POLISI DAN KOMPUTER

Oleh Oentoeng Soerapati *)

Dalam Pra-seminar Kejahatan Perkotaan yang diselenggarakan di Jakarta tgl. 26-27 Oktober 1992, Kapolri Jenderal (Pol) Drs. Kunarto antara lain menyebutkan bahwa kejahatan di perkotaan bisa mendorong empat jenis kejahatan, yaitu ; (1) penyalahgunaan obat terlarang, (2) kejahatan yang bersifat eksploitatif, (3) kejahatan yang bersifat kompetitif termasuk kejahatan dengan kekerasan, dan (4) kejahatan tanpa korban. Di samping itu disinggung pula bahwa kejahatan di perkotaan akan diwarnai oleh perkembangan teknologi dan kemajuan ekonomi. Disebutkannya beberapa contoh kejahatan tersebut, yakni : kejahatan komputer, penipuan dengan *credit card*, uang palsu, pemalsuan merk, korupsi, *corporate crime*, *white collar crime* dan sebagainya. Oleh sebab itu menurut Kapolri dalam rangka menjalankan kebijakan kriminal yang integratif, fungsi-fungsi detektif, preemptif, preventif dan represif dari Polri juga disiapkan untuk menanggulangi kejahatan-kejahatan tersebut.

Kemudian dalam Seminar Nasional Kepolisian Indonesia ke I di Semarang tgl. 10 Juli 1995 Kapolri Jenderal (Pol) Drs. Banurusman Admosemitro menekankan perlunya pemanfaatan partisipasi masyarakat oleh Polri sehubungan dengan perubahan sosial yang terjadi dewasa ini. Dengan cara demikian diharapkan Polri dapat menghasilkan enam keluaran (output) berupa : (1) terkendalinya jumlah kejahatan (crime total) dan kecelakaan lalulintas, (2) meningkatnya penyelesaian kejahatan (crime clearance), (3) Terciptanya ketertiban dan kelancaran Lalu-lintas, (4) meningkatnya partisipasi masyarakat, (5) semakin mantapnya kamtibmas dan (6) semakin tertibnya kondisi (Polri). Dalam seminar itu Kapolri juga sempat mengingatkan perlunya langkah antisipatif Polri dalam menyongsong abad ke 21 terhadap kejahatan berdimensi baru (new dimension crime), kejahatan konvensional dengan teknik baru dan kejahatan dengan sosok baru (new types of crime). Termasuk dalam kejahatan yang sebelumnya tidak dikenal antara lain adalah : kejahatan imigrasi, komputer, merk, paten dan hak cipta serta penyadapan telekomunikasi.

Namun pembahasan yang lebih mendalam mengenai antisipasi terhadap kejahatan komputer tampaknya belum dilakukan. Padahal di-

*) Penulis adalah mantan polisi kini Dosen Fakultas Hukum & Ekonomi UKSW di Salatiga, Lulusan Suscados Kewiraan Lemhannas, 1986.

ramalkan oleh futurolog semacam John Naisbitt dan Alvin Tofler, pada abad ke 21 arus informasi sibernetik (lihat kibernetika : ilmu pengetahuan tentang komunikasi dan pengawasan yang khususnya berkenaan dengan studi bandingan atas sistem pengawasan otomatis. Red) akan kian melimpah sejalan dengan semakin canggihnya komunikasi dan pesatnya perkembangan teknologi komputer. Penggunaan komputer yang semakin meluas, komunikasi yang semakin terbuka, terobosan teknologi yang revolusioner akan menciptakan situasi kriminogenik yang mengancam keamanan informasi yang tersimpan rapat dalam memori komputer. Dengan media elektronik yang semakin canggih seperti itu kiranya sangat diperlukan pemikiran futuristik tentang sosok polisi Indonesia sebagai penegak hukum yang harus malang melintang dalam belantara informasi sibernetik (cybercop). Tulisan ini mencoba menyoroti beberapa aspek yang perlu dipahami oleh anggota Polri dalam menghadapi para penjahat komputer (cybercriminals).

Komputerisasi Informasi

Harian KOMPAS tgl. 18 Maret 1995 memberitakan bahwa dalam rangka HUT ke-50 Kemerdekaan RI, Kapolri menyatakan ingin melihat wajah Polri berubah pada HUT ke 50 RI. Perubahan yang dimaksud adalah Polri yang administrasi operasionalnya terkomputerisasi. Rintisannya sudah dilakukan oleh Poltabes Semarang dan Polwiltabes Bandung, antara lain berkat kegigihan Kolonel (Pol) Drs. Didi Widayadi, M.B.A. beserta tim penciptanya. Dengan pemanfaatan teknologi komputer maka polisi-polisi modern diharapkan dapat melipatgandakan produktivitasnya. Keterbatasan kuantitas sumber daya dianggap tidak harus menghambat efektivitas dan efisiensi jika ditopang oleh teknologi. Hasrat Kapolri untuk melihat wajah Polri yang modern mudah-mudahan terkabul meskipun harus disadari bahwa teknologi adalah ibarat pedang bermata dua. Teknologi komputer dapat menguntungkan jika "dikuasai" Polri tetapi sekaligus dapat merugikan jika malah "menguasai" Polri.

Komputerisasi yang diperkenalkan dalam administrasi Kepolisian Indonesia menggunakan suatu sistem yang dinamakan SPOT (Sistem Pendukung Operasional Terpadu). Sistem ini mula-mula diujicobakan di Poltabes Semarang dan kemudian ditularkan di Polwiltabes Bandung. Dengan sistem ini dapat dilakukan pemantauan *(monitoring)* data dan informasi mengenai perkara, personil, senjata api, satuan Intelpam, Satuan Binmas, satuan Lalu Lintas dan lain sebagainya. Untuk itu dibutuhkan sejumlah tenaga operator komputer untuk meng*input* serta meng*update* data dan informasi dari waktu ke waktu. Dengan sistem itu

diharapkan pimpinan kesatuan Polri dapat melakukan penyimpulan *(assessment)* atau penilaian *(evaluation)* yang cermat untuk pengambilan keputusan *(decision making)* yang lebih tepat. Dengan komputerisasi ini diharapkan juga secara lebih efektif dan efisien dapat dihasilkan enam macam keluaran yang telah disebutkan di atas.

Untuk menerapkan sistem pendukung ini tentunya telah dilakukan analisis yang mencakup aspek-aspek SWOT. Mengenai kekuatan SPOT dikatakan terletak pada keselarasan dengan tujuan peningkatan kinerja Polri. Adapun kelemahan dari SPOT ini adalah mahalnya harga perangkat keras *(hardware)*, masih sederhananya program *(software)* berikut perlindungan sistemnya dan masih sedikitnya tenaga operator dan programmer *(brainware)*. Meskipun demikian peluang bagi penggunaan SPOT cukup luas karena dapat dihubungkan secara *on-line* dengan Perum Pos dan Giro, Pemda, hotel dan lain-lainya. Dari aspek tantangan, kesatuan Polri akan sulit mempekerjakan tenaga sipil yang benar-benar ahli menangani komputer karena gajih yang relatif lebih rendah daripada kalau bekerja di perusahaan-perusahaan. Mendidik personil polisi sendiri menjadi spesialis komputer sangat tergantung pada kemampuan, bakat dan minatnya. Sementara itu menggunakan jasa pakar komputer non-organik akan mengundang risiko karena informasi kepolisian bersifat konfidensial atau rahasia. Tampaknya aplikasi komputer perlu dimasukkan dalam kurikulum pendidikan Polri, bukan hanya pada tingkat akademi atau perguruan tinggi tetapi juga pada tingkat Tamtama dan Bintara.

Polisi Inggris sudah lama mengembangkan sitem komputer yang pas untuk kebutuhan konstabuler sehingga fungsi detektif menjadi lebih efisien, analisis sidik jari dan krimialitas pun semakin mudah. Dengan kemampuan merekam lebih dari 45.000 kejahatan setiap tahun, para detektif dapat menggunakan sistem tersebut untuk mencari tersangka potensial di wilayah geografis tertentu. Sistem komputer itu menghemat biaya, jam kerja dalam menyelusuri berkas-berkas dan memperbaharui catatan kejahatan dan dapat memberi informasi yang rinci tentang kriminalitas di satu daerah, jenis-jenis kejahatan bahkan kode pos tempat kejadian. Di samping itu, di Inggris komputer kini juga semakin diperlukan dalam merancang program simulasi tentang situasi krisis yang dihadapi polisi. Misalnya setelah terjadinya kebakaran hebat di West Yorkshire, polisi setempat dibantu oleh Universitas Leeds bekerja sama dengan perusahaan komputer ISIS untuk merancang suatu sistem yang mempercepat identifikasi korban. Dengan fasilitas CRISIS *(Casualty Recording, Information Sorting and Identification System)* tersebut polisi

kemudian dapat lebih cepat mengungkap identitas para korban sewaktu kapal ferry Zeebrugge tenggelam. Mungkin sudah saatnya juga pendidikan kepolisian di Indonesia menggunakan simulator untuk menghadapi situasi krisis tertentu di samping memantapkan sistem pengendalian huru-hara.

Dalam rangka komputerisasi tersebut kebutuhan akan jaringan informasi semakin dirasakan. Jerman misalnya pembuatan perjanjian bilateral dengan empat negara untuk pertukaran informasi secara terbatas tentang lalu-lintas mata uang dan senjata. Bersama-sama dengan Perancis dan negara-negara Benelux (Belgia, Nederland dan Lexembug), Jerman mengembangkan jaringan SIS *(Schengen Information System)* dalam rangka kooperasi dan koordinasi pelaksanaan tugas kepolisian. Untuk kepentingan imigrasi, jaringan SIS ini kini digunakan pula oleh Italia, Spanyol, Portugal dan negara-negara Inggris, Denmark dan Irlandia juga mempertimbangkan untuk ikut serta. Sebagai kelanjutannya, negara-negara di Eropa Barat kini merencanakan pembuatan EIS *(European Information System)* untuk kepentingan diseminasi dan analisis informasi perpolisian, imigrasi dan perpajakan. Sistem informasi semacam itu sangat penting artinya karena dari sekitar 154 negara anggota Interpol lebih dari 80% pekerjaannya bersangkut paut dengan Eropa. Dalam kejahatan narkotika misalnya jaringan kerja sama *European Drugs Intelligence Unit* cukup membantu pelaksanaan tugas kepolisian sedunia. Dalam jangka panjang, tidak mustahil SPOT yang dikembangkan Polri akan dapat dikaitkan dengan jaringan kerja sama rejional kepolisian ASEAN.

Kriminogenitas Komputer

Kejahatan komputer tampaknya mencakup pelanggaran atas kepentingan tak berwujud *(infringement of intangible interest)* pihak lain. Dalam hubungan ini perlu dibedakan antara penjahat yang menggunakan komputer sebagai alat untuk melakukan kejahatannya dan yang menggunakan komputer sebagai sasaran kejahatannya. Kejahatan komputer sebenarnya dapat dilakukan dengan *modus operandi* yang berbeda-beda. Oleh sebab itu kalaupun ada definisi tentang kejahatan komputer *(computer crime)* secara umum adalah segala macam kejahatan yang bersangkut-paut dengan komputer *(computer-related crime)*.

Pada kejahatan yang dilakukan dengan menggunakan alat komputer, penjahat harus menguasai program tertentu dan mengetahui kode pas komputer milik orang lain. Dengan menelusuri dan mempelajari isi program dalam suatu sistem komputer dapat dibuat mutasi atau transaksi palsu yang menguntungkan penjahat dan merugikan pe-

milik komputer. Teknik yang digunakan dalam hal ini disebut salami slicing, misalnya : seorang pegawai bank Inggris memindahkan sejumlah besar uang bank secara elektronik ke rekeningnya sendiri di suatu bank Swiss. Pencurian saldo uang recehan dari banyak nasabah bank dapat dilakukan secara teratur tetapi tidak kentara dengan komputer karena kebanyakan penyimpan uang di bank tidak memperhatikan jumlah uang kecil. Polri misalnya pernah membekuk suatu komplotan pembobol bank yang mencoba melakukan electronic transfer dari BNI 1946 di AS ke rekening pribadi di beberapa negara. Kejahatan tersebut dapat ditangkal dan diungkap berkat digunakannya sistem SWIFT dalam jaringan perbankan internasional. Pencurian rahasia perusahaan juga dapat dilakukan dengan komputer. Baru-baru ini General Electric telah kecolongan bahan riset dan kata sandinya lewat jaringan Internet.

Pada kejahatan dengan sasaran komputer digunakan teknik menumpukkan apocryph tertentu di atas program yang sudah ada sehingga informasi yang diberikan komputer menjadi berantakan dan tidak dapat dipercaya. Kejahatan ini biasanya dilakukan oleh *programmer* komputer dengan tidak melaksanakan apa yang diperintahkan oleh atasannya. Misalnya : pemrogram komputer pada dinas pajak sengaja mengacaukan informasi tentang kelebihan pembayaran pajak tanpa maksud yang jelas sehingga wajib pajak tidak mendapatkan pelayanan restitusi kelebihan pembayaran pajak. Contoh lain : penjualan kode panggilan telepon untuk hubungan interlokal dan menyambungkannya ke nomor telepon pribadi orang lain sehingga jumlah tagihan rekening telepon yang harus dibayar membengkak. Barangkali motivasi perbuatan ini adalah agar petugas pemeriksa bingung karena program komputer sudah dibuat begitu meyakinkan tetapi informasi yang dihasilkan ternyata tidak cocok. Tanpa pengetahuan yang memadai tentang teknik deteksi terhadap akurasi program komputer, khususnya yang digunakan dalam komputerisasi prosedur administrasi, tentu akan sulit mengungkap adanya ketidakberesan dalam pengolahan informasi.

H.W.K. Kaspersen dalam artikelnya berjudul *De computercrimineel in actie (Tijdschrift voor Kriminologie*, 2 jaargang 32, 1990) menggambarkan beberapa penjahat komputer tradisional sebagai berikut. Pengintip komputer *(computerhacker)* melakukan perbuatannya dengan melihat-lihat informasi yang ada di dalam memori komputer orang lain. Kalau penjahat ini berhasil menembus sistem perlindungan informasi yang biasanya bersifat rahasia disebutlah sebagai penyelundup komputer *(computercracker)*. Kejahatan pengintipan informasi

komputer biasanya diawali dengan hobi untuk menerobos sistem perlindungan komputer milik orang lain. Dengan bekal sebuah PC, suatu program komunikasi tertentu, sebuah pesawat telepon dan sebuah MODEM seorang pengintip sudah dapat menjelajahi program-program yang menyajikan informasi dari segala penjuru dunia. Dengan segala kreativitas, penguasaan teknis dan inventivitasnya seorang pengintip dalam waktu senggangnya dapat terus menerus mencari celah-celah *(loopholes)* dari program tertentu yang sengaja diproteksi sampai berhasil menembus dan mengetahui informasi yang dirahasiakan dengan ketat. Di AS, tidak kurang proyek NASA sempat kelabakan ketika diketahui ada pengintip yang berhasil mengakses ke informasi top secret yang dimilikinya. Baru-baru ini juga dikabarkan pabrik komputer IBM merasa lega karena pakar komputernya berhasil menyumbat akses masuk pengintip misterius ke dalam informasi perusahaannya. Kadang-kadang para pengintip ulung menyelenggarakan suatu Galatic Hacker Party (Amsterdam) atau membentuk suatu Computer Chaos Club (Hamburg) di mana mereka dapat saling memperbincangkan temuan-temuan hasil intipan dari sistem komputer yang prestisius di seluruh dunia. Pengintip komputer dapat saja menemukan kata sandi pembuka (password) dari SPOT yang digunakan Polri untuk mencari tahu data apa saja yang ada.

Sedangkan penyabot komputer *(computersaboteur)* melakukan kejahatannya dengan mengacaukan bekerjanya program komputer tertentu. Kejahatan yang dilakukan misalnya membuat program virus yang dapat mengacau atau menghapus program komputer lain. Penjahat ini dapat meningkatkan diri menjadi teroris komputer *(computerrorist)*. Kejahatan sabotase komputer dapat dilakukan oleh operator atau programer komputer yang dengan sengaja membuat komputer tidak berfungsi sebagaimana mestinya. Menggunakan disket yang terkena virus atau memasukkan virus ke dalam hard disk dapat memperokporandakan atau memusnahkan seluruh data yang semula tersimpan rapi di dalam memori komputer. Ibarat seekor kuda Troya yang membawa sejumlah besar pasukan di dalam tubuhnya, suatu virus komputer dapat berkembang biak dan beranakpinak dengan cepat didalam suatu sistem komputer dan menulari sistem komputer lain. Konon virus-virus semacam Palestina atau Jerusalem yang memusnahkan program setiap Jum'at ketiga belas disebarluaskan terutama dengan disket-disket yang memuat program bajakan. Dalam hal ini sekalipun disket telah diproteksi agar tidak tertular virus, sedikit kelengahan saja dapat membuat pemilik komputer panik karena tiba-

tiba menjumpai virus telah bermukim dalam file komputernya. Demikian pula, meskipun pembuat perangkat lunak dari waktu ke waktu menawarkan berbagai macam penawar virus namun setiap saat penyabot komputer juga menghadirkan virus ciptaan baru sehingga memusingkan kepala para pengguna komputer. Tidak mustahil bahwa pembuat program anti-virus adalah justru pencipta virusnya sendiri. Dalam hubungan ini Polri pernah menangani kasus seorang mahasiswa ITB yang mengakali program komputer dosennya karena merasa jengkel terhadap tindakan dosen tersebut. Namun Polri juga harus waspada jangan sampai SPOT yang dibangga-banggakan menjadi mandul karena disabot.

Adapun penipu komputer *(computerfrauder)* melakukan kejahatan dengan memanipulasi data komputer tertentu untuk keuntungan dirinya. Penjahat ini juga sering disebut pemalsu komputer *(computercounterfeiter)* karena memasukkan informasi palsu ke dalam komputer. Kejahatan pemalsuan komputer merupakan kejahatan yang relatif sederhana, misalnya: pemegang kas mengubah check masuk ke perusahaan menjadi pengembalian barang, lalu menguangkan check itu untuk digunakan sendiri. Kejahatan ini umumnya terjadi sebagai akses dari proses komputerisasi administratif. Pemalsuan dilakukan juga untuk mengibuli sistem mesin penghitung otomatik (automatic teller machine). Dengan menghapal PIN-code kartu yang asli dipijitlah tombol yang pas dengan strip magnetik pada kartu tersebut sehingga memberikan masukan palsu pada komputer di dalam mesin itu. Oleh sebab itu pemilik kartu harus hati-hati agar kodenya tidak diketahui oleh orang lain dan jangan sampai kartunya yang hilang digunakan oleh orang lain . Kejahatan ini dapat diawali dengan pengintipan informasi komputer atau dilakukan bersama-sama dengan sabotase komputer oleh operator komputer amatir yang meniti karir menjadi penjahat profesional. Dalam hal ini Polri telah beberapa kali berhasil mengungkap pemalsuan STNK, pemalsuan kartu telepon dan kartu kredit. Meskipun demikian, sekali lagi SPOT dapat menjadi sasaran empuk untuk pemalsuan data oleh orang-orang yang tidak bertanggungjawab untuk tujuan tertentu.

Penjahat yang disebut sebagai pembajak komputer (computer-pirate) melakukan penjiplakan program komputer yang dibutuhkan oleh banyak orang tanpa seijin pembuat program. Perangkat lunak yang dijiplak itu kemudian digandakan dan dijual lebih murah daripada harga yang ditetapkan pembuatnya. Kejahatan pembajakan perangkat lunak komputer sebenarnya dapat dilakukan oleh setiap orang yang tahu menggunakan komputer hingga

tidak perlu dilakukan oleh spesialis komputer. Hal ini karena dapat dilakukan penyalinan program dengan perintah standard DISKCOPY atau COPYDISK atau perintah lain yang relatif sederhana. Sebagaimana terhadap pengintip komputer, hukum perlu menentukan batas yang jelas kapan seseorang dapat dipidana karena melakukan pembajakan komputer. Pabrik-pabrik penghasil PC pada umumnya membolehkan pembeli komputer menyalin atau menggandakan perangkat lunak yang disertakan dalam penjualan sekedar untuk digunakan bagi keperluan operasional. Jika pengintip informasi dapat dianggap melanggar privacy dari seseorang, pembajakan perangkat lunak juga dapat dianggap melanggar intellectual property seseorang jika dilakukan untuk tujuan komersial. Mengenai hal ini Polri sudah berulangkali melakukan razia terhadap toko-toko peralatan komputer yang menjual perangkat lunak hasil bajakan. Di AS kini misalnya, FBI sedang mencaricari Kevin Mitnick sebagai pencuri perangkat lunak pabrik-pabrik telepon seluler, yang menimbulkan kerugian jutaan dolar dalam pengoperasian komputer dan membocorkan panggilan tugas agen-agen FBI.

Memolisi Penjahat Komputer

Ketika beberapa tahun yang silam Federal Law Enforcement Training Center (FLETC) di Brunswick (Georgia) AS memperkenalkan gagasan tentang polisi robot (Robocop) yang dikendalikan dengan sinar laser banyak pihak yang menganggap gagasan itu mengada-ada. Namun kini pusat pelatihan polisi federal AS itu justru sibuk melatih polisi khusus bidang komputer (cybercop). Kepolisian di negara itu memperkirakan bahwa suatu masa kelak setiap polisi mungkin harus memakai badge pengenal, membawa senjata dan menjinjing komputer laptop. Di samping itu polisi sibernetika mungkin perlu juga melengkapi diri dengan telepon seluler modern, buku teks tulisan sandi dan jaket tahan peluru. FLETC dewasa ini menyelenggarakan 14 program pelatihan yang dari waktu ke waktu dimutakhirkan, antara lain mengenai analisis alat bukti, penyelusuran penipuan dengan kartu kredit, teknik geledah dan tangkap yang legal jika ditemukan bukti kejahatan komputer. Setelah selesai menjalani latihan, para polisi siber netik harus siap menghadapi suasana tak ramah dalam angkasa sibernetik. Khususnya dalam kawasan Internet ada sikap bermusuhan terhadap penegak hukum dan ketakutan terhadap intrusi polisi atau penguasa. Di mata para maniak komputer, pelatihan FLETC itu digambarkan membekali polisi agar siap untuk membabat komputer sebagai mesin yang mengilhami perbuatan-perbuatan yang jahat.

Memang dalam kenyataannya

banyak sekali tantangan bagi FLETC yang juga perlu diwaspadai oleh Polri. Sebut saja *white collar crimes* yang semakin banyak dilakukan dengan menggunakan komputer. Dalam perdagangan obat bius dan pencucian hasil kejahatan *(moneylaundering)* transfer uang yang dilakukan lewat angkasa sibernetik dan menggunakan jaringan Internet untuk bertukar pesan. Komunikasi rahasia antar penjahat narkotika bahkan ada yang dilakukan dengan menyelundup ke voicemail system milik perusahaan lain melalui jaringan telepon selulernya. Di samping itu karena komputer merupakan pusat syaraf transaksi finansial dan sistem komunikasi dunia, mungkin saja digunakan untuk tujuan terorisme. Bayangkan kalau sampai ada penyelundup yang masuk ke sistem transfer dana elektronik dari Bank Sentral AS dan mengacaukannya. Kemacetan total sistem telepon Key New York pada tahun 1992 diduga keras oleh FLETC gara-gara ulah teroris komputer. Polisi Kentucky (AS) pernah membongkar komplotan penyalur terbitan pronografi anak-anak di Inggris berkat informasi dari seseorang di Swiss. Dengan merunut 60 halaman nama-nama file dan 400 tayangan melalui jaringan Internet di Birmingham selama kurang lebih tiga bulan dan meminta bantuan Interpol, Scotland Yard dan polisi setempat akhirnya berhasil menangkap para pengedarnya.

Sehubungan dengan itu Vic Sussman dalam tulisannya tentang Policing Cyberspace (U.S. News & Wolrd Report, January 23, 1995) mempertanyakan, sementara eskalasi perang teknologi antara polisi dan penjahat komputer semakin menjadi-jadi, apa yang bakal terjadi terhadap tradisi orang AS yang menjunjung tinggi privacy dan property ? Kini orang menjadi resah karena masalah-masalah pribadi yang disimpannya dalam komputer dapat diketahui atau diungkap orang lain. Misalnya yang menyangkut : peluang mendapatkan pekerjaan, besarnya tanggungan hutang, riwayat perolehan kredit, kode wilayah pos, nomor kartu jaminan sosial atau kondisi kesehatan dirinya. Hal-hal tersebut dapat saja dijual-belikan atau dimanfaatkan untuk tujuan terentu hanya gara-gara penyalahgunaan komputer. Kalau seseorang banyak memesan makanan berlemak atau membeli sejumlah besar obat-obatan, perusahaan asuransi jiwa yang mendapatkan informasi mungkin enggan menjadi penanggungnya. Apalagi kalau ada catatan bahwa ia adalah perokok berat, pemabok kronis dan pemakan daging mentah yang rekaman mediknya buruk ! Apakah pihak lain tidak berhak mengetahui dan memperoleh informasi yang sesungguhnya tentang seseorang ?

Pengaruh globalisasi dewasa ini memang melanda dunia informasi dengan hebatnya, terlebih setelah

diciptakannya jaringan komputer internasional semacam Internet. Dalam hal ini penggunaan E-mail untuk dapat mengirim pesan khusus diperlukan penulisan rahasia dengan sandi *(encryption)* agar tidak dipahami orang lain. Oleh sebab itu polisi jelas harus menguasi teknologi tulisan sandi *(ceyptography)* yang mutakhir untuk dapat berkomunikasi secara rahasia lewat jaringan Internet meskipun hal itu akan memancing munculnya penjahat sandi komputer *(cryptocriminal)* untuk dapat mengetahui pesan rahasia polisi. Sebaliknya dengan menguasai teknologi tersebut polisi harus pula mampu mengungkap pesan sangat rahasia yang biasanya digunakan dalam komunikasi antar penjahat, meskipun pesan itu tentu biasanya dibuat dalam tulisan sandi yang cukup mutakhir. Di AS kini misalnya telah diundangkan *Digital Telephone Act* yang meskipun ketentuan hukumnya cukup menghormati privacy konsumen telepon tetapi sistem komunikasi yang digunakan oleh perusahaan telepon harus tetap memungkinkan penyadapan telepon *(wiretapping)* oleh polisi. Dengan demikian pabrik telepon boleh menggunakan teknik ekripsi rahasia yang paling mutakhir tetapi harus masih dapat diterobos oleh polisi untuk kepentingan penyidikan.

Penggunaan Internet memang berpengaruh besar bagi kebebasan berbicara sehingga dapat membuat risih atau menjengkelkan pihak tertentu yang menjadi sasaran. Jika datang keluhan kepada polisi, tidak mudah untuk menelusuri siapa pelaku penghinaan atau fitnah lewat jaringan tersebut karena biasanya pengirim pesan adalah anonim. Masalah-masalah rahasia yang menyangkut pribadi seseorang menjadi rawan untuk dibeberkan lewat komputer tanpa perlindungan atau penegakan hukum yang kongkrit. Kebebasan berbicara bagi setiap orang yang semula diagung-agungkan oleh masyarakat negara maju, kini dipertanyakan apakah tidak perlu dibatasi agar tidak melanggar privacy orang lain. Di samping itu perlindungan hak milik intelektual terhadap karya cipta yang diperjuangkan oleh negara- negara maju kini dipertanyakan apakah masih ada manfaatnya. Suatu karya cipta yang ditanyakan lewat jaringan komputer bukan oleh penciptanya sendiri menjadi sulit untuk dilindungi. Melalui Internet, oleh setiap pemakai komputer karya cipta dapat dicopy suatu artikel hasil jiplakan dalam jumlah tak terbatas tanpa seijin penulis artikel aselinya. Termasuk informasi yang dengan mudah disebarluaskan lewat Internet adalah program-program komputer yang berhasil diketahui oleh seseorang agar dapat ditiru oleh orang lain yang berkepentingan sehingga merugikan penciptanya.

Pertanyaan pucuk pimpinan Polri untuk menyiapkan keempat

fungsi kepolisian dalam menghadapi perubahan sosial tentu harus mempertimbangkan kekhasan dan kerumitan kejahatan komputer sendiri. Tampaknya Polri juga perlu lebih cermat menganalisis kekuatan *(strength)*, kelemahan *(weakness)*, peluang *(opportunity)* dan ancaman (threat) yang ada sehubungan dengan komputerisasi informasi kepolisian. Untuk mewaspadai kejahatan komputer atupun memanfaatkan teknologi komputer, pengetahuan dan teknik perpolisian yang konvensional perlu dilengkapi dengan penguasaan teknologi sebernetik dan kriptografik modern. Akan tetapi jika peraturan hukum positif yang masih berlaku tidak cukup mengatur masalah-masalah yang timbul maka polisi juga tidak akan sanggup menanggulangi kejahatan dan penjahat komputer.

LINTASAN PERISTIWA

Defile Polwan kita dalam Upacara Hari Ulang Tahun ke-50 ABRI pada tanggal 5 Oktober 1995, di lapangan Udara Halim Perdana Kusuma.

Bertambah lagi kekuatan Polisi Udara kita dengan diresmikannya pengoperasian pesawat Cassa NC 212-200 oleh Direktur Samapta Polri di lapangan Udara Pondok Cabe pada tanggal 13 Oktober 1995 yang baru lalu.