Cybercrime pada Jasa Perbankan di Indonesia*

Oleh :
Vegitya Ramadhani-Putri, SH, S.Ant

Abstrak

Kejahatan melalui media internet merupakan gangguan dan ancaman kejahatan elektronik yang signifikan terhadap Bank Sentral, dan lembaga perbankan/keuangan, penerbit kartu kredit/kartu pembayaran dan lembaga keuangan lainnya, *merchant*, terutama juga nasabah bank. Penelitian ini menggunakan metode penelitian hukum empiris dengan alat dan teknik pengumpulan data melalui observasi, studi pustaka dan wawancara. Diharapkan penelitian ini dapat memberikan sumbangan berupa kajian ilmiah bagi pengembangan ilmu pengetahuan, khususnya pengembangan di bidang disiplin ilmu hukum yang berkaitan dengan hukum perbankan dan hukum telematika. Mengingat peranan yang sangat vital dari lembaga-lembaga keuangan dalam perekonomian dan dalam rangka menjaga tingkat kepercayaan masyarakat terhadap lembaga keuangan, sesungguhnya terdapat beberapa regulasi yang dapat melindungi kesemua pihak tersebut. Perlindungan tersebut dapat dilakukan dengan mengkriminalisasi setiap penggunaan dan akses tanpa hak yang ditujukan terhadap jaringan komputer institusi / perseorangan tersebut secara *illegal*.

Kata Kunci : *cybercrime, e-commerce*, perbankan.

A. Urgensi E-Commerce dalam Perbankan

Aspek-aspek yang paling fundamental dalam *e-commerce* adalah kerahasiaan (*confidentiality*), keotentikan (*authenticity*), integritas (*integrity*), dan tak terbantahkan (*non-repudiation*). Kerahasiaan (*confidentiality*) yakni pesan yang disampaikan, tidak diketahui oleh pihak manapun yang tidak berkepentingan. Keotentikan (*authencity*) yaitu antara pengirim dan penerima pesan sama-sama yakin siapa yang mengirim pesan dan siapa yang menerima pesan berdasarkan verifikasi keontentikan identitas antara pengirim dan penerima. Integritas (*integrity*) yaitu kepastian bahwa pesan yang dikirim oleh pengirim tetap utuh diterima oleh penerima dan tidak diubah oleh siapapun yang tidak berhak. Aspek yang terakhir yaitu *non-repudiation* yakni keaslian pesan dapat dijadikan alat bukti yang sah dan tidak terbantahkan.[1]

* Artikel ini adalah hasil penelitian Insentif Riset yang dibiayai DIPA Unsri tahun anggaran 2008

[1] Badrulzaman, Mariam Darus, 2001, "***E-Commerce* : Tinjauan dari Hukum Kontrak Indonesia**", Jurnal Hukum Bisnis, Vol.12, 2000

Kemajuan di bidang teknologi informasi dan komputer yang didukung dengan semakin lengkapnya infrastruktur informasi secara global, telah mengubah pola dan cara kegiatan masyarakat dalam berbagai aspek. Bagi perekonomian, kemajuan di bidang teknologi tersebut telah menciptakan efisiensi yang luar biasa. Bagi perbankan, hal tersebut telah mengubah strategi dan pola kegiatannya. Tidak dapat dibayangkan apabila perbankan yang mengelola jutaan nasabahnya harus melakukan kegiatannya tersebut secara manual dan tanpa bantuan komputer. Dalam konteks yang lebih luas, terwujudnya bayangan masyarakat tanpa uang tunai *(less cash society)*, mulai menjadi kenyataan. Masyarakat tidak lagi harus menggunakan uang tunai, namun cukup dengan sebuah "kartu pintar" atau "*online transaction*" dengan menggunakan sarana seperti *e-commerce* atau *e-banking*.

Guna mendukung terwujudnya *less cash society* tersebut, maka kehadiran *cyber law* adalah hal mutlak. Kehadiran berbagai regulasi di sektor sistem perbankan – khusunya terkait dengan perlindungan sistem informasi dan transaksi elektronik – dapat menjadi faktor penting dalam upaya mencegah dan memberantas *cybercrime* tersebut serta dapat memberikan *deterren effect* kepada para pelaku *cybercrime* sehingga akan berpikir jauh untuk melakukan aksinya.

B. Ruang Lingkup Kejahatan Telematika (Cyber-Crime)

Dalam implementasinya, transaksi elektronik dilakukan dengan menggunakan *interconnected network* (Internet), yaitu jaringan komputer yang terdiri dari berbagai macam ukuran jaringan yang saling dihubungkan satu sama lain lewat suatu medium komunikasi sehingga para pengguna jaringan dapat berkomunikasi secara elektronik dan dapat saling mengakses semua layanan (*services*) yang disediakan oleh jaringan lainnya. Sedangkan yang dimaksud dengan jaringan komputer adalah gabungan dari berbagai perlengkapan komunikasi dan komputer yang dihubungkan satu sama lain lewat suatu medium komunikasi, sedemikian sehingga semua pemakai jaringan dapat berkomunikasi secara elektronik[2].

Dengan demikian, berbeda dengan transaksi komersial biasa, transaksi *ecommerce* memiliki beberapa karakteristik yang sangat khusus, yaitu[3]:

[2] Purwadi, Daniel H., 1995, **Belajar Sendiri: Mengenal Internet Jaringan Informasi Dunia**, PT. Elex Media Komputindo, Jakarta, hlm. 1.

[3] Sakti, Nufransa Wira, 2001, **Perpajakan Dalam E-Commerce, Belajar Dari Jepang**, dalam Berita Pajak No. 1443/Tahun XXXIII/15 Mei 2001, hlm. 35.

a. Transaksi tanpa batas: Sebelum era Internet, batas-batas geografi menjadi penghalang suatu perusahaan atau individu yang ingin *go-internasional*, sehingga hanya perusahaan atau individu dengan modal besar yang dapat memasarkan produknya ke luar negeri.
b. Transaksi *anonym*: Para penjual dan pembeli dalam transaksi melalui Internet tidak harus bertemu muka satu sama lainnya.
c. Produk digital dan non digital: Produk-produk digital seperti software komputer, musik dan produk lain yang bersifat digital dapat dipasarkan melalui Internet dengan cara men-*download* secara elektronik.
d. Produk barang tak berwujud: Banyak perusahaan yang bergerak di bidang *e-commerce* dengan menawarkan barang tak berwujud seperti data, software dan ide-ide yang dijual melalui Internet.

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime*. The U.S. Department of Justice memberikan pengertian *computer crime* sebagai:"*...any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution*". Pengertian lainnya diberikan oleh Organization of European Community Development, yaitu: "*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*".

Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" (1989) mengartikan *cybercrime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Sedangkan menurut Eoghan Casey[4], "*Cybercrime is used throughout this text to refer to any crime that involves computer and networks, including crimes that do not rely heavily on computer*". Ia mengkategorikan *cybercrime* dalam 4 kategori yaitu:

- *A computer can be the object of Crime.*
- *A computer can be a subject of crime.*
- *The computer can be used as the tool for conducting or planning a crime.*
- *The symbol of the computer itself can be used to intimidate or deceive.*

Kepolisian Republik dalam hal ini unit *cybercrime* menggunakan parameter berdasarkan dokumen kongres PBB tentang *The Prevention of Crime and The Treatment of Offlenderes* di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal :

[4] Casey, Eoghan, 2001, **Digital Evidence and Computer Crime**, London : A Harcourt Science and Technology Company, hlm. 16

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

Dari beberapa pengertian di atas, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada[5], antara lain:

- *Unauthorized Access to Computer System and Service*
  Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

- *Illegal Contents*
  Merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

- *Data Forgery*
  Merupakan kejahatan dengan memalsukan data pada dokumendokumenpenting yang tersimpan sebagai *scripless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

- *Cyber Espionage*
  Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer)

- *Cyber Sabotage and Extortion*
  Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

- *Offense against Intellectual Property*
  Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

- *Infringements of Privacy*
  Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

[5] Panjaitan, Hinca IP dkk, 2005, **Membangun Cyber Law Indonesia yang Demokratis,** Jakarta : IMLPC

C. *Cybercrime* dalam *Electronic Banking (E-Banking)*

Kejahatan dunia maya atau cybercrime umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi[6]. Contoh kejahatan dunia maya di mana komputer sebagai alat adalah spamming, dan kejahatan terhadap hak cipta dan kekayaan intelektual[7]. Contoh kejahatan dunia maya di mana komputer sebagai sasarannya adalah akses ilegal (mengelabui kontrol akses), malware dan serangan DoS[8]. Contoh kejahatan dunia maya di mana komputer sebagai tempatnya adalah penipuan identitas[9]. Sedangkan contoh kejahatan tradisional dengan komputer sebagai alatnya adalah pornografi anak dan judi online.

Dalam UU Perbankan, baik UU No.7 Tahun 1992, maupun UU No.10 Tahun 1998, diatur mengenai kejahatan perbankan antara lain pada pasal-pasal berikut ini:

- Pasal 46 (1): mengenai penghimpunan dana dari dari masyarakat dalam bentuk simpanan tanpa izin usaha dari BI.
- Pasal 47 : terkait dengan rahasia bank
- Pasal 48: informasi / laporan keuangan bank (membuat, memalsukan, menghilangkan,mengubah, mengaburkan, menyembunyikan, dan lain sebagainya
- Pasal 49 (2): meminta atau menerima, mengizinkan menyetujui imbalan, komisi, uang tambahan, pelayanan, dan lain-lain.
- Pasal 50: mengenai pihak terafiliasi

Selanjutnya, ditegaskan pada pasal berikutnya:

- Pasal 51 ayat (1): Tindak pidana sebagaimana dimaksud dalam Pasal 46, 47, 48 (1), 49, Pasal 50, dan Pasal 51 adalah Kejahatan.
- Pasal 51 ayat (2): Tindak pidana sebagaimana dimaksud dalam Pasal 48 ayat (2) adalah Pelanggaran.

---

[6] Purbo, Onno & AA.Wahyudi, 2001, **Mengenal *E-Commerce***, Jakarta : elex Media Komputindo

[7] Mukti Wibowo, Arrianto, 1998, **Tanda Tangan Digital dan Sertifikat Digital : Apa Itu?**, (artikel belum dipublikasikan), Jakarta

[8] Mukti Wibowo, Arrianto, 2000, "**Kejahatan Kartu Kredit via Internet : Hantu E-Commerce?**", (artikel belum dipublikasikan), Jakarta

[9] Sitompul, Asril, 2001, **Hukum Internet (Pengenalan Mengenai Masalah Hukum di *Cyberspace*)**, Bandung : Citra Aditya Bakti.

Berdasarkan kerangka teknis di atas beserta rangkaian protokol yang dibahas pada penelitian ini, sesungguhnya sistem pengaturan melalui hukum positif merupakan kebutuhan yang mendesak guna melindungi pihak-pihak yang terlibat dalam *e-commerce*. Resiko-resiko dalam bisnis ini bisa diminimalisasi apabila ada kepastian hukum yang tegas dan jelas terhadap mekanisme transaksi yang berkarakter *paperless* ini dengan kekuatan hukum yang setara dengan alat bukti yang diakui dalam hukum perjanjian konvensional[10].

D. Pengaturan Transaksi Elektronis dalam Perbankan

Saat ini pemanfaatan teknologi informasi merupakan bagian penting dari hampir seluruh aktivitas masyarakat. Bahkan di dunia perbankan hampir seluruh proses penyelenggaraan sistem pembayaran telah dilaksanakan secara elektronik (*paperless*). Perkembangan teknologi informasi itu telah memaksa pelaku usaha mengubah strategi bisnisnya dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Pelayanan *electronic transaction (e-banking)* melalui ATM, *phone banking* dan *Internet banking* misalnya, merupakan bentuk-bentuk baru dari *delivery channel* pelayanan bank yang mengubah pelayanan transaksi manual menjadi pelayanan transaksi oleh teknologi[11].

Bagi perekonomian, kemajuan teknologi memberikan manfaat yang sangat besar, karena transaksi bisnis dapat dilakukan secara seketika (*real time*), yang berarti perputaran ekonomi menjadi semakin cepat dan dapat dilakukan tanpa hambatan ruang dan waktu. Begitu juga dari sisi keamanan, penggunaan teknologi, memberikan perlindungan terhadap keamanan data dan transaksi. Contoh mengenai hal ini adalah pada saat terjadi berbagai bencana, bank-bank yang berbasis teknologi sangat cepat melakukan *recovery* karena didukung oleh *electronic data back-up* yang tersimpan di lokasi lain, sehingga dengan cepat dapat kembali melakukan pelayanan kepada nasabahnya.

Namun demikian, di sisi lain, perkembangan teknologi yang begitu cepat tidak dapat dipungkiri telah menimbulkan ekses negatif, yaitu berkembangnya kejahatan yang lebih canggih yang dikenal sebagai *Cybercrime,* bahkan lebih jauh lagi adalah dimanfaatkannya kecanggihan teknologi informasi dan komputer oleh pelaku kejahatan untuk tujuan pencucian uang dan kejahatan terorisme.

---

[10] Ustadyanto, Riyeke, 2001, **Framework E-Commerce**, Yogyakarta : Penerbit Andy

[11] Tim Perundang-undangan dan Pengkajian Hukum, Direktorat Hukum Bank Indonesia, Urgensi **Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan**, pada Buletin Hukum Perbankan dan Kebanksentralan, Edisi 16 Volume 4 Nomor 2, Agustus 2006

Bentuk kekhawatiran tersebut antara lain tergambar dalam kasus yang menyedot perhatian dunia baru-baru ini yaitu tindakan yang konon dilakukan oleh Amerika Serikat yang melakukan kegiatan mata-mata secara kontroversial untuk melacak jutaan transaksi keuangan milik warganya melalui data SWIFT secara *illegal*[12].

Apabila kita berbicara mengenai kejahatan berteknologi tinggi seperti kejahatan Internet atau *cybercrime*, seolah-olah hukum itu ketinggalan dari peristiwanya (*het recht hink achter de feiten aan*). Seiring dengan berkembangnya pemanfaatan Internet, maka mereka yang memiliki kemampuan dibidang komputer dan memiliki maksud-maksud tertentu dapat memanfaatkan komputer dan Internet untuk melakukan kejahatan atau "kenakalan" yang merugikan pihak lain.

Dalam dua dokumen Konferensi PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal, yaitu "*cybercrime*" dan "*computer related crime*". Dalam *back ground paper* untuk lokakarya Konferensi PBB X/2000 di Wina, Austria istilah "*cybercrime*" dibagi dalam dua kategori. Pertama, *cybercrime* dalam arti sempit disebut "*computer crime*". Kedua, *cybercrime* dalam arti luas disebut "*computer related crime*". Secara gamblang dalam dokumen tersebut dinyatakan:

a. *Cybercrime 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. *Cybercrime 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.*

Dengan demikian *cybercrime* meliputi kejahatan, yaitu yang dilakukan:

1. dengan menggunakan sarana-sarana dari sistem atau jaringan komputer (*by means of a computer system or network*) ;
2. di dalam sistem atau jaringan komputer (*in a computer system or network*) ; dan
3. terhadap sistem atau jaringan komputer (*against a computer system or network*).

[12] (*Koran Tempo 29 Juni 2008*)

Dari definisi tersebut, maka dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime)*[13]. Sedangkan yang dimaksud dengan computer-related crime adalah "*had been developed to encompass both the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional form of crime that were now being committed with use or assistance of computer aquipment.*[14]

Sementara itu konsep *Council Of Europe* memberikan klasifikasi yang lebih rinci mengenai jenis-jenis *cybercrime*. Klasifikasi itu menyebutkan bahwa *cybercrime* digolongkan sebagai berikut: *Illegal access, Illegal interception, Data interference, System interference, Misuse of Device, Computer related forgery, Computer related fraud, Child-pornography* dan *Infringements of copy rights & related rights*. Dalam kenyataannya, satu rangkaian tindak *cybercrime* secara keseluruhan, unsur-unsurnya dapat masuk ke dalam lebih dari satu klasifikasi di atas. Selanjutnya hal ini akan lebih rinci dalam penjelasan selanjutnya mengenai contoh-contoh *cybercrime*.

Secara garis besar kejahatan-kejahatan yang terjadi terhadap suatu sistem atau jaringan computer dan yang menggunakan computer sebagai *instrumenta delicti*, mutatis mutandis juga dapat terjadi di dunia perbankan. Kegiatan yang potensial menjadi target *cybercrime* dalam kegiatan perbankan antara lain adalah:

1. Layanan pembayaran menggunakan kartu kredit pada situs-situs toko *online*.
2. Layanan perbankan *online* (*online banking*).

Dalam kaitannya dengan *cybercrime,* maka sudut pandangnya adalah kejahatan Internet yang menjadikan pihak bank, *merchant,* toko *online* atau nasabah sebagai korban, dapat terjadi karena maksud jahat seseorang yang memiliki kemampuan dalam bidang teknologi informasi, atau seseorang yang memanfaatkan kelengahan pihak bank, pihak *merchant* maupun pihak nasabah.

[13] Laporan Konfererensi PBB X/2000, 19-7-2000, hlm.26

[14] Barda Nawawi Arief, 2001, **Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan**, Citra Aditya Bakti, Bandung, hlm. 249 – 250.

Beberapa bentuk potensi *cybercrime* dalam kegiatan perbankan antara lain:

a) *Typo site*: pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada seorang korban salah mengetikkan alamat dan masuk ke situs palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi *user* dan *password* korbannya, dan dapat dimanfaatkan untuk merugikan korban
b) *Keylogger/keystroke logger*: modus ini sering terjadi pada tempat mengakses Internet umum seperti di warnet. Program ini akan merekam karakter-karakter yang diketikkan oleh *user* dan berharap akan mendapatkan data penting seperti *user ID* maupun *password*. Semakin sering mengakses Internet di tempat umum, semakin rentan pula terkena modus operandi yang dikenal dengan istilah *keylogger* atau *keystroke recorder* ini. Sebab, komputer-komputer yang berada di warnet digunakan berganti-ganti oleh banyak orang. Cara kerja dari modus ini sebenarnya sangat sederhana, tetapi banyak para pengguna komputer di tempat umum yang lengah dan tidak sadar bahwa semua aktivitasnya dicatat oleh orang lain. Pelaku memasang program *keylogger* di komputer-komputer umum. Program *keylogger* ini akan merekam semua tombol *keyboard* yang ditekan oleh pengguna komputer berikutnya. Di lain waktu, pemasang *keylogger* akan mengambil hasil "jebakannya" di komputer yang sama, dan dia berharap akan memperoleh informasi penting dari para korbannya, semisal *user id* dan *password*.
c) *Sniffing*: usaha untuk mendapatkan *user ID* dan *password* dengan jalan mengamati paket data yang lewat pada jaringan komputer
d) *Brute Force Attacking*: usaha untuk mendapatkan *password* atau *key* dengan mencoba semua kombinasi yang mungkin.
e) *Web Deface*: *system Exploitation* dengan tujuan mengganti tampilan halaman muka suatu situs.
f) *Email Spamming*: mengirimkan *junk* email berupa iklan produk dan sejenisnya pada alamat email seseorang.
g) *Denial of Service*: membanjiri data dalam jumlah sangat besar dengan maksud untuk melumpuhkan sistem sasaran.
h) *Virus, worm, trojan*: menyebarkan *virus, worm* maupun *trojan* dengan tujuan untuk melumpuhkan system komputer, memperoleh datadata dari sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.

Modus yang pernah muncul di Indonesia dikenal dengan istilah *typosite* yang memanfaatkan kelengahan nasabah yang salah mengetikkan alamat bank *online* yang ingin diaksesnya. Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs asli bank *online* (*forgery*). Jika ada nasabah yang salah ketik dan masuk ke situs bank palsu tersebut, maka pelaku akan merekam *user ID* dan *password* nasabah tersebut untuk digunakan mengakses ke situs yang sebenarnya (*illegal access*) dengan maksud untuk merugikan nasabah. Misalnya yang dituju adalah situs www.*klikbca.com*, namun ternyata nasabah yang bersangkutan salah mengetik menjadi www.klickbca.com.

Perbincangan mengenai *cyber law* (ada yang menyebut *cyberspace law*) di Indonesia sudah dimulai sejak pertengahan tahun 1990-an menyusul semakin berkembang pesatnya pemanfaatan Internet. Dilihat dari ruang lingkupnya, *cyberlaw* meliputi setiap aspek yang berhubungan dengan subyek hukum yang memanfaatkan teknologi Internet yang dimulai pada saat mulai "*online*" dan seterusnya sampai saat memasuki dunia maya. Oleh karena itu dalam pembahasan *cyber law*, kita tidak dapat lepas dari aspek yang menyangkut isu prosedural, seperti jurisdiksi, pembuktian, penyidikan, kontrak/transaksi elektronik dan tanda tangan digital/elektronik, pornografi, pencurian melalui Internet, perlindungan konsumen, pemanfaatan Internet dalam aktivitas keseharian manusia, seperti *e-commerce*, *e-government*, *e-tax*, *e-learning*, *e-health*, dan sebagainya[15].

Jonathan Rosenoer, dalam bukunya "*Cyberlaw – The Law of Internet*" menyebutkan bahwa *cyber law* antara lain mencakup hak cipta, hak merek, pencemaran nama baik, fitnah, penistaan, penghinaan, serangan terhadap fasilitas komputer, pengaturan sumberdaya Internet seperti IP-adress, *domain name*, kenyamanan individu, prinsip kehati-hatian termasuk dalam hal ini adalah *negligence*, tindakan kriminal yang menggunakan TI sebagai alat.

Dengan demikian maka ruang lingkup *cyber law* sangat luas, tidak hanya semata-mata mencakup aturan yang mengatur tentang kegiatan bisnis yang melibatkan konsumen (*consumers*), manufaktur (*manufactures*), *service providers* dan pedagang perantara (*intermediaries*) dengan menggunakan Internet *(ecommerce)*. Dalam konteks demikian kiranya perlu dipikirkan tentang rezim hukum baru terhadap kegiatan di dunia maya[16]. Julian Ding dalam bukunya "*E-Commerce: Law & Practice*", mengemukakan bahwa *e-commerce* sebagai suatu konsep yang tidak dapat didefinisikan. Sebagaimana halnya dengan *cyberlaw*, banyak ahli yang berbeda pendapat mengenai *e-commerce*. *E-commerce* memiliki arti yang berbeda bagi orang yang berbeda.

---

[15] *Cyber Law: The field of law dealing with computers and the Internet, including such issues as intellectual-property rights, freedom of expression, and free access to information.* Lihat: Black's law dictionary, 7th edition, 1999

[16] Yang dimaksud dengan hubungan hukum adalah hubungan yang menimbulkan akibat hukum yaitu hak dan kewajiban (Mertokusumo, Sudikno, 1988, *Mengenal Hukum*, Liberty, Jogjakarta, hlm. 97).

Dalam kaitan itu *United Nations Commission on International Trade Law (UNCITRAL)*, telah mengeluarkan *Legal Guide* tentang *Electronic Funds Transfer* dan *Model Law* tentang *International Credit Transfer*. Meskipun tidak bersifat *mandatory*, *model law* tersebut telah banyak dijadikan referensi oleh negara-negara dalam penyusunan Undang-Undang Transfer Dana.

Dalam *The Model Law on Electronic Commerce* yang dikeluarkan oleh *the United Nations Commissions on International Trade Law (UNCITRAL Model Law on Electronic Commerce)* diatur beberapa prinsip berkaitan dengan transaksi elektronik, antara lain:

a. *Information shall not be denied its legal effect, validity or enforceability solely on the grounds that it is in the form of a data message (Article 5).*
b. *Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference (Article 6).*

Di dalam UU ITE disebutkan bahwa transaksi elektronik adalah hubungan hukum[17] yang dilakukan melalui komputer, jaringan komputer atau media elektronik lainnya. Lebih lanjut yang dimaksud dengan komputer adalah alat pemroses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan. Berdasarkan pengertian tersebut, maka transaksi elektronik memiliki cakupan yang sangat luas, baik mengenai subyeknya yaitu setiap orang pribadi atau badan yang memanfaatkan komputer, jaringan komputer atau media elektronik lainnya, maupun mengenai obyeknya yang meliputi berbagai barang dan jasa.

Sebagai perbandingan, dalam regulasi di bidang transaksi eletronik di Singapura yaitu *Electronic Transaction Act* (ETA), ditentukan beberapa prinsip yang berkaitan dengan transaksi elektronik, antara lain:

a. Tidak ada perbedaan antara data elektronik dengan dokumen kertas;
b. Suatu data elektronik dapat menggantikan suatu dokumen tertulis;
c. Para pihak dapat melakukan kontrak secara elektronik;
d. Suatu data elektronik merupakan alat bukti yang sah di pengadilan;
e. Jika suatu data elektronik telah diterima oleh para pihak, maka mereka harus bertindak sebagaimana kesepakatan yang terdapat pada data tersebut.

[17] Golose, Petrus Reinhard, 2006, **Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri**, pada Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006

Kejahatan di cyberspace ini tidak mengenal batas wilayah (*borderless*) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Semua aksi itu dapat dilakukan hanya dari depan komputer yang memiliki akses Internet tanpa takut diketahui oleh orang lain / saksi mata, sehingga kejahatan ini termasuk dalam *Transnational Crime* / kejahatan antar negara yang pengungkapannya sering melibatkan penegak hukum lebih dari satu negara.

Mencermati hal tersebut dapatlah disepakati bahwa 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. Dampak negatif tersebut menimbulkan suatu kejahatan yang dikenal dengan nama "*cybercrime*" yang tentunya harus diantisipasi dan ditanggulangi. Dalam hal ini Polri sebagai aparat penegak hukum telah menyiapkan unit khusus untuk menangani kejahatan *cyber* ini yaitu Unit V IT / Cybercrime Direktorat II Ekonomi Khusus Bareskrim Polri[18].

E. Penutup

Perkembangan teknologi informasi yang demikian pesatnya haruslah di antisipasi dengan hukum yang mengaturnya. Terkait dengan kejahatan terhadap bank dan nasabah bank yang bersangkutan, maka dalam menangani *cybercrime* haruslah melalui pendekatan hukum yang multidisipliner. Pendekatan yang diperlukan bukan hanya pendekatan hukum pidana, namun juga melalui pendekatan hukum perbankan dan hukum telematika. Bagaimanapun kecanggihan suatu sistem, baik sistem teknologi maupun sistem hukum tidak bisa sepenuhnya sempurna sepanjang waktu. Inovasi-inovasi tetap diperlukan untuk menyokong sistem ini untuk dapat bekerja sebagaimana mestinya. Sistem ini tidak pula bisa bermanfaat secara optimal jika sinergi antara sistem teknologi informasi dan hukum telematika tidak berjalan secara harmonis. Penelitian ini diharapkan dapat dijadikan sepotong bagian dari bahan yang dapat digunakan dalam menegakan hukum di berbagai sektor kehidupan manusia, termasuk pada *cyberworld*. Penelitian ini juga bisa menjadi jalan masuk bagi penelitian lebih lanjut mengenai sistem keamanan, perlindungan konsumen *e-commerce*, dan berbagai aplikasi derivatif dari praktek *card-fraud* dalam jasa perbankan.

[18] Golose, Petrus Reinhard, 2006, **Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri**, pada Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006

Daftar Pustaka

Badrulzaman, Mariam Darus, 2001, "***E-Commerce*** **: Tinjauan dari Hukum Kontrak Indonesia"**, Jurnal Hukum Bisnis, Vol.12, 2000

Arief, Barda Nawawi, 2001, **Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan**, Citra Aditya Bakti, Bandung.

Casey, Eoghan, 2001, **Digital Evidence and Computer Crime**, London : A Harcourt Science and Technology Company.

Golose, Petrus Reinhard, 2006, **Perkembangan Cybercrime dan Upaya Penangananya di Indonesia oleh Polri**, pada Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006

Mertokusumo, Sudikno, 1988, *Mengenal Hukum*, Liberty, Jogjakarta.

Panjaitan, Hinca IP dkk, 2005, **Membangun Cyber Law Indonesia yang Demokratis,** Jakarta : IMLPC

Purbo, Onno & AA.Wahyudi, 2001, **Mengenal *E-Commerce***, Jakarta : Elex Media Komputindo

Purwadi, Daniel H., 1995, **Belajar Sendiri: Mengenal Internet Jaringan Informasi Dunia**, PT. Elex Media Komputindo, Jakarta.

Sakti, Nufransa Wira, 2001, **Perpajakan Dalam E-Commerce, Belajar Dari Jepang**, dalam Berita Pajak No. 1443/Tahun XXXIII/15 Mei 2001.

Sitompul, Asril, 2001, **Hukum Internet (Pengenalan Mengenai Masalah Hukum di *Cyberspace*)**, Bandung : Citra Aditya Bakti.

Tim Perundang-undangan dan Pengkajian Hukum, Direktorat Hukum Bank Indonesia, Urgensi **Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan**, pada Buletin Hukum Perbankan dan Kebanksentralan, Edisi 16 Volume 4 Nomor 2, Agustus 2006

Ustadyanto, Riyeke, 2001, **Framework E-Commerce**, Yogyakarta : Penerbit Andy

Koran Tempo , edisi 29 Juni 2008.

United Nations, Laporan Konfererensi PBB X/2000, 19-7-2000.

Wibowo, Arrianto Mukti, 1998, **Tanda Tangan Digital dan Sertifikat Digital : Apa Itu?**, (artikel belum dipublikasikan), Jakarta

Wibowo, Arrianto Mukti, 2000, **"Kejahatan Kartu Kredit via Internet : Hantu E-Commerce?"**, (artikel belum dipublikasikan), Jakarta

Wisnusubroto, 1999, **Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer**, Yogyakata: Universitas Atmajaya

Regulasi :
Kitab Undang-Undang Hukum Pidana
Kitab Undang-Undang Hukum Perdata

UNCITRAL Model Law on *Electronic Commerce*

UU No.14 Tahun 1967, jo UU No.7 Tahun 1992, jo UU No. 10 Tahun 1998 tentang Perbankan
UU No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik