URGENSI *CYBERLAW* DI INDONESIA DALAM RANGKA PENANGAN *CYBERCRIME* DISEKTOR PERBANKAN

Oleh: Nazarudin Tianotak

ABSTRACT

The globalization of information technology has transformed the world into the cyber era by means of the Internet that presents a virtual reality of cyberspace by offering people a variety of expectations and ease. However, behind it, the problem arises in the form of crime called cyber crime. the banking sector not immune from such crimes. This crime (Cyber crime) knows no borders (borderless) and the time of the incident because the victim and the perpetrator are often located in different countries. Cyber crime can be done through a computer network system itself became the target and the computer it self is the means to commit a crime.

The development of information technology should be so rapidly anticipated the laws that govern them. Negative impacts should be anticipated and addressed by the law relating to the use of information and communication technology. Products laws relating to cyber space (cyber space) is needed to provide security and legal certainty in the use of information technology, media, and communications in order to develop optimally.

Keyword : Cyber crime, Banking

A. LATAR BELAKANG.

Saat ini pemanfaatan teknologi informasi merupakan bagian penting dari hampir seluruh aktifitas masyarakat. Bahkan diseluruh dunia perbankan hampir seluruh proses penyelenggaraan sistem pembayaran telah dilaksanakan secara elektronik (*peparless*).

Perkembangan teknologi infrmasi 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 dan *dilevery channel* pelayanan bank yang mengubah pelayanan transaksi manual menjadi pelayanan transaksi oleh teknologi.

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 keamnanan data dan teransaksi.Namun disisi 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. 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 kontraversial untuk melacak jutaan transaksi keungan milik warganya melalui data SWIFT secara illegal.

Dari uraian pada latar belakang tersebut, maka yang menjadi permasalahan dalam tulisan ini adalah : "**Bagaimana Peran *Cyberlaw* Sebagai Upaya Pencegahan dan Pemberantasan Kejahatan Dunia Maya (*Cybercrime*) Disektor Perbankan**"

B. PEMBAHASAN

1. Kejahatan Dunia Maya (*Cybercrime*)

Apabila kita bebrbicara 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 memilki maksud-maksud tertentu dapat memanfaatkan komputer dan internet untuk melakukan kejahatan atau kenakalan yang merugikan pihak lain.

Dalam dua dokumken 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 yangg dikenal yaitu : *"cybercrime"*, dan *"computer related crime".* Dalam bac ground paper untuk lokakarya konfrensi PBB X/2000 di Wina, Austria, istilah *cybercrime* dibagi dalam dua kategori, yaitu pertama, *cybercrime* dalam arti sempit disebut *computer crime*, kedua *cybercrime* dalam arti luas disebut *computer related crime.*

Dalam dokumen tersebut dinyatakan:

a. *Cybercrime in narrow sanse (computer crime): any legal behaviour directed by means of elctronik operations that targets the security of computer system and data procssed by them.*
b. *Cybercime in a broader sense (computer related crime): any ilegal behaviour commited by means on in reltion to, a computer systemor network, including such crime as illegal possesion, offering or distribution by meaans 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. Didalam sistem atau jaringan komputer *(in a computer system or network*) dan
3. Terhadap sistem atau jaringan komputer (*ageinst a computer system or network*).

Dari defenisi tersebut, maka dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer,[1] sedangkan dalam arti luas, cybercrime mencakup seluruh bentuk baru kejahatan yang ditujukan kepada komputer, jaringan komputer dan penggunanya serta bentuk-bentukk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime*).[2] Sementara itu konsep *Council of Europa* memberikan klasifikasi yang lebih rinci mengenai jenis-jenis cybercrime. Klasifikasi itu menyebutkan bahwa cybercrime digolongkan sebagai berikut : *Illegal Accses, Illegal Interception, Data Interference, System Interference, Misuse Of Device, Computer Related Fotgery, Computer Related Froud, Child-Pornography Dan Infringements Of Copy Rihts & Related Rights.* Dalam kenyataannya, satu rangkaian tindak cybercrime secara keseluruhan, unsur-unsurnya dapat masuk kedalam lebih dari satu kalisifikasi di atas.Selanjutnya hal ini akan lebih rinci dalam penjelasan

---

1 (http://en.pendis.depag.go.id/Jurnal/6.achmad tahir.pdf

2 Laporan Konfrensi PBB X/2000, hlm 26 : *The term computer related crime had been developed to encompass both the entirely new forms of crime that were directed at computers, net work and their users, and the more traditional form of crime that were now being commited whit use or assistence of computer aquipment,* dalam Barda Nawawi Arif, 2001, Masalah Penegakkan Hukum & Kebijakan Penanggulangan Kejahatan, Ctra Aditya Bakti, Bandung, hlm.249-250.

selanjutnya mengenai contoh-contoh *cybercrime.*

Secara garis besar kejahatan-kejahatan yang terjadi terhadap suatu sistem atau jariungan komputer dan yang menggunakan komputer sebagai instrumenta dilecti, nutatis mutandis juga dapat terjadi didunia perbankan. Kegiatan yang potensial yang menjadi target *cybercrime* dalam kegiatan perbankan antara lain adalah :

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

Dalam kaitannya dengan *cybercrime*, maka sudut pandangnya adalah kejahatan internet yang menjadikan pihak bank, marchant, toko on-line atau nasabah sebagai korban, yang dapat terjadi karena maksud jahat seseorang yang memiliki kemampuan dalam bidang teknologii informasi, atau seseorang yang memanfaatkan kelengahan pihak bank, pihak marchant maupun pihak nasabah.

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

1. *Typo site*, pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan alamat situs asli. Pelaku menunggu kesempatan jika seseorang korban salah mengetikkan alamat dan masuk kesitus palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi user dan password korbannya, dan dapat dimanfaatkan untuk merugikan korban.
2. *Keylogger/keystroke logger:* Modus lainnya adalah *keylogger*. Hal 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 reco*rder ini. Sebab komputer-komputer yang ada di warnet digunakan berganti-ganti oleh banyak orang. Cara kerja dari modus ini sebenarnya sangat sedrhana, tetapi banyak para pengguna komputer ditempat umum yang lengah dan tidak sadar bahwa semua aktifitasnya dicatat oleh orang lain. Pelaku memasang program *keylogger* dikomputer-komputer umum, program *keylogger* ini akan merekam semua tombol kyboard yang ditekan oleh pengguna komputer berikutnya. Di lain waktu, pemasang *keylogger* akan mengambil hasil "jebakannya" dikomputer yang sama, dan dia berharap akan memperoleh informasi penting dari para korbannya, semisal *user ID* dan *password*.
3. *Sniffing*: usaha untuk mendapatkan *user ID* dan *password* dengan jalan mengamati paket data yang lewat pada jaringan komputer.
4. *Brute Force Attacking*: Usaha untuk mendapatkan *password* atau *key* dengan mencoba semua kombinasi yang mungkin.
5. *Web Deface*: *System Exploitation* dengan tujuan mengganti tampilan halaman muka satu situs.
6. *Email Spamming*: Mengirimkan junk email berupa iklan produk dan sejenisnya pada alamat email seseorang.
7. *Daniel of Service*: Membanjiri data dalam jumlah sangat besar dengan maksud untuk melumpuhkan sistem sasaran.
8. *Virus worm, trojan*: Menyebarkan *virus worm* maupun *trojan* dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.

Contoh *cybercrime* dalam transaksi perbankan yang menggunakan sarana internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan on-line (*on-line banking*). Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan yang dikenal dengan istilah carding. Prosesnya adalah sebagai berikut, pelaku carding

memperoleh data kartu kredit korban secara tidak sah (*illegal interception*)[3], dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko *on-line* (*forgery*). Modus ini dapat terjadi akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesan barang di toko on-line.

Kegiatan yang kedua adalah perbankan on-line (*on-line banking*). Modus yang pernah muncul di indonesia dikenal dengan istilah *typosite* yang memanfaatkan kelengahan nasabahyang salah mengetikkan alamat bank on-line yang ingin diaksesnya.Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs asli bank on-line (*forgery*). Jika ada nasabah yang salah ketik dan masuk ke situs palsu tersebut, maka pelaku akan merekam *user ID* dan password nasabah tersebut untuk digunakan untuk mengaksesnya di situs yang sebenarnya *(illegal accses)* dengan maksud untuk merugikan nasabah.

2. *Cyber Law* dan Urgensi Undang-Undang IT serta Undang-Undang Transfer Dana.

Cyber Law atau ada yang menyebutnya dengan *Cyberspace law* di indonesia sudah dimulai sejak pertengahan tahun 1990-an menyusul semakin berkembang pesatnya pemanfaatan internet.

Dilihat dari ruang lingkupnya, *cyber law* meliputi setiap aspek yang berhubungan dengan subyek hukum yang memanfaatkan teknologi internet yang dimulai pada saat mulai "on-line" dan seterusnya sampai saat memasuki dunia maya. Oleh karena itu dalam pembahasan *cyber law*, kita tidak dapat lepas dari isu yang menyangkut prosedural, seperti yurisdiksi, pembuktian, penyedikan, kontrak/transaksi elektronik dari tanda tangan digital/elektronik, pornografi, pencurian melalui internet, perlindungan konsumen, pemanfaatan internet dalam aktifitas keseharian manusia, seperti *e-commerce, e-government, e-tax, e-leaning, e-health* dan sebagainya. Dengan demikian maka ruang lingkup *cyber law* sangat luas, tidak hanya semata-mata mencakup aturan-aturan yang mengatur kegiatan bisnis yang melibatkan konsumen (*consumers*), manufaktur *(manufactures*), *service providers* dan pedagang perantara *(intermediares*) dengan menggunakan internet (*e-commerce*). Dalam konteks demikian perlu dipikirkan tentang rezim hukum baru terhadap kegiatan didunia maya.

Uncitral Model Law yang dikeluarkan oleh Majelis umum PBB dengan Resolusi 51/162 tanggal 16 Desember 1996 sebagai aturan dasar untuk mengatur keabsahan, pengakuan dan akibat dari pesan-pesan elektronik (*electronic messanging*) yang didasarkan pada penggunaan komputer dalam perdagangan.[4]

Tujuan utama atau tujuan khusus dari model ini adalah :[5]

1. Memberikan aturan-aturan mengenai *e-commerce* yang ditujukan kepada badan-badan legislatif nasional atau badan pembuat undang-undang suatu negara;
2. Memberikan aturan-aturan yang bersifat lebih pasti untuk transaksi-transaksi perdagangan secara elektronik.

Bandingkan dengan *Electronic Transaction Act* (ETA) Singapura yang menentukan beberapa prinsip yang berkaitan dengan transaksi elektronik, antara lain :[6]

---

[3] Beberapa contoh dari *illegal interception* yaitu antara lain : pengguna kartu asli yang tidak diterima oleh pemegang kartu sesungguhnya (*Non Recived Card*), kartu asli hasil curian atau temuan *(lostitolen card*),kartu asli yang diubah datanya *(altered car*d), kartu kredit palsu (*totally counterfiet*), menggunakan kartu kredit polos yang menggunjakan data asli (white pastic card) penggandaan sales draft oleh oknom pedagang kemudian diserahkan pada oknum marchant lainnya untuk disi dengan trannsaksi fiktif (*record of charge pumping atau multiple imprint*), dan lain-lain.

[4] Rafiqul Islam, *Interntional Trade Law,* (London ; LBC, 1999), hlm. 426

[5] Abdul Bakar Munir, *Cyber Law; Policies and Challenges*, (Malysia, Singapura, Hongkong, Butterworths Asia, 1999), hlm. 213.

[6] Tim Perundang-undangan dan Pengkajian Hukum Bank Indonesia,, Buliten Hukum Perbankan dan

1. Tidak ada perbedaan antara data elektronik dengan dokumen kertas;
2. Suatu data elektronik dapat menggantikan suatu dokumen tertulis;
3. Para pihak dapat melakukan kontrak secara elektronik;
4. Suatu data elektronik merupakan alat bukti yang sah dipengadilan;
5. Jika suatu data elektronik telah diterima oleh para pihak, maka mereka harus bertindak sebagaimana kesepakatan yang tardapat dalam data tersebut.

Transaksi elektronik adalah perbuatan hukum yang dilakukan melalui komputer, jaringan komputer atau media elektronik lainnya[7]. Lebih lanjut yang dimaksud dengan komputer adalah alat proses data elektronik, mengetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika dan penyimpanannya.

Berdasarkan pengertian tersebut, maka transaksi elektronik memiliki cakupan yang sangat luas, baik mengenai subyeknya yaitu tiap orang pribadi atau badan yang yang memanfaatkan yang memanfaatkan komputer, jaringan komputer atau media elektronik lainnya, maupun mengenai obyeknya yang meliputi berbagai barang dan jasa.

Dalam implementasinya, transaksi elektronik dilakukan dengan menggunakan *interconected network* (internet), yaitu jaringan komputer yang terdiri dari berbagai macam ukuran jaringan yang saling dihubungkansatu sama lain lewat suatu medium komunikasi secara elektronik dan dapat saling mengakses semua layanan *(services*) yang disediakan oleh jaringan lainnya.[8] Dengan demikian berbeda dengan transaksi, transaksi e-commerce memiliki beberapa karakteristik yang sangat khusus yaitu:[9]

1. Transaksi tanpa batas, sebelum era internet, batas-batas geografi menjadi penghalang suatu perusahaan atau individu yang ingin go-internationl, sehingga hanya perusahaan atau individu dengan modal besar yang dapat memasarkan produknya ke luar negeri;
2. Transaksi anonym, para penjual dan pembeli dalam dalam transaksi internet tidak harus bertemu muka satu sama lainnya.
3. Produk digital dan non digital, produk-produk digital seperti software komputer, musik dari produk lain yang bersifat digital dapat dipasarkan melalui internet dengan ncara mendownload secara elektronik;
4. Produk barang tak berwujud, banyak perusahaan yang bergerak dibidang *e-commerce* dengan menawarkan barang tak berwujud seperti data, *software* dan ide-ide yang dijual melalui internet.

3. Undang-Undang Informasi dan Transaksi Elektronik (ITE)

Kehadiran undang-undang tentang ITE merupakan usaha untuk melindungi baik masyarakat selaku konsumen jasa maupun pelaku industri dalam mengembangkan inovasi produk layanannya, selain itu diharapkan dapat lebih mendorong pengembangan penggunaan teknologi secara lebih meluas serta sekaligus dapat memberikan keamanan serta kepastian hukum dalam seluruh kegiatan transaksi. Dalam kaitannya dengan transaksi keuangan perbankan, sebagai undang-undang yang menjadi payung bagi kegiatan-kegiatan bank terkait dengan media elektronik termasuk mengenai kegiatan transfer dana secara elektronik, maka keberadaan UU ITE dalam menunjang

Kebanksentralan, Volume 4 Nomor 2, Agustus 2006, hlm. 20.

[7] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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

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

sistem kelancaran pembayaran menjadi sangat penting dan sangat besar kontribusinya.

Dalam kaitan dengan upaya pencegahan tindak pidana, ataupun penangan tindak pidana, UU ITE akan menjadi dasar hukum dalam proses penegakan hukum kejahatan-kejahan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.[10]

Beberapa aspek penting yang terkait dengan aspek pidana yang perlu diatur secara jelas antara lain :

1. Tanggung jawab penyelenggara sistem elektronik, perlu dilakukan pembatasan atau limitasi atas tanggung kawab sehingga tanggung jawab peneyelenggara tidak melampau kewajaran;
2. Informasi elektronik dan tanda tangan yang dihasil oleh suatu sistem informaasi, termasuk print out-nya harus dapat menjadi alat bukti dipengadilan;
3. Perlindungan hukum terhadap bank sentral dan lembaga perbankan/keungan, penerbit kartu kredit/kartu pembayaran dan lembaga keungan lainnya dari kemungkinan adanya gangguan dan ancaman kejahatan elektronik;
4. Ancaman pidana yang bersifat *deterren* terhadap tindak kejahatan elektronik *(Cybercime*), sehingga dapat memberikan perlindungan terhadap integritas sistem dan nilai investasi yang telah dibangun dengan alokasi sumber daya yang cukup besar.

4. Perlunya Undang-Undang Transfer Dana

Meskipun *United Nation Commssion on International Trade Law* (UNCITRAL), telah mengeluarkan Legal Guide tentang elektronik Found Tranfer dan Model Law tentang International Credit Transfer dan tidak bersifat mandatory, tetapi banyak dijadikan referensi oleh negara-negara dalam penyusunan undang-undang transfer dana.

Perkembangan kejahatan terorisme dan pencucian uang yang cenderung memanfaatkan proses transfer dana sebagai sarana dalam melaksanakan kejahatannya, maka kegiatan kegiatan transfer dana perlu mendapatkan pengaturannya dalam bentuk undang-undang tersendiri.

Undang-undang transfer dana ini akan mengatur seluruh aspek kegiatan transfer dana secara konfrehensif yang meliputi tata cara, pelaksanaan transfer dana, hak dan kewajiban para pihak, pembuktian dan alat bukti, perizinan penyelenggara transfer dana, pengawasan transfer dana serta perumusan delik dan sanksi pidananya. Selanjutnya undang-undang ini akan menjadi landasan hukum yang sangat penting untuk melengkapi undang-undang terorisme dan undang-undang tindak pidana pencucian uang dalam rangka upaya negara memerangi kejahatan ini, khusunya dalam rangka perizinan, pengawasan dan pengenaan sanksi terhadap kegiatan-kegiatan *remittance* (pengiriman uang) sesuai dengan *Special Recomendation VI* dari *Financial Action Task Force on Mony Loundring* (FATF) yang menyatakan bahwa setiap penyelenggara transfer dana wajib memperoleh izin dari instansi yang berwenang dan dikenakan sanksi administratif, perdata dan pidana, bagi penyelenggara transfer dana yang tidak memiliki izin serta wajib tunduk pada rekomendasi FATF. Hal ini sejalan pula dengan upaya pemerintah Indonesia untuk meratifikasi *International Convention for the Supression of the Finacing of Terrorism 1999* dalam rangka mencegah dan menanggulangi tindak pidana terorisme.

---

[10] T. Nasrullah, (2003:3), *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme.* Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan Jakarta Raya

C. P E N U T U P

Kesimpulan

1. Modus operandi *cybercrime* sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih seksama akan terlihat bahwa banyak di antara kegiatan-kegiatan tersebut memiliki sifat yang sama dengan kejahatan-kejahatan konvensional. Perbedaan utamanya adalah bahwa *cybercrime* melibatkan komputer dalam pelaksanaannya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional.
2. Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.
3. Hambatan-hambatan yang ditemukan dalam upaya melakukan penyidikan terhadap cybercrime antara lain berkaitan dengan masalah perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Upaya-upaya yang dapat dilakukan untuk mengatasi hambatan yang ditemukan di dalam melakukan penyidikan terhadap cybercrime antara lain berupa penyempurnaan perangkat hukum, mendidik para penyidik, membangun fasilitas forensic computing, meningkatkan upaya penyidikan dan kerja sama internasional, serta melakukan upaya penanggulangan pencegahan.

Saran

Beberapa hal yang dapat dijadikan sebagai saran sehubungan dengan penulisan ini adalah sebagai berikut :

1) Undang-undang tentang cybercrime perlu dibuat secara khusus sebagai *lexspesialis* untuk memudahkan penegakan hukum terhadap kejahatan tersebut.
2) Kualifikasi perbuatan yang berkaitan dengan cybercrime disektor perbankan harus dibuat secara jelas agar tercipta kepastian hukum bagi masyarakat khususnya pengguna jasa perbankan.
3) Perlu hukum acara khusus yang dapat mengatur seperti misalnya berkaitan dengan jenis-jenis alat bukti yang sah dalam kasus cybercrime di sektor perbankan, pemberian wewenang khusus kepada penyidik dalam melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan kasus cybercrime disektor perbankan, dan lain-lain.
4) Spesialisasi terhadap aparat penyidik maupun penuntut umum dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan penegakan hukum terhadap cybercrime disektor perbankan.

DAFTAR PUSTAKA

Abdul Bakar Munir, *Cyber Law; Policies and Challenges*, (Malysia, Singapura, Hongkong, Butterworths Asia), 1999.

Abdul Wahid, dan Muhammad Labib, *Kejahatan Mayantara* (*Cybercrime*), (Bandung: Rafika Aditama). 2005.

Andi, Hamzah, *Aspek-aspek Pidana di Bidang Komputer*: Jakarta: Sinar Grafika. 1990.

Barda Nawawi Arif, 2001, Masalah Penegakkan Hukum & Kebijakan Penanggulangan Kejahatan, Ctra Aditya Bakti, Bandung,.

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

Didik M. Mansur Arief dan Elisatris Gultom,. *Cyber law: Aspek Hukum Teknologi Informasi*: Bandung: Refika Aditama. 2005

Edmon, Makarim,. *Komplikasi Hukum Telematika.* Jakarta: RajaGrafindo. 2003.

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

Romli, Atmasasmita, *Terori Kapita Selekta Kriminologi*. Bandung: Refika Aditama. 2005.

Rafiqul Islam, *Interntional Trade Law*, (London ; LBC, 1999)

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik