MEMBURU KEJAHATAN DI DUNIA MAYA

Tak bisa dipungkiri, cybercrime adalah salah satu tantangan terbesar Polri di era globalisasi. Tapi mengapa payung hukum yang dibutuhkan begitu lambat terkembang?

ANDA mungkin masih ingat ulah Steven Haryanto yang pernah menggegerkan dunia perbankan melalui Internet (*e-banking*) di Indonesia, beberapa tahun lalu? Ya, dialah *hacker* sekaligus jurnalis pada majalah *Master Web* yang dengan sengaja membuat situs 'asli tapi palsu' layanan *Internet banking* Bank Central Asia (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain www.klik-bca.com, www.kilkbca.com, www.clikbca.com, www.klickca.com dan www.klikbac.com. Isi situs-situs 'plesetan' inipun nyaris sama, kecuali tidak adanya *security* untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Jika nasabah BCA salah mengetik situs BCA asli, ia akan masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas personal (PIN) dapat diketahuinya. Diperkirakan, 130 nasabah BCA tercuri datanya. Menurut pengakuan Steven pada situs bagi para *webmaster* di Indonesia, www.webmaster.or.id, tujuan membuat situs plesetan adalah agar publik menjadi lebih berhati–hati dan tidak ceroboh saat melakukan pengetikan alamat situs (*typo site*), bukan untuk mengeruk keuntungan.

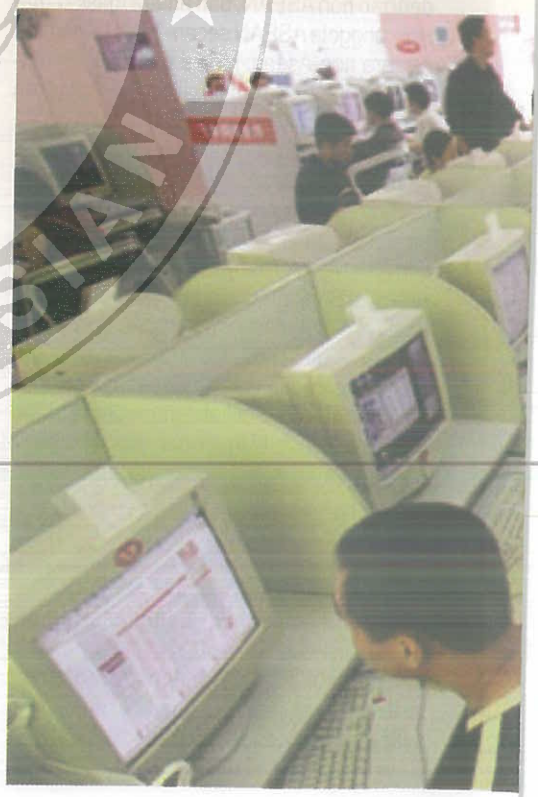
Terlepas baik atau tidak maksud Steven Haryanto, yang jelas kasus itu memperlihatkan betapa kejahatan melalui dunia maya saat ini makin sulit dibendung. Seorang *hacker* seperti Steven Haryanto dapat masuk ke dalam suatu sistem jaringan perbankan untuk mencuri informasi nasabah yang terdapat di dalam server mengenai *data base* rekening bank tersebut, karena dengan adanya *e-banking* jaringan tersebut dapat dikatakan terbuka serta dapat diakses oleh siapa saja. Kalaupun pencurian data yang dilakukan sering tidak dapat dibuktikan secara kasat mata karena tidak ada data yang hilang tetapi dapat diketahui telah diakses secara *illegal* dari sistem yang dijalankan.

Apalagi penggunaan internet belakangan ini bisa dibilang merupakan bagian tak terpisahkan dalam kehidupan hiperaktif masyarakat modern, terutama di perkotaan. Di Indonesia saja, saat ini tercatat pertumbuhan pengguna internet telah mencapai angka lebih dari 20 juta orang. Bisa ditebak, pertumbuhan dan perkembangan para *hecker* di negeri ini mestinya juga seiring dengan pertumbuhan dunia maya itu sendiri.

Menurut hasil pemantauan Asia Pasific Network Information Center (APNIC) pada 2003 dan perusahaan *Security Clear Commerce* di Texas, Amerika Serikat, saat ini Indonesia menduduki peringkat ke 2 setelah Ukraina dalam hal kejahatan *carding* dengan memanfaatkan teknologi informasi (Internet), yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*. Data ini diambil dari persentase jumlah penipuan dalam transaksi. Komunikasi awalnya dibangun melalui *e-mail* untuk menanyakan kondisi barang dan melakukan transaksi. Setelah terjadi kesepakatan, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya. Cara ini relatif aman bagi pelaku karena penjual biasanya membutuhkan 3 – 5 hari untuk melakukan kliring atau pencairan dana sehingga pada saat penjual mengetahui bahwa nomor kartu kredit tersebut bukan milik pelaku barang sudah terlanjur terkirim.

Tapi kejahatan *carding* cuma salah satu contoh yang menonjol. Di luar itu, masih banyak lagi kejahatan yang memanfaatkan Internet. "Ambil contoh *cyber fraud, web deface, software piracy, phising*, penyebaran virus, *cyber prostitution, cyber gambling, cyber terorism*, kejahatan penghinaan, fitnah dan bahkan hingga e-mail yang tidak menyenangkan orang," ungkap Kanit Informasi Teknologi (IT) dan Cyber Crime Bareskrim Mabes Polri, Kombes Petrus R Golose.

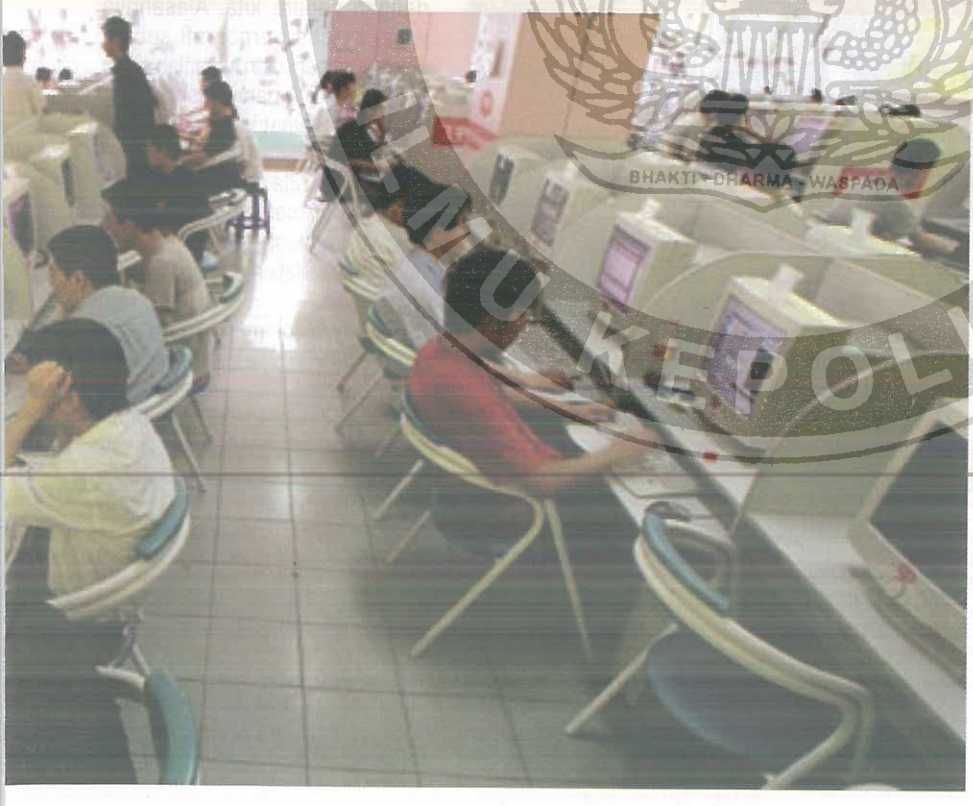
Contoh lain yang juga menonjol adalah ulah seorang *hacker* bernama Dani Hermansyah, ketika pada tanggal 17 April 2004 ia melakukan *deface* dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam website www.kpu.go.id, yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap Pemilu yang sedang berlangsung pada saat itu. Dikhawatirkan, selain nama-nama partai yang diubah, bukan tidak mungkin angka-angka jumlah pemilih yang masuk di sana menjadi tidak aman dan dapat diubah. Untungnya, apa yang dilakukan Dani tersebut tidak dilakukan dengan motif politik, melainkan hanya sekedar menguji suatu sistem keamanan yang biasa dilakukan oleh kalangan *underground* (istilah bagi dunia *hacker*). Terbukti setelah melakukan hal tersebut, Dani memberitahukan apa yang telah dilakukannya kepada *hacker* lain melalui *chat room* IRC khusus *hacker* sehingga akhirnya



tertangkap oleh penyidik dari Polda Metro Jaya yang telah melakukan *monitoring* di *chat room* tersebut.

Faktanya, kejahatan *cyber* kian marak di Indonesia. Lalu apa yang dilakukan pihak kepolisian (Polri) untuk menanggulangi kejahatan transnasional lewat dunia maya ini? Tentu, aparat keamanan tak tinggal diam terhadap tantangan baru yang dipicu arus globalisasi ini. Sesuai tuntutan zaman, pihak kepolisian pun tanggap dengan membentuk unit khusus menanganinya, yaitu UNIT V IT/CYBERCRIME Direktorat II Ekonomi Khusus Bareskrim Polri. Cuma, Petrus sendiri mengakui pengungkapan kejahatan ini masih sangat kecil, dikarenakan banyak kendala dan hambatan yang dihadapi dalam upaya pengungkapannya. "Kejahatan IT/*Cybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara, sehingga butuh penanganan dan pengaturan khusus di luar KUHP," ujarnya.

Artinya, lanjut Petrus, perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya. Kepolisian merupakan lembaga aparat penegak hukum yang memegang peranan penting di dalam penegakan hukum, sebab tanpa adanya hukum yang mengatur dan lembaga yang menegakkan maka dapat menimbulkan kekacauan di dalam perkembangannya.



BELUM ADA UU KHUSUS

Persoalannya, masih kata Petrus, saat ini Indonesia belum memiliki Undang-Undang khusus/ *cyber law* yang mengatur mengenai *cybercrime* walaupun rancangan undang undang tersebut sudah ada sejak tahun 2000. Sebetulnya revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2004 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR, namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki.

Hal yang sama diungkapkan **Azamul Fadhly Noor S.H., M.Hum., DFM dari Direktorat Hukum dan Regulasi PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan. Menurutnya,** sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.

Ia mencontohkan, kejahatan komputer melalui media internet yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait lainnya dapat diancam dengan Ketentuan Pidana yang terdapat dalam Undang-Undang Hak Cipta dan hak-hak terkait lainnya. Demikian pula kejahatan *Drug Traffickers* dapat diancam pidana sesuai dengan ketentuan yang terdapat di dalam Undang-Undang Nomor 5 Tahun 1999 tentang Psikotropika dan Undang-Undang Nomor 22 Tahun 1999 tentang Narkotika. Namun beberapa kekosongan hukum masih terlihat di dalam kasus-kasus yang berkaitan dengan kejahatan data *interferences*, *system interferences*, *illegal interception*, *data theft* dan *misuse device*, yang perlu segera mendapat perhatian dari pembentuk undang-undang.

"Hambatan-hambatan yang ditemukan dalam upaya melakukan penyidikan terhadap *cybercrime* antara lain berkaitan dengan masalah perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Maka-nya, upaya-upaya yang dapat dilakukan untuk mengatasi hambatan yang ditemukan di dalam melakukan penyidikan terhadap *cybercrime* antara lain berupa penyempurnaan perangkat hukum, mendidik para penyidik, membangun fasilitas *forensic computing*, meningkatkan upaya penyidikan dan kerjasama internasional, serta upaya penanggulangan dan pencegahan," papar **Azamul Fadhly Noor** yang pernah **9 tahun bertugas di Kejaksaan dan telah menangani berbagai perkara seperti tindak pidana perbankan, korupsi, *money laundering*, dan cybercrime.**

Penerapan pasal-pasal yang dikenakan dalam kasus *cybercrime* merupakan suatu permasalahan besar yang sangat merisaukan. **Azamul Fadhly** mencontohkan, misalnya ada *hacker* yang melakukan pencurian data apakah dapat ia dikenakan Pasal 362 KUHP? Pasal tersebut mengharuskan ada sebagian atau seluruhnya milik orang lain yang hilang, sedangkan data yang dicuri oleh *hacker* tersebut sama sekali tidak berubah. Hal tersebut baru diketahui biasanya setelah selang waktu yang cukup lama karena ada orang yang mengetahui rahasia perusahaan atau menggunakan data tersebut untuk kepentingan pribadi.

Dengan sederet hambatan yang dihadapi, wajar bisa Kepolisian RI mengharapkan adanya Undang-Undang (UU) yang khusus mengatur mengenai kejahatan di dunia maya (*cybercrime*), menyusul diundangkannya

Rancangan Informasi dan Transaksi Elektronik (RUU ITE) menjadi UU oleh DPR RI belum lama ini. "Setelah UU ITE ini, kami harap nantinya akan dibahas juga undang-undang tentang Tindak Pidana Teknologi Informasi (TPTI)," kata Kombes Polisi Petrus R. Golose, dalam jumpa pers di Jakarta belum lama ini.

Dengan disahkannya RUU ITE menjadi undang-undang, Petrus mengatakan, dapat menjadi payung hukum pertama bagi aparat hukum untuk menindak kejahatan transaksi elektronik di dunia maya. Ia menegaskan pihaknya juga tidak lagi merasa malu bila bertemu dengan organisasi kepolisian internasional seperti Interpol, karena telah memiliki payung hukum kejahatan terkait penyalahgunaan di dunia maya.

Sedangkan Kepala Bagian Penyusunan Program Pelaporan Pemantauan dan Penilaian (Sunprolabnil) Jampidum Kejaksaan Agung, Arif Mulyawan mengatakan disahkannya UU ITE ini merupakan prestasi luar biasa bagi penegakan hukum Indonesia karena dokumen elektronik sekarang bisa menjadi bukti hukum. Arif mengatakan, selama ini memang pihaknya mengalami kendala payung hukum apabila menangani kejahatan yang terkait pemanfaatan teknologi informasi.

Sementara itu Dosen Hukum Telematika Universitas Indonesia Edmon Makarim mengatakan UU ITE ini merangkum dan mendasarkan dari tiga payung hukum mengenai transaksi elektronik internasional yaitu "Uncitral Model Law for e-commerce", "Uncitral Model Law for e-signature" dan "UN Convention on Cybercrime".

Sedangkan Pengamat Telematika Roy Suryo mengatakan meski belum sempurna dan aplikatif, disahkannya UU ITE ini perlu disambut gembira oleh semua pihak. "UU ITE ini akan disempurnakan oleh peraturan pemerintah dibawahnya," kata Roy.

Dalam kesempatan tersebut, Menkominfo Muhammad Nuh mengatakan sesuai pasal 11 Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang disahkan DPR, disebutkan bahwa tanda tangan elektronik mempunyai kekuatan hukum dan akibat hukum yang sah sama dengan tanda tangan konvensional yang menggunakan tinta basah dan meterai. "Undang-undang ini berlaku untuk tiap orang yang melakukan perbuatan hukum baik yang berada di wilayah Indonesia maupun di luar Indonesia, yang memiliki akibat hukum di Indonesia," terang Nuh.

Dengan disahkannya UU ITE oleh DPR, Nuh menjelaskan Indonesia sekarang sudah sejajar dengan negara-negara maju yang telah mempunyai undang-undang terkait pemanfaatan teknologi seperti Amerika Serikat, negara-negara Uni Eropa, Singapura, Malaysia dan India. "Setelah menanti sekitar lima tahun, akhirnya kita punya payung hukum berkait dengan berbagai hal tentang informasi dan transaksi elektronik. Ini maknanya sebagai bangsa kita telah sejajar dengan masyarakat dunia di dalam mengakomodasi kebutuhan masyarakat modern dalam melakukan transaksi elektronik," kata Nuh.

Dia melanjutkan UU ITE memberikan kepastian hukum tentang bentuk-bentuk transaksi elektronik yang dapat dijadikan alat bukti sah. "Selama ini bentuk-bentuk transaksi

elektronik yang hanya dibuktikan sebagai selembar kertas bukti transfer, misalnya, tidak bisa dijadikan alat bukti. Karena, memang belum ada payung hukumnya untuk itu," kata Nuh.

KEENGGANAN KORBAN

Di tempat terpisah, Kombes Petrus R Golose juga mengakui dalam kasus-kasus *cybercrime* yang modusnya seperti kasus *carding* metode, penyelidikan yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika, terutama dalam *undercover* dan *control delivery*. Petugas setelah menerima informasi atau laporan dari Interpol atau *merchant* yang dirugikan melakukan koordinasi dengan pihak *shipping* untuk melakukan pengiriman barang. Cuma yang jadi kendala dalam kasus seperti ini, lanjutnya, adalah laporan yang masuk terjadi setelah pembayaran barang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, di samping adanya kerjasama antara *carder* dengan karyawan *shipping*. Sehingga, apabila polisi melakukan koordinasi, informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu.

Bahkan untuk kasus *hacking* atau memasuki jaringan komputer orang lain secara ilegal dan melakukan modifikasi (*deface*), penyidikannya dihadapkan pada problematika yang lebih rumit lagi, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit. "Belum lagi kendala bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan SDM serta peralatan komputer forensik yang baik," ungkap Petrus.

Dalam hal kasus-kasus lain seperti situs porno maupun perjudian *cyber*, para pelaku melakukan *hosting* pendaftaran di luar negeri yang memiliki yuridiksi berbeda dengan negara kita. Alasannya jelas, karena pornografi secara umum dan perjudian bukanlah suatu kejahatan di Amerika dan Eropa, walaupun alamat yang digunakan berbahasa Indonesia dan operator *website* juga ada di Indonesia. "Kita tidak dapat melakukan tindakan apapun terhadap mereka, karena *website* tersebut bersifat universal dan dapat diakses di mana saja."

Azamul Fadhly Noor mensinyalir, banyak rumor beredar yang menginformasikan adanya penjebolan bank-bank swasta secara *online* oleh *hacker,* tetapi korban menutup-nutupi permasalahan tersebut. Namun, lanjutnya, ini bisa dimaklumi karena berkaitan dengan kredibilitas bank bersangkutan. "Umumnya mereka takut apabila kasus ini tersebar akan merusak kepercayaan masyarakat terhadap bank tersebut. Dalam hal ini penyidik tidak dapat bertindak lebih jauh, karena untuk mengetahui arah serangan harus memeriksa server dari bank yang bersangkutan. Bagaimana aparat bisa melakukan pemeriksaan jika kejadian tersebut disangkal sendiri oleh bank"," ujarnya.

Penindakan kasus *cybercrime* sering mengalami hambatan, terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka misalnya, sering kali tidak dapat ditentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan di mana saja tanpa ada yang mengetahuinya. Sehingga, tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan *IP Address* dari pelaku dan komputer yang digunakan. "Jadi makin sulit apabila pelaku menggunakan warnet, karena saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka. Kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana."

Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di *log server* sudah dihapus biasanya terjadi pada kasus *deface*, sehingga penyidik menemui kesulitan dalam mencari *log* statistik yang terdapat di dalam server. Sebab, biasanya secara otomatis *server* menghapus *log* yang ada untuk mengurangi beban *server*. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti, sedangkan data *log* statistik merupakan salah satu bukti vital dalam kasus *hacking* untuk menentukan arah datangnya serangan.

Pemeriksaan terhadap saksi dan korban, menurut Petrus, banyak mengalami hambatan. Ini karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat (*testimonium de auditu*). "Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada, hal ini terjadi untuk kasus-kasus *hacking*."

Ia kembali mencontohkan kasus *carding* yang saksi korbannya kebanyakan berada di luar negeri. Kondisi ini sangat menyulitkan aparat untuk meminta keterangan dalam berita acara pemeriksaan saksi korban. Apakah mungkin nantinya hasil BAP dari luar negeri yang dibuat oleh kepolisian setempat dapat dijadikan kelengkapan isi berkas perkara? Mungkin apabila tanda tangan digital (*digital signature*) sudah disahkan maka pemeriksaan dapat dilakukan dari jarak jauh dengan melalui *e-mail* atau *messanger*," papar Petrus.

Karena itu, baik Petrus maupun **Azamul Fadhly** sepakat bahwa peranan saksi ahli sangatlah besar sekali dalam memberikan keterangan pada kasus *cybercrime*. Sebab, apa yang terjadi di dunia maya membutuhkan ketrampilan dan keahlian yang spesifik. Saksi ahli dalam kasus *cybercrime* dapat melibatkan lebih dari satu orang, sesuai dengan permasalahan yang dihadapi. Misalnya dalam kasus *deface*, di samping saksi ahli yang menguasai desain grafis juga dibutuhkan saksi ahli yang memahami masalah jaringan serta saksi ahli yang menguasai program," tandas Petrus.

Yang jelas, menurut Petrus, Polri sendiri telah melakukan beberapa tindakan untuk meningkatkan penanganan kejahatan *cyber* yang semakin hari semakin berkembang seiring dengan kemajuan teknologi. Di antaranya, mengirimkan anggotanya untuk mengikuti berbagai macam kursus di negara–negara maju agar dapat diterapkan dan diaplikasikan di Indonesia, antara lain: CETS di Canada, Internet Investigator di Hongkong, Virtual Undercover di Washington, Computer Forensic di Jepang.

Upaya lainnya berupa semaksimal mungkin untuk meng-*up date* dan *up-grade* sarana dan prasarana yang dimiliki, antara lain Encase Versi 4, CETS, COFE, GSM Interceptor, GI 2. Lalu, melakukan kerjasama dalam penyidikan kasus kejahatan *cyber* karena sifatnya yang *borderless* dan tidak mengenal batas wilayah, sehingga kerjasama dan koordinasi dengan aparat penegak hukum negara lain merupakan hal yang sangat penting untuk dilakukan.

Selain itu Polri juga memberikan sosialisasi mengenai kejahatan *cyber* dan cara penanganannya kepada satuan di kewilayahan (Polda) serta pelatihan dan ceramah kepada aparat penegak hukum lain (jaksa dan hakim) mengenai *cybercrime* agar memiliki kesamaan persepsi dan pengertian yang sama dalam melakukan penanganan terhadap kejahatan *cyber* terutama dalam pembuktian dan alat bukti yang digunakan.

Nah, tinggal waktu yang akan membuktikan seberapa cepat Polri mampu mengejar dan mengantisipasi perkembangan teknologi di dunia maya yang makin canggih.

Pornografi, Bisnis Paling "Basah"

Labanya bisa US$ 3.000 per detik

BISNIS apa yang paling menguntungkan? Ini salah satunya: pornografi! Anda mungkin tak percaya. Tapi paling tidak, begitulah yang diungkapkan AWARI (Asosiasi Warung Internet Indonesia) belum lama ini. Menurut AWARI, sebanyak US$ 3.075,64 dibelanjakan untuk pornografi setiap detiknya di seluruh dunia. "Statistik industri pornografi pada 2006 menunjukkan, setiap detiknya sekitar US$ 3.075,64 dibelanjakan untuk pornografi," kata Ketua AWARI, Irwin Day.

Mengutip data sebuah situs *internet reviewer*, Irwin mengatakan, pendapatan industri pornografi global pada 2006 sebanyak US$ 97,06 miliar. Empat negara meraih pendapatan terbanyak dari bisnis pornografi di dunia maya ini, yaitu Cina (US$ 27,40 miliar), Korea Selatan (US$ 25,73 miliar), Jepang (US$ 19,98 miliar), dan Amerika Serikat (US$ 13,33 miliar). Data tersebut juga mengungkapkan, sebanyak 28.258 pengguna internet melihat konten pornografi dan sebanyak 372 pengguna internet mengetikkan kata kunci berkaitan dengan pornografi.

Bagaimana dengan Indonesia? Irwin sendiri mengaku dirinya belum mendapatkan data yang terkait dengan industri pornografi dunia maya di Indonesia. Namun mengutip data dari *Alexa*, ia menyebut 7 dari 100 top site Indonesia merupakan situs porno dan 15 dari 100 top site dapat ditumpangi konten porno. Untuk memblokir akses situs pornografi, lanjutnya, ada tiga teknik penyaringan yang dapat dilakukan yaitu penyaringan di personal computer (PC) alias komputer rumah, penyaringan di proxy/cache server, dan penyaringan dengan menggunakan DNS (Domain Name System). **[jt 02]**