pemalsuan (*forgery*) data komputer, seperti perubahan atau penghapusan data komputer sehingga dianggap sebagai data otentik dengan maksud untuk kegiatan legal;
7. Kejahatan berkenaan penipuan (*fraud*) menggunakan komputer/Internet, seperti mengubah data komputer untuk maksud transaksi memperoleh uang atau barang dengan merugikan pihak lain;
8. Kejahatan yang berhubungan dengan pembuatan, pemilikan, atau distribusi material pornografi dengan anak – anak sebagai model atau sarannya;
9. Kejahatan yang berhubungan dengan pelanggaran copyright dan hak atas kekayaan intelektual;

10. Usaha pembantuan terhadap kejahatan menggunakan komputer;
11. Tanggung jawab perusahaan sehubungan dengan kejahatan tersebut (1) sampai dengan (10) di atas bila dilakukan oleh karyawan atau pemimpin perusahaan.

Adapun yang mengenai hukum positif (*procedural laws*) APEC menekankan perlunya ketetapan dalam bentuk undang – undang yang memberi kewenangan dan acuan prosedur bagi penyidikan dan pemidanaan pelaku kejahatan Teknologi Informasi, yang meliputi antara lain, prosedur tentang:

- a. Ruang lingkup penyidikan;
- b. Kondisi dan upaya perlindungan terhadap hak azasi dan kemerdekaan individu;
- c. Penanganan perawatan data komputer yang tersimpan di penyimpanan data (*hard disk*);
- d. Penanganan penjagaan dan penyingkapan data trafik, sebagaimana terjadi pada otoritas telekomunikasi memperlihatkan jalur komunikasi;
- e. Penyidik mampu memaksa penyedia jasa jaringan komputer untuk memberikan (kepada penyidik) informasi *content* dan *non-content* yang tersimpan dalam jaringan atau sistem komputer mereka;
- f. Pencarian dan penyitaan data komputer yang tersimpan oleh aparat penegak hukum;
- g. Pengumpulan data trafik yang berhubungan dengan komunikasi data secara *real time*;
- h. Intersepsi konten komunikasi elektronik;
- i. Ruang lingkup yurisdiksi dari cybercrime law;
- j. Kondisi di mana ekstradisi dimungkinkan terhadap pelaku kejahatan;

Sedangkan yang mengenai fasilitasi kerja sama internasional, APEC memberikan panduan sebagai berikut:

- a. Kerja sama bantuan teknik dalam penegakan hukum berkaitan dengan pemidanaan kejahatan Teknologi Informasi;
- b. Ketersediaan masing – masing pemerintah untuk memberikan informasi yang berkenaan dengan kejahatan Teknologi Informasi kepada otoritas pemerintah negara lain;
- c. Kerahasiaan dan pembatasan dalam penggunaan informasi atau material yang diberikan selain yang tercantum dalam perjanjian bantuan dan kerja sama;
- d. Penanganan perawatan data komputer yang tersimpan dalam kerangka kerja sama bantuan teknik;

- e. Penanganan penyingkapan data trafik dalam kerangka kerja sama bantuan teknik;
- f. Bantuan kerjasama sehubungan dengan pengaksesan data komputer;
- g. Akses lintas – negara kepada data komputer yang tersimpan dengan ijin atau yang terbuka untuk publik;
- h. Bantuan kerja sama dalam upaya mengumpulkan data yrafik secara *real time*;
- i. Bantuan kerjasama sehubungan dengan intersepsi data konten;
- j. Rancangan point of contact yang bekerja non-stop (24/7).

### **Amerika Serikat**

Amerika Serikat telah membuat pelbagai perundang-undangan yang mengatur pemidanaan terhadap pelaku kejahatan Teknologi Informasi dan yang berkaitan dengan Internet seperti:

1. Access Device Fraud Act of 1984 (18 US Codes Section 1029);
2. Computer Fraud and Abuse Act of 1986 (18 US Codes Section 1030);
3. Wire Fraud Statute of 1952 (18 US Codes Section 1343);
4. Criminal Infringement of a Copyright (the Copyright Act of 1976) (18 US Codes Section 506a);
5. Counterfeit Trademark (the Trademark Counterfeit Act of 1984) (18 US Codes Section 2320);
6. Mail Fraud (18 US Codes Section 1341);
7. Conspiracy to Defraud the US Government (18 US Codes Section 371);
8. False Statements (18 US Codes Section 1001);
9. Identity Theft and Assumption Deterrence Act of 1998 (18 US Codes Section 1028);
10. The Racketeer Influenced and Corrupt Organization Act (RICO) (18 US Codes Section 2511).

## 9. Sanksi Pidana

Sanksi pidana terhadap pelanggaran yang dilakukan dalam pemanfaatan Teknologi Informasi harus diatur secara tegas, apakah hal tersebut dilakukan oleh *hacker*, perorangan maupun suatu badan hukum. Sanksi pidana dalam suatu undang – undang *lex specialist* harus ditetapkan dengan memperhatikan syarat – syarat:

1. mempertimbangkan sanksi yang ditetapkan dalam KUHP untuk kejahatan sejenis, ketentuan sanksi dalam *lex specialist* tidak boleh lebih rendah dari ketentuan yang tercantum dalam KUHP;
2. mempertimbangkan harmonisasi dengan undang – undang lain yang sudah ada terlebih dahulu agar tidak terjadi tumpang tindih produk hukum atau inkonsistensi hukuman;
3. sanksi dapat berupa hukuman penjara dan atau denda.

Dengan memperhatikan syarat – syarat di atas UU-TIPITI menetapkan sanksi pidana sebagai berikut:

1. Terhadap pelaku kejahatan yang memanfaatkan Teknologi Informasi dengan maksud untuk menghilangkan nyawa, harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran obyek-obyek vital dan strategis atau lingkungan hidup atau fasilitas umum atau fasilitas internasional, usaha menggulingkan pemerintahan yang sah, atau membahayakan keamanan negara atau untuk memisahkan sebagian dari wilayah negara atau sebagai bagian dari kegiatan teror kepada orang atau negara lain, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara, paling singkat 10 (sepuluh) tahun dan paling lama 20 (dua puluh) tahun.
2. Terhadap siapa saja yang dengan sengaja dan melawan hukum memanfaatkan Teknologi Informasi untuk melakukan pencurian sebagaimana dimaksud pasal 362 Kitab Undang-Undang Hukum Pidana, sehingga memenuhi ketentuan sebagaimana dinyatakan pada pasal 362 Kitab Undang – Undang Hukum Pidana, dipidana penjara paling singkat 5 (lima) tahun, dan paling lama 15 (lima belas) tahun atau denda sedikit – dikitnya Rp. 500.000.000,- (lima ratus juta rupiah) dan sebanyak-banyaknya Rp.2.000.000.000,-(dua milyar rupiah).

3. Terhadap siapa saja yang dengan sengaja dan melawan hukum memasuki lingkungan dan atau sarana fisik Sistem Informasi tanpa hak atau secara tidak sah menggunakan sandi akses palsu, melakukan pembongkaran tanpa seijin pemiliknya yang sah atau merusak dengan atau tanpa maksud merugikan pemilik sah, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 4 (empat) tahun atau denda sedikit – sedikitnya Rp. 200.000.000,- (dua ratus juta rupiah) dan sebanyak-banyaknya Rp 800.000.000,- (delapan ratus juta rupiah).
4. Terhadap siapa saja yang dengan sengaja dan melawan hukum memasuki lingkungan dan atau sarana fisik Sistem Informasi milik instansi pemerintah, militer, perbankan, atau instansi strategis lainnya tanpa hak atau secara tidak sah dengan menggunakan sandi akses palsu, melakukan pembongkaran atau merusak dengan atau tanpa maksud merugikan instansi yang dituju, dipidana penjara paling singkat 7 (tujuh) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit – sedikitnya Rp. 700.000.000,- (tujuh ratus juta rupiah) dan sebanyak-banyaknya Rp. 1.500.000.000,- (satu milyar lima ratus juta rupiah). Apabila pelaku kejahatan tersebut terbukti telah menyebarkan dan atau mengumumkan informasi yang harus dilindungi kepada pihak yang tidak berwenang, hukuman pidananya ditambah 2 (dua) tahun.
5. Terhadap siapa saja yang dengan sengaja terbukti memanfaatkan Teknologi Informasi untuk melakukan transaksi elektronik, dengan menggunakan identitas palsu, atau identitas milik orang lain, dipidana penjara paling singkat 6 (enam) bulan dan paling lama 3 (tiga) tahun, dan dikenakan denda sedikit- sedikitnya Rp 50.000.000,- (lima puluh juta rupiah). Apabila transaksi elektronik tersebut dilakukan untuk transaksi ekonomi dengan menggunakan alat pembayaran berupa kartu kredit, atau kartu debit atau alat pembayaran lainnya yang bukan miliknya sah, dipidana penjara paling singkat 7 (tujuh) tahun, dan dikenakan denda sebesar 2 (dua) kali dari nilai kerugian yang ditimbulkannya.
6. Terhadap siapa saja yang dengan sengaja dan melawan hukum mengubah, menghapus, atau menghilangkan sebagian data komputer asli, yang mengakibatkan hilangnya keaslian data dan menggunakan data yang tidak asli untuk melakukan kegiatan dan atau keperluan lain yang sah, dikategorikan sebagai tindak pemalsuan,



dan dipidana penjara paling singkat minimal 2 (dua) tahun dan paling lama 5 (lima) tahun.

7. Terhadap siapa saja yang dengan sengaja dan melawan hukum, memasukkan, mengubah, menghapus, atau menghilangkan sebagian data komputer atau mengganggu sistem komputer, yang menimbulkan kerugian bagi orang lain, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun, dan dikenakan denda sedikit-dikitnya 3 (tiga) kali dari nilai kerugian yang ditimbulkan.
8. Terhadap siapa saja yang dengan sengaja dan secara melawan hukum memanfaatkan Teknologi Informasi untuk menyebarkan gambar, tulisan atau secara bersamaan dari keduanya yang mengandung sifat – sifat pornografi, melakukan tindakan sebagaimana dimaksud pasal 281, 282 dan pasal 283 Kitab Undang-Undang Hukum Pidana, sehingga memenuhi ketentuan Pasal 281, 282, 283 KUHP, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun.
9. Terhadap siapa saja yang dengan sengaja dan secara melawan hukum memanfaatkan Teknologi Informasi untuk menyimpan, memproduksi, menyebarkan, atau menawarkan bahan – bahan atau informasi yang bersifat pornografi dengan menggunakan anak – anak sebagai model dan atau sasarannya, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 15 (lima belas) tahun.
10. Terhadap siapa saja yang dengan sengaja memanfaatkan Teknologi Informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan, dipidana penjara 2 (dua) tahun dan paling lama 5 (lima) tahun, atau denda sedikit-dikitnya Rp. 200.000.000,- (dua ratus juta rupiah) dan sebanyak-banyaknya Rp. 1.000.000.000,- (satu milyar rupiah).
11. Terhadap siapa saja yang dengan sengaja dan secara melawan hukum melakukan akses melalui komputer tertentu yang statusnya dilindungi oleh pihak yang berwenang atau melanggar hak akses yang diberikan atau tidak diberikan kepadanya, dengan maksud untuk mencuri atau memperoleh sesuatu yang bukan merupakan haknya, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit – dikitnya Rp. 1.000.000.000,- (satu milyar rupiah) dan sebanyak-banyaknya Rp. 2.500.000.000,- (dua milyar lima ratus juta rupiah).

12. Terhadap siapa saja yang dengan sengaja dan secara melawan hukum memanfaatkan Teknologi Informasi untuk melakukan teror, sehingga memenuhi ketentuan tindak pidana terorisme dimaksud dalam Undang-Undang Pemberantasan Tindak Pidana Terorisme, dipidana penjara paling singkat 10 (sepuluh) tahun dan paling lama 30 (tiga puluh) tahun, atau setidaknya dipidana sesuai Ketentuan yang berlaku dalam Undang-Undang Pemberantasan Tindak Pidana Terorisme.

Berkenaan dengan kejahatan yang menggunakan sistem komputer sebagai sasarannya, UU-TIPITI menetapkan sanksi pidana sebagai berikut:

1. Terhadap siapa saja yang dengan sengaja dan melawan hukum melakukan intersepsi tanpa hak, secara tidak sah, atau ilegal, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun.
2. Terhadap siapa saja yang dengan sengaja terbukti merusak situs Internet milik orang atau badan hukum lain, yang menimbulkan kerugian material bagi orang atau badan hukum lain tersebut dipidana penjara paling singkat 1 (satu) tahun dan paling lama 5 (lima) tahun. Apabila situs Internet yang dirusak tersebut milik pemerintah, militer atau situs Internet lain yang termasuk dilindungi oleh pihak yang berwenang, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 7 (tujuh) tahun.
3. terhadap siapa saja yang dengan sengaja dan melawan hukum terbukti melakukan penyadapan terhadap jaringan komunikasi data atau sistem komputer yang terhubung dalam jaringan komputer lokal maupun global (Internet), yang selanjutnya digunakan untuk kepentingan sendiri atau untuk kepentingan pihak lain, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun.
4. Terhadap siapa saja yang dengan sengaja memalsukan nomor Internet Protocol yang digunakan untuk berkomunikasi dengan orang atau badan hukum lain, yang menimbulkan kerugian material bagi orang atau badan hukum lain dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun.
5. Terhadap siapa saja yang dengan sengaja mengacaukan atau membuat sistem komputer tidak dapat berfungsi sebagaimana mestinya dengan cara merusak data base atau teknologi enkripsi, pada sistem komputer tersebut, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun.

6. Terhadap siapa saja yang dengan sengaja dan secara melawan hukum menggunakan nama domain milik orang atau badan hukum lain, yang menimbulkan kerugian material bagi orang atau badan hukum lain atau bagi pemiliknya yang sah, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun.
7. Terhadap siapa saja yang dengan sengaja dan melawan hukum menggunakan surat elektronik untuk mengumumkan, menawarkan atau menjual barang dan atau jasa yang sifatnya melanggar hukum atau dilarang oleh Undang-Undang, dipidana penjara paling singkat 1 (satu) tahun dan paling lama 3 (tiga) tahun.
8. Terhadap siapa saja yang dengan sengaja dan melawan hukum memalsukan atau menggunakan alamat surat elektronik milik orang atau badan hukum lain tanpa seijin dari orang atau badan hukum tersebut, dipidana penjara paling singkat 1(satu) tahun dan paling lama 5 (lima) tahun.
9. Terhadap siapa saja yang dengan sengaja dan melawan hukum memanfaatkan Teknologi Informasi yang dimaksudkan untuk melanggar hak cipta sebagaimana diatur dalam Undang – Undang Hak Cipta, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 10 (sepuluh) tahun atau setidak-tidaknya sesuai ketentuan yang berlaku dalam Undang-Undang Hak Cipta.
10. Terhadap siapa saja yang dengan sengaja dan melawan hukum memanfaatkan Teknologi Informasi untuk mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seijin yang bersangkutan, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun.

## 10. Penyidikan

Penyidikan yang dilakukan oleh Penyidik Pegawai Negeri Sipil atau Penyidik dari Kepolisian Negara Republik Indonesia meliputi penyidikan kasus fasilitas/sistem Teknologi Informasi sebagai sasaran kejahatan, dan penyidikan kasus Teknologi Informasi yang digunakan sebagai fasilitas kejahatan. Untuk kejahatan yang sasarannya berupa fasilitas dan atau sistem Teknologi Informasi khususnya Internet, contohnya antara lain;

- a. DDoS Attack yaitu penyerangan terhadap sistim operasional,
- b. Merubah tampilan website atau Deface,
- c. Masuk ke suatu sistem komputer secara illegal atau trespassing,
- d. Mengendus atau membajak password milik orang lain atau sniffing,
- e. Tindakan-tindakan lainnya yang dikategorikan sebagai *Hacking/Cracking/Phreaking*,
- f. Membuat dan menyebarkan program yang bersifat merusak (*malicious code*) dalam bentuk Worm, Virus, Trojan horse , Dsb.,
- g. Penyalahgunaan perijinan VoIP (*Voice over Internet Protocol*),
- h. Sengketa atau kejahatan yang menyangkut Domain (penamaan atau alamat website),
- i. Pelanggaran terhadap peraturan-peraturan dalam bidang Teknologi Informasi.

Sedangkan Penyidikan Kasus Teknologi Informasi yang digunakan sebagai fasilitas kejahatan umumnya berupa tindak pidana biasa yang sering terjadi, namun sekarang menggunakan teknologi Informasi (Internet) sebagai alat untuk melakukan kejahatan, contohnya antara lain;

- a. Penipuan biasa menawarkan barang/jasa atau saham di Internet,
- b. Penipuan menggunakan nomor kartu kredit orang lain di Internet,
- c. Kejahatan di bidang Bank offence/Fismondef di Internet,
- d. Pornografi di Internet,
- e. Menawarkan jasa Sex di Internet,
- f. Menyebarluaskan tulisan berbau Sex di Internet,
- g. Mengancam atau menghina seseorang dengan menggunakan e-mail,
- h. Pemerasan dengan menggunakan e-mail,
- i. Propaganda atau terorisme di Internet,

j. Dan sebagainya.

Guna mendukung aktivitas penyidikan, dalam bentuk memberikan bantuan teknis pemeriksaan komputer (*computer examination*) serta menyajikan bukti-bukti elektronik yang diperlukan oleh penyidik, suatu laboratorium forensik khusus pemeriksaan komputer dan Teknologi Informasi pada umumnya, perlu disediakan. Laboratorium forensik ini harus melekat dan bersatu dengan para penyidik karena penyidikan bidang ini memerlukan kecepatan dan ketepatan dalam bertindak, selaras dengan sifat bukti-bukti elektronik yang sangat mudah dihapus atau dihilangkan dalam hitungan detik serta sifat para tersangkanya yang sangat *mobil*. Adapun tanggung-jawab dan kemampuan Laboratorium forensik ini antara lain sebagai berikut:

- a. Bertanggung jawab memelihara dan menjaga *status quo* bukti elektronik (*electronic evidence*) serta menganalisa dan menyajikan bukti elektronik tersebut secara cepat kepada penyidik,
- b. Mampu melakukan pemulihan bukti elektronik (*electronic evidence recovery*) yang sudah dihapus ataupun dirusak, serta mampu mencari kembali catatan elektronik yang sengaja disembunyikan secara logic dan membukanya apabila diproteksi dengan *password* atau di-enkripsi namun tetap syah secara hukum atau berlaku di pengadilan,
- c. Mampu mengoperasikan dan memelihara alat-alat *forensic computing*.
- d. Memberikan pelayanan terhadap masyarakat yang memerlukan, untuk *me-recover* data pada hard disk yang rusak ataupun membuka file/dokumen yang diproteksi atau di-enkripsi,
- e. Menciptakan atau mendisain rutin software sederhana sebagai *investigation tools* yang diperlukan oleh para penyidik, untuk mempermudah dan mempercepat proses penyidikan di kejahatan bidang Teknologi Informasi.

Secara umum penguasaan penyidik Polri tentang operasional komputer dan pemahaman terhadap *hacking* komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus tersebut kejahatan Teknologi Informasi masih sangat minim. Banyak faktor yang mempengaruhi hal tersebut namun dari beberapa faktor tersebut ada yang sangat berpengaruh (*determinan*). Adapun faktor-faktor yang mempengaruhi adalah sebagai berikut:

- c. Kurangnya pengetahuan tentang komputer dan sebagian besar dari mereka belum

menggunakan Internet atau menjadi pelanggan pada salah satu ISP (*Internet Service Provider*).

- d. Pengetahuan dan pengalaman para penyidik dalam menangani kasus-kasus cyber crime masih terbatas. Mereka belum mampu memahami teknik *hacking*, *spoofing*, *stalking*, dan modus – modus operandi para hacker dan profil-profilnya.
- e. Faktor sistem pembuktian yang menyulitkan para penyidik karena Jaksa (Penuntut Umum) masih meminta keterangan saksi dalam bentuk Berita Acara Pemeriksaan (BAP) formal sehingga diperlukan pemanggilan saksi/korban yang berada di luar negeri untuk dibuatkan berita acaranya di Indonesia, belum bisa menerima pernyataan korban atau saksi dalam bentuk faksimili atau email sebagai alat bukti.

## 11. Daftar Referensi

1. **Akdeniz**, et all (2000), *The Internet, Law and Society*, Longman.
2. **APEC** (2002), *Cybercrime Strategy*,  
<http://www.dfat.gov.au/apec/mexico2002/cybersecurity.html>
3. **Bainbridge**, David I. (1993), *Komputer dan Hukum*. Diterjemahkan oleh Prasadi T. Susmaatmadja, Jakarta: Sinar Grafika.
4. **Bernstein**, Terry; et all (1996) *Internet Security for Business*, John Wiley & Son, Inc.
5. **Cameron**, Deb, (1994), *The Internet: A Global Business Opportunity*, 1<sup>st</sup> edition, 1994, Computer Technology Research Corp.
6. **Endeshaw**, Assafa, (2001), *Internet and E-Commerce Law, With Focus on Asia Pacific*, Prentice Hall.
7. **Godwin**, Mike, (1999), *Constitutional Law In Cyberspace*, ConstitutionalLaw for Non-Lawyers.
8. **Hamzah**, Andi, Dr. SH., (1995), *KUHP & KUHPA*, Rineka Cipta.
9. **Kanter & Sianturi** (2002), *Asas – Asas Hukum Pidana Di Indonesia Dan Penerapannya*, Stora Grafika.
10. **Lilley**, Peter (2002), *Hacked, Attacked & Abused, Digital Crime Exposed*, Kogan page.
11. **Mardjono** Reksodiputro, (2002) *Cybercrime and Intelektual Property*, makalah disampaikan dalam Penataran Nasional Hukum Pidana dan Kriminologi Indonesia (ASPEHUPIKI) di Fakultas Hukum Universitas Surabaya, terdapat dalam situs [http://www.komisihukum.go.id/artikel/artikel%20MR/cybercrime\\_MR.htm](http://www.komisihukum.go.id/artikel/artikel%20MR/cybercrime_MR.htm)
12. **Mas Wigrantoro R.S.** (2002), *Sistem Hukum Indonesia Dalam Menghadapi Potensi Kriminalitas di Dunia Cyber*, disampaikan sebagai makalah dalam pelatihan Information Security, diselenggarakan oleh STT Telkom Bandung, 4 April 2002.
13. **Moelyatno**, Prof. SH., (2002), *Asas – Asas Hukum Pidana*, Rineka Cipta.
14. **Muladi**, Prof. Dr. SH, (2003), *Pengaruh Perkembangan Telematika Terhadap Pembuktian Dalam Hukum Acara Pidana*, Paper disampaikan pada Seminar Pengaruh Perkembangan Telematika Terhadap Pengembangan Hukum dan Peraturan Perundang – Undangan, Diselenggarakan oleh: BPHN Depkeh HAM RI dan Koordinator Pengelola Program Doktor Bidang Ilmu Hukum Pasca Sarjana Universitas Pajajaran, Oktober 2003
15. **Onno W. Purbo**, et all. (2001a); *TCP/IP, Standar, Desain, dan Implementasi*, edisi 6, Elex Media Komputindo.
16. **Onno W. Purbo**, et all. (2001b) *Keamanan Jaringan Internet*, edisi 3, Gramedia Jakarta.
17. **Overly**, Michael R., (1999), *e-policy How to Develop Computer, Email, and Internet Guidelines to Protect Your Company and Its Assets*, AMACOM.
18. **Power**, Dennis M, (2002) *Internet Legal Guide*, Wiley.
19. **Romli Atsasmita**, Prof. Dr. SH., LL.M., (2003) *Kejahatan Melalui Teknologi Informasi Dan Dampaknya Terhadap Hukum Pidana Nasional*, disampaikan pada Seminar Pengaruh Perkembangan Telematika Terhadap Pengembangan Hukum dan Peraturan Perundang – Undangan, Diselenggarakan oleh: BPHN Depkeh HAM RI

- dan Koordinator Pengelola Program Doktor Bidang Ilmu Hukum Pasca Sarjana Universitas Pajajaran, Oktober 2003.
20. **Saidin**, H. OK. (2003), Aspek Hukum Hak Kekayaan Intelektual, Raja Grafindo Persada, edisi 3.
  21. **Smedinghoff**, Thomas J.(1999), ed, Online Law, Addison-Wesley.
  22. **Subekti**, R. Prof. SH., (1995), Hukum Pembuktian. Edisi II. Jakarta: Pradnya Paramita.
  23. **Subekti**, R. Prof. SH. & R. Tjirosudibio, (1992), Kitab Undang – Undang Hukum Perdata, Pradnya Paramita.
  24. **Sunaryati** Hartono C.F.G., Prof. Dr. SH. Editor (2000), Business And The Legal Profession in an Age of Computerization and Globalisation, Bagian II, Implications of Computerization Upon The Development of Law and the Legal Profession, Yayasan Hak Azasi Manusia, Demokrasi Dan Supremasi Hukum.
  25. **Sundari S. Arie**, Hj., Dr. MH., SH (2003), Pengaruh Perkembangan Telematika Dalam Transaksi Bisnis Perbankan, Paper disampaikan pada Seminar Pengaruh Perkembangan Telematika Terhadap Pengembangan Hukum dan Peraturan Perundang – Undangan, Diselenggarakan oleh: BPHN Depkeh HAM RI dan Koordinator Pengelola Program Doktor Bidang Ilmu Hukum Pasca Sarjana Universitas Pajajaran, Oktober 2003.
  26. **Tapscott**, Don, ed, (1999), Creating Value in The Networked Economy, Harvard Business Review.
  27. **Thomas & Loader**, eds.(2000), Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Routledge.
  28. **Thurrow**, Lester C, (1999), Buidling WEALTH, The New Rules for Individuals, Companies, and Nations in a Knowledge-Based Economy, Harper Collins.
  29. **U.S. Department of Justice**, Legal Frameworks For Combating Cybercrime, Resource Material for the APEC Workshop on cybercrime, 2002.
  30. -----, Undang – Undang Perlindungan Terhadap Kekayaan Intelektual, meliputi: UU RI Nomor 14/2001 tentang Paten, UU RI Nomor 15/2001 tentang Merek, dan UU RI Nomor 19/2002 tentang Hak Cipta.
  31. -----, Undang – Undang RI Nomor 36 tahun 1999 tentang Telekomunikasi.