TINDAK PIDANA KOMPUTER DAN UPAYA PEMBUKTIAN[1]

Oleh: Martinus Jefry Clinton Purba[2]
Eske N. Worang[3]
Marhcel Maramis[4]

ABSTRAK

Tujuan dilakukannya penelitian ini yaitu untuk mengetahui bagaimana bentuk-bentuk penyalahgunaan computer dan bagaimanakah upaya pembuktian tindak pidana computer di manadengan metode penelitian hukum normatif disimpulkan: 1. Tindak pidana di bidang komputer itu dilakukan oleh seseorang tidak didasari motivasi untuk mendapatkan uang sebagaimana halnya kejahatan konvensional, karena orang yang melakukan tindak pidana di bidang komputer ini hanya sekedar *'challenge'* dan merasa tertantang untuk dapat menjawab permasalahan-permasalahan yang memerlukan pemikiran yang *smart* dan juga hanya karena kesenangan belaka, dan berusia relatif muda. Sebagai akibat terjadinya penyalahgunaan komputer, maka bermunculanlah bentuk-bentuk tindak pidana di bidang komputer seperti: *joy computing, hacking, the trojan horse, data diddling, data leakage, wiretapping,* dan banyak lagi lainnya. 2. Penggunaan alat bukti digital berupa *e-mail* haruslah dipakai oleh hakim dalam membuktikan dan menentukan seseorang telah melakukan tindak pidana computer. Bukti digital ini dapat dikategorikan sebagai alat bukti surat dan petunjuk. Upaya pembuktian yang dapat dilakukan oleh penyidik dalam rangka mencari kebenaran materiil dalam perkara *cybercrime/computer crime* adalah: melakukan pengumpulan barang bukti kejahatan *cybercrime/computer crime*, melakukan pemeriksaan terhadap pelaku dan saksi-saksi kejahatan *cybercrime/computer crime*, melakukan digital forensik terhadap barang bukti elektronik yang diguankan oleh pelaku kejahatan *cybercrime/computer crime* di laboratorium forensik, melakukan analisa terhadap waktu/dokumen pelaku melakukan kejahatan dengan waktu/dokumen hasil yang didapat dari laboratorium forensik terhadap barang bukti yang digunakan oleh pelaku kejahatan *cybercrime/computer crime* dan melakukan pemeriksaan terhadap ahli bahasa, ahli digital forensik dan ahli ITE.

Kata kunci: tindak pidana komputer; pembuktian;

PENDAHULUAN

A. Latar Belakang

Revolusi teknologi informasi berawal sejak ditemukannya komputer yang dalam perkembangannya menciptakan suatu dunia tersendiri yang lazim disebut dengan dunia maya *(cyber space).*

Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, terutama dalam kaitannya dengan proses pembuktian tindak pidana. Apalagi penggunaan komputer untuk tindak kejahatan memiliki karakteristik tersendiri atau berbeda dengan kejahtan yang dilakukan dengan tidak menggunakan komputer. Perbuatan atau tindakan pelaku, alat bukti ataupun barang bukti dalam tindak pidana biasa dapat dengan mudah untuk di identifikasi, tidak demikian halnya dengan kejahatan yang dilakukan dengan menggunakan komputer.

B. Rumusan Masalah

1. Bagaimana bentuk-bentuk penyalahgunaan komputer?
2. Bagaimanakah upaya pembuktian tindak pidana komputer?

C. Metode Penelitian

Metode pendekatan yang digunakan adalah yuridis normatif.

PEMBAHASAN

A. Bentuk-Bentuk Penyalahgunaan Komputer

Semakin canggih dan berkembangnya ilmu pengetahuan dan teknologi, memudahkan manusia untuk melakukan semua aktivitasnya. Seiring dengan kemajuan tersebut bermunculan pulalah kejahatan-kejahatan dengan modus operandi yag semakin canggih pula, salah satunya adalah kejahatan di bidang komputer. Kejahatan di bidang komputer bermula dari adanya penyalahgunaan komputer itu sendiri. Untuk mengetahui bentuk-bentuk penyalahgunaan komputer yang

[1] Artikel Skripsi
[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM. 17071101039
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

digolongkan sebagai tindak pidana di bidang komputer maka ada baiknya diketahui bagaimana atau mengapa terjadi suatu tindak pidana di bidang komputer.

Muladi, Guru Besar Fakultas Hukum Universitas Diponegoro Semarang berpendapat, bahwa yang sangat menarik dari tindak pidana di bidang komputer adalah 'motivasi' dilakukannya perbuatan tersebut.[5]

Lebih lanjut Muladi mengatakan bahwa pelaku tindak pidana komputer dalam melakukan perbuatannya 'semata-mata bukan karena uang', tetapi ada unsur *'challenge'*. Yang dipikirkan oleh mereka bukan karena profit, melainkan bagaimana mengakali *(outsmart)* suatu sistem komputer dan melakukannya untuk kesenangan.

Di samping itu, tidak komputer ini adalah merupakan salah satu bentuk tindak pidana canggih yang dilakukan dengan teknik tinggi/teknik intelektual, sehingga sangat sulit untuk dimengerti oleh orang awam yang tidak menguasai teknik dari komputer.

Kalangan *security* data di Amerika Serikat sendiri menyebutkan komputer sebagai: *"Unsmoking Gun"*, karena memang komputer tidak memberikan sesuatu indikasi apapun yang memperingatkan bahwa telah terjadi kesalahan.[6]

Sejalan dengan ungkapan tersebut di atas, mantan Ketua Yayasan LBHI Mulya Lubis berpendapat bahwa:

> "Tindak pidana komputer ini termasuk *"White collar crime"* yaitu tindak pidana yang dilakukan oleh kalangan orang kantoran dan menggunkan teknik yang canggih dan rukit untuk dapat dibuktikan hanya dengan pasal-pasal pidana kontroversial".[7]

Hal senada dikemukakan oleh Koesparmono Irsan dalam makalahnya yang berjudul: "Kejahatan, di kota-kota yang dapat diperkirakan pada PJPT II", menyebutkan bahwa:

> "Kejahatan komputer *(computer crime)* termasuk kejahatan dimensi baru, yang dilakukan secara perorangan, kelompok atau suatu badan bahkan dengan motivasi untuk mendapatkan keuntungan yang sebesar-besarnya atau untuk membuka rahasia perusahaan/negara dalam rangka menggoyahkan perusahaan/negara".[8]

Jika kita simak kembali *"modus operandi"* pelaku tindak pidana komputer yaitu:

- merusak efisiensi data;
- merampas atau mencuri data yang disentralisasi dalam komputer;
- alat yang digunakan adalah komputer yang menjadi korban;
- sasarannya antara lain negara (pemerintah), perusahaan-perusahaan, bank,

menurut Edward R. Buck dalam sebuah buku: *"Introduction to date security and controls",* dihubungkan dengan pendapat yang dikatakan oleh Mulyadi bahwa pelaku tindak pidana komputer dalam melakukan tindakannya bukan semata-mata karena uang melainkan ada unsur *challenge* dan kesenangan, jelaslah disini bahwa pelaku tindak pidana di bidang komputer tersebut adalah seseorang yang mempunyai ciri-ciri sebagai berikut:

- menyenangi tantangan;
- usia antara 18 sampai dengan 46 tahun;
- dorongan untuk maju sangat tinggi;
- *energetic*;
- senyum dan ramah;dan
- cerdas;

Biasanya mempunyai tendensi yang kuat untuk melakukan tindak pidana tersebut. Dikarenakan kemampuan yang dimilikinya berada di atas kemampuan rata-rata orang yang lain, maka orang tersebut dapat menjadi sumber informasi atau tempat bertanya yang baik bagi sesama ataupun kalau ia adalah seorang karyawan suatu perusahaan maka ia dapat menjadi sumber informasi bagi sesama karyawan lainnya atau bahkan pimpinan perusahaannya.

Don Parker dalam bukunya *"Crime by Computer"* sebagaimana dikutip oleh Widyopramono dalam bukunya "Kejahatan di bidang Komputer", mengatakan bahwa sebagian pelaku kejahatan komputer adalah anak muda, berusia 18 – 30 tahun, para pelaku biasanya cerdas, penuh hasrat, punya motivasi

[5] Widyopramono,*Op-Cit,* hlm-32.

[6] *Ibid*, hlm-33.

[7] Majalah Mingguan Tempo, *Kejahatan Komputer Masuk ke Indonesia,* No. 34 Tahun XVII, 24 Oktober 1987, Jakarta, hlm-44.

[8] Harian Suara Karya, *Seminar Penanggulangan Kejahatan Komputer,* 18 Desember 1987, Jakarta, hlm-2.

tinggi, berani, petualang dan orang terdidik yang ingin menghadapi tantangan teknis.[9]

Melihat apa yang sudah disebutkan oleh Edward R. Buck yang dihubungkan dengan pendapat dari Muladi dan pendapat dari Donn Parker di atas, maka menurut pendapat penulis bahwa orang yang memiliki sifat dan ciri-ciri yang demikian adalah orang yang mempunyai sifat yang tepat yang dapat menjadi orang yang dapat bekerja sebagai 'pengolah data' pada suatu perusahaan. Biasanya orang-orang yang demikian, adalah orang yang sangat ramah dan sangat mudah untuk berhubungan dengan siapa saja dari segala tingkatan yang ada. Sehingga dengan demikian tidak heran kalau yang bersangkutan sangat akrab dengan prosedur-prosedur perusahaan, arsip dan data perusahaan, struktur organisasi serta batas-batas perlindungan yang ada pada perusahaan. Karena sifat yang dimilikinya menunjukkan bahwa yang bersangkutan mempunyai dorongan untuk maju sangat besar serta menyenangi publikasi dan tantanganan, adalah tidak mengherankan kalau dia mempunyai prinsip pantang dilewati atau pantang menyerah. Seandainya dia menemukan suatu persoalan yang sulit dicari jawabannya, maka dia akan mengutak-atik persoalan itu sampai ditemukan jawabannya.

Oleh karena itu apabila kemampuan yang dimiliki oleh yang bersangkutan tidak dibarengi dengan landasan moral yang tinggi, maka peluang untuk menghancurkan sistem yang ada pada perusahaan atau instansi pemerintah; mengambil dan membuat duplikasi dari *document system;* mengadakan percobaan-percobaan; merusak; menyelundup ataupun mengambil data yang bukan miliknya adalah sangat besar. Kesimpulannya adalah bahwa terjadinya tindak pidana di bidang komputer dikarenakan atau terletak pada orangnya atau pelakunya yang memang sangat mahir dengan peralatan teknologi canggih, *smart* dan sangat menyukai tantangan serta merupakan suatu kesenangan belaka, namun tidak mempunyai motivasi untuk melakukan suatu perbuatan yang tergolong sebagai kejahatan konvensional yang bertujuan untuk mendapatkan uang.

Hal tersebut yang senada dengan pendapat penulis pernah juga dikatakan oleh mantan Jaksa Agung RI Hari Suharto bahwa:

"kejahatan dengan komputer tidak dapat dilakukan oleh sembarang orang, kalau tidak ahlinya tentu tidak dapat melakukan kejahatan dengan menggunakan komputer".[10]

Sehubungan dengan penyalahgunaan komputer sehingga mengakibatkan timbul/terjadinya tindak pidana di bidang komputer, maka muncul pula perbuatan-perbuatan penyalahgunaan yang baru pula yang dikategorikan dalam bentuk-bentuk tindak pidana di bidang komputer.

Untuk mendapatkan gambaran mengenai bentuk penyalahgunaan komputer dan kesulitan-kesulitan yang dialami dalam mengatasi/menyelesaikan tindak pidana komputer, dibawah ini akan penulis paparkan beberapa contoh kasus tindak pidana komputer sebagai berikut:

Kasus I

Pegawai *computer operation* pada suatu Universitas dan ia juga sebagai mahasiswa disitu, melakukan perubahan-perubahan secara tidak sah pada *data base* mahasiswa, ia mengubah nilai-nilai yang didapatnya, menambah kredit untuk dirinya sendiri pada kursus-kursus yang sama sekali tidak dikutinya. Kecurangan ini diketahui secara tidak sengaja dan ia dipaksa untuk mengundurkan diri. Tidak ada sangkaan resmi baginya, karena dua alasan yaitu:

- perkara ini akan sulit diadili, karena buktinya berbelit-belit. Tampaknya seperti ada orang yang menciptakan nama pemakai palsu untuk meng-*access* data dari *'data base'* komputer, dan karena buruknya sistem kontrol yang ada, sehingga sulit untuk menentukan atau mengenali si pemakai. Ada banyak oarang yang diberi hak untuk meng-*access* sistem komputer, karena itu dengan mudah mahasiswa tersebut dapat membantah bahwa sangkaan tersebut adalah sangkaan palsu.
- Pihak Universitas khawatir kejadian tersebut akan memalukan dan merugikan pihaknya bila dipublikasi.

Kasus II

[9] Widyopramono, *Op-Cit,* hlm-34.

[10] Harian Suara Karya, *Op-Cit*.

Seorang *programmer* yang bekerja di sebuah bank mengubah program, sehingga setiap penarikan uang dari rekening bank-nya akan tercatat. Supaya rekeningnya tetap seimbang, ia menyadap rekening bank orang lain yang dianggapnya cukup kaya, untuk menutup jumlah uang yang diambilnya dari bank. Kecurangan ini terbongkar ketika rekening bank yang disadapnya ternyata tidak sekaya yang diduga. Pemilik rekening berkeras untuk memaksa bank menunjukkan kertas penarikan uang dari bank yang asli, karena adanya transaksi yang kurang jelas. Dan kertas tersebut tidak dapat diketemukan. Karena curiga, pihak bank meneruskan penelitian/penyelidikannya. Hasil pemeriksaan antara program asli dan duplikat mengatakan adanya perbedaan yang cukup menyolok. *Programmer* tidak dapat menjelaskan bagaimana rekening bank-nya dalam beberapa waktu terakhir jauh lebih besar dari pendapatannya. Karena khawatir banknya akan di cap tidak becus, maka pihak bank hanya memecat pegawainya tanpa mengajukannya ke persidangan, layaknya seperti perkara pidana.[11]

Dari dua contoh kasus di atas, dapatlah dilihat bentuk ancaman/gangguan yang diakibatkan penyalahgunaan dari komputer. Berikut ini akan dipaparkan beberapa bentuk penyalahgunaan komputer yang merupakan atau dapat menimbulkan ancaman/gangguan sebagai berikut :[12]

1. *Joycomputing,* yaitu pencurian waktu operasi komputer. Pelanggar memakai komputer orang lain tanpa izin. Disini menyangkut pencurian waktu.
2. *Hacking,* yaitu memasuki atau mengakses secara tidak sah. Orang yang memasuki/mengakses komputer secara tidak sah (tanpa izin) dengan suatu alat terminal.
3. *The Trojan Horse*, yaitu mengubah, menambah, menghapus data. Memanipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain. Umumnya dilakukan secara insidental, sehingga sulit dideteksi secara dini. Cara yang dilakukan, dapat bermacam-macam di antaranya adalah :
   - Mengubah program yang ada sehingga program tersebut akan melakukan penghitungan pembulatan yang salah. Sejumlah kecil uang akan dipotong dari suatu jumlah yang besar dari rekening-rekening tertentu dan menyimpan hasil potongan tersebut pada rekening tertentu. Para korban biasanya tidak menyadarinya, cara ini dikenal dengan istilah *salami methode*.
   - Mengubah program yang ada untuk memasukkan transaksi-tansaksi tertentu, sehingga transaksi tersebut dapat dikenal oleh sistem *specification.* Transaksi yang tidak dikenal ini, mungkin dimasukkan bersama-sama dengan transaksi lainnya.
   - Mengubah program yang ada sehingga dapat memanipulasi *balance* serta menutupnya dengan suatu debit baru pada suatu *account*. Dengan demikian *balance* suatu *account* akan tetap kelihatan sama.
4. *Data leakage*, yaitu pembocoran data rahasia ke luar perusahaan (instansi). Ini menyangkut bocornya data keluar terutama mengenai data yang harus dirahasiakan, jadi pembocoran data komputer dapat berupa rahasia negara, rahasia perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu. Ada banyak data dan program menyangkut keuangan negara yang mesti dilindungi. Jelaslah, bahwa data dan program militer termasuk rahasia negara. Data harus dibedakan dengan informasi, dari datalah dapat diperoleh informasi. Pada kebocoran data, data rahasia tersebut ditulis dalam kode-kode tertentu sehingga dapat dibawa ke luar tanpa diketahui. Misalnya, ada gambar-gambar lukisan di dinding batu suatu gua. Ini merupakan data, yang dapat memberi informasi bagi orang bahwa demikianlah cara orang dahulu kala melukis. Bagi orang yang lebih ahli mungkin lukisan

[11] Widyipramono, *Op-Cit*, hlm-35.
[12] *Ibid.* hlm. 37-39

itu dapat memberi informasi mengenai keadaan ratusan tahun yang lalu di negeri itu. Dapat diketahui sebagai sejarah bangsa bersangkutan.

2. *Data diddling,* yaitu mengubah data yang sah menjadi tidak sah atau mengubah *input* atau *output,* yang termasuk pemalsuan data. Misalnya, seorang pegawai komputer *operation* pada suatu universitas dan kebetulan sebagai mahasiswa juga disitu, telah melakukan perubahan-perubahan secara tidak sah pada data base mahasiswa. Ia telah mengubah nilai-nilai yang didapatnya, menambah kredit untuk dirinya sendiri pada kursus-kursus yang sama sekali tidak pernah diikutinya.
3. *To frustrate data communication,* yaitu menggagalkan atau menyia-nyiakan data. Ini disebut dengan penyia-nyiaan data komputer. Istilah penyia-nyiaan data komputer ini merupakan istilah umum dari N. Keijzer dalam ceramahnya yang berjudul 'Hukum Pidana Belanda Dan Penylahgunaan Komputer' di BPHN Jakarta tahun 1986, yang mempunyai arti : suatu perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak/menghancurkan media disket dan media penyimpanan sejenis lainnya yang berisikan data atau program komputer, sehingga akibat perbuatan tersebut data atau program yang dimaksud menjadi tidak berfungsi lagi dan pekerjaan-pekerjaan yang melalui proses komputer tidak dapat dilaksanakan. Misalnya, seorang *programmer* sebuah perusahaan telah menyisipkan sebuah *logic bomb* ke dalam suatu sistem. Apabila nama *programmer* itu dihapus dari *file personel,* maka seluruh *file* akan musnah atau rusak. Dengan cara ini perusahaan akan tetap bergantung kepada *programmer* yang bersangkutan.
4. *Software piracy,* yaitu pembajakan hak cipta terhadap perangkat lunak komputer *(software).* Dapatlah disimpulkan disini bahwa terhadap pembajakan perangkat lunak *(software)* komputer, UU Hak Cipta dapat diterapkan. Ini sudah menjadi kecenderungan dunia perangkat lunak komputer sebagai suatu karya yang bersifat hukum hak cipta.
5. *Wiretapping.* Melalui saluran transmisi data (baik berupa kabel telepon, serat optik, ataupun satelit), biasanya amat mudah untuk melakukan penyadapan data secara ilegal.

Dari bermacam bentuk penyalahgunaan komputer seperti yang dipaparkan di atas, maka muncullah bentuk-bentuk tindak pidana di bidang komputer.

Donn Parker, dalam bukunya Widyopromono memberikan klasifikasi terhadap tindak pidana komputer berdasarkan bentuk penyalahgunaan komputer, dimana beliau memandang tindak pidana komputer itu dari sudut empat (4) peranan komputer dalam tindak pidana komputer, yaitu :[13]

1. Komputer sebagai obyek,
   Dalam hal ini termasuk kasus-kasus perusakan terhadap komputer, data atau program yang ada di dalamnya atau perusakan terhadap sarana-sarana komputer seperti AC dan peraltan listrik yang menunjang operasi komputer.
2. Komputer sebagai subyek,
   Komputer dapat merupakan atau menimbulkan tempat atau lingkungan untuk melakukan tindak pidana seperti : pencurian, penipuan dan pemalsuan yang tidak tradisionil akan tetapi yang emnyangkut harta benda dalam bentuk baru yaitu berbentuk pulsa-pulsa elektronik dan guratan-guratan magnetis.
3. Komputer sebagai alat,
   Dalam beberapa tipe dan cara-cara tindak pidana dipergunakan komputer sehingga peristiwa tindak pidananya adalah kompleks dan susah diketahui. Misalnya, seseorang yang mengambil warkat-warkat penyetoran dari suatu bank dan mencetak nomor rekeningnya sendiri dengan tinta magnetis pada warkat-warkat tersebut, yang kemudian diletakkan kembali pada tempatnya di bank, dari mana kemudian para nasabah mengambil dan mengisinya sebagai bukti penyetoran. Pada waktu

[13] *Ibid,* hlm- 40.

komputer memproses data di warkat-warkat tersebut, komputer mengkreditir rekening dari oknum itu, yang kemudian menarik uangnya dengan cek dari rekeningnya sebelum para nasabah yang menyetor tadi mengajukan protesnya.

4. Komputer sebagai simbol,
   Suatu komputer dapat dipergunakan sebagai simbol untuk melakukan penipuan atau ancaman. Hal ini termasuk suatu penipuan lewat iklan dari suatu 'biro jodoh' yang menyatakan bahwa biro tersebut memakai komputer untuk membantu si korban mencari jodoh, akan tetapi ternyata biro jodoh tersebut sama sekali tidak menggunakan komputer untuk keperluan tersebut.

Lain lagi apa yang diberikan oleh Muhammad Jumhana dalam "Info Komputer', sebagaimana dikutip oleh Widyopramono, bahwa bentuk-bentuk tindak pidana komputer antara lain sebagai berikut :[14]

1. Kejahatan komputer yang berupa memperalat komputer untuk suatu kejahatan. Kejahatan dengan memperalat komputer berkembang seiring dengan aplikasi komputer di berbagai kehidupan. Misalnya, kejahatan membobol bank dengan melalui sarana komputer sebagai alatnya.
2. Kejahatan dengan perangkat komputer, adalah bentuk kejahatan yang tindakannya berupa tindakan yang menjadikan komputer dan perangkatnya, baik *software* maupun *hardware* dijadikan sebagi obyek dari tindakan kejahatan tersebut. Misalnya, menggandakan program tanpa izin pemilik. Termasuk juga dalam tindak pidana Hak Cipta atau tindak pidana yang menyebabkan kerusakan komputer atau data milik orang lain.

Dari bentuk-bentuk tindak pidana di bidang komputer yang sudah dikemukakan sebelumnya, maka penulis mengambil kesimpulan bahwa terhadap tindak pidana komputer ini dapat diadakan klasifikasi yang meletakkan sebagian besar dari tindak pidana komputer dalam empat (4) kategori. Ke empat kategori tersebut adalah sebagai berikut:

1. Sabotase atas fasilitas-fasilitas komputer dan vandalisme;
2. Penggunaan atas fasilitas-fasilitas komputer tanpa wewenang sebagai pencurian;
3. Kejahatan terhadap barang (pencurian melalui penggunaan komputer);
4. Kejahatan terhadap data (pencurian informasi).

Selain dari apa yang sudah dikemukakan di atas, dan dari banyaknya perbedaan diantara para ahli dalam mengklasifikasikan bentuk-bentuk kejahatan komputer *(computer crime)*, maka dapat disimpulkan bahwa 'kejahatan komputer' itu sebagai berikut:

1. kejahatan-kejahatan yang menyangkut data atau informasi komputer;
2. kejahatan-kejahatan yang menyangkut program atau software komputer;
3. pemakaian fasilitas-fasilitas komputer tanpa wewenang untuk kepentingan-kepentingan yang tidak sesuai dengan tujuan penegelolaan atau operasinya;
4. tindakan-tindakan mengganggu operasi komputer;
5. tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjangnya.

B. Pembuktian Telah Terjadi Tindak Pidana Komputer

Sudah menjadi pendapat umum, bahwa membuktikan berarti memberi kepastian kepada hakim tentang adanya peristiwa-peristiwa tertentu. Baik dalam hukum acara perdata maupun dalam hukum acara pidana, pembuktian memegang peranan yang sentral.

Pada hakekatnya pembuktian dimulai sejak diketahui adanya suatu peristiwa hukum. Namun perlu diketahui bahwa tidak semua peristiwa hukum terdapat unsur-unsur pidana. Apabila ada unsur-unsur pidana (bukti awal telah terjadi tindak pidana), barulah proses tersebut dimulai dengan mengadakan penyelidikan, penyidikan, penuntutan, persidangan dan seterusnya.

Hukum acara pidana sendiri menganggap pembuktian merupakan bagian yang sangat

[14] Muh Jumhana dalam Widyopramono, *Ibid*. hlm. 39

esensial untuk menentukan nasib seorang terdakwa. Bersalah atau tidaknya seoarang terdakwa sebagaimana yang didakwakan dalam surat dakwaan, ditentukan pada proses pembuktiannya. Atau dengan kata lain, pembuktian merupakan suatu upaya untuk membuktikan kebenaran dari isi surat dakwaan yang disampaikan oleh jaksa penuntut umum, yang kegunaannya adalah untuk memperoleh kebenaran materil terhadap :

a. perbuatan-perbuatan manakah yang di anggap terbukti menurut pemeriksaan persidangan;
b. apakah telah terbukti bahwa terdakwa berasalah atas perbuatan-perbuatan yang didakwakan kepadanya;
c. tindak pidana apakah yang dilakukan sehubungan dengan perbuatan-perbuatan itu;
d. hukuman apakah yang harus dijatuhkan kepada terdakwa.

Hal-hal tersebut di atas, dalam persidangan dapat menimbulkan tiga kemungkinan putusan hakim, yaitu :

1. jika pengadilan berpendapat bahwa dari hasil pemeriksaan di persidangan kesalahan terdakwa atas perbuatan yang didakwakan kepadanya tidak terbukti secara sah dan tidak meyakinkan, maka terdakwa diputus bebas.
2. jika pengadilan berpendapat bahwa perbuatan yang didakwakan kepada terdakwa terbukti, tetapi perbuatan itu tidak merupakan suatu tindak pidana, maka terdakwa diputus lepas dari segala tuntutan hukum.
3. jika pengadilan berpendapat bahwa dari hasil pemeriksaan di persidangan kesalahan terdakwa atas perbuatan yang didakwakan kepadanya terbukti secara sah dan meyakinkan, maka terdakwa diputus dipidana.

Ilmu pengetahuan hukum, dalam rangka membuktikan bersalah tidaknya seseorang mengenal empat sistem pembuktian sebagai berikut:[15]

1. Pembuktian berdasarkan keyakinan hakim belaka *(Conviction in time)*.[16]
2. Sistem pembuktian berdasarkan undang-undang secara positif *(Positief Wettelijke Bewijstheorie)*.[17]
3. Sistem pembuktian berdasarkan keyakinan hakim atas alasan yang logis *(La Conviction Raisonnee)*.[18]

Menurut teori sistem pembuktian ini, peranan keyakinan hakim sangat penting. Namun hakim baru dapat menghukum seorang terdakwa apabila ia telah meyakini bahwa perbuatan yang bersangkutan terbukti kebenarannya. Keyakinan tersebut harus disertai dengan alasan-alasan yang berdasarkan atas suatu rangkaian pemikiran (logika). Hakim wajib menguraikan dan menjelaskan alasan-alasan apa yang mendasari keyakinannya atas kesalahan terdakwa. Alasan tersebut harus benar-benar bisa diterima oleh akal. Sistem pembuktian ini mengakui adanya alat bukti tertentu tetapi tidak ditetapkan oleh undang-undang. Banyaknya alat bukti yang digunakan untuk menentukan bersalah atau tidaknya terdakwa merupakan wewenang hakim sepenuhnya. Tentu saja hakim harus bisa menjelaskan alasan-alasan mengenai putusan yang diambilnya.

4. Sistem pembuktian menurut undang-undang secara negatif *(Negatief Wettelijke Bewijstheorie)*.[19]

Dalam konteks pidana, maka perihal pembuktian merupakan bagian yang paling esensial untuk membuktikan atau menyatakan bahwa seseorang telah melakukan suatu tindak pidana. Pada hakekatnya dalam pembuktian suatu perkara pidana, telah dilakukan semenjak diketahuinya atau adanya suatu peristiwa. Peristiwa yang diamksud di sini adalah peristiwa hukum. Suatu peristiwa hukum belum tentu mengandung unsur pidana, untuk itu perlu dibuktikan lebih lanjut bahwa suatu peristiwa hukum dinyatakan sebagai tindak pidana. Setelah diketemukan bukti awal bahwa

[15] Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP; Pemeriksaan Sidang Pengadilan, Banding, Kasasi dan Peninjauan Kembali*, Edisi Kedua, Sinar Grafika, Jakarta, 2005, hlm.277- 279.

[16] *Ibid,* hlm. 277 .

[17] *Ibid,* hlm. 278.

[18] Yahya Harahap, *Op-Cit,* hlm. 277-278

[19] *Ibid,* hlm. 278

suatu peristiwa dinyatakan sebagai suatu tindak pidana barulah dapat dilakukan penyelidikan dan penyidikan.

Pasal 183 KUHAP berbunyi : "Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang sah melakukannya". Berdasarkan bunyi Pasal 183 ini, terlihat bahwa hukum acara kita memiliki kecenderungan menganut teori pembuktian secara negatif. Seseorang baru dapat dinyatakan bersalah jika minimal dua alat bukti yang sah seorang hakim memperoleh keyakinan bahwa terdakwa telah melakukan suatu tindak pidana. Menurut Simons, pemidanaan didasarkan pada pembuktian berganda yaitu pada peraturan perundang-undangan dan keyakinan hakim dan menurut undang-undang, dasar keyakinan hakim tersebut bersumberkan pada peraturan perundang-undangan.

Keyakinan yang dimiliki oleh hakim haruslah berdasarkan ketentuan yang ada dalam KUHAP. Artinya seoarang hakim dalam memutus perkara terbatas pada alat bukti yang tertera dalam KUHAP. Sistem pembuktian ini yang nantinya mengarahkan proses pembuktian di dalam pengadilan, dengan begitu para praktisi hukum khususnya hakim akan dapat memutus suatu perkara secara subyektif.

Melihat penjelasan Pasal 183 KUHAP, di mana syarat pembuktian menurut cara dan alat bukti yang sah lebih ditekankan pada perumusan yang tertera dalam undang-undang untuk menentukan salah atau tidaknya seorang terdakwa dan untuk menjatuhkan pidana kepada seorang terdakwa harus :

- kesalahannya terbukti dengan sekurang-kurangnya 'dua alat bukti yang sah';
- dan dengan sekurang-kurangnya dua alat bukti yang sah tersebut, hakim akan memperoleh keyakinan bahwa tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukan suatu tindak pidana.

Jika melihat konstruksi hukumnya, maka keyakinan hakim hanyalah pelengkap.[20] Tidak dibenarkan menjatuhkan hukuman kepada terdakwa yang kesalahannya tidak terbukti secara sah berdasarkan ketentuan perundang-undangan yang berlaku, kemudian keterbuktian tersebut digabung dan didukung dengan keyakinan dari hakim.

Seperti telah kita ketahui bahwa tindak pidana komputer memilki karakteristik yang sangat berbeda. Pada tindak pidana yang biasa, penyelidik/penyidik melakukan investigasi di lapangan dan mengumpulkan seluruh alat bukti dan barang bukti yang diperlukan untuk kepentingan penuntutan. Alat bukti dan barang bukti tersebut bersifat fisik. Kalaupun ditemukan bukti yang tidak berwujud, alat bukti yang tidak berwujud tersebut akan memiliki kekuatan pembuktian dengan dukungan alat bukti lainnya. Lalu bagaimana dengan tindak pidana komputer ini? Dari alat-alat bukti yang ada dalam Pasal 184 KUHAP, dapatkah diterapkan untuk tindak pidana komputer?

Dalam memasuki dunia komputer berarti kita memasuki dunia digital yang hanya terdiri dari pulsa-pulsa listrik dan kumpulan logika angka nol (0) dan satu (1). Digital merupakan hasil teknologi yang mengubah sinyal menjadi kombinasi urutan bilangan nol (0) dan satu (1) untuk proses informasi yang mudah, cepat dan akurat.[21]

Komputer mengolah data yang ada secara digital melalui sinyal listrik yang diterimanya atau dikirimkannya. Pada prinsipnya, komputer hanya mengenal dua arus yaitu on atau off. Kombinasi dari arus on dan off inilah yang mampu membuat komputer banyak melakukan banyak hal. Proses komunikasi dan komputer digital menghasilkan atribut-atribut khas yaitu benda-benda digital contohnya sebuah file dokumen, medan elektronik magnetik pada piringan *hard disc* dan lain sebagainya. Atribut-atribut yang khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer inilah yang disebut 'bukti digital'.

Proses komunikasi dan komputer digital yang demikian ini oleh kelompok kerja yang bernama *standard working group on digital evidence (SWGDE)* mendefinisikan sebagai 'semua informasi yang memiliki nilai pembuktian yang kuat yang disimpan atau di

[20] *Ibid.*

[21] Jack Febrian, *Pengetahuan Komputer dan Teknologi Informasi,* Informatika, Bandung, 2004, hlm-145.

transmisikan dalam bentuk-bentuk sinyal-sinyal listrik digital'.[22]

Jika melihat alat-alat bukti yang terdapat dalam Pasal 184 KUHAP, menjadi pertanyaan di sini yaitu dimanakah kita akan menggolongkan digital yang dikatakan oleh kelompok kerja SWDGE di atas sebagai alat bukti dan mempunyai nilai pembuktian yang kuat? Dalam peradilan di Indonesia, keadaan ini menyulitkan Jaksa untuk membuktikan kesalahan terdakwa mengingat masih sedikitnya para penegak hukum memahami masalah ini.

Menurut Rapin Mudiardjo dalam IPTEKnet disebutkan bahwa, Pengadilan Negeri Jakarta Timur telah membuat suatu kemajuan dengan membuat suatu keputusan terhadap suatu kasus pidana yang mengetengahkan bukti *e-mail* sebagai salah satu alat bukti.[23] Dalam kasus tersebut, hakim memvonis terdakwa dengan hukuman satu tahun penjara, karena terbukti telah melakukan tindakan cabul berupa penyebaran tulisan dan gambar yang mengandung pornografi. Hakim kemudian menghadirkan saksi ahli untuk menjelaskan apakah bukti *e-mail* tersebut bisa di manipulasi. Keterangan ahli tersebut digunakan oleh hakim untuk memastikan apakah dalam transfer data melalui *internet mail (e-mail)* tersebut telah terjadi tindakan manipulasi. Setelah mendengar keterangan ahli, kemudian hakim memutus terdakwa telah terbukti melanggar Pasal 282 KUHP.

Dari kasus ini dapat dilihat bahwa proses pembuktian tindak pidana komputer menggunakan alat bukti digital berupa *e-mail* yang kemudian didukung dengan keterangan ahli. Dengan demikian maka kasus tersebut sudah memenuhi persyaratan seperti yang terdapat dalam Pasal 183 KUHAP yaitu 'sekurang-kurangnya terdapat dua alat bukti yang sah' sehingga hakim dapat mengambil keputusan mengenai tindak pidana tersebut.

Pada kasus tindak pidana komputer, seringkali alat bukti menjadi permasalahan dan kendala untuk proses pembuktian, karena dalam tindak pidana komputer si pelaku pasti akan mengusahakan agar supaya kejahatan atau penyalahgunaan komputer yang dilakukannya tidaklah dapat dibuktikan. Adalah benar bahwa kejahatan komputer tidak langsung meninggalkan bukti fisik, namun dalam kasus tindak pidana komputer, semua aspek pendukung, media dan atribut khas pelaku adalah semua yang berhubungan dengan sistem komputerisasi dan komunikasi digital, dan semua ini nantinya akan dicari keterkaitannya yang bersifat fisik.

Dari kasus yang diuraikan di atas, sebenarnya para pelaku meninggalkan bukti berupa bukti digital yang merupakan kunci dari tindak pidana komputer yang telah dilakukan. Dalam kasus tindak pidana komputer, bukti digital yang ditinggalkan dapat berupa : *data log* yang tersimpan di server suatu jaringan, dimana data log tersebut merupakan rekaman aktivitas pengguna internet, didalamnya terdapat *IP Address (IP Address* : alamat *Internet Protocol* yaitu, sistem pengamatan di *network* yang di presentasikan dengan sederetan kombinasi angka) dari si pengguna. Melalui *IP Address* ini dapat diketahui dari mana asal si pelaku, akan terlihat juga mencakup waktu dilakukannya koneksi internet. Selain itu juga dapat dilihat dari hubungan telepon, yaitu hasil *print-out* perusahaan telepon. Kepada siapa telepon ditujukan, dan didalamnya juga di terangkan mengenai lamanya (waktu) pembicaraan.

Sebuah sistem komputer yang aman biasanya dilengkapi dengan *spoofing* suatu *software*, yang jika ada aktivitas internet akan merekam *caller* ID, dan di sana dapat terlihat siapa yang mengakses sistem komputer tersebut. Jika ada orang lain yang mengakses sistem komputer tanpa suatu otoritas maka hal tersebut dapat terdeteksi. Penyelidik atau penyidik dapat mengambil rekaman tersebut sebagai bukti digital.

Menjadi suatu permasalahan adalah jika si pelaku mengetahui hal tersebut, biasanya dia akan menghapus atau menyembunyikan aksinya tersebut. Di sinilah peran seorang ahli dalam memberikan suatu penjelasan di sidang pengadilan, bahwa data digital tersebut adalah sah dan dapat dipertanggungjawabkan secara hukum. Standarisasi dari sistem tersebutlah yang menjadi sandaran berpikir dari setiap argumen yang muncul di pengadilan. Langkah pertama yang dilakukan oleh seorang ahli adalah memeriksa apakah suatu sistem tersebut dapat di percaya. Jika sistem tersebut

[22] Hayri, *Bukti Digital Kunci Penguak Kejahatan Cyber*, PC Media, Jakarta, 2004, hlm-76.

[23] Rapin Mudiardjo, *IPTEKnet,* April 2005, hlm-3.

dapat di percaya, otomatis data digital atau elektronik yang ada dalam komputer tersebut dapat dipertanggungjawabkan dan dapat diajukan sebagai alat bukti/barang bukti yang memiliki kekuatan yang sama dengan alat bukti lain yang ada dalam Pasal 184 KUHAP.

PENUTUP

A. Kesimpulan

1. Tindak pidana di bidang komputer itu dilakukan oleh seseorang tidak didasari motivasi untuk mendapatkan uang sebagaimana halnya kejahatan konvensional, karena orang yang melakukan tindak pidana di bidang komputer ini hanya sekedar *'challenge'* dan merasa tertantang untuk dapat menjawab permasalahan-permasalahan yang memerlukan pemikiran yang *smart* dan juga hanya karena kesenangan belaka, dan berusia relatif muda. Sebagai akibat terjadinya penyalahgunaan komputer, maka bermunculanlah bentuk-bentuk tindak pidana di bidang komputer seperti: *joy computing, hacking, the trojan horse, data diddling, data leakage, wiretapping,* dan banyak lagi lainnya.
2. Penggunaan alat bukti digital berupa *e-mail* haruslah dipakai oleh hakim dalam membuktikan dan menentukan seseorang telah melakukan tindak pidana computer. Bukti digital ini dapat dikategorikan sebagai alat bukti surat dan petunjuk. Upaya pembuktian yang dapat dilakukan oleh penyidik dalam rangka mencari kebenaran materiil dalam perkara *cybercrime/computer crime* adalah: melakukan pengumpulan barang bukti kejahatan *cybercrime/computer crime*, melakukan pemeriksaan terhadap pelaku dan saksi-saksi kejahatan *cybercrime/computer crime*, melakukan digital forensik terhadap barang bukti elektronik yang diguankan oleh pelaku kejahatan *cybercrime/computer crime* di laboratorium forensik, melakukan analisa terhadap waktu/dokumen pelaku melakukan kejahatan dengan waktu/dokumen hasil yang didapat dari laboratorium forensik terhadap barang bukti yang digunakan oleh pelaku kejahatan *cybercrime/computer crime* dan melakukan pemeriksaan terhadap ahli bahasa, ahli digital forensik dan ahli ITE.

B**. Saran**

Sebagai saran yang dapat penulis berikan, bahwa mengingat dan menyadari betapa besar bahaya yang ditimbulkan akibat dari tindak pidana di bidang komputer, yang tidak saja dalam bentuk kerugian material yang tinggi, tetapi juga hilangnya rasa kepercayaan masyarakat terhadap negara atau perekonomian negara, maka aparat penegak hukum harus mampu mengungkap dan menuntaskan di persidangan dengan jitu terhadap kasus-kasus tindak pidana di bidang *computer/cybercrime*. Para ahli hukum harus segera memperbaharui Kitab Undang-Undang Hukum Acara Pidana (KUHAP) khususnya pasal yang mengatur tentang alat-alat bukti yang sah dengan memperhatikan perkembangan dan kemajuan ilmu pengetahuan dan teknologi. Demikian juga bahwa diperlukan peningkatan kualitas para penegak hukum (polisi, jaksa dan hakim) dalam menangani tindak pidana komputer mengingat modus operandi dari tindak pidana komputer sangat berbeda dengan kejahatan konvensional

DAFTAR PUSTAKA

Hamzah, Andi., *Hukum Pidana Yang Berkaitan Dengan komputer*, Sinar Grafika, Jakarta, 1996.

……., *KUHP dan KUHAP*, Rineka Cipta, Jakarta, 2000.

……., *Hukum Acara Pidana Di Indonesia*, Sapta Artha Jaya, Jakarta.

Harahap, M. Yahya., *Pembahasan, Permasalahan Dan Penerapan KUHAP,* Sinar Grafika, Jakarta, 2013.

Lembaga Pendidikan Komputer Indonesia-Amerika, *Mengenal Dunia Komputer*, Jakarta.

Maramis Frans, *Hukum Pidana Umum dan Tertulis di Indonesia*, Rajwali Pers, Jakarta, 2013

Mudiardjo, Rapin., *IPTEKnet*, 2005.

Moeljatno, *Azas-Azas Hukum Pidana,* Bina Aksara, Jakarta, 1983

Poernomo, Bambang, *Azas-Azas Hukum Pidana,* Ghalia Indonesia, Jakarta, cet. ke-3, 1978

Prinst, Darwan., *Hukum Acara Pidana Suatu Pengantar*, Djambatan, Jakarta, 1989.

Prodjodikoro, Wirjono *Asas-asas Hukum Pidana di Indonesia,* edisi ketiga, Refika Aditama, Bandung, 2003

Randy, Yusuf., *Seminar Penanggulangan Kejahatan Komputer*, Jakarta, 1988.

Reksodiputro, Mardjono., *Kejahatan Komputer*, Makalah dalam Lokakarya

Bab-bab Kodifikasi Hukum Pidana, BPHN, Jakarta, 1988..

S.R. Sianturi, *Azas-Azas Hukum Pidana di Indonesia dan Penerapannya*, Alumni AHM-PTHM,Jakarta, 1989

Wahid, Abdul dan Mohammad Labib., *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama , Bandung, 2005.

Widyopramono., *Kejahatan Di bidang Komputer*, Pustaka Sinar Harapan, Jakarta, 1994.