097

KEJAHATAN KOMPUTER

(Suatu catatan sementara dalam rangka KUHP Nasional yang akan datang)

Oleh : Mardjono Reksodiputro.

Dunia komputer semakin hari semakin maju. Ia mulai memasuki banyak bidang dalam kehidupan sehari-hari di Indonesia. Sebagaimana terjadi di negeri maju, teknologi canggih komputer telah menimbulkan pula masalah hukum. Masalah yang sama mulai kita hadapi juga di Indonesia. Karangan berikut ini menguraikan beberapa pemikiran akibat berkembangnya komputer di negara kita, dihubungkan dengan pembentukan kitab undang-undang hukum pidana nasional yang akan datang.

Dalam rangka perancangan KUHP Nasional kita timbul pertanyaan : "Apakah tidak sudah waktunya untuk memperluas jangkauan hukum pidana Indonesia dengan menyusun suatu rancangan undang-undang yang mengatur penyalahgunaan komputer (*computer abuse*)? Dan bilamana hal ini dirasa perlu, bagaimana cara melakukannya? Maksud makalah ini adalah memberi tinjauan sementara tentang permasalahan ini, yang mungkin dapat dipergunakan sebagai salah satu bahan bagi panitia khusus, yang masih harus dibentuk, untuk memberikan pendapat yang menyeluruh disertai saran-saran kepada BPHN Departemen Kehakiman. Makalah lain yang disusun penulis setahun yang lalu (Februari 1987) ditutup dengan pendapat agar dicegah penyusunan rancangan undang-undang yang "kurang-dalam" dipikirkan, sehingga dapat mengakibatkan kerugian dalam pengembangan industri komputer dan pengembangan teknologi komputer di negara kita. Maksud makalah yang sekarang adalah memperjelas pendapat tersebut disertai beberapa saran sementara.

Pertanyaan yang diajukan di atas timbul, antara lain karena masyarakat mulai dikagetkan dengan beberapa peristiwa kejahatan yang mendapat sorotan luas dalam media massa cetak. Ada dua peristiwa manipulasi bank yang menarik perhatian. Pertama, pada tahun 1983 di Bank Rakyat Indonesia (BRI)Yogyakarta dan kedua, pada

Computer di mana-mana.

tahun 1986 di Bank Negara Indonesia 1946 (BNI 1946) di New York. Manipulasi yang dilakukan di kedua bank ini, mempergunakan bantuan kecanggihan peralatan komputer. Sejak saat itu mulai dipertanyakan "kemampuan" KUHP (WvS) warisan Hindia Belanda kita, untuk "mengejar" pelaku-pelaku kejahatan yang mempergunakan alat canggih komputer ini. Dan mulailah timbul istilah "kejahatan komputer", yang sempat pula diseminarkan oleh beberapa kalangan swasta. Sebenarnya kedua peristiwa di atas merupakan kejahatan biasa (tradisional) dan bukan kejahatan "baru" dan masih mungkin diselesaikan melalui KUHP yang sekarang berlaku (misalnya sebagai "penipuan"—Titel XXV, "pemalsuan surat"—Titel XII, "penggelapan"—Titel XXIV). Perbedaannya hanya pada alat yang dipergunakan, yaitu komputer yang menyimpan data elektronik, dan menimbulkan permasalahan dalam pembuktian (bandingkan pula permasalahan yang timbul pada waktu untuk pertamakali ditemukan alat telekomunikasi: telegrap, telepon dan radio).

Kalau begitu, apakah yang merupakan permasalahan kita dalam penyalahgunaan komputer ini? (dalam makalah ini "penyalahgunaan komputer" dan ' kejahatan komputer" dipergunakan sebagai istilah yang sama). Sebagaimana dikemukakan dalam makalah Februari 1987, masyarakat modern sekarang sedang dalam masa peralihan dari "masyarakat industri" ke "masyarakat informasi". Dalam masyarakat informasi ini yang merupakan ciri utamanya adalah penggabungan antara pengetahuan informasi dengan pengetahuan telekomunikasi. Kalau tadinya komputer telah mendobrak cara-cara penyimpanan, pengolahan

dan penyampaian data di dalam pusat-pusat 'otak elektronik' (otomatisasi), maka sekarang pusat-pusat tersebut saling dihubungkan pula melalui alat-alat telekomunikasi (antara lain telepon). Pengambilan keputusan, pelaksanaan dan pemantauan (monitoring) dilakukan berdasarkan data yang tersedia dalam pusat-pusat tadi, yang saling berhubungan (juga melampaui batas-batas wilayah negara) melalui alat telekomunikasi. Kegiatan ini menjadi lebih abstrak, rumit (*complex*) dan sukar terlihat. Penggunaan kertas, sebagai media penyampaian data dan informasi, makin berkurang (kertas dapat dilihat dan diraba), sehingga kesalahan-kesalahan (baik karena kelalaian, maupun kesengajaan) tidak begitu cepat dapat diketahui lagi. Lebih jauh lagi, alat canggih komputer ini memerlukan ahli-ahli khusus (ahli–komputer) untuk menanganinya, yang jumlahnya terbatas. Manipulasi data komputer sering pula sukar ditelusuri (apalagi oleh "orang awam") karena relatif mudahnya pula untuk "menghapus" jejak. Inilah secara sederhana inti permasalahan kita. Pertanyaannya kini menjadi: "seberapa jauh hukum pidana dapat dan harus dipergunakan untuk menghambat penyalahgunaan komputer, *tanpa* mengurangi arus data dan informasi yang lancar" (yang sangat diperlukan dalam masyarakat informasi adalah kecepatan dalam "transfer data").

Penyalahgunaan komputer dapat dibagi dalam kategori sebagai berikut: (a) manipulasi komputer, (b) spionase komputer, (c) sabotase komputer, (d) pemakaian secara tidak-sah komputer, dan (e) "memasuki" secara tidak–sah sistem–komputer (Jongerius, 1987). Pada umumnya pembahasan penyalahgunaan 'biasa' menyangkut: manipulasi, pemakaian secara tidak–sah (*unauthorized use*) dan "memasuki" secara tidak–sah (*anauthorized access*). Kerugian yang diderita di sini umumnya bersifat *(prive)* pribadi: manusia maupun perusahaan. Dalam hal "spionase", hal ini sudah menyangkut data rahasia, seperti rahasia negara tetapi dapat juga menyangkut rahasia perusahaan (seperti *software piracy* dan *high technology theft*). Kejahatan dalam bentuk ' sabotase" akan dapat menimbulkan efek kerugian yang besar pada masyarakat, karena caranya dengan "merusak" atau ' menghancurkan" peralatan dan atau sistem jaringan komputer.

Pendekatan yang lain dilakukan oleh Komisi Kejahatan Komputer Belanda (1985–1986) dalam laporannya April 1987, yaitu dengan membedakan antara perlindungan untuk "sarana" (*middelen*) dan perlindungan untuk "data (*gegevens*). Dalam hal *sarana* disarankan agar dijadikan tindak pidana: (a) menghancurkan, merusak, membuat tidak dapat dipakai atau pun menimbulkan gangguan dalam kerja sarana komputer, dan (b) apa yang dinamakan "computervredebreuk (analog dengan "huisvredebreuk", pasal 167 KUHP), yaitu "memasuki" secara melawan hukum sistem komputer atau bagian yang dilindungi oleh sistem pengamanan komputer (SIMANKOM, menurut istilah Jusuf Randy). Mengenai perlindungan untuk *data* disarankan agar dijadikan tindak pidana: (a) membuat tidak dapat dipakai atau menghapus atau membuat tidak dapat "dimasuki" data bersangkutan, (b) memanipulasi data, seperti

menghilangkan, mengubah atau menambah data lain, dan (c) hal-hal yang melanggar perlindungan terhadap data yang harus dirahasiakan atau bersifat eksklusif atau bersifat konfidensial. Dicatat pula bahwa sebagian dari perlindungan ini terletak dalam bidang perlindungan "transfer data" atau telekomunikasi. Pembagian oleh komisi ini pada dasarnya tidak berbeda dengan kategori-kategori yang disebut pada awal butir 4 ini.

Dalam laporan Komisi Belanda ini terlihat adanya saran untuk menyempurnakan WvS Belanda – dengan cara: (1) membuat pasal (aturan) baru, (2) menambah pasal yang ada dengan beberapa kata (kalimat), dan (3) mengubah pasal yang sudah ada. Amandemen (perubahan) pada WvS Belanda ini mengikuti perkembangan di beberapa negara maju lainnya. Namun, rupanya tidak semua negara merasa perlu menambah atau mengubah undang-undang hukum pidananya. Yang tidak mengubah adalah: Belgia, Iceland dan Jepang. Sedangkan yang sudah mengubah adalah antara lain: Swedia (1973), Inggris (1981), Kanada (1985) Denmark (1985), Amerika Serikat (UU Federal, 1984, 1986), dan Jerman Barat (1986); cara yang dipergunakan berbeda-beda, yaitu: (a) pasal-pasal tersendiri atau undang-undang baru, (b) menyesuaikan perumusan delik yang ada, dan (c) menambah bab baru (tersendiri) dalam undang-undang hukum pidana yang ada (Jongerius, 1987).

Piragoff (1986) memberikan 10 (sepuluh) nasihat pada mereka yang akan merencanakan peraturan tentang penyalahgunaan komputer (lihat makalah Februari 1987). Beberapa akan dibahas di bawah ini. Nasihat ke–1, 4 dan 5 adalah tentang "computer–related conduct" yang diresahkan masyarakat dan 'kepentingan masyarakat' yang dirasakan telah dilanggar. Mengenai "computer–related conduct" yang dianggap masyarakat telah mencapai keresahan dapat diajukan di sini 2 (dua) macam perbuatan: (1) manipulasi komputer (Sieber, 1986, menama kannya *fraud by computer manipulation* sebagai bagian dari *computer–related economic crimes*), dan (2) men 'kopi' dan menjual kopi "computer software" secara tidak–sah ("software piracy). Perbuatan yang ke 2 ini, lebih termasuk dalam bidang pelanggaran hak milik intelektual (paten, hak cipta) dan seharusnya dilindungi melalui undang-undang paten (Indonesia belum mempunyainya) atau undang-undang hak cipta (UU 1984). Dalam hal perbuatan ke–1, contoh kasus BRI dan BNI 1946 di atas telah menunjukkan adanya keresahan yang timbul dalam masyarakat (kalangan perbankan dan penegak hukum). Karena Indonesia mempunyai undang-undang tindak pidana ekonomi dan perbuatan manipulasi komputer, khususnya dalam dunia perbankan seperti contoh di BRI dan BNI 1946 ini, dapat menimbulkan kerugian ekonomi yang besar, maka mungkin dapat dipertanyakan apakah perbuatan semacam ini tidak harus termasuk pula dalam tindak pidana ekonomi di Indonesia. Akan halnya 'kepentingan masyarakat' yang perlu mendapat KUHP, hal ini memang sepatutnya dipermasalahkan dahulu agar dapat dimasukkan dalam sistematik yang sesuai dalam KUHP Nasional nantinya. Mengambil contoh dari laporan Komisi

Belanda (1987) dapatlah misalnya dibedakan antara 3 (tiga) macam kepentingan yang perlu mendapat perlindungan, yaitu: (a) tersedianya (*beschikbaarheid*) sarana dan data, (b) integritas "data processing (DP) system" dan data yang ada di dalamnya, dan (c) sifat eksklusif yang (sering) dipunyai sarana dan data tersebut. Nasihat berikut dari Piragoff (1986) yang ingin dikutip pula di sini adalah nasihat ke 9 dan 10. Yaitu yang memperingati kita agar penambahan atau perubahan undang-undang hukum pidana (dalam rangka kejahatan komputer ini) jangan sampai menimbulkan *unwarranted legal or socio-economic effects* dan jangan pula terjadi *over-criminalization.* Nasihat ini menganjurkan kita agar 'berhemat' dengan mempergunakan undang-undang hukum pidana dan apabila memang perlu menciptakan aturan pidana baru, agar perumusan aturannya dibatasi jangkauannya dan disusun dengan kata dan kalimat yang tepat (jangan membuat 'aturan karet'). Oleh karena itulah perlu dipikirkan dengan matang: (a) berapa luasnya kerugian potensial yang mungkin terjadi bilamana ada pelanggaran, (b) adakah padanan dalam aturan lama yang berlaku, (c) tidakkah aturan baru ini akan mengganggu 'kelancaran informasi' dan (d) harmonisasi dengan peraturan perundang-undangan negara lain (internasional).

Dengan memperhatikan pengertian-pengertian di atas (butir 1 sampai dengan 4) serta pembatas-pembatasan dalam butir 5 ini, maka akan disajikan di bawah beberapa contoh penyusunan aturan tentang penyalahgunaan komputer yang dasar dan kerangkanya diambil dari laporan Komisi Belanda (1987). Dalam hal ini dipergunakan ketiga macam kepentingan *(belangen)* yang dijadikan dasar usul komisi, yaitu: (a) tersedianya sarana dan data, (b) integritas "DP system" dan data, serta (c) bersifat eklusif sarana dan data.

Sudah dijelaskan di atas bahwa dalam masyarakat modern yang (akan) berkembang menjadi masyarakat informasi terdapat 'ketergantungan' pada data dan informasi yang diperoleh melalui sarana komputer. Hal ini berarti bahwa perlindungan agar tersedianya sarana dan data ini menjadi mutlak (seperti juga perlindungan terhadap instalasi listrik, air, telekomunikasi, kereta api, dll). Karena 'sarana komputer' dapat dianggap masuk dalam pengertian ' barang" dalam KUHP, maka perlindungan umum telah ada terhadap pencurian (pasal 362) dan penghancuran serta perusakan (pasal 406). Namun, karena 'data komputer' tidak dapat dianggap sebagai 'barang' menurut KUHP (kecuali alat rekaman data seperti: diskette, tape), maka dianggap perlu menambah suatu pasal (analog pasal 406 KUHP) yang memidana perbuatan "menjadikan tidak dapat dipergunakan, menjadikan tidak dapat dicapai (*ontoegankelijk maakt*) atau menghapus data. . ." (usul ke–4 Komisi). Selanjutnya diperlukan aturan baru yang memungkinkan perlindungan dalam rangka 'bahaya umum terhadap orang dan barang' (Titel VII KUHP). Disarankan oleh Komisi pasal yang analog dengan 191 bis dan 191 ter KUHP, yang memidana perbuatan "menghancurkan, merusak, membuat tidak dapat dipakai, mengganggu kerja sarana dan data. . .", baik sengaja (usul ke–1 Komisi) maupun karena kelalai-

an (usul ke–2 Komisi). Dalam rangka ini disarankan pula untuk menambah pasal 408 KUHP dengan memungkin "data" termasuk di dalamnya (usul ke–3 Komisi).

Sebagaimana terlihat di atas, usul-usul pembaharuan ini menyangkut Titel VII dan Titel XXVII KUHP. Penghancuran, perusakan dan sebagainya ini dapat dikategorikan sebagai sabotase komputer. Akibatnya dapat sangat besar sekali pada kelangsungan bekerjanya masyarakat dan kerugiannya mungkin sukar dinilai. Dalam hal perbuatan itu ditujukan pada 'sarana' (*hardware*), maka tidak timbul permasalahan besar dalam penggunaan hukum pidana. Namun, kalau perbuatan tersebut ditujukan pada 'data' (*software*), maka akan timbul permasalahan dalam pembuktian dan juga penafsiran dari perbuatan tersebut (bagaimana menafsirkan perbuatan 'merusak' data, yang merupakan impuls-impuls listrik, padalah perekam datanya sendiri tidak rusak?).

Yang dimaksud dengan 'integritas data *processing* (DP) system' adalah dapat berfungsinya dengan sempurna sarana dan data sesuai dengan maksudnya. Oleh karena itu perlindungan dilakukan terhadap perbuatan yang akan mengganggu berfungsinya sarana dan data tersebut secara sempurna. Misalnya dengan membuat sarana tidak bekerja dengan baik (bekerja dengan gangguan). Perbuatan ini sudah dapat ditampung oleh pasal 406 KUHP, karena itu Komisi tidak mengajukan usul. Lain halnya dalam hal integritas data. Di sini gangguan dalam berfungsinya data dengan sempurna dapat dilakukan melalui perbuatan: mengubah data (sehingga membuat arti lain pada data yang ada), menambah data dan mengambil data. Untuk hal ini diusulkan oleh Komisi untuk mengamendir usul ke 4 di atas (lihat butir–6) sehingga memuat pula perbuatan: 'mengubah' dan "menambah' data.

Mengubah dan menambah data ini merupakan salah satu cara menuju perbuatan kejahatan lain, yaitu memperkaya diri atau orang lain melalui "computer fraude" (contoh kasus BRI dan BNI 1946). Kejahatan ini sebenarnya dapat dituntut berdasarkan ketentuan tindak pidana penipuan dan pemalsuan surat serta yang sejenis yang telah terdapat dalam KUHP. Di Denmark terdapat aturan khusus tentang penipuan melalui komputer ini sebagai berikut :

> *"Any person who, for the purpose of obtaining for himself or for others an unlawful gain, by changing, adding or erasing informations or programs or in other ways unlawfully tries to influence the result of electronic data processing by an act or ommision, shall be guilty of computer fraud". (Jongerius, 1987).*

Dalam hal tindak pidana 'pemalsuan surat' akan dipergunakan pasal 263 KUHP maka kesukarannya adalah penafsiran istilah surat (*geschriften*). Di Inggris dalam hal "forgery and counterfeiting" dipergunakan istilah "instrument" yang kemudian diperluas juga meliputi "any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical or other means" (Jongerius, 1987).

Yang perlu dilindungi pula adalah sifat eksklusif sarana dan data. Pertama-tama dapat dilihat *pemakaian* eksklusif sarana dan data tersebut. Hal ini menyangkut bila mengenai sarana, perbuatan yang dikenal dengan nama

"joy-computing" (analog dengan "joy-riding"). Apabila hal ini dilakukan dari luar (untuk membedakan penggunaan di dalam lingkungan, misalnya: kantor, instansi, perusahaan) maka harus dipergunakan bantuan alat telekomunikasi (telepon); karena itu sebaiknya hal ini diatur dalam undang-undang telekomunikasi (PTT) bersangkutan. Bila mengenai data, maka perbuatan pemakaian secara tidak sah ini dilindungi melalui undang-undang hak cipta (bila mengenai "program komputer") dan undang-undang paten (bila menyangkut program yang terdapat dalam "memori komputer"). Hak yang kedua yang dapat pula dilihat di sini, adalah perlindungan terhadap *sifat rahasia dan pribadi* sarana dan data tersebut. Cara pelanggaran di sini adalah perbuatan: pemakaian sarana secara tidak sah, memperoleh pengetahuan atau meng 'kopi' data secara tidak sah, serta "memasuki" secara tidak sah "DP system".

Untuk melindungi sifat rahasia dan pribadi (konfidensial) data, Komisi mengusulkan untuk memidana perbuatan yang diberi nama "computer-vredebreuk" (analog dengan "huisvredebreuk", pasal 167 KUHP). Perbuatan yang dapat dipidana di sini adalah: "memasuki secara melawan hukum sistem komputer yang telah diberi sistem pengamanan komputer" (usul ke–15 Komisi). Pembocoran rahasia (negara maupun perusahaan) diusulkan untuk dipidana dengan mengubah pasal 112 KUHP (kejahatan terhadap keamanan negara) dan pasal 323 KUHP (usul ke 13 dan ke–14 Komisi). Untuk menambah pasal baru yang bertujuan memidana perbuatan: "dengan sengaja dan dengan tujuan mencari keuntungan menyampaikan atau memakai data yang diperoleh melalui kejahatan" (usul ke–16 Komisi). Terakhir, dalam rangka melindungi sifat rahasia dan pribadi data dari penggunaan secara melawan hukum alat telekomunikasi yang dipakai dalam "memindahkan" data (*data transfer*) telah diusulkan 7 aturan. Mula-mula dalam bidang sarana umum telekomunikasi diusulkan perubahan pasal 139c WvS Belanda (mendengarkan atau menyadap percakapan telepon) dan perubahan pasal 519 bis KUHP (usul ke–16 dan ke–7 Komisi). Di samping itu perlu dilindungi pula kerahasiaan data yang dipindahkan dalam lingkungan terbatas (tertutup) dan karena itu diusulkan perubahan pasal 139a dan 139b WvS Belanda (usul ke–8 dan ke–9 Komisi). Di samping pemindahan data melalui sarana umum dan yang terjadi dalam lingkungan terbatas, masih ada kemungkinan ketiga, yaitu pemindahan data melalui jaringan-jaringan komunikasi *intern*, misalnya pada suatu perusahaan multinasional.

Salah satu cara untuk membendung pada tahap awal kemungkinan penyalahgunaan komputer (kejahatan komputer) adalah dengan memasang pengaman dalam bentuk aturan pidana di "ambang pintu sistem komputer". Oleh karena itulah maka pasal tentang "computervredebreuk" yang diusulkan Komisi merupakan salah satu pasal kunci. Perbuatan yang dinamakan pula "unauthorized access" ini, akan memungkinkan "penyadapan" dan "pengambilan" data secara melawan hukum. Dalam hal penyadapan, data akan tetapi sampai di si-alamat sedangkan dalam hal pengambilan tidak. Contoh aturan untuk "unauthorized ac-

cess" adalah dari Denmark :

> *"Any person who unjustifiably obtains access to another person's informations or programs meant to be used in data processing services, shall be liable. . ."*

Sedangkan untuk penyadapan data dapat dilihat contoh dari Finlandia:

> *'Anyone who, without authority (. . .) – intercepts or attempts to intercept any telecommunication message being transmitted in a telecommunication network, such as telephone conversation, telegram, or text, picture or data transmission (. . .)*

(Jongerius, 1987).

Data dapat di 'kopi' secara melawan hukum ataupun diambil (diasingkan). Bedanya adalah bahwa dalam hal di 'kopi' secara illegal, pemilik masih dapat menguasai data. Juga peng'kopi' an ini dapat dilakukan secara cepat dan sukar terlihat (kadang-kadang pemilik pun tidak mengetahui bahwa data-nya di'kopi').

Dalam KUHP, khususnya dalam delik yang menyangkut harta benda (*vermogensdelicten*) istilah: "voorwerpen", "goed" dan "zaak" sering kali terdapat. Masalahnya apakah istilah-istilah tersebut sudah dapat mencakup "data komputer". Kalau menyangkut "rekaman data" (*diskette, tape*) hal ini tidak merupakan masalah, tetapi dapat dibayangkan bahwa dalam beberapa pasal KUHP tertentu, mungkin juga obyek kejahatannya adalah "data komputer" dalam arti murni (bukan rekaman datanya). Karena itu Komisi mengusulkan penambahan kalimat "atau data yang mempunyai nilai kekayaan (*vermogenswaarde*) dalam lalu-lintas perdagangan" pada pasal-pasal KUHP berikut ini: 231 (menarik barang dari penyitaan), 368 dan 369 (pemerasan), 378 dan 383 (penipuan), 397 dan 399 serta 404 (merugikan kreditur atau yang berhak) (usul ke–17 Komisi). Selanjutnya Komisi juga berpendapat perlu melindungi "credit-cards" (*betaalpassen*) dari pemalsuan dan karena itu mengusulkan setelah pasal 263 dan 264 KUHP (pemalsuan surat) pasal baru yang memidana perbuatan pemalsuan "credit cards" (usul ke–18 Komisi). Dalam hubungan dengan kejahatan pemerasan (pasal 368 KUHP) Komisi pun melihat adanya kemungkinan perbuatan tersebut dilakukan dengan "mengancam disertai kekerasan" terhadap data (membuat tidak dapat dipakai, tidak dapat "dimasuki" atau dihapus). Karena itu diusulkan perubahan pasal 89 KUHP Buku Kesatu (arti istilah kekerasan) sehingga mencakup pula perbuatan: "membuat tidak dapat dipergunakan, tidak dapat "dimasuki" atau menghapus data" (usul ke–19 Komisi)

Ketiga macam usul di atas merupakan usaha Komisi untuk menutup lubang-lubang yang masih ada dalam usaha menyempurnakan WvS Belanda (dalam makalah ini di mana mungkin dipergunakan pasal KUHP/WvS Hindia Belanda) untuk dapat mengejar kejahatan komputer. Dalam usaha ini Komisi rupanya berusaha melakukan perubahan itu secara 'hemat', kadang-kadang diajukan alasan bahwa kemajuan ilmu pengetahuan belum cukup untuk melakukan perubahan aturan (misalnya dalam hal istilah rapat dalam pasal 173 KUHP belum perlu ditafsirkan mencakup pula 'rapat melalui alat telekomunikasi', atau yang dikenal dengan *"teleconferencing"*) atau dengan alasan bahwa yurisprudensi yang berlaku sudah dapat memperluas jangkauan suatu istilah (misalnya penger-

tian "geschriften" atau "surat" dalam pasal 263 KUHP).

Seperti disampaikan pada butir 1 makalah ini, untuk Indonesia masih perlu dibentuk suatu *"panitia ad hoc"* yang mengkaji permasalahan penyusunan aturan-aturan hukum pidana yang dapat menanggulangi penyalahgunaan komputer (*computer abuse*) atau kejahatan komputer (*computer crime; computer criminaliteit*). Seperti dinasihatkan oleh Piragoff (1986) dan juga dilakukan oleh Komisi Belanda, yang pertama-tama harus dilakukan adalah memeriksa undang-undang hukum pidana yang berlaku, sejauh mana masih dapat dipakai dalam lingkungan komputer (*computer environment*). Selanjutnya perlu diperhatikan pula bahwa terdapat perbedaan antara "data" dan "informasi" serta harus dipisahkan pula pengertian "sarana".

Dengan meminjam sistematik yang dipergunakan dalam laporan Komisi Belanda dapatlah disimpulkan bahwa: perbuatan-perbuatan yang tidak-sah (melawan hukum) yang perlu dipidana adalah sebagai berikut (laporan Komisi, Bab II, paragraf 1.2, butir 28)

a. Untuk melindungi kepentingan "tersedianya" (*beschikbaarheid*) sarana (*middelen*), maka perbuatan yang perlu dipidana adalah:
   - sabotase, penghancuran, perusakan, membuat tidak dapat dipakai, mengambil, mengganggu, dan membuat tidak dapat digunakan oleh pemakai yang sah;

   sedangkan untuk data (*gegevens*), maka perbuatan yang perlu dipidana adalah :
   - menghapus, menghilangkan, membuat cacat, dan membuat tidak dapat "dimasuki";

b. Untuk melindungi kepentingan "integritas' (*integriteit*) sarana, maka perbuatan yang perlu dipidana adalah :
   - manipulasi,

   sedangkan untuk data, maka perbuatan yang perlu dipidana adalah;
   - memasukkan data yang tidak benar, dan menambah ;

c. Untuk melindungi kepentingan "eksklusivitas" (*exclusiviteit*) sarana, maka perbuatan yang perlu dipidana adalah :
   - secara tidak-sah mencari 'jalan masuk", dan memakai secara tidak-sah;

   sedangkan untuk data, maka perbuatan yang perlu dipidana adalah :
   - memperoleh pengetahuan, menyebarkan, mengumumkan, pemakaian secara tidak benar dan melanggar undang-undang, men 'kopi', menggunakan untuk tujuan komersial.

Selanjutnya beberapa kesimpulan dan saran ingin disampaikan sebagai penutup :

1. Pengaturan untuk menanggulangi penyalahgunaan (kejahatan) komputer sebaiknya diintegrasikan dalam KUHP dan tidak dalam bentuk undang-undang tersendiri;
2. Masih perlu dikaji lebih lanjut apakah bentuk pengaturan ini dalam bab KUHP tersendiri atau dengan cara menambah dan mengubah pasal dalam sistematik KUHP;
3. Pengaturan ini harus dilakukan dengan "hemat" dan tidak mengubah asas-asas yang berlaku serta dirumuskan secara tepat agar jangkauannya terbatas; hal ini adalah un-

tuk mencegah akibat-akibat sampingan (dalam sistem hukum dan sistem sosial-ekonomi) yang tidak dimaksudkan dan dapat mengganggu perkembangan industri komputer dan perkembangan teknologi komputer di Indonesia;

4. Kategori perbuatan penyalahgunaan komputer dalam: (a) manipulasi komputer, (b) spionase komputer, (c) sabotase komputer, (d) pemakaian secara tidak-sah komputer, dan (e) "memasuki" secara tidak-sah sistem komputer, dapat dipergunakan sebagai dasar kerja dengan memperhatikan pula pembagian (pendekatan) yang dilakukan Komisi Kejahatan Komputer di Belanda dalam laporannya tahun 1987;
5. Perhatikan khusus harus diberikan pada kategori "manipulasi komputer", karena perbuatan ini merupakan kejahatan "computer fraud" sebagai bagian dari "computer-related economic crimes" yang dapat menimbulkan kerugian besar bagi pembangunan di Indonesia; karena itu perlu dipikirkan pemasukannya dalam undang-undang tindak pidana ekonomi;
6. Disarankan agar dibentuk panitia "ad hoc" yang bertugas mempelajari secara khusus permasalahan: "seberapa jauh hukum pidana dapat dan harus dipergunakan untuk menghambat penyalahgunaan komputer, *tanpa* mengurangi arus data dan informasi yang lancar yang dibutuhkan dalam masyarakat informasi Indonesia".

Daftar Pustaka

C.B.M. Jongerius, *Informatietechniek dan Strafrecht–Verslag van en Studie naar Wetgeving omtrent Computer–Criminaliteit in Andere Leiden*, 1987.

D.K. Piragoff, *Combatting Computer Crime With Criminal Law*, 1986.

Informatietechniek dan Strafrecht–*Rapport van de Commissie Computer–Criminaliteit*, April 1987.

Mardjono Reksodiputro, *Beberapa Catatan tentang Penyalahgunaan Komputer dalam Masyarakat Informasi Suatu Tinjauan Umum dan Sementara*, Februari 1987.

U. Sieber, *New Legislative Responses to Computer–Related Economic Crimes and Infringements of Privacy*, 1986.

If a man will begin with certanties, he whall end in doubts; but if he will be content to begin with doubts, will end in certainties.

(Francis Bacon).