PROSPEK PENGATURAN KEJAHATAN KOMPUTER DI MASA MENDATANG

Oleh:
Ikhsan Yusda PP
Jurusan Teknologi Informasi
Politeknik Negeri Padang
E-Mail: **ikhsan_yusda@yahoo.com**

INTISARI

Kejahatan komputer semakin menjadi persoalan internasional dan membutuhkan kerja sama internasional, sehubungan dengan meningkatnya transnational/transborder data flow melalui jaringan komunikasi internasional. Dari sini jelas, bahwa menanggulangi kejahatan komputer bukan lagi masalah negara per negara, tetapi membutuhkan kerjasama internasional yang erat, khususnya dalam penelitian kriminologis, perubahan rumusan undang-undang, pengembangan strategi pengamanan dan penuntutan. Serta kriminalisasi terhadap kejahatan komputer merupakan kebutuhan mengingat dampak yang luas dari kejahatan tersebut baik terhadap fungsi, fungsi infrastruktur publik, bahaya umum terhadap barang dan jasa maupun terhadap ketenteraman hidup sesama. Bahan-bahan penyusunan kriminalisasi dapat berasal dari perkembangan di negara-negara lain dan pandangan-pandangan yang tumbuh di Indonesia. Over criminalization harus dihindarkan agar tidak menghambat perkembangan teknologi informatika.

***Kata kunci**:* Computer *Mistake, Kejahatan Komputer, Over Criminalization, Teknologi Informatika*.

ABSTRACT

Computer crime is increasingly becoming an international issue and requires international cooperation, due to the increasing transnational/transborder data flow through international communication networks. From this it is clear that coping with computer crime is no longer a country-by-country issue, but requires close international cooperation, particularly in criminological research, changes in the formulation of laws, the development of security and prosecution strategies. And criminalization of computer crime is a necessity given the widespread impact of the crime on the function, function of public infrastructure, the general danger to goods and services and to the peacefulness of peer life. The materials for the preparation of criminalization can come from developments in other countries and the growing views of Indonesia. Over criminalization should be avoided so as not to hinder the development of informatics technology.

***Key words**: Computer Mistake, Computer Crimes, Over Criminalization, Informatics Technology*.

1. PENDAHULUAN

Dewasa ini komputer sudah merupakan suatu alat bantu yang amat bermanfaat bagi masyarakat dan di gunakan pada pelbagai aktvitas manusia dalam kehidupannya ,sepert; rumah tangga, sekolah, perdagangan dan pemerintahan. Namun, dengan penggunaan kmoputer yang semakin meningkat tersebut pada akhirnya disadari, bahwa pelbagai kemungkinan yang buruk dapat atau telah terjadi, baik yang diakibatkan oleh keteledoran dan kekurangan kemampuan, maupun kesengajaan yang dilandasi sikap bathin yang tidak terpuji.

Sebagai gambaran dalam hal ini dapat dicontohkan apa yang disebut *computer mistakes* yang dapat mencakup:

a) data entry errors.
b) error in copmuter programs.
c) mishanding of computer output.
d) equipment melfunctions dan
e) electrical problems, humanity problem atau persoalan lingkungan hidup yang lain.

Kesalahan-kesalahan diatas, jelas akan mempengaruhi kebijakan yang didasarkan atas sistem komputer. Dalam hal ini, misalnya saja ada istilah *garbage out* (GIGO) yang artinya *feeding incorrect data into the computer will resoult incorrect output*. (Stair, 1986: 120).

Contoh hasil sampingan lain dari kemajuan teknologi komputer adalah terjadinya pengangguran yang semakin meningkat sebagai akibat penggunaan komputer, sehingga sering dikatakan bahwa penggunaan komputer yang luas di lingkungan kerja akan menimbulkan dehumanisasi. Belum lagi hal-hal yang menyangkut kesehatan, seperti; compuphobia, yaitu perasaan ketidak amanan kerja, kehilangan kontrol, ketidak mampuan, dan sebagainya. Bisa

DOI 10.21063/JTIF.2018.V6.1.24-31

juga dalam bentuk *electronic smog* sebagai akibat radiasi frekuensi radio yang katanya dapat menimbulkan kanker.

Tanpa mengesampingkan hal-hal yang sangat positif dari berkembangnya teknologi *komputer*, peninjauan terhadap sisi negatif penggunaan komputer justru akan menyadarkan kita bahwa:

"for *those who can adapt and benefit from Computers, it will he the best times. For those who don't or can't, it will be the worst of timer*".

Dari sekian banyak akibat negatif penggunaan komputer, sebenarnya yang paling meresahkan dewasa ini adalah kejahatan komputer (*computer crimes*). Kejahatan komputer tersebut bisa berupa:

a) add, delete or change inputs to the computer system;
b) modify or develop computer programs that commit th froud;
c) Alter or modify the data files used by the computer system;
d) Operate the computer system in a way to commit froud; dan
e) Divery or misuse valid output from the computer system.

Dalam hal ini muncul istilah-istilah, misalnya; *data diddling* (modifying data before it is processed). *Trojan Horse* technique (an approach where the criminal is able to money from computer and related bank accounts), dan *masque-rading* (an approach where the criminal pretends to be an authorized user). Yang sangat menarik dari kejahatan komputer ini adalah motivasi dilakukannya perbuatan tersebut, seringkali dikatakan bahwa, pelaku tindak pidana komputer melakukan perbuatannya semata-mata karena uang, tetapi ada unsur *challenge*. Yang dipikirkan oleh mereka bukan hanya profit, melainkan bagaimana mengakali (outsmarting) suatu sistem komputer dan melakukan untuk kesenangan. (Arthur, 1984: 201).

Kejahatan komputer semakin menjadi persoalan internasional dan membutuhkan kerja sama internasional, sehubungan dengan meningkatnya *transnational/transborder data flow* melalui jaringan komunikasi internasional. Dari sini jelas, bahwa menanggulangi kejahatan komputer bukan lagi masalah negara per negara, tetapi membutuhkan kerjasama internasional yang erat, khususnya dalam penelitian kriminologis, perubahan rumusan undang-undang, pengembangan strategi pengamanan dan penuntutan, sebagaimana yang telah dilakukan oleh Council of Europe.

Studi perbandingan internasional terhadap kejahatan komputer sangat penting. Hal ini dapat dikaji dari pendapat OECD yang menyatakan bahwa:

Computer-related criminality clearly has important economic implications, although precise figures are hard to come by. The international character of the computer-related crime phenomenon, which is due to the internationalization and computer service, has also been recognised, and with it the necessity for Member countries to exchange information on their experiences and on the solutions to be adopted to face the fenomenon flows could be the result or a situation in which certain Member countries have legal instrument to deal with computer-related crime. While others do not. This study attempts to identify the various policies in Member countries, as well as the acts or behaviour constituting what it has been agreed to call computer related crime, in order to approach a consensus to coordinated and adopt solutions at the international level to avoid such acts or behaviour. (OECD. 1986: 6).

Dalam rangka penanggulangan kejahatan komputer melalui sarana hukum ini, hukum perdata, hukum administrasi maupun hukum pidana dapat digunakan secara komplementer, disamping tindakan-tindakan pencegahan lain yang bersifat non-yuridis. Selanjutnya, sepanjang hukum pidana hendak digunakan, haruslah selalu diingat sifat hukum pidana yang mempunyai fungsi subsidair, mengingat sifatnya yang keras, yakni; janganlah menggunakan hukum pidana, apabila masih ada sarana-sarana lain yang memadai. Ini merupakan asas pembahas (*limiting principle*) untuk mencegah apa yang disebut *unforseen consequences in other areas of the legal and socio economic system.*

2. TINJAUAN KEPUSTAKAAN

2.1. Anatomi Kejahatan Komputer

Untuk tidak menimbulkan salahsatu tafsir, sebaiknya pahami terlebih dulu atau disepakati terlebih dahulu definisi kejahatan komputer (*computer crime atau computer related crime*). Kelompok ahli yang dibentuk oleh OECD, menyatakan komputer dapat didefinisikan dalam kerangka pengertian *computer abuse*, yakni:

Any illegal, unethical or unauthorized behavior involving authomatic data processing and or transmissing of data.

DOI 10.21063/JTIF.2018.V6.1.24-31

Definisi ini meliputi antara lain:

1. Computer-related economic crimes (computer froud, computer espionage, computer sabotage;
2. Computer related offences against the citizens right to privacy superindividual interest (offences against national security or control of transborder data flow). (Sieber, 1986: 76-77).

Selanjutnya, sepanjang menyangkut computer related economic crime, 5 (lima) fenomena yang menonjol adalah:

a. froud by computer manipulation;
b. computer espionage, software piracy, high technology theft;
c. computer sabotage;
d. theft of service; dan
e. unauthorized access to DP-system.

Disamping hal-hal diatas, muncul pula istilah-istilah yang khas komputer, misalnya; hacking untuk menggambarkan *unauthorized access to DP-system* dari negeri Belanda, dengan pengalamannya memidana pelaku tindak pidana yang mengambil mobil orang lain untuk bersenang-senang tanpa niat untuk memiliki mobil tersebut dalam bentuk tindak pidana *joyriding*, muncul istilah *joycomputting* bagi mereka yang secara tidak syah mencuri service atau mencuri waktu dalam penggunaan komputer.

Untuk memperjelas ruang lingkup kejahatan komputer, hal tersebut dapat dilihat dalam ruang lingkup sebagai:

a) komputer sebagai instrumen untuk melakukan kejahatan tradisional, seperti; pencurian, penipuan, penggelapan uang atau deposito kredit, penyalahgunaan credit card dan pemalsuan;
b) komputer dan perangkatnya sebagai obyek penyalahgunaan, seperti; *computer sabotage* yang dapat mencakup perbuatan-perbuatan *destroys or alter data, renders it, meaningless, useless or ineffective, itnterferes with its lawful use, interferes with any person entitled thereto*;
c) penyalahgunaan yang berkaitan dengan komputer atau data yang dapat berkaitan dengan *interception of communication or functions of computer system, unauthorized use of computer system* (mencakup *unauthorized obtaining of computer service or time dan unauthorized use of computer system*); dan
d) unauthorized acquisition, disclosure or use of information and data.

3. PEMBAHASAN

3.1. Permasalahan Kejahatan Komputer dalam Hukum Pidana

Di pelbagai negara, langkah-langkah yuridis untuk menangkal kejahatan komputer terus dilakukan. Sebagai ilustrasi dapat dikemukakan disini pelbagai langkah legislatif yang dilakukan untuk menghadapi *froud by computer manipulation*. Didalam sistem hukum Kontinental hal ini biasanya diusahakan untuk diatasi dengan ketentuan-ketentuan hukum yang berkaitan dengan penipuan (*fraud*) dan pemalsuan (*forgery*), sedangkan di negeri-negeri Anglo Amerika cenderung untuk mengaitkan atau memasukkannya (misalnya; mengenai deposito uang) dalam ketentuan-ketentuan tentang pencurian dan penggelapan (*theft and embezzelment*).

Mengaitkan begitu saja kejahatan komputer dengan kejahatan-kejahatan tradisional tidak begitu gampang. Misalnya, untuk adanya pencurian dan penggelapan diperlukan perbuatan berupa mengambil suatu barang kepunyaaan orang lain. Kesulitan akan timbul bilamana si pelaku mengambil deposit uang berkaitan dengan *cash dispensers*.

Demikian pula, apabila menyangkut tindak pidana penipuan (*fraud*) yang di pelbagai negara diperlukan adanya syarat bahwa seseorang telah dicurangi adalah komputer. Hal ini sulit diterapkan apabila yang dicurangi adalah komputer. Sepanjang menyangkut pemalsuan masalah yang timbul adalah; apakah *electronical stored data* termasuk dokumen yang dipalsukan, padahal untuk ini biasanya disyaratkan adanya pernyataan yang dapat dilihat dan dibaca.

Pelbagai penafsiran yang sulit tersebut menimbulkan dampak terhadap langkah-langkah legislatif yang akan dilakukan. Pendekatan pertama yang dapat dilakukan dalam hal ini disebut sebagai pendekatan global (*global approach*), yang menghendaki adanya pengaturan baru yang bersifat umum terhadap kejahatan komputer yang mencakup pelbagai bentuk perbuatan berupa; manipulasi, perusakan, pencurian dan penggunaan komputer secara melawan hukum dan tanpa kewenangan (*access to DP-system*). Hal ini tampak misalnya, pada Swedish Data Act, 1973.

Pendekatan lain disebut sebagai pendekatan evolusioner (*evolutionery approach*) yang berusaha untuk mengadakan pembaharuan atau amandemen terhadap perumusan kejahatan-kejahatan tradisional, dengan menambah objek dan cara-cara dilakukannya

DOI 10.21063/JTIF.2018.V6.1.24-31

kejahatan komputer dalam perumusannya. Penambahan dala hal ini dapat berarti modifikasi atau berupa suplementasi. Contoh yang jelas dalam hal ini adalah Penal Code Amandement Act, 1985 di Canada.

Pendekatan yang ketiga yang merupakan kompromi antara pendekatan global dan pendekatan evolusioner dilakukan dengan cara mencantumkan komputer didalam Kodifikasi Hukum Pidana.

Langkah-langkah legislatif diatas, sesuai pula dengan pengkajian OECD yang menyatakan bahwa:

The differing combinations of these factors explain differences in legislative policy. Although it is difficult to fit countries legal systems, complex as they are, into any simple classification, it is possible to identify two types of policy, even if this classification may be questioned for certain specific acts:

a. One regards computer-related crime as presenting no special features requiring any particular new measures, and sees no need for any distinction between information and computerised information, the commiting an act already covered by existing law. The paramount problem is considered to be the security systems and compensation for damage caused to private assets. This attitude has been adopted at the time being by Belgium, Iceland and Japan;
b. A second attitude is to consider that legislatif measure are needed: two methods being, one, to amend existing law provisions in order to encompass this new from of deliquency, the other, to establish new incriminations to add the computer dimension (these two methods can be used together). The following countries are following this approach: Australias, Austria, Canada, Denmark, Finland, France, Germany, Greece, Italy, Netherland, Norway, Portugal, Sweden, Switzerland, the United Kingdom, and the United States. (OECD, 1986: 12-13).

Selanjutnya, dalam hal *computer espionage*, *program piracy and copying of chips*, permasalahan yang sangat menonjol adalah sampai seberapa jauh *incorporeal information* dapat dicakup oleh ketentuan-ketentuan atau penggelapan. Hal ini jelas berkaitan dengan teorti tentang hak milik berupa barang (*property theory*) yang harus dikembangkan sehubungan dengan adanya perbedaan antara *corporeal property and intellectual property rights* dan antara *theft of tangible thing and theft of information*.

Selanjutnya, dalam hal *computer sabotage* persoalan tidak akan timbul apabila yang dirusak adalah komputer sebagai perangkat keras, dan perusakan tersebut bersifat fisik. Akan tetapi, persoalan akan timbul bilamana terjadi perusakan yang bersifat non-fisik, khususnya apabila data dihapuskan. Misalnya, di Australia, Canada, Denmark, Italy, perusakan informasi dinyatakan sebagai perusakan barang, karena dianggap merusak fungsi barang tersebut secara fisik. Sebaliknya, di Belgia Finnish, misalnya, tanpa adanya kerusakan fisik dianggap tidak ada perusakan barang. Di Canada dengan adanya amandemen tahun 1985, tindak pidana Mischief (merusak barang) mencakup pula *Mischief in relation to data*.

Kemudian sepanjang menyangkut *unauthorized access DP-systems* kebutuhan untuk dilakukanya kriminalisasi semakin meningkat sehubungan dengan meningkatnya penggunaan *remote data processing system*. Pelbagai negara yang telah mengundang peraturan baru dalam hal ini mensyaratkan, bahwa *punishing access only in cases where the accessed data are protected only in cases where the perpetrator has harmful intentions, or in cases where information is obtained, modified or demaged*.

Hal yang cukup menarik adalah berkaitan dengan *computer related in infringements of privacy*. Kebutuhan hukum untuk mengatur hal ini (baik hukum pidana, hukum perdata maupun hukum administrasi) semakin meningkat sehubungan dengan kecanggihan teknologi untuk mengumpulkan, menyeleksi, menghubungkan dan menyebarkan data, dan hal ini menimbulkan ketakutan didalam masyarakat berupa ancaman rahasia pribadi seseorang. Dengan memperhatikan pelbagai negara, OECD berusaha untuk membuat bentuk *model law* yang diharapkan dapat dijadikan pedoman oleh pelbagai negara untuk mengatur *criminal privacy protection* ini, dalam rangka menghindarkan apa yang dinamakan *under and over criminalization*. Azas-azas ini mencakup hal-hal sebagai berikut:

1) Berdasarkan atas kenyataan, bahwa perlindungan rahasia pribadi lebih bersifat perdata dan administratif, sehingga sudah selayaknya apabila hukum pidana digunakan sebagai sarana terakhir (*ultima ratio principle*).
2) Masing-masing ketentuan pidana yang akan dibuat harus secara tepat dan teliti

DOI 10.21063/JTIF.2018.V6.1.24-31

menggambarkan perbuatan yang dilarang dan harus dihindarkan perumusan yang bersifat samar dan umum (*precision principle*).

3) Perbuatan yang dikriminalisasikan harus digambarkan secara jelas dalam ketentuan hukum pidana (*clearness principle*).
4) Perumusan pelanggaran terhadap kerahasiaan pribadi harus dilakukan dengan menghindarkan perumusan yang bersifat global. Asas kulpabilitas menghendaki adanya pertimbangan terhadap keraguan yang disebabkan oleh kepentingan yang dirusakkan, perbuatan-perbuatan yang dilakukan, status pelaku tindak pidana, dan sebagainya. (*principle of difterentiation*).
5) Perbuatan yang dilakukan dengan kesengajaan. Kriminalisasi perbuatan-perbuatan culpa mensyaratkan pembenaran khusus. (*principle of intents*).
6) Pemidanaan hanya dilakukan atas permintaan si korban. (*principle of victim application*). (Sieber, 1986: 95-96).

Asas-asas diatas sangat baik, dan hal ini sesuai dengan asas-asas utama hukum pidana, baik yang terpancar dari asas legalitas (Pasal 1 ayat 1 KUHP) maupun dari asas subsidiaritas.

Dari uraian diatas menjadi semakin jelas, bahwa adalah salah untuk menyatakan kejahatan-kejahatan tradisional yang dilakukan dengan bantuan komputer sebagai kejahatan komputer (*computer crime*). Demikian juga, apabil secara fisik komputer menjadi objek perusakan. Apalagi bilamana kita menggunakan definisi kejahatan komputer sebagaimana dirumuskan oleh OECD *(any illegal, unethical or unauthorized behaviour involving automatic data processing and/or transmitting of data*). Di pelbagai negara hal ini tetap diatasi dengan ketentuan tindak pidana tentang pencurian, penipuan, penggelapan dan pemalsuan serta tindak pidana lain yang terkait. Hanya saja mungkin dalam hal ini perlu diadakan beberapa modifikasi. Sebagai contoh dapat dikemukakan disini, apakah deposito kredit dapat disamakan dengan barang atau hanya merupakan sebuah klaim. Selanjutnya, dalam penipuan, cukuplah bahwa kecurangan yang dilakukan dengan alat komputer tersebut disamakan dengan syarat penipuan yang tradisional berupa bahwa orang tersebut dengan rangkaian kata-kata bohong. Demikian pula sepanjang menyangkut pemalsuan, apakah persyaratan sesuatu yang dapat dilihat dapat diperluas dengan sarana lain. Meskipun demikian, OECD telah berhasil menyusun daftar *computer related criminality* dan hal ini merupakan *common denominator* sebagai hasil perbandingan hukum dan kebijakan legislatif di pelbagai negara. Daftar tersebut mencakup hal-hal sebagai berikut:

a. The input, alteration, erasure and/or suppression of computer data and/or computer programmes made wilfully with the intens to commit an illegal transfer of funds or of another thing of value;
b. The input, alteration, erasure and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made wilfully with the intens to commit a forgery;
c. The input, alteration, erasure and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made wilfully with intens to hinder the fungtioning of a computer and/or telecommunication system;
d. The infringement of the exclusive right of the owner of a protected computer programme and put in on the market;
e. The access to or interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either (1) by infringement of security measure or (ii) for other dishonest or harmful intentions. (OECD, 1986: 64-65).

3.2. Kendala Hukum Positif dan Tindakan Legislatif

Sesuai dengan azas-azas pembatas dalam hukum pidana sehubungan dengan asas legalitas tersebut diatas terutama asas *lex certa*, tampaknya tidak mudah untuk menerapkan begitu saja pasal-pasal KUHP terhadap kejahatan komputer. Apakah *joycomputing* berupa penggunaan tanpa izin dan melampaui wewenang (*furtum usu*) suatu komputer dapat diatasi demikian saja dengan Pasal 362 KUHP (pencurian)? Apakah dalam hal ini dapat dikategorikan sebagai pencurian listrik, yang di Indonesia sudah dianggap barang?

Selanjutnya, apakah hacking pada sebuah komputer dengan perantaraan sebuah terminal dapat disamakan demikian saja dengan memasuki rumah tanpa izin (*huisvredebruk*) sebagaimana diatur oleh Pasal 167 KUHP yang mensyaratkan kehadiran seseorang?

Kemudian, apakah manipulasi data dengan cara mengubah menambah atau menghapus dapat

DOI 10.21063/JTIF.2018.V6.1.24-31

digolongkan pada delik klasik perusakan barang sebagaimana diatur dalam Pasal 406 KUHP? Dalam hal ini misalnya saja Canada melalui Criminal Law Amandement Act 1985 telah memperjelas perumusan mischief yang mencakup pula *"everyone who wilfully: (a) destroys or alters data; (b) renders data meaningless, useless or ifeffective; (c) obstrucs, interrups or interferes with the lawful use of data; or (d) obstrucs interrups or denies access to data to any person who is entitled to access thereto"*.

Demikian pula halnya dengan memperoleh keterangan (data) secara tidak syah dalam kaitannya dengan rahasia kenegaraan, rahasia perusahaan dan sebagainya, jelas tidak dapat dengan sendirinya diatasi pasal-pasal KUHP (Pasal 112 dan sebagainya, Pasal 322 dan 323 KUHP, Pasal 234 KUHP, dan sebagainya).

Selanjutnya, akan timbul pertanyaan pula, sampai seberapa jauh *software piracy* dapat dikategorikan sebagai pelanggaran hak cipta. Di Indonesia, dalam UU No. 7 Tahun 1987, ditegaskan bahwa program komputer atau computer programme dalam kaitannya dengan karya ilmu pengetahuan seni dan sastra, termasuk ciptaan yang dilindungi (Pasal 11).

Untuk mengatasi hal tersebut diatas, jelas diperlukan tindakan legislatif yang cermat dengan mengingat suatu hal yakni jangan sampai perundang-undangan menjadi terpana pada perkembangan teknologi sehingga membuat peraturan *overlegislate*, yang pada gilirannya justru akan membawa dampak negatif, baik dibidang hukum lainnya maupun dibidang sosial ekonomi.

Disamping masalah-masalah yang timbul dalam hukum pidana substantif tersebut diatas, tampaknya masalah lain akan muncul yakni dalam hukum acara pidana, baik yang bersifat nasional maupun yang bersifat antar negara. Yang bersifat nasional antara lain adalah persoalan sampai seberapa jauh *computer records* dapat dijadikan alat bukti di sidang pengadilan.

Selanjutnya, masalah internasional akan muncul sehubungan dengan kemungkinan dilakukan kejahatan komputer melalui *remote data processing* yang dilakukan disuatu negara, tetapi akibatnya terjadi di negara lain. Dalam hal ini akan muncul persoalan yang berkaitan dengan azas territorialitas dan ekstradisi untuk menghindarkan, misalnya saja double jeopardy. Jelas, dalam hal ini diperlukan kerjasama internasional melalui harmonisasi hukum, baik hukum pidana substantif maupun hukum acara pidana.

Kompleksitas masalah yang terjadi digambarkan oleh OECD sebagai berikut:

With respect to the transnational aspects of computer related criminal activity, important issues have beeb noted which point to the desirability for international co-operation in repressing and controlling such activity: however, no attempt has been made in this study to resolve such issues. These issue deserve furter consideration by Member countries and appropriate international bodies. Issues that have been identified include, inter alia, problems resulting from different yuridiction among Member countries in connection with a specific case, as well as the appicability and adequecy of international legal instruments such as treaties on extradition and mutual legal assistence in criminal matters.

3.3. Pandangan Yang Berkembang

Kriminalisasi terhadap kejahatan komputer merupakan kebutuhan mengingat dampak yang luas dari kejahatan tersebut baik terhadap fungsi, fungsi infrastruktur publik, bahaya umum terhadap barang dan jasa maupun terhadap ketenteraman hidup sesama.

Mardjono Reksodiputro menyarankan agar pengaturan hukum pidana terhadap kejahatan komputer memperhatikan hal-hal sebagai berikut:

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 sistematika 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 untuk 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 syah komputer; dapat dipergunakan sebagai dasar kerja dengan memperhatikan pula pembagian (pendekatan) yang dilakukan Komisi Kejahatan Komputer di Belanda dalam laporannya tahun 1987;

DOI 10.21063/JTIF.2018.V6.1.24-31

5. Perhatian 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, sehingga 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. (Reksodiputro, 198: 12-13).

4. PENUTUP

4.1. Kesimpulan

Sehubungan dengan usaha pembaharuan KUHP nasional, pada lokakarya bab-bab kodefikasi hukum pidana di Jakarta pada tanggal 18-19 Januari 1988 telah dihasilkan kesimpulan-kesimpulan sebagai berikut:

1. Bahwa dipandang perlu untuk memasukkan materi kejahatan dengan mempergunakan piranti/sarana komputer dalam Konsep Rancangan Undang-undang termaksud diatas, dengan usulan sebagai berikut:
   a. Mengadakan penambahan, perubahan dan penyisipan mengenai kejahatan-kejahatan dengan mempergunakan piranti sarana komputer ke dalam pasal-pasal yang telah ada atau bilamana perlu diadakan pengaturan dalam bab tersendiri.
   b. Perumusan agar dilakukan secara cermat dan hati-hati guna menghindarkan terjadinya kriminalisasi dan proteksi yanng berkelebihan serta harus dapat mengakomodasikan hasil perkembangan teknologi sehingga tidak menghambat perkembangan ekonomi dan teknologi.
   c. Mengadakan kategorisasi dan definisi agar terdapat keseragaman yang dimasukkan ke dalam Ketentuan Umum Konsep Rancangan Undang-undang termaksud, dengan mempelajari/memperbandingkan kasus-kasus yang terjadi dan peraturan perundang-undangan yang berlaku di negara-negara ASEAN.
   d. Dibentuk panitia Ad-Hoc yang bertugas untuk mempelajari masalah-masalah yang berhubungan dengan penyalahgunaan komputer (Computer abuse/computer fraud), yang anggotanya antara lain terdiri dari unsur-unsur:
      - Kementerian Kehakiman
      - Mahkamah Agung
      - Kejaksaan Agung
      - Kementerian-kementerian Perhubungan & Telekomunikasi
      - HANKAM
      - POLRI
      - Kantor Konsultan Hukum dan IKADIN
      - Asosiasi Pengusaha Komputer
      - Perguruan Tinggi.
   e. Mempergunakan sejauh mungkin cara pendekatan yang dilakukan oleh Komisi Kejahatan Komputer Belanda (Komisi Franken) dalam laporannya bulan April 1987 yang disesuaikan dengan kondisi di negara kita.
2. Untuk menampung kebutuhan dalam menanggulangi kejahatan yang menggunakan piranti sarana komputer, bilamana menyangkut kepentingan negara, agar tidak ditutup kemungkinan diterapkannya Undang-undang Pemberantasan Tindak Pidana Korupsi (Undang-undang No. 3 Tahun 1971), Undang-undang tentang Tindak Pidana Subversi (Undang-undang No. 11/PNPS/1963) dan Undang-undang tentang Tindak Pidana Ekonomi (Undang-undang No. 7/Drt/1955 Jo. Undang-undang No. 8/Drt/1958).
3. Jika dalam perkembangannya dikemudian hari memang diperlukan, tidak ditutup kemungkinan disusun suatu Undang-undang tentang Kejahatan Komputer secara tersendiri.

4.2. Saran-saran

Mengingat victimisasi yang sangat luas dari *computer abuse* baik terhadap kepentingan negara, kepentingan umum maupun kepentingan perseorangan, kriminalisasi terhadap perbuatan tersebut harus dilakukan. Langkah legislatif yang dapat dilakukan adalah dengan menggunakan pendekatan evolusioner dan pendekatan kompromis. Pendekatan global sebaiknya dihindarkan agar tidak merusak sistematik hukum pidana.

Bahan-bahan penyusunan kriminalisasi dapat berasal dari perkembangan di negara-negara lain dan pandangan-pandangan yang tumbuh di Indonesia. *Over criminalization* harus dihindarkan

DOI 10.21063/JTIF.2018.V6.1.24-31

agar tidak menghambat perkembangan teknologi informatika.

DAFTAR PUSTAKA

Gillis, M. Arthur. 1984. *Microcomputers in Financial Institutions*. Illionis. DOW Jones-Irwin, Homewood.

Muladi. 1988. *Penanggulangan Kejahatan Komputer dengan Hukum Pidana*. Makalah.

OECD. 1986. *Information Computer Communication Policy*. Paris.

Pirogoff, D.K. *Combating Computer Crime with Criminal Law*. Jakarta. Djambatan.

Parker, Donn B. 1988. *Crime by Computer*. New York. Charles Scribner's Sons.

Reksodiputro, Margono. 1988. *Kejahatan Komputer (Suatu Catatan Sementara dalam rangka KUHP Nasional yang akan datang)*. Makalah dalam Lokakarya Bab-bab kodifikasi Hukum Pidana. Jakarta. BPHN.

Report of the Committe on Computer Crime, Information Technology and Criminal Law. 1987. Staatssuitgeverij. Ministerie van Justitie.

Sieber, U. 1986. *New Legislative Responses to Computer Related Economic Crimes and Infringements of Piracy Comparative and International Solutions*. Universiteit Amsterdam. Symposium.

Stair, JR, Ralp M. 1986. *Computers in Today's World*. Illionis. Irwin, Homewood.

DOI 10.21063/JTIF.2018.V6.1.24-31