PENGUATAN HUKUM *CYBER CRIME* DI INDONESIA DALAM PERSPEKTIF PERATURAN PERUNDANG-UNDANGAN

Oleh:

Muh. Alfian
Fakultas Hukum Universitas Muhammadiyah Purworejo
E-mail: vian.muh@gmail.com

Abstrak

Kemajuan teknologi telah mengubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perkembangan Internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif sekaligus negatif. Kejahatan dunia maya *(cyber crime)* ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Dilihat dari modus operandi dari *cyber crime* terbagi menjadi 2 (dua) bagian yaitu kasus *carding* dan kasus penipuan di *website.* Oleh karena semakin berkembangnya *cyber crime,* maka penegakan hukum *cyber crime* di Indonesia dan melalui sarana penal maupun non-penal.

Kata kunci: ***Cyber Crime,* Penegakan Hukum, Penal, Non-Penal**

A. PENDAHULUAN

Kemajuan teknologi telah mengubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet.[1] Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata *(real)* ke realitas baru yang bersifat maya *(virtual).* Realitas yang kedua ini biasa dikaitkan dengan internet dan *cyber space*.[2]

Perkembangan internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif ataupun negatif. Dampak yang bersifat positif membawa banyak manfaat dan kemudahan yang di dapatkan dari teknologi ini. Tetapi tidak dapat dipungkiri bahwa teknologi internet membawa dampak negatif yang tidak kalah banyaknya. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian

---

[1] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime),* PT. Refika Aditama, Jakarta, hlm. 103.

[2] *Ibid.*

dan penipuan menjadi lebih canggih melalui penggunaan media komputer secara *online* dengan resiko tertangkap yang sangat kecil.[3] Misalnya, *e-commerce* tidak sedikit membuka peluang bagi terjadinya tindak pidana penipuan, seperti yang dilakukan oleh sekolompok pemuda di Medan yang memasang iklan di salah satu website terkenal *"Yahoo"* dengan seolah-olah menjual mobil mewah Ferrari dan Lamborghini dengan harga murah sehingga menarik seorang pembeli dari Kuwait.

Berkaitan dengan istilah 'penyelenggaraan sistem elektronik' yang tidak lain adalah penyelenggara negara, orang, badan usaha, dan/atau masyarakat yang memanfaatkan sistem elektronik misalnya untuk pelayanan publik. Setiap penyelenggara negara, orang, badan usaha, dan/atau masyarakat yang memanfaatkan sistem elektronik harus tunduk pada ketentuan dalam UU ITE, diantaranya tidak melakukan perbuatan menyebarkan informasi elektronik yang dilarang, seperti pornografi, perjudian, berita bohong, pengancaman. Bagi yang memanfaatkan sistem elektronik tidak melakukan perbuatan tanpa hak seperti merusak sistem elektronik, memanipulasi informasi, menyadap informasi milik orang lain. Bagi para pelaku yang melakukan perbuatan yang dilarang akan dikenakan sanksi sesuai ketentuan dalam UU ITE.

Setiap penyelenggara bertanggungjawab terhadap sistem elektronik yang diselenggarakan, kecuali berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. Pihak bank bertanggungjawab terhadap sistem elektronik berupa ATM yang diselenggarakan. Ketika ada *hacker* yang menyerang sistem elektronik itu sehingga transaksi elektronik terganggu, maka pihak bank bertanggung jawab untuk memulihkan kembali sistem elektronik itu dan melaporkan ke pihak Kepolisian atas serangan tersebut, sehingga Polisi dapat melakukan penyidikan untuk mencari bukti-bukti dan pelakunya.

Dunia perbankan melalui internet *(e-banking)* Indonesia dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang *hacker* dan jurnalis. Lelaki asal Bandung ini 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 *wwwklik-*

[3] Petrus Reinhard Golose, *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia oleh Polri,* Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006, hlm. 29-30.

bca.com, *kilkbca.com*, *clikbca.com*, *klickca.com*, dan *klikbac.com*. Isi situs-situs plesetan ini nyaris sama. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna *(user id)* dan nomor identitas personal 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 berhati-hati dan tidak ceroboh saat melakukan pengetikan alamat situs *(typo site),* bukan untuk mengeruk keuntungan.[4]

Nasabah yang tertipu akan login ke dalam website palsu dan mulai mengisi informasi penting mengenai data pribadi, seperti nomor kartu kredit, PIN, nomor rekening, password, tanggal lahir, atau nama ibu kandung. Si korban merasa telah mengunjungi website asli bank yang ia gunakan yang tidak lain website palsu. Data pribadi tadi telah dimiliki oleh pelaku phising dan akan digunakanannya untuk mengakses rekening atau kartu kredit korban. Korban yang tertipu baru akan menyadari penipuan saat ia menerima surat pernyataan dari bank atau penerbit kartu kreditnya.

Dari realitas tindak kejahatan tersebut di atas bisa dikatakan bahwa dunia ini tidak lagi hanya melakukan perang secara konvensional akan tetapi juga telah merambah pada perang informasi. Menurut Peter Stephenson dalam bukunya yang berjudul *Investigating Computer-Related Crime,* perang informasi adalah usaha untuk mengakses, mengubah, mencuri, dan menghancurkan suatu sistem komputer.[5] Berdasarkan uraian tersebut maka penting mengetahui bagaimana penegakan hukum *cyber crime* melalui sarana penal maupun non-penal di Indonesia.

B. METODE PENELITIAN

Penelitian ini menggunakan penelitian hukum normatif, yang menekankan pada studi dokumen dalam penelitian kepustakaan untuk mempelajari data sekunder di bidang hukum yang berhubungan dengan permasalahan dan tujuan penelitian ini. Pendekatan yang digunakan adalah pendekatan konseptual dan

---

[4] *Ibid.,* hlm. 31-32.

[5] Peter Stephenson, 2000, *Investigating Computer-Related Crime: A Handbook For Corporate Investigators*, CRC Press, London-New York-Washington D.C., hlm. 109.

pendekatan historis. Pendekatan konseptual dalam penelitian ini dimaksudkan untuk mencari dasar penegakan hukum *cyber crime* di Indonesia dan melalui sarana penal maupun non-penal penegakan hukum *cyber crime* di Indonesia. Pendekatan historis dilakukan dalam kerangka pelacakan penerapan penegakan hukum *cyber crime* di Indonesia dan melalui sarana penal maupun non-penal dalam penegakan hukum *cyber crime* di Indonesia.

C. HASIL DAN PEMBAHASAN

1. Penegakan Hukum Cyber Crime dengan Sarana Penal

Cyber crime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[6] Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *Cyber Crime,* yaitu *cyber crime* dan *computer related crime*.[7] Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama*, cyber crime* dalam arti sempit *(in a narrow sense)* disebut *computer crime.* Kedua*, cyber crime* dalam arti luas *(in a broader sense)* disebut *computer related crime.* Lengkapnya sebagai berikut.

a. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*
b. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Menurut Muladi, sampai saat ini belum ada definisi yang seragam tentang *cyber crime* baik nasional maupun global. Kebanyakan masih

[6] Abdul Wahid dan Mohammad Labib, *Op. Cit.,* hlm. 40.
[7] Barda Nawawi Arief, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Kencana Predana Media Group, Jakarta, hlm. 24.

menggunakan *soft law* berbentuk *code of conduct* seperti Jepang dan Singapura.[8]

Intrumen internasional yang berkaitan dengan *cyber crime* adalah *Convention on Cyber Crime* tanggal 23 November 2001 di kota Budapest Hongaria telah membuat dan menyepakati *Convention on Cyber Crime* yang kemudian dimasukkan dalam *European Treaty Series* dengan nomor 185.[9] Kualifikasi kejahatan dunia maya *(cyber crime),* sebagaimana dikutip Barda Nawawi Arief, adalah kualifikasi *Cyber Crime* menurut *Convention on Cyber Crime* 2001 di Budapest Hongaria adalah sebagai berikut.[10]

a. *Illegal access* yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
b. *Illegal interception* yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.
c. *Data interference* yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
d. *System interference* yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.
e. *Misuse of Devices* yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer, *password* komputer, kode masuk *(access code).*
f. *Computer related Forgery* yaitu pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik).
g. *Computer related Fraud* yaitu penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data computer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

---

[8] Suara Merdeka, situs: http://www.suaramerdeka.com/harian/0207/24/nas13.htm., diakses 1 Juli 2014.
[9] Ahmad M. Ramli, 2006, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia,* PT Refika Aditama, Bandung, hlm. 23.
[10] Barda Nawawi Arief, *Op. Cit.,* hlm. 246-247.

Tindak pidana di atas (Pasal 35 sampai dengan 40) diancam dengan pidana penjara (maksimumnya berkisar antara 1 (satu) sampai dengan 5 (lima) tahun) dan/atau pidana denda (maksimumnya berkisar antara Rp. 100.000.000,00 (seratus juta rupiah) sampai dengan Rp. 500.000.000,00 (lima ratus juta rupiah). Indonesia sedang melakukan pendekatan evolusioner untuk mengatur kegiatan di *cyber space* dengan memperluas pengertian-pengertian yang terdapat di dalam Rancangan Undang-Undang KUHP yang ada sebelumnya tidak memperluas pengertian-pengertian yang terkait kegiatan-kegiatan *cyber space.* Konsep Rancangan Undang-Undang KUHP 2000, dimana konsep ini mengalami perubahan sampai dengan 2004 yaitu[11] Dalam *Buku I* (Ketentuan Umum) dibuat Ketentuan Mengenai:

a. Pengertian "barang" (Pasal 174 sampai dengan Pasal 178) yang di dalamnya termasuk benda tidak berujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer.[12]
b. Pengertian "anak kunci" (Pasal 178 sampai dengan Pasal 182) yang di dalamnya termasuk kode rahasia, kunci masuk computer, kartu *magnetic,* sinyal yang telah deprogram untuk membuka sesuatu. Menurut Agus Raharjo, maksud dari anak kunci ini kemungkinannya adalah *password* atau kode-kode tertentu seperti privat atau *public key infrastructure*.[13]
c. Pengertian "surat" (Pasal 188 sampai dengan Pasal 192) termasuk data tertulis atau tersimpan dalam disket, pita magnetic, media penyimpanan komputer atau penyimpanan data elektronik lainnya.
d. Pengertian "ruang" (Pasal 189 sampai dengan Pasal 193) termasuk bentangan atau terminal computer yang dapat diakses dengan cara-cara tertentu. Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau mayantara atau *cyber space* atau *virtual reality*.
e. Pengertian "masuk" (Pasal 190 sampai dengan Pasal 194) termasuk mengakses komputer atau masuk ke dalam sistem komputer. Pengertian

[11] Barda Nawawi Arief, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan,* PT. Citra Aditya Bakti, Bandung, hlm.131-133.

[12] Penyebutan Pasal 174 sampai dengan Pasal 178 dan sebagainya dalam tulisan ini, maksudnya adalah Pasal 174 Konsep 2000 dan Pasal 178 Konsep 2004 (edisi Desember 2004 yang diserahkan kepada Menkumham tanggal 4 Januari 2005).

[13] Agus Raharjo, 2002, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* PT Citra Aditya Bakti, Bandung, hlm. 236.

masuk menurut Agus Raharjo di sini adalah masuk ke dalam sistem jaringan informasi global yang disebut internet dan kemudian baru masuk ke sebuah situs atau *website* yang di dalamnya berupa *server* dan komputer yang termasuk dalam pengelolaan situs. Jadi ada 2 pengertian masuk, yaitu masuk ke internet dan masuk ke situs.[14]

f. Pengertian "jaringan telepon" (Pasal 191 sampai dengan Pasal 195) termasuk jaringan komputer atau sistem komunikasi komputer.

Sementara dalam **Buku II** dinyatakan bahwa dengan dibuatnya ketentuan seperti di atas, maka konsep tidak atau belum membuat delik khusus untuk *cyber crime* atau *computerrelated crime.* Konsep juga mengubah perumusan delik atau menambah delik-delik baru yang berkaitan dengan kemajuan teknologi, dengan harapan dapat menjaring kasus-kasus *cyber crime.* Untuk sementara dimasukkan dalam Bab V (Tindak Pidana Terhadap Ketertiban Umum) antara lain:

a. menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis (Pasal 263 sampai dengan Pasal 300);
b. memasang alat bantu teknis untuk tujuan mendengar atau merekam pembicaraan (Pasal 264 sampai dengan Pasal 301);
c. merekam (memiliki atau menyiarkan) gambar dengan alat bantu teknis di ruangan tidak untuk umum (pasal 266 sampai dengan Pasal 303).

Untuk sementara dimasukkan dalam Bab VIII (Tindak Pidana yang membahayakan Keamanan Umum Bagi Orang, Barang, dan Lingkungan Hidup):

a. mengakses komputer tanpa hak (Pasal 368, Pasal 371, Pasal 372, dan Pasal 373 Konsep 2004);
b. pornografi anak melalui sistem komputer (Pasal 374 Konsep 2004).

Merusak/membuat tidak dapat dipakai bangunan untuk sarana/prasarana pelayanan umum (antara lain bangunan telekomunikasi/komunikasi lewat satelit/komunikasi jarak jauh) Pasal 630 Konsep 2004. Sementara masalah Pencucian uang *(Money Laundering)* terdapat di dalam Pasal 719 sampai dengan Pasal 722 Konsep 2004).

---

[14] *Ibid.,* hlm. 237.

Dari uraian di atas dapat diketahui bahwa ada 2 (dua) usaha Pemerintah dalam menanggulangi *cyber crime* yang menggunakan sarana penal, yaitu dengan membuat Undang-Undang mengenai Teknologi Informasi atau Telematika dan upaya memperluas pengaturan-pengaturan *cyber space* dalam Rancangan Undang-Undang KUHP dengan memperluas beberapa pengertian yang berkaitan dengan kegiatan di *cyber space*.

Menurut Barda Nawawi Arief, bahwa berbagai Rancangan Undang-Undang RUU KUHP, RUU ITE (Informasi dan Transaksi Elektronik) masih tumpang tindih pengaturan atau formulasi tindak pidana yang berkaitan dengan Kejahatan Dunia Maya. Kebanyakan negara, pengaturan (kebijakan formulasi) tentang kejahatan dunia maya diintegrasikan ke dalam KUHP, walaupun ada juga yang menempatkan dalam undang-undang tersendiri di luar KUHP.[15]

Ada beberapa peraturan perundang-undangan yang berkaitan dengan masalah computer, di antaranya adalah sebagai berikut.

a. Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta

Suatu program atau data mempunyai nilai puluhan kali lipat dibandingkan nilai dari komputer atau media lainnya dimana data atau program tersebut tersimpan yang menjadikan banyak orang yang ingin mengambilnya secara tidak sah untuk disalah gunakan atau diambil manfaat tanpa izin pemiliknya.[16] Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, bahwa program komputer adalah sekumpulan intruksi yang diujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak Cipta untuk program komputer berlaku selama 50 tahun (Pasal 30).

Harga program komputer/*software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan

[15] Barda Nawawi Arief, *Op. Cit.,* hlm. 134-135.
[16] *Ibid.*

harga yang sangat murah. Maraknya pembajakan *software* di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik Hak Cipta. Tindakan pembajakan program komputer tersebut merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)".

b. Undang-undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Money laundering dikenalkan sebagai hasil kejahatan pada tahun 1920 di Chicago oleh Al-Capone, yang digunakan untuk memperoleh kembali keuntungannya dari perjudian dan minuman keras. Yang dimaksud dengan *money laundering* adalah suatu proses dimana hasil perolehan dari aktivitas kejahatan, dikirim, ditransfer, diubah atau dicampur menjadi hasil perolehan dari aktivitas yang sah, dengan tujuan untuk menyembunyikan asal kebenaran perolehan keuntungan tersebut atau dari mana sumber memperoleh uang tersebut.[17]

Tujuan *money laundering* adalah untuk memproses dana yang diperoleh dari aktivitas ilegal menjadi dana yang legal. Faktanya *money laundering* merupakan kegiatan bisnis terbesar nomor tiga (3) dalam produksi mobil di seluruh dunia dan terbesar adalah dari kegiatan perdagangan narkotika dan perdagangan obat terlarang. Kegiatan *money laundering* menyebabkan korupsi di bidang keuangan dan industri, korupsi di bidang birokrasi pemerintahan yang ketiganya adalah mempengaruhi sistem pemerintahan.[18] Undang-undang ini merupakan undang-undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu

---

[17] James R. Richards, 1999, *Transnational Criminal Organizations, Cyber Crime and Money Laundering; A Handbook for law Enforcement Officers, Auditors and Financial Investigators,* CRC Press, London New Work Washington, D.C., hlm. 123.

[18] *Ibid.*

yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) huruf (q)).

Dalam Undang-undang Pencucian Uang, proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk aplikasi pendaftaran, jumlah rekening masuk dan keluar serka kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

Meskipun Undang-undang Nomor 25 tahun 2003 telah diundangkan, akan tetapi tingkat korupsi, penebangan/perdagangan kayu liar *(illegal logging),* produksi dan peredaran gelap narkotika dan psikotropika berskala internasional masih tinggi. Demikian pula pembobolan bank dengan motif pembayaran likuiditas bank, kegiatan ekspor-impor fiktif acap kali terjadi di tanah air kita tercinta ini. Kejahatan tersebut sarat dengan pencucian uang, aliran dana hasil kejahatan bergulir dari satu bank ke bank yang lain di tanah air maupun ke luar negeri.[19]

c. Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Undang-undang Nomor 15 Tahun 2003 mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan

[19] Eddy O.S. Hiariej, dkk., 2006, *Bunga Rampai Hukum Pidana Khusus*, Pena Pundi Aksara Jakarta, hlm. 119.

dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap internet lebih sulit dibandingkan pelacakan melalui *handphone*.

Meskipun sejak awal tahun 2003 kita telah memiliki undang-undang anti-teror, namun pada kenyataannya tidak membuat jera para pelaku, sebab pasca pengesahan undang-undang tersebut, aksi teror masih marak di tanah air. Bahkan sampai pertengahan tahun 2005 terorisme global masih melanda dunia, seperti peledakan di ingris, disusul peledakan di Turki sampai pada peledakan di Mesir.[20]

Berkaitan dengan penggunaan hukum pidana, Nigel Walker sebagaimana dikutip oleh Muladi, mengatakan bahwa ada 6 enam syarat prinsip yang harus diperhatikan oleh pembentuk undang-undang, yaitu:[21]

a) hukum pidana tidak digunakan semata-mata untuk tujuan pembalasan;
b) tindak pidana yang dilakukan harus menimbulkan kerugian dan korban yang jelas;
c) hukum pidana tidak digunakan apabila masih ada cara lain yang lebih baik dan lebih prima;
d) kerugian yang ditimbulkan karena pemidanaan harus lebih kecil daripada akibat tindak pidana;
e) harus mendapat dukungan masyarakat; dan
f) harus dapat diterapkan dengan efektif.

Perlu diperhatikan juga pendapat Sudarto mengenai penggunaan hukum pidana dan kriminalisasi suatu perbuatan menjadi tindak pidana, sebagai berikut.[22]

a) Hukum pidana harus digunakan untuk mewujudkan masyarakat adil dan makmur, merata materiil dan spiritual. Hukum pidana bertugas untuk menanggulangi kejahatan dan tindakan penanggulangan itu sendiri untuk kesejahteraan masyarakat atau untuk pengayoman masyarakat.

---

[20] *Ibid,* hlm. 219-221.
[21] Muladi, 1990, *Proyeksi Hukum Pidana Materiil Indonesia di Masa Mendatang,* Pidato Pengukuhan Guru Besar Universitas Diponegoro Semarang, hlm. 7 dan 28.
[22] Sudarto, 1986, *Hukum dan Hukum Pidana,* Alumni, Bandung, hlm. 36-40.

b) Hukum pidana digunakan untuk mencegah atau menanggulangi perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian pada masyarakat. Penggunaan sarana hukum pidana dengan sanksi yang negatif perlu disertai dengan perhitungan biaya yang harus dikeluarkan dan hasil yang diharapkan akan dicapai *(cost and benefit principle).*

2. Penegakan Hukum *Cyber Crime* dengan Sarana non-Penal

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda Nawawi Arief sebagai berikut.[23]

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana.
b. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana *control social* yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya).
c. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan *"kurieren am symptom",* oleh karena itu hukum pidana hanya merupakan "pengobatan simptomatik" dan bukan "pengobatan kausatif".
d. Sanksi hukum pidana merupakan "remedium" yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif.
e. Sistem pemidanaan bersifat fragmentair dan individual/personal, tidak bersifat struktural/fungsional.
f. Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif.
g. Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan "biaya tinggi".

[23] Barda Nawawi Arief, 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana,* PT Citra Aditya Bakti, Bandung, hlm. 46-47.

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu, pencegahan kejahatan tidak melulu harus menggunakan hukum pidana. Agar penegakan hukum *cyber crime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Dalam Resolusi Kongres PBB VIII/1990 mengenai *computer-related crimes* sebagaimana dikutip oleh Barda Nawawi Arief, bahwa menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:[24]

a. Melakukan Modernisasi hukum pidana material dan hukum acara pidana
b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
c. Melakukan langkah-langkah untuk membuat peka warga warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer
d. Melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime*
e. Memperluas *rule of ethics* dalam penggunaan computer dan mengajarkannya melalui kurikulum informatika
f. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime.*

Menurut Agus Raharjo bahwa salah satu langkah lagi agar penanggulangan *cyber crime* ini dapat dilakukan dengan baik, maka perlu dilakukan kerja sama dengan *Internet Service Provider* (ISP) atau penyedia jasa internet. Meskipun *Internet Service Provider* (ISP) hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi *Internet Service Provider* (ISP) memiliki catatan mengenai ke luar atau masuknya seorang

[24] Barda Nawawi Arief,*Op. Cit.,* hlm. 238-239.

pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat *log file* yang ada.[25] Ada beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet yang telah dibangun yaitu sebagai berikut.[26]

a. Mengatur akses *(access control)*

   Salah cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme *authentication* dan *access control.*

b. Menutup *service* yang tidak digunakan

   Seringkali dalam sebuah sistem (perangkat keras dan atau perangkat lunak) diberikan beberapa servis yang dijalankan sebagai *default,* seperti pada sistem UNIX yang sering dipasang dari *vendor*-nya adalah *finger, telnet, ftp, smtp, pop, echo* dan sebagainya. Sebaiknya servis-servis ini kalau tidak dipakai dimatikan saja. Karena banyak kasus terjadi yang menunjukkan *abuse* dari servis tersebut atau ada lubang keamanan dalam servis tersebut. Akan tetapi *administrator* sistem tidak menyadari bahwa servis tersebut dijalankan di komputernya.

c. Memasang Proteksi

   Proteksi ini bisa berupa *filter* (secara umum) dan yang lebih spesifik lagi adalah *firewall. Filter* ini dapat digunak untuk memfilter *e-mail,* informasi, akses atau bahkan dalam *level packet*. Sebagai contoh, di sistem UNIX ada paket program *topwrapper* yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis untuk *telnet* dapat dibatasi untuk sistem yang memiliki nomor IP tertentu atau memiliki *domain* tertentu. Sementara *firewall* digunakan untuk melakukan *filter* secara umum. Ada juga program *filter* internet yang bernama *ZeekSafe.* Program ini bisa memblokir situs-situs yang tidak diinginkan. Selain itu, ada juga program filter yang lain, yaitu *We-Blocker,* sama dengan *ZeekSafe,* program ini bisa menentukan parameter apa saja yang akan membatasi akses ke *website* yang dianggap tidak layak dilihat.

d. *Firewall*

[25] Agus Raharjo,*Op. Cit.,*hlm. 248.
[26] *Ibid,* hlm. 252-260.

Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang ke luar dan masuk harus melalui *firewall* ini. Tujuan utama dari *firewall* adalah untuk menjaga *(prevent)* agar akses (ke dalam maupun ke luar) dari orang tidak berwenang *(unauthorized access)* tidak dapat dilakukan. *Firewall* bekerja dengan mengamati paket *Internet Protocol* (IP) yang melewatinya. Berdasarkan konfigurasi dari *firewall,* maka akses dapat diatur berdasarkan *Internet Protocol* (IP) *address, port* dan arah informasi.

e. Pemantau adanya serangan

Sistem pemantau *(monitoring system)* digunakan untuk mengetahui adanya tamu tidak diundang *(intruder)* atau adanya serangan *(attack).* Nama lain dari sistem ini adalah *Intruder Detection System* (IDS). Sistem ini dapat memberi tahu administrator melalui *email* maupun melalui mekanisme lain seperti *pager.* Ada beberapa cara untuk memantau adanya *intruder,* baik yang sifatnya aktif maupun pasif.

f. Pemantau integritas sistem

Sistem ini dijalankan secara berkala untuk menguji integritas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire.* Program ini dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya program ini dijalankan dan membuat data *base* mengenai berkas-berkas atau direktori yang ingin kita amati beserta *signature* dari berkas tersebut. *Signature* berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berbeda dengan yang ada di data *base* sehingga ketahuan adanya perubahan.

g. Audit: Mengamati berkas *log*

Segala kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut *log file* atu *log* saja. Berkas *log* ini sangat berguna untuk mengamati penyimpanan yang terjadi. Kegagalan untuk masuk ke sistem *(login)* misalnya tersimpan dalam berkas *log.* Untuk itu pada *administrator* diwajibkan untuk rajin memelihara dan menganalisis berkas *log* yang dimilikinya.

h. *Back up* secara rutin

Sering kali intruder masuk dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang ditemui. Jika *intruder* ini berhasil menjebol sistem dan masuk sebagai *superuser,* maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya *back up* yang digunakan secara rutin merupakan hal yang esensial.

i. Penggunaan enkripsi untuk meningkatkan keamanan

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di internet yang masih menggunakan *plain text* untuk *authentication* seperti penggunaan pasangan *userid* dan *password.* Informasi ini dapat dilihat dengan mudah dengan program penyadap atau pengendus *(sniffer).* Untuk meningkatkan keamanan *server world wide web* dapat digunakan enkripsi pada tingkat *socket.* Dengan menggunakan *enkripsi,* orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke *server* WWW.

Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh *Netscape.* Selain *server* WWW dari *Netscape* dapat juga dipakai *server* WWW dari *Apache* yang dapat dikonfigurasi agar memiliki fasilitas *Secure Socket layer* (SSL) dengan menambahkan *software* tambahan *SSLeay*-implementasi *Secure Socket Layer* (SSL) dari *Eric Young*-atau *Open Secure Socket Layer* (SSL). Penggunaan *Secure Socket Layer* (SSL) memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan pemerintah melarang ekspor teknologi enkripsi (kriptografi) dan paten *Public Key Partners* atas *Rivest-Shamir-Adleman* (RSA) *public key cryptography* yang digunakan pada *Secure Socket Layer* (SSL). Oleh karena itu, implementasi *SSLeay Eric Young* tidak dapat digunakan di Amerika Utara (Amerika dan Kanada) karena melanggar paten *Rivest-Shamir-Adleman* (RSA) dan RC4 yang digunakan dalam implementasinya.

j. *Telnet* atau *shell* aman

Telnet atau *remote login* yang digunakan untuk mengakses sebuah *remote site* atau computer melalui sebuah jaringan computer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan *user id* dan *password.* Informasi tentang *user id* dan *password* ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya kemungkinan *password* bisa kenak *sniffing.* Untuk menghindari hal ini bisa memakai enkripsi yang dapat melindungi adanya *sniffing.* Selain itu bisa juga memakai *firewall,* alat ini untuk melindungi data-data penting. Akan tetapi sistem pengamanan yang telah dipaparkan di atas tadi tidak menjamin aman 100% (seratus persen), oleh karena itu dianjurkan untuk terus memantau perkembangan sistem pengamanan internet.

Dari paparan penegakan hukum dengan sarana non-penal ini, maka membutuhkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *Cyber,* Jaksa *Cyber,* Hakim *Cyber* dalam rangka penegakan hukum *Cyber Crime* di Indonesia. Tanpa adanya penegak hukum yang mempuni di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini *locos delicti*-nya bisa lintas negara.

Berdasarkan uraian di atas, maka dapat dipahami bahwa kejahatan apapun bentuknya baik konvensional maupun kejahatan yang dilakukan melalui media internet atau *cyber crime* tidak akan lepas dari hukuman. Seiring dengan itu di dalam hukum positif dikenal dengan *adagium* “setiap kejahatan tidak boleh dibiarkan berlalu tanpa hukuman” *(aut punere aut de dere, nullum crimen sine poena).*

D. PENUTUP

1. Kesimpulan

Berdasarakan uraian permasalahan di atas dapat disimpulkan bahwa penegakan hukum *cyber crime* dapat dilakukan dengan sarana penal dan melalui sarana non-penal. Penegakan hukum *cyber crime* tidak cukup hanya dengan sarana penal, karena sarana penal merupakan *ultimum remidium* yang memiliki banyak kelemahan. Oleh karena itu, penegakan hukum *cyber crime* yang harus diutamakan adalah sarana non-penal, oleh karena sarana

non-penal merupakan sarana *preventif* terhadap terjadinya kejahatan *cyber crime.*

2. Rekomendasi
   a. Penegakan hukum *cyber crime* tidak cukup hanya melalui sarana penal dan non-penal, akan tetapi perlu ditambah kerja sama antar negara. Kerja sama ini bisa berbentuk ekstradisi atau harmonisasi hukum pidana subtantif.
   b. Dalam rangka penegakan hukum *cyber crime,* maka sangat penting segera mempersiapkan penegak hukum yang menguasai teknologi informasi.

DAFTAR PUSTAKA

Buku

Collarick, Andrew, 2006, *Cyber Terrorism; Political and Economic Implications,* IDEA Group Publishing.

Hiariej, Eddy O.S, dkk, 2006, *Bunga Rampai Hukum Pidana Khusus,* Pena Pundi Aksara, Jakarta.

Labib, Mohammad dan Wahid, Abdul, 2005, *Kejahatan Mayantara (Cyber Crime),* PT. Refika Aditama, Bandung.

M. Ramli, Ahmad, 2006, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia,* PT. Refika Aditama, Bandung.

Nawawi Arief, Barda, 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, PT. Citra Aditya Bakti, Bandung.

_____, 2003, *Kapita Selekta Hukum Pidana,* PT. Citra Aditya Bakti, Bandung.

_____, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan,* PT. Citra Aditya Bakti, Bandung.

_____, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan,* Kencana Predana Media Group, Jakarta.

Raharjo, Agus, 2002, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* PT. Citra Aditya Bakti, Bandung.

Richards, James R., 1999, *Transnational Criminal Organizations, Cyber Crime and Money Laundering; A Handbook for law Enforcement Officers, Auditors and Financial Investigators,* CRC Press, London New Work Washington, D.C.

Stephenson, Peter, *Investigating Computer-Related Crime: A Handbook For Corporate Investigators,* London New York Washington D.C: CRC Press, 2000.

Sudarto, 1986, *Hukum dan Hukum Pidana,* Alumni, Bandung.

Sumber Lain

Muladi, 1990, *Proyeksi Hukum Pidana Materiil Indonesia di Masa Mendatang,* Pidato Pengukuhan Guru Besar Universitas Diponegoro Semarang.

Reinhard Golose, Petrus, *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia oleh Polri,* Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006.

Draft III RUU Teknologi Informasi, 2001, disusun oleh FH UNPAD bekerja sama dengan Ditjen Pos dan Telekomunikasi.

Suara Merdeka, http://www.suaramerdeka.com/harian/0207/24/nas13.htm.