# MASALAH KEJAHATAN KOMPUTER DAN KENDALA-KENDALA YANG DIHADAPI DALAM PENYELESAIAN DAN PENANGGULANGAN

Oleh Drs. Susetio Pramusinto *)

## Pendahuluan

### Latar Belakang Pengkajian Kejahatan Komputer

a. Komputer sebagai produk teknologi tinggi dimanfaatkan untuk kemajuan bangsa dan negara, tetapi dapat juga mempunyai dampak negatif karena disalahgunakan untuk maksud-maksud negatif.

b. Dalam Era komputer ini perlu difahami hal yang terkait antara teknologi komputer dengan perkembangan informasi dan komunikasi yang semakin meluas dewasa ini, di mana ketiganya saling melengkapi. Maka perlu difahami akibat-akibatnya yang timbul baik yang bersifat positif, maupun terutama yang negatif.

c. Terhadap akibat negatif dari kemajuan teknologi komputer mengarah ke bentuk kejahatan perlu difahami oleh para penegak hukum terutama mendalami pengertian-pengertian dan istilah-istilah teknis yang berperan dalam kasus-kasus kejahatan komputer.

d. Bentuk kejahatan komputer yang terjadi di Bank, untuk menangani secara tuntas ada 3 macam terkait yang perlu berperan dalam kasus-kasus kejahatan dengan komputer yaitu; 1. subjek terdiri dari operator, programmer, analisis, konsultan, nasabah dan cashier; 2. modus Operandi, meliputi teknik-teknik, cara-cara merubah program, dan menghapus serta menyadap data yang sebenarnya ; 3. obyek meliputi individu, kelompok lembaga finansial, alat-alat dan pasal-pasal KUHP atau Undang-undang lainnya.

### Permasalahan Yang Diperkirakan Meliputi :

(1) Bagaimana usaha dan upaya yang dilakukan sehingga diperoleh kesatuan berfikir dan pendapat, terutama bagi yang ikut berperan dalam kasus-kasus kejahatan.

(2) Bagaimana upaya melakukan pencegahan, pengawasan dan pengamanan terhadap dampak negatif itu.

Sebagai data awal kejahatan komputer digambarkan seperti di bawah ini :

---

*) Penulis adalah Pok Ahli PTIK, Jakarta.

**Data Awal Kejahatan Komputer**

| No. | Periode | Jumlah Perkara | Jumlah Kerugian | Bank Sasaran | | |
|---|---|---|---|---|---|---|
| | | | | Pemerintah | Swasta | Asing |
| 1. | 1982/1983 | 15 | 5.357.066.001 | 4 | 7 | 4 |
| 2. | 1983/1984 | 8 | 7.162.440.556 | 4 | 1 | 3 |
| 3. | 1984/1985 | 4 | 1.789.449.463 | 2 | 2 | – |
| 4. | 1985/1986 | 7 | 2.190.487.528 | 2 | 4 | 1 |
| 5. | 1986/1987 | 12 | 15.175.000.000 | 1 | 10 | 1 |
| 6. | 1987/1988 | 19 | 3.983.789.000 | 2 | 2 | 1 |
| 7. | 1988/1989 | 46 | 12.150.451.566 | 2 | 2 | – |

**Sumber : DON. B. PARKER**

**Kasus Kejahatan Ekonomi Yang Ada Kaitannya Dengan Penyalah gunaan Komputer**

**5 Fenomena Kejahatan Ekonomi**

(1) Penggelapan oleh manipulator dengan Komputer
(2) Spionase Komputer, pembajakan soft-ware dan pencurian teknologi tinggi
(3) Sabotase Komputer
(4) Pencurian dari jasa-jasa/Services
(5) Pemilikan yang tidak sah atas sistem (data-processing)

Kejahatan Komputer Atau Kejahatan Yang Berkaitan Dengan Komputer dirumuskan sebagai berikut :

Tingkah laku yang tidak sah, tidak etis, atau tidak resmi/autorized, melibatkan proses data secara otomatis dan/atau penyiaran/pengiriman data.

**Penggelapan Oleh Manipulator Dengan Komputer**

Dalam kasus penggelapan dengan komputer banyak sistem Hukum Pidana menghadapi kesulitan dalam menerapkan perundang-undangan pidana yang tradisionil. Menurut definisi perundang-undangan mengenai pencurian, dan mencuri barang diamanatkan dalam banyak sistem hukum seperti, Jerman, Luxemburg, atau Jepang memerlukan pelaku kejahatan, mengambil item/benda atau milik orang lain. Dalam banyak negara peraturan Undang-Undang juga menyebabkan kesulitan sejauh manipulasi "Cash Dispencers" (pembebasan uang kontan). Definisi menurut perundang-undangan mengenai penggelapan dalam kebanyakan sistem hukum seperti di Denmark, Finlandia, Jerman, Yunani, Italia, Jepang, Luxemburg, Norwegia, Swedia dan Swiss, mengharuskan seseorang

yang tertipu Penetapan Undang-Undang mengenai pemalsuan di kebanyakan negara seperti di Belgia, Perancis, Belanda, Finlandia, Jerman, Italia, Luxemburg dan Swiss melakukan sesuatu hal yang dapat dilihat dan dibaca, dari pernyataan (statement yang tercantum dalam dokumen). Dan oleh karena itu tidak dapat meliputi penyimpanan data elektronik. Secara konsekwen oleh sebab itu banyak sistem hukum Barat menghadapi kesulitan dan mencari pemecahan agar menghindari memperluas perkataan/perumusan dalam peraturan perundangan yang ada. Undang-Undang baru yang meliputi penipuan oleh komputer yang telah dilaksanakan itu di Swedia dengan "Data-Act" tahun 1973. Amerika Serikat Extensive State Legislation dimulai tahun 1974. Undang-Undang Pemilikan Uang Palsu dan Penipuan oleh komputer dan penyalah gunaan tahun 1984. Di Inggris Undang-Undang mengenai pemalsuan Uang dan pencurian dalam tahun 1981. Di Kanada perubahan/Amandemen Peraturan Pidana pada tahun 1985. Bills/Peraturan dan Proposal perubahan mengenai penipuan komputer itu dewasa ini didiskusikan khususnya di Australia, Austria, Finlandia, Perancis, Jerman, Jepang, Norwegia, Portugal, Swedia dan Swiss.

**Spionase Komputer Pembajakan Program Dan Meng-Copy Chips**

Menimbang peliputan pidana dan perdata dari spionase komputer suatu pendekatan sistematis hukum harus membedakan 3 aspek :

a) Perlindungan mutu semua data disimpan dalam komputer
b) Perlindungan tambahan untuk program komputer
c) Perlindungan khusus untuk komputer CHIPS

**Perlindungan Data Umum Dalam Sistem Komputer**

Jika informasi diperoleh dengan mengambil kepunyaan orang lain berupa carierre informasi jasmani (seperti daftar dokumen/paper, tape atau disc) peraturan perundang-undangan mengenai ini yang klasik tentang pencurian, pencurian warisan, penggelapan, tidak menimbulkan suatu persoalan khusus di dalam semua sistem Undang-Undang di negeri Barat. Akan tetapi meskipun demikian, kemampuan mengenai memproses data dan sistem komunikasi untuk mengcopy/menyalin data secara cepat, tidak kentara dan sering melalui fasilitas komunikasi telah menggantikan, kebanyakan pencurian dari pembawa informasi traditional dengan perbuatan menyalin informasi ke dalam peralatan data. Oleh karena itu timbul pertanyaan mengenai apa perluasan tercapainya secara murni mengenai informasi pribadi dapat atau harus mencakup penetapan perlindungan Undang-Undang ini. Dalam banyak hukum di negara-negara seperti Jerman dan Italia, seorang itu enggan untuk memperlakukan Penetapan-Penetap-

an Undang-Undang traditional terhadap pencurian dan penggelapan (warisan) kepada abstraksi dari informasi secara tidak sah, oleh karena perundang-undangan/hukum pada umumnya memperlakukan mengambil milik pribadi/jasmani dengan maksud/tujuan secara tetap mengambil sesuatu yang berharga dari korbannya.

**Membuat Komputer Lebih Aman**

Perangkat prinsip-prinsip pengamanan dapat digunakan untuk mengevaluasi berbagai alternatif penanganan/cara-cara pengamanan.

(1) Mengurangi risiko.
Setiap cara pengamanan yang diusulkan/disarankan harus dievaluasi dengan dasar berhasil guna dalam mengurangi risiko dari ancaman yang ditemukan/diketahui.

(2) Pembeayaan dan perencanaan dari penampilan setiap cara pengamanan yang diusulkan harus dievaluasi berdasarkan pembeayaan yang akan dilibatkan untuk menerapkan, menggunakan dan memeliharanya. Juga penurunan dari penampilan orang-orang atau fungsi yang dihalangi oleh pengamanan harus diperhitungkan/diperhatikan.

(3) Tidak adanya kepercayaan terhadap rahasia yang direncanakan/dikonstruksikan.

**Langkah-langkah Pengamanan**

1. Dari segi teknis.
   a) Buatlah perencanaan terlebih dahulu mengenai sistem yang akan diterapkan. Bagian mana dulu yang bisa dicoba dikomputerisasi dengan risiko kegagalan minimal.
   b) Buatlah perencanaan yang matang untuk menghadapi hal-hal yang tak diinginkan, misalnya kegagalan perangkat (keras dan lunak).
2. Dari manajemen perusahaan/instansi.
   a) Persiapkan operator secara matang, sehingga mereka tidak canggung untuk menggunakan komputer.
   b) Persiapkan operator yang dapat dipercaya dan memiliki ketelitian yang cukup tinggi.
   c) Persiapkan jenjang pemakai dengan hak-hak yang jelas untuk menghindari penyalahgunaan komputer.

**Kendala Yang Dihadapi Dalam Penyidikan Dan Penuntutan Terhadap Delik Komputer**

A. Penerapan Hukum Pidana Materiil atau Substantif

1) Perbedaan penafsiran tentang jenis delik yang harus diterapkan terhadap perbuatan mengotak-atik (mengacess) komputer atau alat yang diotomatisasikan untuk mendapatkan keuntungan secara melawan hukum atau perbuatan menggelapkan

data atau program komputer atau data informasi.

Sejumlah delik dikemukakan dalam hal ini antara lain pencurian, penggelapan, penipuan, korupsi (ini khusus di Indonesia mungkin juga di Malaysia) bahkan perbuatan mengotak-atik atau mengaccess komputer untuk memperoleh rahasia negara atau militer di Indonesia dapat digolongkan sebagai delik mata-mata yang termasuk subversi di Indonesia.

2) Bagi perbuatan yang belum tersedia rumusan deliknya baik di dalam KUHP maupun di luar KUHP seperti memasukkan virus ke komputer, mendengar (menguping) pembicaraan melalui alat bantu (alat yang diotomatisasikan) tanpa izin dan sebagainya.

Lebih sulit lagi karena Hukum Pidana yang dianut di Indonesia (sumber Belanda) melarang penerapan analogi, berbeda misalnya dengan KUHP RRC yang boleh menerapkan analogi, artinya diambil rumusan delik yang paling dekat dengan perbuatan yang dilakukan.

**Penerapan Hukum Pidana Formal (Acara)**

Karena delik yang menyangkut komputer itu sangat sulit dibuktikan, maka beberapa masalah yang timbul seprti "penyitaan, perampasan barang-barang bukti" dan sebagainya. Apakah data informasi program komputer dapat dipandang sebagai benda sehingga dapat disita dan sebagainya. Apakah data program dapat dipandang sama dengan tulisan sehingga dapat diajukan sebagai alat bukti tulisan menurut Pasal 184 KUHAP.

**Studi Kasus Kejahatan Komputer Dalam Kegiatan Perbankan**

Penggunaan komputer dalam perbankan telah meningkatkan kecepatan, ketepatan pelayanan dan kegiatan pembukuan serta efisiensi kerja. Keterlibatan manusia yang mengerjakan proses pembukuan telah banyak dikurangi, sehingga faktor-faktor kesalahan manusia dalam proses kerja pun dapat ditekan seminimal mungkin. Namun demikian timbul masalah lain yaitu berupa sangat tergantungnya faktor keamanan proses pembukuan pada sedikit manusia yang menguasai rahasia kode pengaman komputer, baik yang berupa "USER ID" maupun "Pass-Word". Dengan kata lain bila orang-orang tersebut mempunyai itikad tidak baik atau kurang berhati-hati dalam memegang rahasia jabatan, sangat besar kemungkinan terjadinya manipulasi pembukuan keuangan Bank yang dapat berakibat kerugian besar dan sulit terdeteksi dalam waktu yang singkat.

**Objek Kejahatan**

Objek kejahatan dapat berupa Bank atau Nasabah Bank. Berupa

Bank apabila dana dari pos-pos pembukuan bank, ditempatkan secara melawan hak dalam posisi yang dapat diambil oleh pelaku kejahatan atau kelompok pelaku kejahatan. Dan demikian pula halnya dengan nasabah Bank, meskipun setelah melalui klaim perdata oleh nasabah dapat saja akhirnya kembali pihak Bank harus bertanggung jawab atas kerugian yang timbul

**Subjek Kejahatan**

Pelaku kejahatan komputer di dalam perbankan secara teoritis sangat banyak kemungkinannya dapat dilakukan oleh orang luar, orang dalam ataupun gabungan dari keduanya. Dari perkara-perkara yang sudah ditangani, sampai saat ini sekarang hanya dijumpai dua kelompok saja dari tiga yang secara teotertis dapat melakukan kejahatan tersebut di atas. Pelaku terbanyak adalah orang dalam yang pada umumnya berstatus petugas pelaksana pembukuan yang baik secara sengaja maupun tidak sengaja berhasil mengetahui rahasia pimpinannya yang berwenang. Kemudian menyalahgunakannya untuk kepentingan pribadi.

**Modus Operandi**

Modus Operandi para pelaku tindak pidana dalam bidang komputer ini secara umum adalah berupa manipulasi pembukuan yang dapat dijelaskan sebagai berikut :

a) **Pembukaan sistem Pengamanan**

Sistem pembukuan keuangan dengan komputer selalu dilindungi dengan sistem/pengaman, berupa "USER ID" dan "Password". Tujuan sistem pengaman ini adalah, agar supaya hanya pejabat yang berwenang saja yang dapat melakukan perintah-perintah penting pada sistem pembukuan komputer. Dalam hal pelaku kejahatan bukan penjahat yang berwenang itu sendiri, maka pihak pelaku kejahatan perlu mengetahui "USER ID" dan "Password" yang dipakai oleh si pejabat tersebut. Dari kasus yang pernah ditangani pembukaan sistem pengaman ini diketahui dilakukan oleh para tersangka dengan cara-cara sebagai berikut :

1) *Curi pandang*, yaitu si pelaku memperhatikan layar monitor komputer atau ketukan tangan si pejabat yang berwenang pada "Key-Board" komputer, ketika si pejabat membuka sistem pengaman sehingga diketahui olehnya "USER ID" dan "Password" yang digunakan.

2) *Kelalaian Pejabat*, yaitu karena pejabat sedang sibuk, *secara sadar* memerintahkan pada bawahannya untuk membuka sistem pengaman, dengan memberi tahu "USER ID" dan "Password". Ada pula suatu Bank yang lupa merubah "USER ID dan "Password" yang dipakai untuk latihan penggunaan komputer sehingga

berlaku terus ketika komputer sudah beroperasi secara sesungguhnya di dalam Bank.

b) Masukan data

1) Ke dalam komputer dimasukkan data yang tidak benar, berupa setoran-setoran fiktif bagi rekening-rekening tertentu atau pos-pos keuangan yang telah disiapkan oleh pelaku.
2) Selanjutnya dibuat perintah kepada komputer (perintah tidak sah) untuk mentransfer dana dari rekening fiktif atau pos-pos keuangan tersebut pada 1) ke rekening seorang di bank lain yang telah disiapkan sebelumnya sebagai rekening penampungan hasil kejahatan. Cara ini biasanya dilaksanakan pada Bank-Bank dengan sistem komputer bank-bank yang telah berhubungan/access dengan sistem komputer bank-bank lain baik dalam suatu negara ataupun antar negara. Pada bank-bank dengan sistem komputer yang belum berhubugan/access, biasanya dilakukan sebagai berikut :

Setelah dana masuk dalam rekening-rekening tertentu di bank tersebut, dana dipindah bukukan ke rekening penampungan di Bank lain dengan cara menyetor cek atau bilyet Giro di Bank lain tersebut, atau ada pula yang ditarik tunai di kantorkantor cabang lain dari cabang yang sama.

Dari uraian di atas dapat dikenali beberapa modus operandi :

1) Melakukan transfer dana dari Pos keuangan tertentu dalam pembukuan Bank, langsung ke rekening penampungan, yang telah disiapkan di Bank lain.
2) Melakukan transfer perdana dari Pos keuangan tertentu dalam pembukuan Bank ke rekening nasabah tertentu, yang telah disiapkan oleh tersangka di Bank yang sama untuk kemudian dipindahbukukan ke Bank lain.
3) Melakukan penyetoran fiktif kedalam rekening-rekening tertentu di Bank yang sama, untuk kemudian ditarik ke kantor-kantor Cabang lain dari Bank yang sama.

Kesemuanya dilakukan setelah tersangka memperoleh "USER ID dan "Password" dengan cara seperti tersebut dalam huruf a)

**Daftar Kasus-kasus Kejahatan Komputer**

I. Kasus BRI cabang Jogyakarta 15 September 1982, kebobolan Rp. 845.000.000,00

II. Kasus BRI Tangarong KALTIM akhir tahun 1985, kerugian Rp. 137.000.000,00 (Tabanas fiktif)

III. Kasus BNI 1946 cabang Matraman, kerugian Rp. 50 Milyard, tertangkap tahun 1965

IV. Kasus BNI Cabang New-York tanggal 31 Desember 1986, kerugian US $ 18.732.500 (± 25 Milyard rupiah)

V. Kasus pencurian uang di Bank New-York, kerugian US $ 100.000

VI. Kasus pencurian uang di Bank Cabang Amerika tanggal 23 Mei 1972, kerugian US $ 2000 oleh Programmer.

VII. Penggelapan uang dengan menggunakan Terminal Komputer tahun 1973 pada Bank Union Saving di New-York, kerugian US$ 1.500.000.

VIII. Penggelapan melalui program pada tahun 1975 Modus Operandi dengan menambahkan beberapa angka pada program komputer.

IX. Penggelapan secara kerja sama di sebuah Bank di New-York. Membuat float palsu antara dua bank selama 4 tahun, kerugian US$ 900.000 Modus Operandi dengan menggelapkan dan merubah catatan Deposit serta memalsukan program Komputer.

X. Pencurian melalui program di sebuah Bank : seorang memprogram dengan membuka rekening koran RC di mana ia bekerja. Secara bebas mengambil uang, setelah membuat Program meng-ignore overdraft pada RC nya melebihi dana yang dimiliki di Bank tersebut.

XI. Pencurian oleh seorang operator pada sebuah bank di New Yearsy USA, caranya memanipulasi "Saving Account balance sebesar US$ 126.000/Manipulasi data.

XII. Mengumpulkan dari angka-angka yang telah dibuang. Seorang Programmer di sebuah Ban USA dalam perhitungan bunga, menghilangkan angka 4 angka terakhir di belakang koma. Kemudian membuka RC dengan nama palsu. Berhasil menggaet US$ 10.000. Modus dengan membuat program khusus.

XIII. Wire-Fraud Case. Konsultan komputer dari Security Pacific Bank di Los Angeles mempelajari EFT (Elektronik Funds Transfer), berhasil mentransfer beberapa transaction selama 8 hari ke RC miliknya sendiri se-besar US$ 8.000.000 di Irving Treast Company New-York.

XIV. Pencurian dengan mengunakan MCR Code. Seorang nasabah Boston Bank USA mendistribusikan setumpukkan "Bank Deposit Slip" yang telah diberi dengan nomor code "Account" dari RC yang ia miliki di Bank tersebut. Dalam prosessing Bank tersebut hanya dipergunakan MICR Code. Dengan ini pelaku dapat menggaet uang sebesar US$ 50.000.

XV. Kasus di Bank simpan pinjam New-York. Seorang kasir supervisor pada Bank simpan pinjam

mempunyai kebiasaan berjudi, memilih account yang secara teratur bunga diambil 3 bulan sekali, 4 kali setahun baru melihat account. Tiap hari memakai sistem komputer untuk membuat koreksi suatu account tertentu sebesar US$ 54.000. Manipulasi "Switching Deposito Account" selama 3 tahun mendapat dana US$ 1.500.000

## P e n u t u p

Dari uraian terdahulu maka dapat diambil kesimpulan sebagai berikut : Menghadapi permasalahan yang diperkirakan untuk selanjutnya memperoleh kesatuan berfikir dan pendapat, terutama bagi para pelaku yang terlibat dalam kasus-kasus kejahatan. Untuk itu telah diadakan forum LOKAKARYA mengenai pengkajian tentang kejahatan komputer dalam bulan Nopembre 1991 di PTIK Jakarta. Dari kajian-kajian itu dapat ditemukan kasus-kasus yang dihadapi dalam dekade abad 20. Selanjutnya ditinjau perangkat hukum (Pidana), apakah sudah dapat memenuhi cara-cara penanggulangannya. Segi pengamanan ("Internal Security" pun harus diciptakan/diusahakan dalam rangka pencegahan kejahatan yang telah menelan kerugian jutaan rupiah. Sebagai pelengkap untuk memperoleh fakta-fakta di lapangan disajikan studi kasus yang sekaligus menjelaskan mengenai, obyek kejahatan, subyek kejahatan dan tak dilupakan modus operandi yang khas dalam kejahatan komputer ini.

Mudah-mudahan uraian yang singkat ini dapat memberikan gambaran mengenai kejahatan dengan teknologi tinggi ini. Semoga bermanfaat bagi yang berkepentingan.

## Daftar Pustaka


**H.W.K. Kaspersen,** Kejahatan Komputer Dan Hukum Pidana.

**Don.B.Parker,** Kejahatan Komputer.

**Hendrata B.S. EIT,** Manajemen Dan Teknik Pengamanan Komputerisasi Perusahaan.

**Ir. Styo Budi Utomo,** Perlindungan Data.

**Dr. Andi Hamzah, S.H.,** Penuntutan Perkara Kejahatan Komputer.

**Barul Kifli, S.H.,** Pengaruh Kejahatan Komputer Terhadap Perbankan Di Indonesia.

**Drs. Susetio Pramusinto,** Latar Belakang Gagasan Pengkajian Kejahatan Komputer.

**Drs. M. Soewardja,** Studi Kasus Kejahatan Komputer Dalam Perbankan.