

PENEGAKAN HUKUM TERHADAP CYBER CRIME

Oleh: Riza Nizarli*

ABSTRAK

Kata Kunci: Penegakan, *Cyber*

Kemajuan teknologi telah membawa perubahan dan pergeseran yang cepat dalam suatu kehidupan tanpa batas. Pemanfaatan teknologi tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat disajikan melalui hubungan jarak jauh dan mereka yang ingin mengadakan transaksi tidak harus bertemu muka, akan tetapi cukup melalui peralatan komputer dan telekomunikasi. Perkembangan teknologi informasi juga membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial dan telah membalikkan segalanya yang jauh jadi dekat yang khayal jadi nyata. Namun dibalik kemajuan itu, juga telah melahirkan keresahan-keresahan baru dengan munculnya kejahatan yang canggih dalam bentuk *cyber crime*.

A. PENDAHULUAN

Perkembangan teknologi komputer, telekomunikasi dan informatika di era globalisasi bukanlah suatu hal yang fiktif melainkan sudah menjadi kenyataan yang diwujudkan dalam berbagai bentuk. Penyebaran informasi telah melintasi batas-batas wilayah dan perbedaan waktu sudah tidak lagi memisahkan manusia. Dengan kemajuan dan perkembangan telekomunikasi multimedia, ruang lingkup dan kecepatan komunikasi lintas batas meningkat, ini berarti masalah hukum yang berkaitan dengan yurisdiksi dan penegakan serta pemilihan hukum yang berlaku terhadap suatu sengketa multi-yurisdiksi akan bertambah penting dan konflik (Ny. Tien S. Saifullah : 2001:96).

Pemanfaatan teknologi tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat disajikan melalui hubungan jarak jauh dengan mudah dapat diperoleh. Mereka yang ingin mengadakan transaksi tidak harus bertemu muka *face to face*, cukup melalui peralatan komputer dan telekomunikasi.

* Dosen Pengajar Hukum Pidana Khusus pada Fakultas Hukum Unsyiah dan Unmuha

Fenomena perdagangan dengan kecanggihan teknologi yang dikenal dengan internet (*electronic commerce* yang disingkat dengan *e-commerce*) hanyalah salah satu bentuk dari perubahan perilaku masyarakat yang timbul akibat revolusi teknologi informasi. Massachusetts Institute of Technology yang bermarkas di Boston telah lama mempunyai system informasi yang komprehensif untuk menangani sebagian besar urusan akademis dan administrasi seperti proses pengajaran, penugasan, diskusi, pratikum, teleconference, pendaftaran mahasiswa baru, register ulang, pembayaran, data kemajuan akademik, penelitian telah ditangani dengan baik.

Kita memang tidak dapat membantah bahwa penerapan teknologi informasi akan menimbulkan berbagai perubahan sosial. Karena itu perlu untuk diperhatikan bagaimana upaya melakukan transformasi teknologi dan industri dalam mengembangkan struktur sosial yang kondusif. Tanpa adanya partisipasi masyarakat dan peranan hukum, upaya pengembangan teknologi tidak saja kehilangan dimensi kemanusiaan tetapi juga menumpulkan visi inovatifnya.

Peranan hukum diharapkan dapat menjamin bahwa pelaksanaan perubahan itu akan berjalan dengan cara yang teratur, tertib dan lancar. Perubahan yang tidak direncanakan dengan sebuah kebijakan hukum acap kali akan menimbulkan berbagai persoalan baru dalam masyarakat. Di sinilah hukum akan berfungsi dalam menghadapi perubahan masyarakat. Fungsi hukum dalam masyarakat ada dua yaitu;

1. Produk hukum harus mampu mengangkat peristiwa-peristiwa (gejala hukum) dalam masyarakat ke dalam hukum sebagai sarana pengaturan masyarakat di masa akan datang. Fungsi pengaturan diwujudkan dengan dibentuknya norma-norma yang merupakan alat pengawas masyarakat (*social control*). Fungsi ini bertujuan agar orang-orang bertingkah laku sesuai dengan harapan masyarakat umum yang telah diwujudkan dalam norma hukum yang dibentuk bersama.
2. Fungsi kedua dimaksudkan untuk menjamin kelangsungan hidup masyarakat dalam suasana perubahan masyarakat yang terus menerus terjadi. Ini

dimaksudkan agar setiap perubahan masyarakat sesuai dengan tujuan-tujuan yang telah direncanakan atau dikehendaki.

Dampak tersebut tidak selalu berlangsung demikian, karena di pihak lain timbul itikad tidak baik untuk mencari keuntungan dengan melawan hukum, yang berarti melakukan kejahatan.

Dari sisi perkembangan fenomena tingkah laku sosial ini Naisbitt dalam bukunya *Global Paradox* menyebutkan bahwa dengan perkembangan yang eksplosif dalam telekomunikasi mendorong pula kekuatan simultan timbulnya ekonomi global yang luas (John Naisbitt, 1994:53). Telekomunikasi akan melengkapi infrastruktur setiap industri dan perusahaan yang bersaing dalam pasar dunia. Bisnis telekomunikasi akan berkembang berlipat ganda kearah interkoneksi global. Dalam proses interkoneksi tersebut industri telekomunikasi dikombinasikan pemanfaatannya dengan telepon, televisi, komputer, dan konsumen elektronik menjadi kekuatan global, namun jika tidak hati-hati dapat menciptakan kekacauan. Selanjutnya Naisbitt juga mengemukakan bahwa akan terdapat “*New Rules*” atau norma berupa “*Code of conduct*” universal pada abad ke 21.

Dalam keadaan tersebut akan timbul gerakan masyarakat untuk mengembangkan hukum, peraturan, norma tidak tertulis dan upaya-upaya untuk memelihara harmonisasi sosial. Jika suatu kejahatan terjadi, masyarakat akan bereaksi bahwa hal tersebut merupakan hal yang salah, yang perlu dicegah.

Pencegahan melalui pengaturan dapat terbatas pada lokasi tertentu, kota, negara bahkan global. Seperti halnya kejahatan *cyber crime* yang telah berkembang di Indonesia, perlu adanya pengaturan agar dapat mencegah dampak negatif, sehingga terjadinya kondisi sosial yang harmonis.

Makin populernya pemakaian internet untuk pelbagai keperluan seperti *e-banking* dan *e-commerce*, telah meningkat terjadinya tindak pidana di bidang ini. Kejahatan di bidang ini meliputi tindak pidana penipuan, penggelapan, *hacking*, pidana di bidang komunikasi, atau pengrusakan system komputer yang belum

seluruhnya dapat dijangkau dengan undang-undang yang berlaku (Heru Soeprapto, 2001:4).

Internet telah membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial yang dahulu ditetapkan dengan sangat rigid. Masyarakat baru dengan kebebasan beraktivitas dan berkreasi sedang mencoba membangun kebudayaan baru di ruang maya yang dikenal dengan *cyber space*. Istilah ini lahir dari William Gibson seorang penulis fiksi ilmiah (*science fiction*) dalam novelnya yang berjudul *Neuromancer and virtual light* (Freddy Harris, 2001:4).

Kelahiran internet telah membalikkan segalanya, yang jauh jadi dekat, yang khayal jadi nyata, dan *paper-based* menjadi *paperless*. Namun dibalik kemerlapan itu, internet juga melahirkan keresahan-keresahan baru. Seperti munculnya kejahatan yang canggih dalam bentuk "*cyber crime*". Hal ini ditambah dengan pesatnya perkembangan situs-situs porno, penyerangan terhadap privacy seseorang, perdagangan terhadap barang illegal atau hadirnya situs-situs yang mencemaskan masyarakat.

Di dalam dunia perbankan perkembangan *cyber crime* cukup mengejutkan dengan terjadi beberapa kasus yang merugikan pihak perbankan seperti; kasus pembobolan BNI New York oleh mantan karyawannya sendiri, mutasi kredit fiktif melalui komputer di BDN Cabang Bintaro Jaya, pencurian dana di Bank Danamon Pusat. Sementara itu sejumlah nasabah pemegang *credit card* juga mengeluh, karena nomor kartu kreditnya telah dipakai pihak lain untuk melakukan transaksi *e-commerce* sehingga menimbulkan kerugian yang cukup besar. Keresahan-keresahan ini membuat sebahagian masyarakat meminta jaminan keadilan dan kepastian hukum di bidang *cyber space*.

Dari fenomena di atas, timbul sebuah pertanyaan apakah memang ada hukum di bidang *cyber space*? Jika kita lihat konsep dasar lahirnya *cyber space* (ruang maya) dari perkembangan teknologi informasi, khususnya internet hanya merupakan sebuah media pengantar sebagaimana media-media pengantar dalam bentuk lainnya. Akan tetapi internet memiliki karakteristik tersendiri yang membedakannya dengan

media pengantar lain, seperti media cetak, penyiaran atau telekomunikasi. Keistimewaannya dalam mengkonvergensi berbagai bentuk media di atas, telah menjadikan internet sebagai media pengantar yang relatif sempurna.

Karena konsep internet sebagai media pengantar, maka hubungan para pihak di internet hanya akan terjadi bila para pihak mempunyai keinginan bersama didukung itikad baik untuk menggunakan internet sebagai media dalam membangun hubungannya. Oleh karena itu, ketika terjadi hubungan para pihak, maka pada saat itu pula terjadi hubungan hukum di antara mereka. Pada saat timbulnya hubungan hukum, maka saat itu pula diperlukan efektivitas terhadap jaminan dan perlindungan hukum di *cyber space*.

Kelahiran hukum di *cyber space* tentu akan membawa perdebatan panjang di antara para akademisi hukum, praktisi hukum, maupun warga masyarakat yang terlibat secara langsung atau tidak terhadap dampak dari revolusi teknologi informasi. Perdebatan ini terjadi karena hubungan hukum yang timbul di dalam internet, keabsahannya masih menjadi tanda tanya besar. Hal ini terjadi karena adanya berbagai pendapat mendasar antara hukum internet dengan hukum nasional yang berlaku sekarang.

Dari uraian di atas maka berbagai permasalahan yang akan muncul kepermukaan antara lain masalah pembuktian dari data elektronik yang belum dikenal sebagai alat bukti di dalam hukum nasional sebagaimana diatur dalam Pasal 184 KUHP, ketidakjelasan kedudukan (domisili) para pihak saat melakukan transaksi, sejauhmanakah kewenangan aparat penegak hukum untuk mengambil tindakan hukum bila terjadi kejahatan serta berbagai persoalan lain sampai saat ini masih menjadi perdebatan berbagai kalangan. Di lain pihak kita tidak dapat membantah adanya tuntutan dari pelaku bisnis yang meminta dikeluarkan hukum nasional yang mengatur masalah jaminan hukum di bidang internet. Tulisan ini bertujuan untuk mencari usaha dalam penegakan hukum terhadap *cyber crime*.

B. PERKEMBANGAN *CYBER CRIME*

Salah satu ciri dari kehadiran masyarakat informasi (*information society*) adalah adanya pemanfaatan internet yang semakin luas dalam berbagai bidang kehidupan. Masyarakat informasi sendiri merupakan konsekuensi dari perkembangan teknologi informasi yang telah membawa perubahan dan pergeseran yang sangat cepat ke dalam suatu kehidupan dunia tanpa batas (*boorderless world*) yang pada gilirannya mempengaruhi mekanisme perdagangan, baik secara nasional maupun internasional (Ismamulhadi, 2002:78).

Perkembangan teknologi informasi telah menyebabkan aktivitas berbagai sektor kehidupan khususnya di bidang sosial dan ekonomi, berkembang semakin pesat dan cepat. Bahkan hubungan di bidang sosial ekonomi di masyarakat, terutama masyarakat internasional, boleh dikatakan dewasa ini telah memasuki suatu masyarakat yang berorientasi kepada informasi. Hubungan-hubungan (interaksi) melalui teknologi informasi tersebut tidak lagi secara fisik sebagaimana yang terjadi selama ini, namun interaksi tersebut secara *virtual* atau *cyber space* (dunia maya).

Sistem informasi dan teknologi telah digunakan dibanyak sektor kehidupan, mulai dari perdagangan/bisnis (*electronic Commerce*), pendidikan (*electronic education*), kesehatan (*tele-medicine*), transportasi, industri, pariwisata serta lingkungan sampai sektor hiburan (Suhono Harso Supangkat, 2000,44) bahkan sekarang timbul pula di bidang pemerintahan (*e-government*). Teknologi informasi mencakup sistem yang mengumpulkan (*collect*), menyimpan (*store*), memproses, memproduksi dan mengirim informasi dari dan ke industri ataupun masyarakat secara efektif dan cepat (Saefullah Wiradipradja dan Danrivanto Budhijanto, 2002,88)

Menurut Freddy Haris (2001:5) ditemukannya internet sebagai suatu sistem antar jaringan dimulai dari konsep *Galantic Network* yang dirancang oleh J.C.R. Licklider dari Massachussetess Instituse Teknologi (MIT). Konsep ini kemudian terus digodok oleh *Defanse Advanced Research Project Agency* (DARPA). Sejak itu internet yang mula dikembangkan hanya untuk keperluan militer, riset dan

pendidikan terus berkembang memasuki berbagai sektor kehidupan manusia, termasuk aktivitas bisnis.

Dalam sistem komputer, teknologi internet adalah hal baru (mulai pada tahun 1995 dipergunakan untuk umum termasuk bisnis), sedangkan untuk kepentingan proyek militer Amerika Serikat mulai digunakan sejak tahun 1969 yang bernama ARPANET.

Sejak dikenalnya jaringan internet, maka mulai pula dikenal kejahatan komputer (*Cyber crime*) dan masuk dalam permasalahannya adalah tentang HAKI (Hak Kekayaan Intelektual/ *Intellectual Property Right*) dan *e-commerce* (perdagangan melalui internet). (Mardjono Reksodiputro, 2001:3).

Akibat dari perkembangan teknologi informasi tersebut menyebabkan perkembangan interaksi di bidang sosial dan ekonomi berlangsung dalam dunia maya, maka diperlukan pengaturan yang bersifat khusus, karena tidak tertampung lagi dalam hukum atau peraturan perundang-undangan konvensional. Maka saat ini berkembang suatu bidang hukum baru yang dikenal dengan *cyber law* (Saefullah Wiradipradja dan Danrivanto Budhijanto, 2002,89).

Dalam upaya mendapatkan informasi dan pemahaman yang memadai dan menyeluruh tentang *cyber law* sebagai suatu hukum yang baru dengan bentuk pengaturan yang bersifat khusus (*sui generis*) atas kegiatan-kegiatan di dalam *cyber space*, ruang lingkup dari *cyber law* menurut Jonatha Rosenoer (Saefullah Wiradipradja dan Danrivanto Budhijanto: 2002:99) antara lain mencakup:

1. *Copyright* (Hak Cipta);
2. *Trademark* (Hak Merek);
3. *Dafamation* atau dapat dianalogikan sebagai pencemaran nama baik;
4. *Privacy*;
5. *Duty of Care*;
6. *Criminal Liability*;
7. *Procedural Issues*;
8. *Electronic Contracts & Digital Signature*;
9. *Electronic Commerce*;
10. *Electronic Government*;
11. *Pornografi*; dan
12. Pencurian (*theft*),

Menurut Mardjono Reksodiputro (2001:1), berdasarkan kerangka (Sistemik) *Draf Convention on Cyber Crime* dari Dewan Eropa (Draf No, 25 Desember 2000) yang telah ditandatangani oleh 30 negara pada bulan Nopember 2001 di Budapest, Hungaria, Barda Nawawi Arief telah menyorikan delik-delik menjadi:

1. Delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk disini:
 - a. mengakses sistem komputer tanpa hak (*illegal access*);
 - b. tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
 - c. tanpa hak merusak data (*data interference*);
 - d. tanpa hak mengganggu sistem (*system interference*);
 - e. menyalahgunakan perlengkapan (*misuse related of devices*)
2. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer; *computer related offences; forgery and fraud*).
3. Delik-delik yang bermuatan pornografi anak (*contetn related offences, child pornogarfi*).
4. Delik-delik yang berhubungan dengan hak cipta (*offences related to infrigements of copyright*).

Mieke Komar Kantaatmadja dan Ahmad M. Ramli dalam tulisannya *Kajian dan Evaluasi Hukum Nasional dalam Pemanfaatan Teknologi Informasi* juga menjelaskan beberapa permasalahan hukum yang perlu dicermati dalam persiapan regulasi dalam kaitannya dengan *cyber space* (Saefullah Wiradipradja dan Danrivanto Budhijanto, 2002,89)yaitu:

1. Aspek Hukum Perjanjian dan Tandatangani Digital;
2. Pelanggaran Hukum dalam Bentuk Akses Ilegal terhadap Jaringan Komputer;
3. Penyalahgunaan Password dalam Era Ekonomi Digital; dan
4. Keterkaitan Hak atas Kepemilikan Intelektual (HAKI) dengan Sistem Informasi (Hak Cipta, Merek, Paten, Informasi Rahasia/Rahasia Dagang (*trade secret*) dan Disain Industri.

Apabila kita mengikuti kasus-kasus *cyber crime* yang terjadi dan jika hal tersebut dikaji dengan menggunakan kriteria hukum pidana konvensional, maka hukum *cyber crime* bukanlah kejahatan yang sederhana (Barita Saragih, 2002).

Untuk menjerat pelaku kejahatan melalui internet, Tim penyusun RUU KUHP Baru juga telah berusaha memasukkan pasal-pasal baru untuk menghadapi masalah *cyber crime* yaitu Pasal 188 untuk data komputer, Pasal 189 untuk terminal komputer, Pasal 190 untuk akses ke system komputer dan Pasal 191 tentang jaringan telepon yang termasuk jaringan komputer (Mardjono Reksodiputro, 2001:3).

Menurut Heru Soeprapto (2001:4) tim interdep juga pernah berencana menyisipkan satu dua pasal dalam KUHP dengan harapan agar pasal-pasal tersebut dapat dioperasionalkan dalam menghadapi kejahatan komputer. Namun rencana itu belum kunjung direalisasi, padahal dengan berkembangannya pemakaian internet, *e-commerce*, *e-business*, *e-banking* untuk pelbagai kepentingan sudah mendesak agar dapat dilakukan langkah-langkah yang kongkrit. Langkah-langkah ini merupakan hal yang penting untuk penegakan hukum terhadap *cyber crime*.

Jika kita lihat dalam peraturan perundang-undangan yang konvensional, maka perbuatan pidana yang dapat digunakan dibidang *cyber crime* adalah; penipuan, kecurangan, pencurian dan perusakan, yang dilakukan secara langsung (dengan menggunakan bagian tubuh secara fisik dan pikiran) oleh si pelaku. Sementara itu jika hal tersebut dilakukan dengan memanfaatkan sarana komputer, maka *cyber crime* dapat berbentuk sebagai berikut (Heru Soeprapto:2001:6):

1. Penipuan komputer (*computer fraud*) yang mencakup:
 - a. Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan komputer/siber dengan melawan hukum, ialah dalam bentuk penipuan data dan penipuan program, yang terinci adalah:
 - i. Memasukkan intruksi yang tidak sah, ialah dilakukan oleh seorang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (transfer).
 - ii. Mengubah data input, yang dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum (memasukkan daftar gaji pegawai melebihi yang seharusnya).
 - iii. Merusak data, dilakukan seseorang untuk merusak *print-out* atau *output* dengan maksud untuk mangaburkan,

- menyembunyikan data atau informasi dengan itikad tidak baik.
- iv. Penggunaan komputer untuk sarana melakukan perbuatan pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.
 - b. Perbuatan pidana penipuan, yang sesungguhnya dapat termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan diri dari kewajiban (pajak) atau untuk memperoleh sesuatu yang bukan hak/milikinya melalui sarana komputer.
 - c. Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses komputer mentransfer rekening orang ke rekeningnya sendiri, sehingga merugikan orang lain.
 - d. Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang bersama-sama untuk melakukan penipuan dengan sarana komputer.
 - e. Pencurian ialah dengan sengaja mengambil dengan melawan hukum hak atau milik orang lain dengan maksud untuk dimilikinya sendiri.
2. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.
 3. *Hacking*, ialah melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.
 4. Perbuatan pidana komunikasi, ialah *hacking* yang dapat membobolkan sisten *on-line* komputer yang menggunakan sistem komunikasi.
 5. Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian. Termasuk dalam golongan perbuatan ini adalah berupa penambahan atau perubahan program, informasi, media, sehingga merusak sistem, demikian pula sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan menggunakan sara komputer/telekomunikasi.
 6. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk mendapatkan keuntungan melalui perdagangan.

Jenis perbuatan pidana tersebut di atas dapat berlaku jika komputer dihubungkan dengan teknologi telekomunikasi dan informasi, sehingga menjadi *cyber crime*, terutama dengan perkembangan teknologi internet.

Pesatnya pemanfaatan jasa internet, ternyata telah menimbulkan dampak negatif lain yaitu dalam bentuk kejahatan yang kemudian dikenal dengan *cyber crime* yang merupakan perkembangan lanjut dari *computer-crime*. Menurut Rene L Pattiradjawane (2000), dalam menjelaskan tantangan perkembangan *cyberlaw*, menyebutkan konsep hukum *cyberspace*, *cyberlaw* dan *cyber line* yang dapat menciptakan komunitas penggunaan jaringan internet yang luas (60 juta), yang melibatkan 160 negara menimbulkan kekusaran para praktisi hukum untuk menciptakan pengamanan melalui regulasi khususnya perlindungan terhadap milik pribadi.

Untuk menghadapi perkembangan *cyber crime* yang melibatkan berbagai pihak dengan yurisdiksi teritorial, waktu, hukum, negara, pemerintah, sistem yang berbeda, apakah masih dapat diselesaikan dengan hukum nasional yang berlaku atau perlu pembaharuan atau perlu adanya suatu konvensi internasional.

C. PENEGAKAN HUKUM TERHADAP *CYBER CRIME*

Hukum selama ini dipahami hanya sebagai perangkat norma atau kaedah belaka yang sifatnya idealitas sebagai patokan mengenai sikap tindak atau perilaku masyarakat. Karena tidak dipahami sebagai tindak atau perilaku yang teratur sehingga wajar saja hukum kita bersifat formalistik dan legalistik. Hal ini tercermin dari praktek penegakan hukum (*law enforcement*) di dalam masyarakat yang mengedepankan hukum dalam arti positif semata.

Sementara itu, pembangunan hukum selama ini dititik beratkan pada hal-hal yang menyangkut substansi hukum (*legal substance*) tetapi lupa memperhatikan efektivitasnya di dalam masyarakat. Hal ini menyebabkan hukum dibuat demikian modern tidak berlaku efektif di dalam masyarakat bahkan tidak jarang ditolak.

Hal yang benar adalah yang dapat dipahami masyarakat, jelas redaksinya, jelas tujuannya dan ada kepentingan masyarakat yang dilindungi. Oleh karena itu hukum dibuat harus konkret atau harus di konkretisasikan. Masyarakat harus mengetahui keberadaan hukum tersebut, untuk apa (tujuan) hukum itu diberlakukan,

apakah ada kepentingan mereka yang dilindungi oleh hukum tersebut dan bagaimana hukum itu diberlakukan dan apa sanksinya.

Pengetahuan dan pemahaman terhadap hukum yang berlaku membantu menghindari masyarakat dari rasa curiga (*prejudice*) ataupun apriori. Selanjutnya hukum harus dapat memberikan kejelasan tentang sanksinya bila hukum itu dilanggar. Sanksi dapat merupakan suatu sarana untuk membuat orang merasa takut untuk melanggar.

Berkaitan dengan hal tersebut di atas maka dalam menegakkan hukum terhadap *cyber crime* perlu dipikirkan sejauhmana hukum itu harus diatur sehingga tidak menimbulkan permasalahan baru.

Perlu kita yakini bahwa perkembangan teknologi dan informasi akan memacu pertumbuhan jenis kejahatan tertentu, karena perkembangan teknologi dan informasi selalu diikuti dengan perkembangan kriminalitas. Oleh karena itu, hukum pidana harus mengikuti perkembangan kriminalitas sehingga diharapkan dapat memberi perlindungan dan rasa keadilan dalam masyarakat, serta hukum tidak ketinggalan zaman, bahkan hukum harus dapat mencegah dan mengatasi kejahatan yang bakal muncul (Bakat Purwanto, 1995:4). Hukum pidana sebagai bagian dari keseluruhan hukum pada prinsipnya mempunyai fungsi dan tugas sebagai alat untuk melindungi hak asasi setiap orang maupun kepentingan masyarakat dan negara agar tercapai keseimbangan, ketertiban, ketenteraman dan keamanan dalam menjaga kehidupan masyarakat (Adenan, 1995:74).

Pemanfaatan komputer oleh penjahat dapat digunakan untuk melakukan kejahatan seperti kasus pembobolan BNI New York, BRI Cabang Brigjen Katamso Yogya, BDN Cabang Bintaro Jaya, Bank Danamon Pusat, Bank Danamom Glodok Plaza, percobaan pembobolan Union Bank of Switzerland (UBS), kasus Mustika Ratu dan banyak kasus-kasus lainnya.

Dari uraian kasus-kasus tersebut di atas, dapat diketahui bahwa kejahatan tersebut dilakukan dengan menggunakan peralatan komputer, telekomunikasi dan

informasi, namun landasan hukum yang digunakan adalah KUH Pidana yang belum memasukkan aturan hukum dengan aspek teknologi baru.

Untuk penegakan hukum terhadap *cyber crime* maka ada beberapa tindakan yang dapat dilakukan, seperti membuat peraturan perundang-undangan baru atau menambah beberapa pasal dalam peraturan perundang-undangan yang telah ada dan menentukan yurisdiksinya (Saefullah Wiradipradja dan Danrivanto Budhijanto, 2002:91).

Beberapa negara seperti Amerika Serikat dan Kanada pemanfaatan teknologi informasi telah diatur secara nasional yang kemudian disusul oleh negara-negara yang tergabung dalam Uni Eropa. Di Asia seperti Singapura, India dan Malaysia telah mengatur pula kegiatan-kegiatan di dunia maya ini.

Amerika serikat selain melakukan penyesuaian (berupa amandemen) terhadap undang-undang yang memiliki relevansi dengan teknologi informasi juga dilakukan penyusunan undang-undang baru. Sesuai dengan sistem hukum yang dianut oleh Amerika Serikat, Kanada, Inggris, Singapura, Malaysia, India yaitu system hukum Anglo-Saxon, maka pengaturan mengenai pemanfaatan teknologi informasi dilakukan secara sektoral dan rinci. Setiap undang-undang hanya dimaksudkan untuk mengatur satu kegiatan tertentu saja. Apabila ditinjau dari sudut penerapannya, memang nampak lebih praktis dan terukur, namun kadang-kadang muncul kendala untuk mensinergikan dengan undang-undang lain yang memiliki keterkaitan.

Bagi Indonesia, sesuai dengan sistem hukum yang berlaku (kontinental) kiranya lebih tepat bila pengaturan tetatang pemanfaatan teknologi informasi disusun dalam suatu undang-undang yang bersifat pokok, namun mencakup sebanyak mungkin permasalahan (*umbrella provisions*). Mernurut E. Saefullah Wiradipradja dan Danrivanto Budhijanto(2002:91) Indonesia perlu pengaturan atas kegiatan-kegiatan *cyber space* dilandasi oleh tiga pemikiran utama yaitu:

1. adanya kepastian hukum bagi para pelaku kegiatan-kegiatan di *cyber space* mengingat belum terakomondasinya secara memadai dalam peraturan perundang-undangan yang telah ada.

2. upaya untuk mengantisipasi implikasi-implikasi yang ditimbulkan akibat pemanfaatan teknologi informasi, dan
3. adanya variable global yaitu perdagangan bebas dan pasar terbuka (WTO/GATT)

Berkaitan dengan bentuk pengaturan di dalam *cyber space*, dapat ditinjau dari dua pendekatan, yaitu apakah perlu menciptakan norma-norma baru dan peraturan-peraturan khusus untuk kegiatan/aktivitas di *cyber space* atau apakah cukup diterapkan model-model peraturan yang dikenal di dunia nyata (konvensional) saja.

Apabila diterapkan begitu saja kedua pendekatan tadi, ternyata sulit sekali memberlakukan ketentuan-ketentuan yang berlaku dalam dunia nyata ke dalam dunia maya. Karena ada beberapa ketentuan hukum konvensional yang tidak dapat diterapkan atau sulit untuk diterapkan dalam kegiatan-kegiatan *cyber space*, seperti tentang alat bukti, tandatangan, tempat atau domisili para pihak dalam kontrak, pengertian di muka umum dalam kasus pornografi. Oleh karena itu diperlukan ketentuan-ketentuan khusus dalam beberapa hal tertentu yang bersifat spesifik yang berlaku di *cyber space*.

Untuk mengupayakan peraturan perundang-undangan berkaitan dengan “*computerrelated offences*” menurut Andi Hamzah (1993:43) perlu dilakukan beberapa langkah antara lain:

1. penetapan perbuatan apa yang menjadi interest berbagai pihak;
2. penelitian mengenai, apakah peraturan perundang-undangan yang berlaku dapat digunakan memproses kejahatan komputer dan siber;
3. identifikasi penyalahgunaan komputer dan siber yang melanggar kepentingan masyarakat;
4. identifikasi kepentingan masyarakat yang perlu dilindungi dalam kaitannya dengan penggunaan komputer, informasi dan telekomunikasi;
5. identifikasi dampak penetapan peraturan terhadap aspek sosial dan ekonomi.

Dalam menutup sarannya Andi Hamzah mengingatkan juga agar tidak terjadi “*over criminalization*”.

Dalam rangka penegakan hukum terdapat perbedaan pendapat tentang perlu tidaknya membentuk peraturan perundang-undangan baru dengan merumuskan tindak/perbuatan pidana atau *cyber crime*. (Heru Soeprapto, 2001:14) Muladi dan Himawan dengan alasan masing-masing mengatakan bahwa perumusan kejahatan komputer baru akan selalu ketinggalan dengan cepatnya perkembangan teknologi, undang-undang tradisional masih dapat digunakan, perlu hemat mempergunakan pengaturan baru.

Sementara itu ada yang berpendapat perlunya dibuat ketentuan khusus seperti; Teuku M. Radie, J.E. Sahetapy, Mulya Lubis, Sudama Sastraanjoyo, yang pada pokoknya memberi alasan bahwa hukum pidana yang ada tidak siap menghadapi kejahatan komputer, untuk menghadapi *white collar crime*, tindak pidana komputer adalah pidana khusus oleh karena itu perlu hukum khusus (Yosef Ardi, 2000).

Pada saat pembuatan undang-undang yang berkaitan dengan *cyber space* juga perlu diperhatikan mengenai kompetensi pengadilan dalam menangani perkara *cyber crime*. Mengenai yurisdiksi dalam kegiatan *cyber space* perlu diperhatikan sejauhmanakah suatu negara memberi kewenangan kepada pengadilan untuk mengadili pelaku tindak pidana dalam kegiatan *cyber space*, khususnya dalam pemanfaatan teknologi informasi.

Untuk menuntut seseorang ke pengadilan ada dua hal yang harus diperhatikan (Ny. Tien Saefullah, 2002:100) yaitu;

1. Apakah pengadilan yang bersangkutan berwenang untuk memeriksa suatu perkara? Hal ini menyangkut subject matter jurisdiction, yaitu yurisdiksi yang bersifat mutlak, sehingga tidak dapat disimpangi;
2. Apakah pengadilan yang bersangkutan berwenang untuk memaksakan putusan terhadap orang lain yang bersalah.

Kewenangan pengadilan untuk mengadili perlu diatur terlebih dahulu dengan tujuan untuk mengantisipasi adanya penolakan untuk mengadili dari pengadilan dengan alasan tidak memiliki yurisdiksi untuk mengadili dan menghukum pelaku-pelaku *cyber crime* (*lack of jurisdiction*). Jika terjadi penolakan maka akan terjadi

ketidakadilan dan ketidak pastian hukum, karena pelakunya akan bebas tanpa melalui proses pengadilan. Akibatnya orang akan mengulangi melakukan perbuatan tersebut, bahkan mungkin akan melakukan kejahatan yang lebih berbahaya lagi.

Menurut Darrel Munthe, yurisdiksi di *cyber space* membutuhkan prinsip-prinsip yang jelas dari hukum internasional dan hanya melalui prinsip-prinsip dalam yurisdiksi hukum internasional negara-negara dapat dibebankan untuk mengadopsi pemecahan yang sama terhadap yurisdiksi *cyber space* (Ny. Tien S. Saefullah, 2002:101). Pendapat di atas, dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip yurisdiksi yang berlaku dalam hukum internasional oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuan-ketentuan untuk menanggulangi *cyber crime*.

Selain masalah yurisdiksi perlu juga diatur secara jelas tentang alat-alat bukti yang dapat dipergunakan sebagai beban pembuktian.

Dalam penggunaan *cyber space*, beberapa masalah dalam pembuktian akan timbul misalnya system “*digital signature*” yang berkaitan dengan hukum yang ada. Banyak negara mensyaratkan bahwa suatu transaksi harus disertai dengan bukti tertulis, dengan pertimbangan untuk adanya kepastian hukum.

Permasalahan yang akan terjadi bagaimana sebuah dokumen elektronik yang ditandatangani dengan “*digital signature*” dapatkah dikategorikan sebagai bukti tertulis?. Di Inggris, bukti tertulis haruslah berupa tulisan (*typing*), ketikan (*printing*), litografi (*lithographi*) fotografi, atau bukti-bukti yang mempergunakan cara-cara lain yang dapat memperlihatkan atau mengolah kata-kata dalam bentuk yang terlihat secara kasat mata. Definisi dari bukti tertulis itu sendiri sudah diperluas hingga mencakup juga telex, telegram atau cara-cara lain dalam telekomunikasi yang menyediakan rekaman dari perjanjian. Indonesia sendiri dalam Pasal 26 A Undang-undang No. 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi juga telah memperluas pengertian tentang alat yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) KUHAP.

Dalam Pasal 26 A disebutkan alat bukti yang dalam bentuk petunjuk khusus untuk tindak pidana korupsi juga dapat diperoleh dari:

- a. alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau serupa dengan itu;
- b. dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Dari fakta-fakta tersebut di atas jelaslah bahwa dokumen elektronik yang ditandatangani dengan sebuah "*digital signatuil*" dapat dikategorikan sebagai bukti tertulis. Tetapi terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dari dokumen elektronik atau "*digital signature*" yaitu adanya syarat bahwa dokumen tersebut harus dapat dilihat, dikirim dan disimpan dalam bentuk kertas.

Berkaitan dengan dokumen elektronik juga dapat timbul masalah bagaimana cara untuk menentukan dokumen yang asli dan salinan. Karena telah menjadi prinsip hukum umum bahwa;

- a. dokumen asli mestilah dalam bentuk perjanjian tertulis yang ditandatangani oleh para pihak yang melaksanakan perjanjian;
- b. dokumen asli hanya ada satu dalam setiap perjanjian;
- c. semua reproduksi dari perjanjian tersebut merupakan salinan.

Ketika sebuah perjanjian transaksi menggunakan "*digital signature*" yang disebut sebagai dokumen asli tempat "*digital signature*" itu dibubuhkan pada dasarnya adalah sebuah dokumen elektronik. Dokumen elektronik ini berada dalam memori komputer tempat perjanjian itu dilakukan. Konsekuensinya, setiap hasil print-out dari memori komputer tersebut, baik dalam bentuk kertas atau pun dalam bentuk lain, adalah sebuah salinan yang pada dasarnya tidak akan pernah memiliki nilai kepastian hukum yang sama dengan dokumen aslinya.

Mengingat semakin maraknya *cyber crime* di masa akan datang, maka sudah sepatutnya pemerintah segera mengambil langkah-langkah proaktif untuk menanggulangi dampak negatif yang akan timbul dari *cyber crime*. Untuk itu cara yang terbaik adalah dengan membuat aturan yang jelas dan tegas mengenai *cyber crime* agar terdapat kepastian hukum bagi pihak yang terlibat.

D. PENUTUP

Perkembangan teknologi komputer, telekomunikasi dan informatika di era globalisasi telah melintasi batas-batas wilayah, ini berarti masalah hukum yang berkaitan dengan yurisdiksi dan penegakan serta pemilihan hukum yang berlaku terhadap suatu sengketa multi-yurisdiksi akan bertambah penting dan konflik.

Makin populernya pemakaian internet untuk pelbagai keperluan seperti *e-banking* dan *e-commerce*, telah meningkat terjadinya tindak pidana dibidang ini. Kejahatan dibidang ini meliputi tindak pidana penipuan, penggelapan, *hacking*, pidana di bidang komunikasi, atau pengrusakan system komputer yang belum seluruhnya dapat dijangkau dengan undang-undang yang berlaku.

Kelahiran internet telah membalikkan segalanya, yang jauh jadi dekat, yang khayal jadi nyata, namun dibalik kemergelapan itu, juga melahirkan keresahan-keresahan baru, di antaranya muncul kejahatan yang canggih dalam bentuk "*cyber crime*".

Di dalam dunia perbankan perkembangan *cyber crime* cukup mengejutkan dengan terjadi kasus pembobolan BNI New York oleh mantan karyawannya sendiri, mutasi kredit fiktif melalui komputer di BDN Cabang Bintaro Jaya, pencurian dana di Bank Danamon Pusat. Sementara itu sejumlah nasabah pemegang *credit card* juga mengeluh, karena nomor kartu kreditnya telah dipakai pihak lain untuk melakukan transaksi *e-commerce* sehingga menimbulkan kerugian yang cukup besar. Keresahan-keresahan ini membuat sebahagian masyarakat meminta jaminan keadilan dan kepastian hukum di bidang *cyber space*.

Berkaitan dengan hal tersebut di atas maka dalam menegakkan hukum terhadap *cyber crime* perlu dipikirkan sejauhmana hukum itu harus diatur sehingga tidak menimbulkan permasalahan baru.

Daftar Pustaka

- Adenah M, (1995), *Kejahatan Kerah Putih, sebagai Tindak Pidana*, BPHN Departemen Kehakiman, Jakarta.
- Andi Hamzah (1993), *Hukum Pidana yang Berkaitan dengan Komputer*, Sinar Grafika, Jakarta.
- Barita Saragih (2002), “Tantangan Hukum Atas Aktivitas Internet”, *Kompas Minggu*, 9 Juli 2002.
- Bakat Purwanto (1995), *Bentuk Kejahatan Baru Akibat Perkembangan Iptek*, BPHN, Departemen Kehakiman.
- John Naisbitt (1994), *Global Parado William Marrow and Company*, Mc, New York.
- Suhono Harso (2000), *Tehnologi Informasi dan Ekonomi Digital: Persiapan Regulasi di Indonesia*, Jurusan teknik Elektro, bersifat Teknologi, Bandung.
- Rene L Pattiradjawane (2002), “Media Konvenjensi dan Tantangan Masa Depan, Kompas, 21 Juli 2000.
- Freddy Haris (2001), “ Pengantar Menanti Hukum di *Cyberspace*”, *Jurnal Hukum & Teknologi*, No. 1 Vol. 1 Tahun 2001, LKHT-FHUI, Jakarta.
- Heru Soeprapto (2001), “Kejahatan Komputer dan Siber serta Antisipasi Pengaturan Pencegahannya di Indonesia” *Jurnal Hukum Bisni*, Volume 12, 2001, Yayasan Pengembangan Hukum Bisnis, Jakarta.
- Ismamulhadi (2002), “Penyelesaian Sengketa Dalam Perdagangan Secara Elaktronik” *Cyber Law: Suatu Pengantar*, Pusat Studi Cyber Law, UNPAD, Bandung.
- Mardjono Reksodiputro (2001), *Cybercrime and Intelectual Property*, Bahan Penataran Nasional Hukum Pidana dan Kriminologi Indonesia (ASPEHUPIKI), Fakultas Hukum Universitas Surabaya.

Ny. Tien S. Saefullah (2002), “Yurisdiksi sebagai Upaya Penagakan Hukum dalam Kegiatan *Cyberspace*”, *Cyber Law: Suatu Pengantar*, Pusat Studi *Cyber Law*, UNPAD, Bandung.

Saefullah Wiradipradja, E dan Danrivanto Budhijanto (2002), “ Perspektif Hukum Internasional tentang *Cyber Law*”, *Cyber Law: Suatu Pengantar*, Pusat Studi *Cyber Law*, UNPAD, Bandung, 2002.

Yusuf Andi (2000), “Meroket Bisnis e-Commerce” Kompas, 21 Juli 2000).

PENEGAKAN HUKUM TERHADAP CYBER CRIME

O

L

E

H

Riza Nizarli

Dosen Fakultas Hukum Unsyiah
Darussalam, Banda Aceh