PERLINDUNGAN HUKUM PIDANA TERHADAP NASABAH BANK DALAM PENGGUNAAN FASILITAS INTERNET BANKING ATAS TERJADINYA CYBER CRIME

SKRIPSI

YUDI PRATAMA TANJUNG
07140193

FAKULTAS HUKUM
UNIVERSITAS ANDALAS
PADANG
2011

LEMBAR PENGESAHAN
No. Reg. 3399/PK IV/ 08/ 2011

PERLINDUNGAN HUKUM PIDANA TERHADAP NASABAH BANK DALAM PENGGUNAAN FASILITAS *INTERNET BANKING* ATAS TERJADINYA *CYBER CRIME*

Disusun Oleh:

Yudi Pratama Tanjung
07 140 193

Program Kekhususan : Hukum Pidana (PK IV)

Telah Dipertahankan Di depan Tim Penguji Pada Tanggal 08 Agustus 2011

Yang Bersangkutan Telah Dinyatakan Lulus Oleh Tim Penguji, Terdiri Dari:

Dekan	**Pembantu Dekan 1**
Prof. Dr. Yuliandri, SH, MH.	**Yoserwan, SH, MH, LLM.**
NIP. 196207181988101001	**NIP. 196212311989011002**
Pembimbing I	**Pembimbing II**
Apriwal Gusti, SH	**Yusrida, SH, MH**
NIP. 195304181981031001	**NIP. 195910071986032001**
Penguji I	**Penguji II**
Fadillah Sabri, SH, MH	**Yoserwan, SH, MH, LLM**
NIP. 195901111986031002	**NIP. 196212311989011002**

PERLINDUNGAN HUKUM PIDANA TERHADAP NASABAH BANK DALAM PENGGUNAAN FASILITAS *INTERNET BANKING* ATAS TERJADINYA *CYBER CRIME*

(Yudi Pratama Tanjung, 07140193, Fakultas Hukum, Universitas Andalas, 84 hlm, 2011)

ABSTRAK

Lembaga Keuangan pada dasarnya mempunyai peran yang sangat strategis dalam mengembangkan perekonomian suatu bangsa. Di era globalisasi dan informasi, lembaga keuangan dalam hal ini perbankan memberikan layanannya tidak saja melalui model-model konvensional, tetapi kini sudah mulai beralih pada pemanfaatan teknologi informasi. Perkembangan teknologi informasi, telekomunikasi, dan internet menyebabkan mulai munculnya aplikasi bisnis yang berbasis internet. Salah satu aplikasi yang paling banyak digunakan saat ini adalah *Internet Banking*. Oleh karena itu perlu diketahui bagaimana perlindungan hukum pidana yang diberikan kepada nasabah bank pengguna fasilitas *internet banking* atas terjadinya *cyber crime* dan siapa yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik ? Penelitian ini bersifat yuridis-normatif, teknik pengumpulan data melalui studi kepustakaan dan alat pengumpulan data dalam bentuk studi dokumen. Dari penelitian yang penulis lakukan dapat disimpulkan bahwa perlindungan hukum terhadap nasabah diawali dari perlindungan hukum yang dibuat oleh internal bank sendiri sebagai penyelenggara sistem elektronik *internet banking*, namun aturan yang dibuat sepihak oleh pihak bank cenderung menguntungkan pihak penyusun dan pembentuk aturan itu sendri. Perlindungan hukum juga diberikan oleh hukum pidana terhadap nasabah bank pengguna fasilitas *internet banking* melalui ketentuan-ketentuan pidananya dengan menjerat pelaku yang melakukan *cyber crime* landaskan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transkasi Elektronik. Mengenai yang bertanggungjawab atas segala akibat hukum yang terjadi dalam pelaksanaan transaksi elektronik juga diatur oleh Pasal 21 ayat (2), (3), (4) dan (5) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Untuk menentukan pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik, diperlukan suatu proses pembuktian yang sesuai dengan undang-undang. Sebelum dibawa kedepan persidangan untuk pembuktian, bukti elektronik haruslah melalui pengolahan terlebih dahulu. Pengolahan ini dilakukan melalui suatu cabang ilmu hukum pidana yang disebut komputer forensik. Dalam penelitian ini penulis tidak menemukan adanya suatu Undang-Undang khusus yang memberikan perlindungan hukum pidana terhadap nasabah bank terutama pengguna fasilitas *internet banking*, maka penulis menilai diperlukannya suatu peraturan khusus yang memberikan perlindungan terhadap nasabah bank, terutama pengguna fasilitas *internet banking*.

KATA PENGANTAR

Syukur Alhamdulillah, berkat rahmat dan hidayah Allah SWT, skripsi yang berjudul **"Perlindungan Hukum Pidana Terhadap Nasabah Bank Dalam Penggunaan Fasilitas *Internet Banking* Atas Terjadinya *Cyber Crime*"** dapat diselesaikan oleh penulis. Skripsi ini merupakan tugas akhir yang diajukan untuk meraih gelar Sarjana Hukum (S.H) pada Fakultas Hukum Universitas Andalas Padang. Shalawat beriring salam juga penulis sampaikan kepada Rasulullah SAW.

Dengan penuh rasa hormat, pada kesempatan ini penulis menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada Papa Dedy Defriady dan Mama Susi Delmiati dan Bunda Chandrawati Martini yang ananda cintai dan banggakan, yang telah mendidik dan membesarkan ananda dengan penuh kasih saying dan dukungannya, yang telah bekerja keras secara moril dan materil demi kelanjutan studi ananda. Adikku Fajar Riandi Tanjung, Fadhil Maulana Tanjung, dan Calista Putri Chanda Dedi. Selanjutnya kepada Paman Errozyan August dan Bibi Susy Bhudiharty yang telah banyak memberi dukungan moril maupun materil dalam penulisan skripsi ini. Serta penulis mengucapkan terima kasih yang sedalam-dalamnya kepada yang terhormat :

1. Bapak Prof. Dr. Yuliandri, S.H, M.H selaku Dekan Fakultas Hukum,
2. Bapak Yoserwan S.H, M.H, LLM selaku Pembantu Dekan I, Bapak Frenadin Adegustara S.H, M.H, selaku Pembantu Dekan II, dan Bapak Kurniawarman selaku Pembantu Dekan III.
2. Bapak Prof. Dr. Ismansyah S.H, M.H selaku Ketua Jurusan Bagian Pidana Fakultas Hukum Universitas Andalas Padang dan Ibu Nelwitis S.H, M.H

selaku Sekretaris Jurusan Bagian Pidana Fakultas Hukum Universitas Andalas Padang.

3. Bapak Apriwal Gusti S.H selaku Pembimbing I dan Ibu Yusrida S.H, M.H selaku Pembimbing II yang telah meluangkan waktu dan fikirannya serta memberikan petunjuk dan nasehat yang sangat berguna untuk hasil terbaik penulisan skripsi ini.
4. Bapak Ibu Dosen dan seluruh staf pengajar Fakultas Hukum Universitas Andalas Padang atas ilmu yang telah diberikan kepada penulis.
5. Seluruh staf karyawan dan karyawati Fakultas Hukum Universitas Andalas Padang.
6. Kerabat serta rekan-rekan angkatan 2007 yang penulis cintai, terutama teman-teman terdekat penulis, Adri, Niko, Ifri, Aji, Dona, Valery, Prima, Havis, Resi, Dini, yang telah memberikan semangat dalam penulisan skripsi ini.
7. Sahabat penulis diluar fakultas hukum Rani Monariska, Novia Sari, Silvia Anugrah, Intan Dwi Sartika, dan Eka Hamdani.

Untuk semua rekan yang tidak dapat penulis sebutkan namanya satu persatu, juga penulis ucapkan terima kasih kepada semua pihak yang telah membantu penulis. Hanya Allah sajalah yang akan membalas kebaikan-kebaikan tersebut.

Penulis menyadari bahwa kesempurnaan hanya milik-Nya dan skripsi ini jauh dari kesempurnaan. Karena itu, penulis berharap adanya kritik dan saran yang bersifat membangun demu perbaikan di masa yang akan datang, semoga skripsi ini bermanfaat bagi pembaca.

Padang, Juli 2011

Penulis

Yudi Pratama Tanjung

DAFTAR ISI

ABSTRAK..... i

KATA PENGANTAR..... ii

DAFTAR ISI v

BAB I PENDAHULUAN..... 1

A. Latar Belakang..... 1

B. Perumusan Masalah..... 11

C. Tujuan Penelitian..... 11

D. Manfaat Penelitian..... 12

E. Kerangka Teoritis..... 12

F. Kerangka Konseptual..... 13

G. Metode Penelitian..... 16

BAB II TINJAUAN PUSTAKA..... 19

A. Pengertian Nasabah Bank..... 19

B. Asas dan Tujuan Perlindungan Nasabah..... 19

C. Bank Selaku Penghimpun Dana Masyarakat..... 21

1. Pengertian Bank..... 21

2. Fungsi Bank..... 21

3. Usaha Bank Umum..... 22

D. Kewajiban Bank Dalam Penyelenggaraan *Internet Banking*..... 23

E. Pengertian *Internet Banking*..... 26

F. Perkembangan *Cyber Crime*..... 32

BAB III HASIL DAN PEMBAHASAN..... 42

A. Perlindungan Hukum Pidana Terhadap Nasabah Bank Dalam Penggunaan Fasilitas *Internet Banking* Atas Terjadinya *Cyber Crime*..... 42

1. Prosedur Dan Perlindungan Hukum Pengguna Fasilitas *Internet Banking* Ditinjau Dari Pengaturan Internal Oleh Bank..... 42
2. Ketentuan Pidana Penggunaan Fasilitas *Internet Banking* Yang Berkaitan Dengan *Cyber Crime*..... 55

B. Yang Bertanggungjawab Atas Akibat Hukum Dalam Pelaksanaan Transaksi Elektronik Menurut Undang-Undang Informasi Dan Transaksi Elektronik 67

BAB IV PENUTUP..... 82

A. Kesimpulan..... 82

B. Saran..... 83

DAFTAR PUSTAKA

BAB I

PENDAHULUAN

A. Latar Belakang

Peradaban dunia pada masa kini dicirikan dengan fenomena kemajuan teknologi informasi dan globalisasi yang berlangsung hampir di semua bidang kehidupan. Globalisasi pada dasarnya bermula dari awal abad ke-20, yakni pada saat terjadi perubahan dari sisi transportasi dan elektronika yang menyebarluaskan dan mempercepat perdagangan antar bangsa, disamping pertambahan dan kecepatan lalu lintas barang dan jasa.[1]

Perubahan-perubahan yang dibawa oleh arus globalisasi menimbulkan dampak, baik yang bersifat positif maupun negatif. Siapapun di belahan dunia ini, baik negara-negara maju maupun negara-negara berkembang (*developed/under-developed countries*), tidak ada pilihan lain untuk menghadapi arus globalisasi termasuk dampak negatifnya. Salah satu dampak negatif yang ditimbulkan oleh proses globalisasi adalah munculnya kejahatan-kejahatan yang berdimensi global, seperti penyelundupan, pembajakan (*piracy/hijacking*), pencucian uang (*money laundering*), *human trafficking*, terorisme dan *cyber crime*.[2]

Begitu juga di dunia perbankan. Peran teknologi disini sangatlah mutlak, kemajuan suatu sistem perbankan sudah barang tentu ditopang oleh peran teknologi informasi. Semakin berkembang dan kompleksnya fasilitas yang diterapkan perbankan untuk memudahkan pelayanan, itu berarti semakin beragam dan kompleks adopsi teknologi yang dimiliki oleh suatu bank. Tidak dapat

---

[1] Gultom, Elisatris dan Dikdik M. Arief Mansur, *Cyberlaw Aspek Hukum Teknologi Informasi,* PT Refika Aditama, Bandung, 2009, hlm 1

[2] Al. Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika,* Atma Jaya Yogyakarta, Yogyakarta, 2010, hlm 91

dipungkiri, dalam setiap bidang termasuk perbankan penerapan teknologi bertujuan selain untuk memudahkan operasional intern perusahaan, juga bertujuan untuk semakin memudahkan pelayanan terhadap *customers*. Apalagi untuk saat ini, khususnya dalam dunia perbankan hampir semua produk yang ditawarkan kepada *customers* serupa, sehingga persaingan yang terjadi dalam dunia perbankan adalah bagaimana memberikan produk yang serba mudah dan cepat.[3]

Kemajuan dan perkembangan teknologi, khususnya telekomunikasi, multimedia dan teknologi informatika (telematika) pada akhirnya dapat merubah tatanan organisasi dan hubungan sosial kemasyarakatan. Dimana masyarakat berubah juga karena telah terbiasa dengan keadaan yang praktis hingga tidak mau merepotkan diri serta meluangkan waktu untuk mengunjungi tempat-tempat yang seharusnya didatangi untuk melakukan transaksi. Hal ini tidak dapat dihindari, karena fleksibilitas dan kemampuan telematika dengan cepat memasuki berbagai aspek kehidupan manusia.

Salah satu bentuk perkembangan teknologi informasi yang dapat berguna bagi kemajuan industri perbankan adalah internet. Internet merupakan jaringan komputer global di dunia yang saat ini digunakan oleh jutaan orang di seluruh penjuru dunia. Melalui internet seseorang dapat berkomunikasi, memperoleh berbagai macam komunikasi yang dibutuhkan dan bahkan dapat melakukan perdagangan dengan pihak yang berada di belahan dunia lain dengan cepat dan mudah. Internet telah menghadirkan realitas kehidupan baru menjadi tidak terbatas. Dengan media internet orang dapat melakukan berbagai aktivitas yang dalam dunia nyata sulit dilakukan, karena terpisah oleh jarak, menjadi lebih

---

[3] Ronny Prasetya, *Pembobolan ATM Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan,* Pustaka Publisher, Jakarta, 2010, hlm 25

mudah. Suatu realitas yang berjarak berkilo-kilo meter dari tempat kita berada, dengan media internet dapat dihadirkan di hadapan kita. Kita dapat berbelanja, berbincang-bincang, belajar, melakukan transaksi bisnis, dan berbagai aktivitas lain layaknya dalam kehidupan nyata.[4]

Melalui penggunaan internet sebagai pertukaran informasi di bidang komunikasi, maka waktu dan tempat bukanlah menjadi penghalang untuk melakukan transaksi perbankan. Oleh karenanya internet banyak dipergunakan dalam kegiatan perbankan di berbagai negara maju, sebagai alat untuk mengaskses data maupun informasi dari seluruh penjuru dunia. *Electronic Fund Transfer* (EFT) merupakan salah satu contoh inovasi dan penggunaan teknologi internet yang mendasar dalam Teknologi Sistem Informasi (TSI) di bidang perbankan. Contoh dari produk EFT antara lain meliputi Anjungan Tunai Mandiri (ATM), *electronic home banking* (biasa disebut *internet banking*), dan *money transfer network*. Kejahatan *internet banking* juga merupakan salah satu kejahatan di dalam dunia maya atau disebut sebagai *cyber crime* di bidang perbankan.[5]

Internet banking adalah layanan perbankan yang memungkinkan nasabah melakukan transaksi perbankan melalui internet, dan pada situs yang bersangkutan disediakan layar-layar untuk melakukan transaksi.[6] Sekarang ini *internet banking* bukan lagi menjadi sebuah istilah yang asing bagi masyarakat Indonesia khususnya yang tinggal di wilayah perkotaan. Hal ini disebabkan semakin banyaknya perbankan nasional yang menyediakan layanan tersebut. Di masa mendatang, layanan ini tampaknya bukan lagi layanan yang akan

---

[4] Labib, Mohammad dan Abdul Wahid, *Kejahatan Mayantara (cyber crime)*, Refika Aditama, Bandung, 2005, hlm 74

[5] *Ibid,* hlm 26

[6] Tb. Irman S, *Anatomi Kejahatan Perbankan*, MQS Publishing, Bandung, 2006, hlm 197

memberikan keuntungan bagi bank yang menyelenggarakannya, melainkan sudah seperti keharusan. Keadaannya akan sama seperti pemberian fasilitas ATM. Semua bank akan menyediakan fasilitas tersebut. Namun, tampaknya dibalik perkembangan ini terdapat berbagai permasalahan hukum yang mungkin kemudian hari dapat merugikan masyarakat jika tidak diantisipasi dengan baik.

Layanan yang diberikan *internet banking* kepada nasabah berupa transaksi pembayaran tagihan, informasi rekening, pemindahbukuan antar rekening, infomasi terbaru mengenai suku bunga dan nilai tukar valuta asing, administrasi mengenai perubahan *Personal Identification Number* (PIN), alamat rekening atau kartu, data pribadi dan lain-lain, terkecuali pengambilan uang atau penyetoran uang. Karena untuk pengambilan uang masih memerlukan layanan ATM dan penyetoran uang masih memerlukan bantuan bank cabang.[7]

Praktik *internet banking* ini jelas akan mengubah strategi bank dalam berusaha. Setidaknya ada faktor baru yang bisa mempengaruhi pengkajian suatu bank untuk membuka cabang baru atau menambah ATM. *Internet banking* memungkinkan nasabah untuk melakukan pembayaran-pembayaran secara *online*. *Internet banking* juga memberikan akomodasi kegiatan perbankan melalui jaringan komputer kapan saja dan dimana saja dengan cepat, mudah dan aman karena didukung oleh sistem pengamanan yang kuat. Hal ini berguna untuk menjamin keamanan dan kerahasian data serta transaksi yang dilakukan oleh nasabah. Selain itu, dengan *internet banking*, bank bisa meningkatkan kecepatan layanan dan jangkauan dalam aktivitas perbankan. Dalam perkembangan teknologi perbankan seperti *internet banking*, pihak bank harus memperhatikan

[7] *Ibid,* hlm 28

aspek perlindungan nasabah khususnya keamanan yang berhubungan dengan privasi nasabah. Keamanan layanan *online* ada empat, yaitu keamanan koneksi nasabah, keamanan data transaksi, keamanan koneksi *server*, dan keamanan jaringan sistem informasi dari *server*. Selain itu, aspek penyampaian informasi produk perbankan sebaiknya disampaikan secara proporsional, artinya bank tidak hanya menginformasikan keunggulan atau kekhasan produknya saja, tapi juga sistem keamanan penggunaan produk yang ditawarkan.

Pengamanan *internet banking* berupa pemakaian sistem *firewall* untuk pembatasan akses. Pengamanan berlapis ini, tentu saja ditambah dengan keamanan yang dipunyai oleh setiap nasabah berupa identitas pengguna (*user ID*) dan PIN. Ditambah lagi dengan program *Secure Sockets Layer*[8] (SSL) 3.0 dengan sistem pengacakan 128 *bit*. Pengaman tersebut oleh bank disesuaikan dengan standar internasional. Meskipun demikian, masih banyak nasabah yang ragu menggunakan *internet banking* dengan berbagai alasan, beberapa diantaranya yaitu pertama mengenai kapasitas jaringan internetnya, jika berjuta-juta orang mengakses bank yang sama dan dalam waktu yang bersamaan. Ada dua kemungkinan, nasabah akan kecewa mengira komputernya rusak atau sistem yang dibangun tidak mampu menampung serbuan transaksi tersebut. Alasan kedua adalah kenyamanan nasabah tidak maksimal dalam melakukan transaksi di internet. Nasabah bank biasanya tidak berani melakukan usaha terhadap uangnya yang tersimpan di kas bank. Kekhawatiran nasabah adalah takut salah tekan tombol sehingga uangnya melayang dari rekening. Terakhir mengenai sistem keamanan yang dibangun perbankan itu sendiri. Keamanan sistem informasi

[8] *Ibid*, hlm 29

bisnis perbankan pada dasarnya merupakan bisnis yang berisiko tinggi. Terdapat sedikitnya 8 macam resiko utama yang berkaitan dengan aktivitas perbankan, yaitu strategi, reputasi, operasional (termasuk yang disebut resiko transaksi dan legal), kredit, harga, kurs, tingkat bunga, dan likuiditas. Di samping itu, penggunaan Teknologi Sistem Informasi (TSI) terdapat resiko yang bersifat teknis dan khusus, yang berbeda dengan penggunaan sistem manual. Resiko yang dimaksud antara lain resiko kekeliruan pada tahap pengoperasian, resiko akses oleh pihak yang tidak berwenang, resiko kehilangan atau kerusakan data.

Berbagai upaya preventif memang telah diterapkan oleh kalangan perbankan di Indonesia yang menyelenggarakan layanan *internet banking*. Misalnya, dengan diberlakukannya fitur faktor bukti otentik kedua (*two factor authentication*) yang menggunakan *token*. Penggunaan *token* ini akan memberikan keamanan yang lebih tinggi dibandingkan bila hanya menggunakan nama nasabah pengguna layanan *internet banking* (*username*), PIN, dan *password* saja. Akan tetapi dengan adanya penggunaan *token* ini, tidak berarti transaksi *internet banking* bebas dari resiko.[9]

Dalam praktek *internet banking* terdapat berbagai macam serangan atau ancaman bagi pihak pengguna dan penyedia layanan *internet banking*. Contohnya serangan seperti *man in the middle attack* dan *trojan horses* dapat mengganggu keamanan layanan. Gambaran umum dari aktifitas yang sering disebut *man in the middle attack* yaitu penyerang membuat sebuah *website* dan membuat nasabah pengguna layanan *internet banking* atau *user* masuk ke *website* tersebut. Agar berhasil mengelabui *user, website* tersebut harus dibuat semirip mungkin dengan

[9] *Ibid,* hlm 30

website bank yang sebenarnya. Kemudian *user* memasukkan *password*-nya, dan penyerang kemudian menggunakan informasi ini untuk mengakses *website* bank yang sebenarnya. Untuk mengecoh *token*, penyerang dapat mengirimkan *challenge-response* kepada *user* sebelum melakukan transaksi ilegal. Sedangkan, *trojan horses* adalah program palsu dengan tujuan jahat, yang disusupkan kepada sebuah program yang umum dipakai. Di sini para penyerang meng-*install trojan* kepada komputer *user*. Ketika *user* mulai *login* ke *website* banknya, penyerang menumpangi sesi tersebut melalui *trojan* untuk melakukan transaksi yang diinginkannya. Untuk mencegah serangan-serangan tersebut, bank penyedia layanan *internet banking* perlu melakukan sosialisasi aktif dan intensif kepada para nasabahnya mengenai penggunaan layanan jasa *internet banking* yang baik dan aman. Selain itu, diperlukan suatu ketentuan yang mengatur perbankan nasional yang memiliki pusat penyimpanan, melakukan proses data atau informasi dan transaksi perbankan. Serta perlu dibentuk sebuah unit kerja khusus atau divisi pengamanan dan pencegahan kejahatan perbankan di dalam struktur bank tersebut dan Bank Indonesia yang fungsinya untuk melakukan penerapan kebijakan pengamanan sistem, melakukan penelitian untuk pencegahan terhadap ancaman atau kejahatan yang sudah ada maupun yang mungkin terjadi dan melakukan tindakan pemulihan (*recovery*) serta pemantauan transaksi perbankan selama 24 jam.[10]

Dalam rangka melakukan pengawasan terhadap perbankan, Bank Indonesia perlu melakukan audit terhadap sistem teknologi informasi dan komunikasi yang digunakan oleh perbankan untuk setiap kurun waktu tertentu.

---

[10] *Ibid,* hlm 31

Serta melakukan *training* mengenai pemahaman dan pengendalian akses nasabah maupun pegawai perbankan tentang jaringan sistem *internet banking*, agar seluruh pegawai perbankan mengetahui bahwa merekapun juga di pantau. Juga diperlukan ketentuan (Peraturan atau UU) agar perbankan bertanggung jawab dengan mengganti uang nasabah yang hilang akibat kelemahan sistem pengamanan *internet banking*, misalnya perbankan lalai meningkatkan sistem pengamanan *internet banking*. Terakhir, perlu digunakan perangkat lunak seperti komputer deteksi untuk aktifitas rekening nasabah, agar apabila terjadi kejanggalan transaksi, seperti pengambilan uang nasabah yang melampaui jumlah tertentu, sehingga dapat ditangani dengan cepat. Menambah persyaratan formulir identitas pada waktu pembukaan rekening baru untuk pemeriksaan pada *data base* yang menghimpun daftar orang bermasalah dengan institusi keuangan. Saat ini sudah terdapat teknologi dan peraturan hukum yang dapat membuat *internet banking* menjadi aman, akan tetapi pihak perbankan dan pemerintah perlu terus mengupayakan agar penyelenggaraan *internet banking* lebih aman dan terjamin.[11]

Terdapat beberapa hal yang dapat dilakukan pihak perbankan untuk meningkatkan keamanan *internet banking* misalnya melakukan standardisasi dalam perbuatan aplikasi *internet banking*. Contohnya, formulir *internet banking* yang mudah dipahami, sehingga *user* dapat mengambil tindakan yang sesuai, dan membuat buku panduan bila terjadi masalah dalam *internet banking* serta memberi informasi yang jelas kepada *user*.[12]

Walaupun begitu ketat pengamanan yang dilakukan oleh pihak bank namun ada saja celah yang dapat dimanfaatkan untuk melakukan suatu tindakan

---

[11] *Ibid,* hlm 32
[12] *Ibid*

kriminal. Hal ini terlihat dari berbagai kasus pemboboloan rekening nasabah melalui internet banking. Seperti yang terjadi pada tanggal 26 Agustus 2010 pada Rahmawati (24), salah seorang nasabah Permata Bank cabang Balikpapan. Rahmawati menabung di Permata Bebas dengan nomor rekening 4000878345. Ia sangat terjekut ketika mengetahui saldo rekeningnya tinggal Rp. 4.471,00 dari Rp. 31.996.950,00. Setelah diminta *print out* rekening dari pihak Bank Permata , diketahui telah ada orang lain yang menggunakan akun milik Rahmawati di layanan PermataNet. Orang tersebut tampaknya mengetahui persis semua data rekening milik Rahma, seperti *username* (nama yang digunakan di layanan tersebut), *password* (kata sandi), termasuk PIN / *Personal Indentification Number* (nomor identifikasi). Si pembobol beraksi pada 26 Agustus 2010 pukul 21.40 WIB, lalu beberapa jam kemudian, yaitu pada 27 Agustus 2010 pukul 00.30 dan 00.36. Menurut keterangan pengacara korban seluruhnya ada tiga transaksi yang dilakukan, masing-masing senilai Rp. 9.175.000,00 lalu Rp.9.190.000,00 kemudian terakhir Rp. 9.150.000,00. Transaksi pertama masuk ke rekening nomor 4100697381 atas nama Kerry Sunbadji, yang kedua dikirim ke rekening nomor 8010437785 atas nama Junaidi Halim, dan yang ketiga masuk ke rekening nomor 1210415331 atas nama Arif Aulia. Atas laporan Rahma ke Polresta Balikpapan tanggal 1 September 2010, maka ketiga rekening tersebut diblokir oleh Bank Permata.[13]

Praktek *internet banking* telah berlangsung tanpa didukung aturan yang memadai, baik regulasi yang dibuat oleh pemerintah selaku pembentuk peraturan perundang-undangan maupun oleh Bank Indonesia.

---

[13] Dikutip dari http://www.republika.co.id/berita/br...ah-rp-255-juta. Diakses tanggal 1 Februari 2011.

Kekosongan hukum dalam praktek *internet banking* dapat menimbulkan implikasi hukum sebagai berikut :

1. Tidak adanya pedoman yang jelas dan tegas bagi bank yang menyelenggarakan *internet banking;*
2. Tidak adanya kejelasan mengenai hak, kewajiban dan tanggung jawab dari pihak-pihak terkait dengan kegiatan *internet banking* yang meliputi bank, nasabah, dan pihak ketiga;
3. Setiap bank dengan leluasa dapat menetapkan aturan-aturannya sendiri kepada nasabahnya yang seringkali merugikan kepentingan nasabah;
4. Tidak adanya perlindungan yang memadai terhadap ancaman dan pengelolaan atas data dan informasi nasabah;
5. Tidak adanya parameter yang jelas dan baku bagi pengawasan terhadap bank-bank yang menerapkan *internet banking*;
6. Terbukanya kemungkinan terjadinya tindak kriminal dengan menggunakan fasilitas *internet banking*.

Melihat fakta yang terjadi di lapangan kemungkinan terjadinya tindak kriminal dengan menggunakan fasilitas *internet banking* sangatlah besar. Hal ini tidak menutup kemungkinan kedepannya akan terjadi tindak kejahatan *internet banking* di dunia siber.

Bertitik tolak dari apa yang telah dikemukakan diatas, maka penulis tertarik meneliti permasalahan ini dengan mengangkat judul " **PERLINDUNGAN HUKUM PIDANA TERHADAP NASABAH BANK DALAM PENGUNAAN FASILITAS *INTERNET BANKING* ATAS TERJADINYA *CYBER CRIME* "**

B. Perumusan Masalah

Agar penelitian ini dapat tersusun secara sitematis, maka penulis merasa perlu melakukan perumusan masalah terlebih dahulu.

Adapun yang menjadi pokok penelitian antara lain :

1. Bagaimanakah perlindungan hukum pidana terhadap nasabah bank dalam penggunaan fasilitas *internet banking* atas terjadinya *cyber crime*?
2. Siapa yang bertanggungjawab atas akibat hukum dalam kegiatan transaksi elektronik menurut Undang-Undang Informasi dan Transaksi Elektronik?

C. Tujuan Penelitian

Antara lain, adalah :

1. Untuk mengetahui perlindungan hukum pidana yang diberikan kepada nasabah bank terkait penggunaan fasilitas *internet banking* atas terjadinya *cyber crime*.
2. Untuk mengetahui siapa yang bertanggungjawab atas akibat hukum dalam kegiatan transaksi elektronik menurut Undang-Undang Informasi dan Transaksi Elektronik.

D. Manfaat Penelitian

Hasil penelitian skripsi ini diharapkan dapat memberikan manfaat bagi lingkungan akademis (teoritis), lingkungan peradilan dan lingkungan kehidupan secara praktis, yaitu :

1. Manfaat Teoritis

a. Memberikan sumbangan pemikiran di bidang hukum pidana khusus, terutama yang berhubungan dengan tindak pidana *internet banking* dalam perbankan. Dengan adanya pemikiran ini diharapkan dapat memperkaya wawasan dan pemikiran serta pengetahuan baik untuk sendiri ataupun kalangan akademisi sebagai bibit unggul yang akan menjadi generasi penerus bangsa di masa yang akan datang.

b. Memberikan gambaran yang lebih nyata mengenai perlindungan hukum pidana terhadap nasabah bank dalam terjadinya tindak pidana *internet banking*.

2. Manfaat Praktis

Hasil penelitian ini diharapkan dapat membantu dan memberi masukan serta tambahan pengetahuan mengenai hukum pidana khususnya yang berkaitan dengan permasalahan tindak pidana *internet banking* dalam dunia perbankan. Khususnya bagi nasabah bank yang menggunakan pelayanan *internet banking*.

E. Kerangka Teoritis dan Konseptual

1). Kerangka Teoritis

Dalam pembahasan perlindungan hukum terhadap nasabah dalam penggunaan fasilitas *internet banking* atas terjadinya *cyber crime*, teori yang

utama digunakan adalah teori perlindungan hukum. Teori perlindungan hukum dalam penelitian ini didasari pada teori perlindungan hukum yang dikemukakan oleh Philipus M. Hardjon, dimana perlindungan hukum dapat dilakukan dalam wujud perlindungan hukum preventif. Artinya, ketentuan hukum dapat dihadirkan sebagai upaya pencegahan atas tindakan pelanggaran hukum. Upaya pencegahan ini diimplementasikan dengan membentuk aturan-aturan hukum yang sifatnya normatif.[14]

2) Kerangka Konseptual

Suatu kerangka konsepsional, merupakan kerangka yang menggambarkan hubungan antara konsep-konsep khusus, yang ingin atau akan diteliti. Suatu konsep bukan merupakan gejala yang akan diteliti, akan tetapi merupakan suatu abstraksi dari gejala tersebut. Gejala itu sendiri biasanya dinamakan fakta , sedangkan konsep merupakan suatu uraian mengenai hubungan-hubungan dalam fakta tersebut.[15]

Untuk menjawab permasalahan dalam penelitian skripsi ini perlu didefenisikan beberapa konsep dasar dalam rangka menyamakan persepsi, yaitu sebagai berikut :

1. Perbankan adalah segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya;[16]

---

[14] Budi Agus Riswandi, *Aspek Hukum Internet Banking*, PT RajaGrafindo Persada, Jakarta, 2005, hlm. 200

[15] Soerjono Soekanto, *Pengantar Penelitian Hukum,* Penerbit Universitas Indonesia, Jakarta, 1986, hlm 132.

[16] Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankan, Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Pasal 1 angka 1.

2. Bank adalah badan usaha yang menghimpun dana dari msyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup orang banyak.[17]
3. Nasabah adalah pihak yang menggunakan jasa bank;[18]
4. Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchage* (EDI), surat elektronik (*electronic mail*), telegram, teleteks, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah yang memiliki arti oleh orang yang mampu memahaminya;[19]
5. Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya;[20]
6. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf , tanda, angka, kode akses,

[17] Pasal 1 angka 2.
[18] Pasal 1 Angka 16.
[19] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Tahun 2008 Nomor 58 Pasal 1 angka 1.
[20] Pasal 1 angka 2.

symbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya;[21]

7. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan , mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik;[22]
8. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik;[23]
9. Internet berasal dari kata *Interconnection Networking* yang mempunyai arti hubungan komputer dengan berbagai tipe yang membentuk sistem jaringan yang mencakup seluruh dunia (jaringan komputer global) dengan melalui jalur telekomunikasi seperti telepon, *radio link*, satelit, dan lainnya.
10. *Internet Banking* adalah layanan yang diberikan oleh bank kepada nasabah, dengan memanfaatkan media internet untuk melakukan transaksi perbankan.
11. *Cyber crime* secara umum adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan.[24]

---

[21] Pasal 1 angka 4
[22] Pasal 1 angka 5
[23] Pasal 1 angka 9
[24] http://id.m.wikipedia.org/wiki/Kejahatan_dunia_maya diakses tanggal 16 Juni 2011

F. Metode Penelitian

Guna memperoleh data yang dibutuhkan sebagai bahan dalam penulisan ini maka metode yang dipergunakan dalam penelitian ini adalah :

a. Metode Pendekatan

Adapun metode penelitian yang digunakan dalam penulisan skripsi ini adalah metode penelitian yuridis normatif. Penelitian hukum normatif adalah penelitian hukum yang meletakkan hukum sebagai sebuah bangunan sistem norma. Sistem norma yang dimaksud adalah mengenai asas-asas, norma, kaidah dari peraturan perundangan, serta doktrin.[25]

Menurut Peter Mahmud Marzuki penelitian hukum normatif adalah :

> "... suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum untuk menjawab permasalahan hukum yang dihadapi. ... Penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai preskripsi dalam menyeleasikan masalah yang dihadapi ..."[26]

b. Jenis Data

Dalam penelitian pada umumnya dibedakan antara data yang diperoleh secara langsung dari masyarakat dan dari bahan-bahan pustaka. Yang diperoleh dari masyarakat dinamakan data primer (data dasar), sedangkan yang diperoleh dari bahan-bahan pustaka lazimnya dinamakan data sekunder.

Data sekunder dapat berupa bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Bahan hukum primer yaitu semua dokumen peraturan yang mengikat dan ditetapkan oleh pihak-pihak yang berwenang yakni berupa peraturan perundang-undangan yang berkaitan dengan judul skripsi ini.

---

[25] Achmad, Yulianto, Mukti Fajar ND, *Dualisme Penelitian Hukum Normatif & Empiris*, Pustaka Pelajar, Yogyakarta, 2010, hlm 33.

[26] *Ibid.*

Bahan hukum sekunder yaitu semua dokumen resmi yang merupakan informasi atau hasil kajian tentang berkaitan dengan perlindungan hukum pidana terhadap nasabah bank dalam penggunaan fasilitas *internet banking* atas terjadinya *cyber crime* seperti buku-buku teks, seminar hukum, karya tulis ilmiah, jurnal hukum, dan beberapa sumber dari situs internet yang berkaitan dengan persoalan yang dikemukakan penulis dalam skripsi ini. Bahan hukum tersier yaitu semua dokumen yang berisi konsep-konsep dan keterangan-keterangan yang mendukung bahan hukum primer dan bahan hukum sekunder seperti kamus, ensiklopedia, biblografi, dan lain lain.

c. Teknik dan Alat Pengumpulan Data

Dalam memperoleh dan mengumpulkan data-data bagi penelitian ini penulis menggunakan teknik pengumpulan data melalui studi kepustakaan dengan alat pengumpulan data dalam bentuk studi dokumen. Penelitian ini dilakukan dengan cara menganalisis bahan dalam bentuk, peraturan perundang-undangan, buku-buku bacaan, jurnal-jurnal, artikel-artikel, dan penjelajahan situs internet yang berkaitan dengan masalah yang ingin dikemukakan dalam penulisan skripsi ini.

d. Analisis Data

Adapun jenis analisis data yang dilakukan dalam skripsi ini adalah analisis data kualitatif, yaitu dengan cara menguraikan data-data sekunder yang telah diperoleh secara sistematis. Kegiatan analisis dilakukan dengan pemeriksaan terhadap data-data yang telah terkumpul berkaitan dengan judul skripsi ini. Sehingga analisis yang dilakukan dapat memberikan jawaban mengenai

perlindungan hukum pidana terhadap nasabah bank dalam penggunaan fasilitas *internet banking* atas terjadinya *cyber crime.*

BAB II

TINJAUAN PUSTAKA

A. Pengertian Nasabah Bank

Sebagaimana disebutkan dalam Undang-Undang Nomor 10 Tahun 1998 tentang perbankan pada Pasal 1 angka 16, pengertian nasabah adalah pihak yang menggunakan jasa bank. Dalam Pasal 1 angka 17, nasabah penyimpan adalah nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan. Sedangkan pada Pasal 1 angka 18, pengertian nasabah debitur adalah nasabah yang memperoleh fasilitas kredit atau pembiayaan berdasarkan prinsip syariah atau yang dipersamakan dengan itu berdasarkan perjanjian bank dengan nasabah yang bersangkutan.[27]

B. Asas dan Tujuan Perlindungan Nasabah

Perlindungan hukum merupakan satu upaya mempertahankan dan memelihara kepercayaan masyarakat/konsumen sebagai nasabah, maka sudah seharusnya dunia perbankan memberikan perlindungan hukum. Lembaga perbankan adalah lembaga yang mengandalkan kepercayaan masyarakat. Dengan demikian guna mengekalkan kepercayaan masyarakat terhadap bank, pemerintah harus berusaha melindungi masyarakat dari tindakan lembaga ataupun oknum yang tidak bertanggungjawab yang dapat merusak kepercayaan masyarakat. Karena bila suatu saat terjadi kelunturan kepercayaan masyarakat terhadap bank,

[27] Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan Pasal 1 angka 16, 17, 18

maka hal tersebut merupakan bencana bagi perekonomian negara yang sangat sulit dipulihkan kembali.[28]

Pasal 2 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menyatakan bahwa "Perbankan Indonesia dalam melakukan usahanya berdasarkan demokrasi ekonomi dengan menggunakan prinsip kehati-hatian". Sedangkan Pasal 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan bahwa "Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi". Jadi bank sebagai penghimpun dana masyarakat dan penyeleggara sistem elektronik berdasarkan kedua Undang-Undang ini bank dalam melakukan usahanya harus menggunakan prinsip kehati-hatian dari berbagai resiko yang timbul dari penyelenggaraan usaha, khususnya dalam penyelenggaraan *internet banking*.

Selanjutnya terkait tujuan perlindungan nasabah bercermin pada Pasal 4 Undang-Undang Perbankan yang menyatakan bahwa "Perbankan Indonesia bertujuan menunjang pembangunan nasional dalam rangka meningkatkan pemerataan, pertumbuhan ekonomi, dan stabilitas nasional ke arah peningkatan kesejahteraan rakyat banyak". Sedangkan pada Pasal 4 huruf e Undang-Undang Informasi dan Transaksi Elektronik menjelaskan bahwa "Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk : e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi". Penulis menyimpulkan bahwa tujuan

---

[28] Muhammad Djumhana, *Hukum Perbankan di Indonesia,* PT Citra Aditya Bhakti, Bandung, 2000, hlm 167

perlindungan nasabah adalah untuk memberikan rasa aman dan kepastian hukum pada nasabah sebagai pengguna jasa bank, khususnya pengguna fasilitas *internet banking*.

C. Bank Selaku Penghimpun Dana Masyarakat

1. Pengertian Bank

Berdasarkan Pasal 2 Undang-Undang Perbankan yang menegaskan bahwa "Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak".

Dalam prakteknya di dunia perbankan Bank terbagi dua jenis yaitu Bank Umum dan Bank Perkreditan Rakyat. Pengertian Bank Umum berdasarkan Pasal 1 angka 3 Undang-Undang Perbankan adalah "bank yang melaksanakan kegiatan usaha secara konvesional dan atau berdasarkan Prinsip Syariah yang dalam kegiatannya memberikan jasa dalam lalu lintas pembayaran". Kemudian Pengertian Bank Perkreditan Rakyat berdasarkan Padal 1 angka 4 Undang-Undang Perbankan adalah "bank yang melaksanakan kegiatan usaha secara konvensional atau berdasar Prinsip Syariah yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas pembayaran".

2. Fungsi Bank

Berlandaskan pada Pasal 3 Undang-Undang Perbankan, fungsi utama perbankan di Indonesia adalah "sebagai penghimpun dan penyalur dana masyarakat".

3. Usaha Bank Umum

Pasal 6 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menegaskan usaha bank umum meliputi :

a. Menghimpun dana dari masyarakat dalam bentuk simpanan berupa giro, deposito berjangka, sertifikat deposito, tabungan, dan/atau bentuk lainnya yang dipersamakan dengan itu;
b. Memberikan kredit;
c. Menerbitkan surat pengakuan hutang;
d. Membeli, menjual, atau menjamin atas risiko sendiri maupun untuk kepentingan dan atas perintah nasabahnya;
    1. Surat-surat wesel termasuk wesel yang diakseptasi oleh bank yang masa berlakunya tidak lebih lama daripada kebiasaan dalam perdagangan surat-surat dimaksud;
    2. Surat pengakuan hutang dan kertas dagang lainnya yang masa berlakunya tidak lebih lama dari kebiasaan dalam perdagangan surat-surat dimaksud;
    3. Kertas perbendaharaan negara dan surat jaminan pemerintah;
    4. Sertifikat Bank Indonesia (SBI),
    5. Obligasi,
    6. Surat dagang berjangka waktu sampai dengan 1 (satu) tahun;
    7. Instrumen surat berharga lain yang berjangka waktu sampai dengan 1 (satu) tahun;
e. Memindahkan uang baik untuk kepentingan sendiri maupun untuk kepentingan nasabah;

f. Menempatkan dana pada, meminjam dana dari, atau meminjamkan dana kepada bank lain, baik dengan menggunakan surat, sarana telekomunikasi maupun dengan wesel unjuk, cek atau saranna lainnya;

g. Menerima pembayaran dari tagihan atas surat berharga dan melakukan perhitungan dengan antar pihak ketiga;

h. Menyediakan tempat untuk menyimpan barang dan surat berharga;

i. Melakukan kegiatan penitipan untuk kepentingan pihak lain berdasarkan suatu kontrak;

j. Melakukan penempatan dana dari nasabah kepada nasabah lainnya dalam bentuk surat berharga yang tidak tercatat di bursa efek;

k. *Dihapus,*

l. Melakukan kegiatan anjak piutang, usaha kartu kredit dan kegiatan wali amanat;

m.. Menyediakan pembiayaan dan atau melakukan kegiatan lain berdasarkan Prinsip Syariah, sesuai dengan ketentuan yang ditetapkan oleh Bank Indonesia;

n. Melakukan kegiatan lain yang lazim dilakukan oleh bank sepanjang tidak bertentangan dengan Undang-undang ini dan peraturan perundang-undangan yang berlaku.

D. Kewajiban Bank Dalam Penyelenggaraan *Internet Banking*

Dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dinyatakan bahwa kewajiban bank adalah :

1. Untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbulnya resiko kerugian sehubungan dengan transaksi nasabah yang dilakukan melalui bank. (Pasal 29 ayat (4));
2. Setiap bank wajib menjamin dana masyarakat yang disimpan pada bank yang bersangkutan. (Pasal 37B ayat (1));
3. Bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44, dan Pasal 44A. (Pasal 40 ayat (1));
4. Untuk kepentingan peradilan dalam perkara pidana, Pimpinan Bank Indonesia dapat memberikan izin kepada polisi, jaksa atau hakim untuk memperoleh keterangan dari bank mengenai simpanan tersangka atau terdakwa pada bank. (Pasal 42 ayat (1));
5. Atas permintaan, persetujuan atau kuasa dari Nasabah Penyimpan yang dibuat secara tertulis, bank wajib memberikan keterangan mengenai simpanan Nasabah Penyimpan pada bank yang bersangkutan berhak memperoleh keterangan mengenai simpanan Nasabah Penyimpan tersebut. (Pasal 44A ayat (1)).

Sedangkan kewajiban bank sebagai penyelenggara sistem elektronik yang tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah :

1. Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap

beroperasinya sistem elektronik sebagaimana mestinya. (Pasal 15 ayat (1));

2. Penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya. (Pasal 15 ayat (2));
3. Sepanjang tidak ditentukan lain oleh Undang-Undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut :
   a. dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;
   b. dapat melindungi ketersediaan, keutuhan, keontetikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
   c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
   d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan
   e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

   (Pasal 16 ayat (1)).

Bila dihubungkan kedua peraturan perundang-undangan ini maka dapat penulis simpulkan bahwa bank selaku penghimpun dana masyarakat sekaligus

sebagai penyelenggara sistem elektronik *internet banking* berkewajiban untuk menjamin dana masyarakat yang disimpan pada bank dan juga merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, sekaligus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggungjawab terhadap beroperasinya sistem elektronik sebagaimana mestinya termasuk melindungi ketersediaan, keutuhan, keontetikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut.

E. Pengertian *Internet Banking*

Internet merupakan jaringan komputer atau jaringan yang menghubungkan komputer di seluruh dunia dengan menggunakan protokol komunikasi atau dinamakan *internet protokol* (IP). Pengertian dari internet (*interconnection networking*) sendiri adalah infrastruktur teknis yang menghubungkan jutaan *personal computer* yang dioperasikan orang perorangan dan organisasi ke semua aspek penjuru melalui jaringan telekomunikasi kemudian yang mengatur integritas suatu jaringan internet adalah TCP/IP (*Transmission Control Protocol/Internet Protocol*).[29]

Adapun pengertian dari *Internet Banking* menurut Karen Frust adalah sebagai berikut:

> *Internet banking is the use of internet as remote delivery channel for banking services, including traditional services, such as opening a deposit account or transferring funds among different accounts, as well as new*

[29] Rezqy Fardj, "Hukum dan *Internet Banking*" dikutip dari *http://rezqy-fardj.blog.friendster.com/2008/04/hukum-dan-internet-banking* diakses tanggal 5 Januari 2011

banking services, such as electronic bill presentment and payment, wich allow customers to receive and pay bill over bank's website.[30]

Pendapat Karen Frust tersebut dapat kurang lebih mengatakan bahwa *internet banking* adalah penggunaan internet sebagai saluran pengiriman jarak jauh bagi jasa pelayanan bank, termasuk pelayanan tradisional seperti pembukaan akun deposit atau mentransfer dana di antara akun-akun yang berbeda, dan juga pelayanan perbankan yang baru seperti pengadaan dan pembayaran tagihan elektronik yang memungkinkan nasabah untuk menerima dan membayar tagihan melalui *website*.

Pengertian ini tidak jauh berbeda dengan pendapatnya Efraim Turban, meskipun ia memberikan istilah *internet banking* dengan istilah *online banking*. Selengkapnya, ia menyatakan : "*online banking, includes various banking activities conducted from home, business, or on the road instead of at a physical bank location*" dari pengertian ini, dapat didefenisikan secara sederhana bahwa *internet banking* merupakan suatu bentuk pemanfaatan media internet oleh bank untuk mempromosikan dan sekaligus melakukan transaksi secara *online*, baik dari produk yang sifatnya konvensional maupun yang baru.[31]

Sedangkan menurut David Whitely, *internet banking* didefenisikan sebagai salah satu jasa pelayanan yang diberikan bank kepada nasabahnya dengan maksud agar nasabah dapat mengecek saldo rekening dan pembayaran tagihan selama 24 jam tanpa perlu datang ke kantor cabang.[32]

Internet banking merupakan sistim elektronik perbankan yang yang cukup banyak digunakan oleh masyarakat dan akan terus berkembang. *Internet banking*

---

[30] Budi Agus Riswandi, *Aspek Hukum Internet Banking, op. cit.* hlm. 20
[31] *Ibid*, hal 21
[32] *Ibid, hal 44*

merupakan bagian atau salah satu dari produk *Electronic Fund Transfer* yang secara sederhana dapat diartikan sebagai sistem transfer dana yang dilakukan dengan menggunakan sarana elektronik juga komputer. *Electronic Fund Transfer System* (*EFTs*) di Indonesia merupakan bagian dari teknologi sistem informasi yang dikembangkan dalam rangka meningkatkan efektifitas dan efisiensi dalam pelaksanaan tugas dan pelayanan bank kepada masyarakat luas.

EFTs adalah suatu sistem yang pada umumnya di terapkan bank, dimana dengan bantuan peralatan komputer maka telah memungkinkan seseorang dapat melakukan pemindahan/transfer uang dari suatu bank kepada bank lain secara otomatis.

Menurut Pasal 1 angka 2 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dimaksud transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

Pada dasarnya *EFTs* adalah transfer dana, yaitu pemindahan uang dari satu lokasi ke lokasi lain, yang dilakukan dengan suatu sistem komputerisasi tanpa menggunakan kertas.

Hanya dengan memberi perintah atau petunjuk melalui peralatan elektronik, maka nasabah dapat melakukan transfer pada saat itu juga tanpa harus datang ke bank. Transfer dengan *EFTs* ini jauh lebih efisien dan sangat membantu nasabah yang memiliki mobiltas tinggi.

Walaupun *electronic fund transfer* (EFT) terutama *internet banking* banyak memberikan kemudahan, namun tetap mempunyai dampak negatif dari

pelaksaannya, karena EFT sendiri mengandung berbagai kelemahan/kerentanan, yaitu[33] :

1. Transaksi dengan *EFT system* dapat dipengaruhi oleh berbagai cara yang tidak sah.
2. Dana dapat dipindahkan secara instan tanpa adanya penelitian ulang oleh petugas terhadap transaksi-transaksi individual.
3. Dana *EFT* mempunyai nilai ekonomis yang lebih tinggi daripada nilai dana itu sendiri sehingga melahirkan godaan-godaan ke arah kejahatan.
4. Sangatlah mungkin secara periodik, sebagian besar data bank dirusak dari jarak jauh yang dapat menimbulkan peluang terjadinya kejahatan, pemerasan dan terorisme.
5. Karena kejahatan *EFT* memerlukan unsur pendukung intelektual dan sekaligus merupakan tantangan intelektual, bagi banyak orang hal itu dapat menimbulkan hasrat untuk memperoleh keuntungan finansial.
6. Kejahatan *EFT* sangat sulit dideteksi karena dana atau data dapat dipindahkan atau dimanipulasi oleh perintah-perintah tersembunyi di dalam perangkat lunak komputer canggih; dan dinamika tindak kriminal hanya dapat dipahami oleh beberapa ahli/pakar dari lembaga itu sendiri.
7. Kejahatan *EFT* sangat jarang dilaporkan karena publisitas dapat menarik perhatian untuk munculnya cara-cara pengerusakan integritas sistem *EFT*, dapat memberi kesan lemahnya organisasi/kelembagaan atau dapat meningkatkan premi asuransi.

---

[33] Barda Nawawi Arief, *Tindak Pidana Mayantara : Perkembangan Kajian Cyber Crime di Indonesia,* Raja Grafindo, Jakarta, 2006, hlm 55

8. Perundang-undangan yang tidak cukup mampu dan tepat untuk mengusut/menuntut kejahatan *EFT.*

Di samping itu, dampak negatif dapat ditimbulkan dari sistem teknologi canggih yang melekat pada *EFT system.* Salah satu masalah besar yang diungkapkan dalam *Selected EFT Issues,* antara lain pengaruh ketergantungan pada sistem teknologi yang kompleks/canggih terhadap kesejahteraan dan keamanan nasional (*naational welfare and security*). Dikhawatirkan meningkatnya ketergantungan pada *EFT* akan meningkatkan kerentanan (*vulnerability*: sifat mudah diserang) oleh musuh, teroris, dan bencana alam. Para teroris mungkin menyerang sistem *EFT* dengan berbagai alasan dan motivasi. Di samping itu, dinyatakan pula bahwa apabila masyarakat tergantung pada sistem teknologi canggih, maka adanya kegagalan atau gangguan terhadap sistem itu dapat menimbulkan krisis (*crisis*), bahkan terkadang menimbulkan bencana/malapertaka (*catastrophe*), dan dapat menyebabkan kerugian ekonomi dan penderitaan yang sangat besar.[34]

Untuk menghindari dampak-dampak negatif diatas maka ada beberapa aspek yang harus dipenuhi oleh setiap penyelenggara *internet banking* (bank), atau persyaratan kemanan yang harus dijaga penyelenggara *internet banking* guna perlindungan hukum terhadap nasabah pengguna *internet banking*, antara lain adalah:[35]

1) *Cofidentiality* (kerahasiaan)

Aspek *confidentiality* memberi jaminan bahwa data-data tidak dapat disadap oleh pihak lain yang tidak berwenang. Serangan terhadap

[34] *Ibid,* hlm 56.

[35] Dikutip dari http://ekaeldoneris.wordpress.com/2008/12/09/perlindungan-hukum-bagi-nasabah-pengguna-internet-banking/.html. Diakses tanggal 24 April 2011

aspek ini adalah penyadapan nama *account* dan PIN dari pengguna *internet banking.*

2) *Integrity* (integritas/keutuhan)

Aspek *integrity* menjamin integritas data, dimana tidak boleh berubah atau diubah oleh pihak-pihak yang tidak berwenang. Salah satu cara untuk melindungi hal ini adalah dengan menggunakan *checksum, signature* atau *certificate.* Mekanisme *signature* akan dapat mendeteksi adanya perubahan terhadap data.

3) *Authentication* (autentisitas)

Aspek *Authentication* digunakan untuk meyakinkan orang mengakses servis dan juga server (*web*) yang memberikan servis. Mekanisme yang umum digunakan untuk melakukan *authentication* di sisi pengguna biasanya terkait dengan :

1. Sesuatu yang dimiliki (misal : kartu ATM, *chipcard*)
2. Sesuatu yang diketahui (misal : *user id, password,* PIN)
3. Sesuatu yang menjadi bagian dari diri (misal : sidik jari, iris mata)

Salah satu kesulitan melakukan *authentication* adalah biasanya kita hanya menggunakan *user id / account number* dan *password* / PIN. Keduanya hanya mencakup satu hal saja (yang diketahui) dan mudah disadap.

Sementara itu mekanisme untuk menunjukkan keaslian server (situs) adalah dengan *digital sertificate*. Sering kali hal ini terlupakan dan sudah terjadi kasus di Indonesia yang berkaitan dengan situs *internet*

banking palsu. Situs palsu akan memiliki sertifikat berbeda dengan situs *internet banking* yang asli.

4) *Non-Repudiation* (tidak dapat disangkal)

Aspek *non-repudiation* menjamin bahwa jika nasabah melakukan transaksi maka dia tidak dapat menolak telah melakukan transaksi. Hal ini dilakukan dengan menggunakan *digital signature* yang diberikan oleh kripto kunci publik (*public key crypto system*).

5) *Availability*

Aspek *availability* difokuskan kepada ketersediaan layanan. Bila sebuah bank menggelar layanan *internet banking* dan kemudian tidak bisa menyediakan layanan tersebut ketika dibutuhkan oleh nasabah, maka nasabah akan mempertanyakan keaandalannya dan meninggalkan layanan tersebut. Bahkan mungkin nasabah akan pindah ke bank yang dapat memberikan layanan lebih baik. Mekanisme pengamanan untuk menjaga ketersediaan layanan antara lain menggunakan *back up sites, Intusion Detection System* (IDS), *network monitoring, Disaster Recocery Plan* (DRP), *Business Process Resumption*. Istilah-istilah diatas adalah teknik dan mekanisme untuk meningkatkan keamanan.

F. Perkembangan *cyber crime*

Cyber crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Beberapa julukan yang diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain, sebagai kejahatan dunia maya (*cyber space/virtual space offence*), dimensi

baru dari *high tech crime*, dimensi baru dari *transnational crime,* dan dimensi baru dari *white collar crime*.

Istilah cyber crime saat ini merujuk pada kejahatan yang dilakukan oleh seseorang atau kelompok orang dengan pemanfaatan jasa komputer atau internet.[36] Ada ahli yang menyamakan antara tindak kejahatan cyber (cyber crime) dengan tindak kejahatan komputer, dan ada ahli yang membedakan diantara keduanya. Meskipun belum ada kesepahaman mengenai defenisi kejahatan teknologi informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer.[37]

Secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia cyber (cybercrime) adalah "Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut"

Bila seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer. Keragaman aktivitas kejahatan yang berkaitan menimbulkan perbendaharaaan bahasa baru, misalnya *hacking,cracking, virus, time bomb, worm, troyan horse, logical bomb, spaming, hoax*, dan lain-lain sebagainya. Masing-masing memiliki karakter berbeda dan implikasi yang diakibatkan oleh tindakannya pun tidak sama.

---

[36] Ermansyah Djaja, *Penyelesaian Sengketa Hukum Teknologi Informasi dan Transaksi Elektronik,* Pustaka Timur, Yogyakarta, 2010, hlm 32

[37] Gultom, Elisataris dan Dikdik M. Arief Mansur, *Cyberlaw Aspek Hukum Teknologi Informasi, loc. cit.*

Barda Nawawi Arief menunjuk pada kerangka (sistematik) *Draft Convention on Cyber Crime* dari Dewan Eropa (Draft No. 25, Desember 2000). Beliau menyamakan peristilahan antara keduanya dengan memberikan defenisi *cybercrime* sebagai "*crime related to technology, computers and internet*" atau secara sederhana berarti kejahatan yang berhubungan degan teknologi, komputer dan internet.[38]

Andi Hamzah dalam bukunya Aspek-aspek Pidana di Bidang Komputer menyatakan bahwa "Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Penyalahgunaan komputer (*computer abuse*) untuk pertama kalinya dimulai di sistem yang digunakan oleh militer, kemudian menyebar ke arena ilmiah, dan akhirnya ke aplikasi-aplikasi dunia bisnis dan pribadi, termasuk dunia perbankan. Tampaknya tidak dapat dihindari bahwa perubahan dalam bidang teknologi yang tidak berkesudahan itu telah mengakibatkan kejahatan komputer menjadi semakin canggih dan semakin banyak keragamannya. Pertumbuhan tiba-tiba dan secara besar-besaran penggunaan komputer telah menjadi penyumbang utama dari pertumbuhan kejahatan komputer. Semakin maju teknologi, semakin bertambah pula jumlah dan komplesitas kejahatan komputer.

Ada beberapa faktor yang menjadi penyebab makin berkembangnya kejahatan komputer. Faktor-faktor tersebut adalah :[39]

1. Biaya untuk membeli komputer semakin lama semakin murah; dimikian pula biaya untuk menjadi pengguna internet. Faktor ini menyebabkan makin banyaknya jumlah pengguna internet.

---

[38] Labib, Mohammad dan Abdul Wahid, *Kejahatan Mayantara (cyber crime), op. cit.* hlm 74.
[39] Syahdeni, Sutan Remy, *Kejahatan & Tindak Pidana Komputer,* Pustaka Utama Grafiti, Jakarta, 2009, hlm 47.

2. Mudahnya akses kepada jaringan informasi dan komunikasi; pemasangan *wifi* (*wireless fidety*) yang semakin banyak dan makin tersebar di tempat-tempat umum juga semakin memudahkan pengguna komputer untuk mengakses internet. Munculnya telepon-telepon seluler yang dilengkapi dengan fasilitas internet bukan saja menambah jumlah pengguna internet tetapi juga memudahkan untuk mengakses internet; artinya mengakses internet tidak harus melalui komputer atau laptop.
3. Praktis hampir mengenai semua hal dapat diperoleh informasinya melalui internet; termasuk pula informasi mengenai bagaimana cara melakukan *hacking* bahkan cara merakit bom.
4. Mengakses internet dapat dilakukan dari mana pun termasuk dari tempat yang tersembunyi dari penegak hukum dan dari pihak yang menjadi sasaran (korban kejahatan).
5. Pengakses dan pengguna jaringan komputer/internet bersifat anonim (tidak diketahui siapa yang menggunakan jaringan itu) dan tidak mudah dilacak; karena sifatnya yang demikian itu, maka banyak yang mengatakan bahwa tindak pidana komputer adalah suatu "*perfect crime*".
6. Bukti-bukti elektronik/digital (*electronik* atau *digital evidence*) mudah dihapus atau diubah; penghapusan atau pengubahan bukti yang terdapat dalam suatu komputer dapat dengan mudah dilakukan oleh mereka yang memiliki keahlian *hacking* dan

pelaksanaan dapat dilakukan melalui komputer lain dan dari tempat lain.

7. Penegak hukum tidak dapat mengendalikan internet; misalnya muncul *child pornography* yang menjamur dan kesulitan untuk dicegah ataupun ditindak. Demikian pula halnya dengan *cyberstalking* atau penyebarluasan *malware* (virus, *worm,* dan *trojan horse*) yang tidak terkendali di internet.

Faktor-faktor diataslah yang menyebabkan *cyber crime* berkembang sangat cepat, *cyber crime* dapat dilakukan kapan saja dan dimana saja tanpa terpengaruh oleh jarak, berbeda dengan kejahatan biasa atau tradisional.

Dalam perkembangan *cyber crime* banyak yang mempertanyakan perbedaan yang mendasar atau karakteristik pembeda antara *cyber crime* dengan kejahatan biasa atau kejahatan tradisional yang sering terjadi. Pada dasarnya ada beberapa karakteristik yang membedakan antara kejahatan komputer (*computer crime* atau *cyber crime*) dan kejahatan tradisional (*real-world crime*). Perbedaan tersebut adalah:[40]

1. Sekalipun banyak kejahatan tradisional yang juga dapat dilakukan dengan menggunakan komputer sehingga karena itu jenis-jenis kejahatan tradisional menjadi kejahatan komputer, misalnya *child pornography*, *character assassination* dengan menyebarluaskan info negatif mengenai seseorang atau suatu organisasi (dan info itu tidak perlu harus suatu info rekayasa, tetapi dapat berupa info yang benar yang selama ini diupayakan oleh korban untuk tidak diketahui umum), pencurian identitas (*identity*

[40] *Ibid,* hlm 44.

theft) seseorang untuk tujuan melakukan kejahatan yang diatasnamakan pemilik identitas, perjudian internet yang ilegal, namun banyak pula kejahatan tradisional yang tidak dapat dilakukan dengan komputer sehinggga tidak dapat menjadi kejahatan komputer. Kejahatan tradisional yang tidak dapat dilaksanakan dengan komputer misalnya perkosaan, pemukulan fisik, perampokan, dan pencurian harta fisik korban.

2. Kejahatan komputer menggunakan metode atau teknik yang berbeda dengan yang digunakan untuk melakukan kejahatan tradisional di dunia nyata. Misalnya, metode atau teknik untuk melakukan terorisme yang disebut *cyberterorism* adalah menggunakan komputer dan program komputer. Contoh lain adalah *child pornography* yang dilakukan dengan menempatkan foto atau film porno ke dalam situs porno di internet. Sebelumnya hal itu dilakukan di dunia nyata dengan memproduksi foto atau film dan didistribusikan secara non-elektronik.
3. Di antara jenis-jenis kejahatan komputer terdapat kejahatan-kejahatan baru yang sebelumnya tidak dikenal sebagai jenis-jenis kejahatan tradisional. Misalnya, kejahatan *cybersquatting*, penyebaran *malware* (virus, *worm, Trojan horse, dan spyware*), *cracking, hactivism, cyberterorrism, phising, carding,* dan masih banyak lagi yang lain.
4. Karakteristik yang paling fundamental dari kejahatan tradisional adalah bahwa jarak antara pelaku dan korbannya bersifat nyata (fisik) ketika kejahatan itu dilakukan. Sementara itu, pada *cyber crime* jarak antara pelaku kejahatan dan korbannya bersifat non fisik atau virtual.

5. Kejahatan komputer dapat dilaksanakan oleh pelakunya dari jarak jauh. Tidak demikan halnya pelaksanaan kejahatan tradisional yang harus dilakukan secara berhadapan. Misalnya tidak mungkin bagi seseorang untuk meperkosa apa bila pemerkosa dan koban terisah jarak 70 kilometer.
6. Kejahatan komputer dapat dilakukan dari tempat yang tidak dapat dideteksi oleh penegak hukum. Sering kejahatan komputer rilakukan oleh orang dalam dan dilakukan dari lokasi yang berada di gedung perusahaan itu sendiri.
7. Skala dari kejahatan tradisional terbatas karena kejahatan tersebut cenderung merupakan *one-to-one crime*, yaitu seseorang pelaku mengarahkan kejahatannya kepada satu orang (atau kepada beberapa korban atau sekelompok orang saja) sebagai sasarannya. Sementara itu, kejahatan komputer dapat ditujukan kepada sasaran yang jumlahnya banyak sekali.
8. Kerugian finansial yang diakibatkan oleh kejahatan komputer dapat sangat luar biasa dibandingkan dengan yang diakibatkan oleh kejahatan tradisional.
9. Kerusakan fisik akibat kejahatan komputer sangat luar biasa yang untuk memperbaikinya dapat memakan waktu lama disamping sangat mahal.
10. Kejahatan komputer dapat dilaksanakan tanpa kehadiran orang lain di samping atau di dekat pelaku kejahatan itu, sehingga hampir mustahil bagi penegak hukum untuk dapat menampilkan saksi mata. Paling-paling hanya dapat menampilkan saksi yang menyatakan bahwa pelaku yang

bersangkutan *mengutak-atik* komputer pada tanggal tertentu, jam tertentu, dan di tempat tertentu.

11. Pelaku kejahatan komputer yang sangat "canggih" akan mampu untuk segera menghilangkan rekam jejak perbuatannya sehingga tidak dapat dibaca oleh penegak hukum. Rekam jejak tersebut diperlukan untuk dijadikan bukti bagi penyidik. Rekam jejak tersebut berwujud bukti elektronik (*electornic evidence*).

Dari pernyataan diatas terlihat perbedaan mendasar antara kejahatan tradisional dengan *cyber crime*. *Cyber Crime* beroperasi di dunia virtual, tanpa mengenal jarak dan waktu, menggunakan metode dan teknik yang berbeda dengan kejahatan tradisional yang terjadi di dunia nyata.

Seiring berkembangnya teknologi informasi maka banya pula muncul jenis *cyber crime* yang dapat mengganggu dan meresahkan masyarakat. Dari waktu ke waktu jenis-jenis kejahatan komputer bermunculan dan berpacu dengan upaya pembentuk undang-undang untuk menjerat kejahatan tersebut. Berikut adalah beberapa *cyber crime* baru yang telah muncul dan dikenal, diantaranya :

1. *Cybersquatting*

   Cybersquatting adalah perbuatan yang dilakukan oleh seseorang spekulator untuk mendaftarkan suatu *domain name* mendahului pihak lain, yaitu pihak yang sesungguhnya akan menggunakan *domain name* tersebut. *Domain name* adalah nama dari suatu website internet. Tujuan pelaku mendahului mendaftarkan *domain name* adalah untuk ditawarkan kepada pihak yang sesungguhnya akan menggunakan *domain name* tersebut dengan memperoleh keuntungan besar.

2. *Phising* atau *Identity theft*

Phising merupakan salah satu bentuk dari kejahatan internet yang disebut *indentity theft* atau pencurian identitas. Caranya melalui pengiriman *e-mail* palsu kepada seseorang atau suatu perusahaan atau organisasi dengan menyatakan bahwa pengirim bahwa pengirim adalah suatu entitas bisnis yang sah. Pengiriman *e-mail* palsu itu bertujuan untuk menipu penerima agar mengungkapkan informasi ngenai diri penerima. Pengirim *e-mail* tersebut menampilkan *e-mail* itu dalam bentuk dan dengan isi seperti suatu *e-mail* yang tidak palsu. Penerima akan mengira bahwa *e-mail* yang diterimanya adalah asli dan menanggapi *e-mail* tersebut dengan mengunjungi *webiste* pengirim *e-mail* dan kemudian terpancing untuk mengungkapkan informasi mengenai diri penerima, antara lain berupa *password,* nomor *credit card*, nomor *social security,* dan nomor rekening bank sebagaimana yang diminta oleh pengirim *e-mail*. *Website* tersebut tidak lain adalah *website* palsu yang memang sengaja dibuat untuk mencuri informasi pribadi dari korbannya.

3. *Carding*

Carding atau *credit card fraud,* adalah kejahatan kartu kredit yang merupakan salah satu bentuk pencurian (*theft*) dan kecurangan (*fraud*) di dunia internet yang dilakukan oleh pelakunya dengan menggunakan kartu kredit (*credit card*) curian atau kartu kredit palsu yang dibuat sendiri. Tujuannya untuk membeli barang-barang secara tidak sah atas beban rekening dari pemilik kartu kredit yang sebenarnya (yang asli) untuk menarik dana secara tidak sah dari suatu rekening bank milik orang lain.

BAB III

PEMBAHASAN PERMASALAHAN

A. Perlindungan Hukum Pidana Dalam Penggunaan Fasilitas *Internet Banking* Atas Terjadinya *Cyber Crime.*

1. Prosedur Dan Perlindungan Hukum Penggunaan Fasilitas *Internet Banking* Ditinjau Dari Pengaturan Internal Oleh Bank.

Perlindungan hukum atas data pribadi dan dana nasabah dalam penyelenggaraan layanan *internet banking* dengan pendekatan pengaturan secara internal dari penyelenggara *internet banking* itu sendiri. Oleh, karena itu, untuk mendapatkan hasil yang meyakinkan di sini akan dikaji dari dua layanan *internet banking* terbesar di Indonesia, yakni pengaturan ada pada layanan *internet banking* Bank Mandiri dengan situs www.bankmandiri.co.id dan layanan *internet banking* Bank BCA dengan situs www.klikbca.com.

Pengkajian akan difokuskan pada kebijakan internal atas perlindungan data sekaligus dana nasabah dalam dua situs di atas. Sebagaimana diketahui bahwa Bank Mandiri dan Bank BCA merupakan bank yang telah cukup lama menyelenggarakan layanan *internet banking* yang sifatnya *transactional web*, meskipun dalam peristilahan layanan *internet banking* dari Bank Mandiri menggunakan nama *electronic banking*.

Beberapa layanan *internet banking* yang ditawarkan dalam situs www.bankmandiri.co.id meliputi :

a. transfer dana;

b. pembayaran;

c. informasi rekening;

d. aktivitas transaksi;

e. fasilitas cek;

f. *update profile;*

g. personalisasi;

h. notifikasi SMS.

Dalam hal pemanfaatan layanan *internet banking*-nya, Bank Mandiri mempersyaratkan untuk melakukan pendaftratan (*registration*). Apabila langkah ini telah dilakukan, layanan Bank Mandiri dapat diakses melalui layanan *internet banking*nya. Oleh karena itu, layanan *internet banking* sifatnya merupakan media bagi pemasaran produk dan sekaligus sebagai sarana mempermudah transaksi, karena transaksi tersebut dapat dilaksanakan secara *online.*

Sementara itu, dalam layanan *internet banking* yang ada pada situs www.klikbca.com terdiri dari dua kategori, yakni layanan individual dan layanan bisnis. Layanan individual dibagi lagi yang meliputi pembelian, pembayaran, transfer dana dan informasi rekening. Sementara itu layanan bisnisnya menyediakan produk simpanan seperti kredit modal kerja, kredit investasi, dan Bank Garansi. Di sini juga disediakan fasilitas ekspor impor seperti L/C, *negotiation,* dan *discounting.*[41]

Langkah ekspansif yang dilakukan kedua bank melalui implementasi layanan *internet banking* merupakan hal yang menguntungkan di satu sisi dan di sisi lain mengambil risiko atas segala kelemahan baik dari segi teknologi maupun dari sisi yuridis.[42]

---

[41] Budi Agus Riswandi, *Aspek Hukum Internet Banking,* hlm 202

[42] *Ibid,* hlm 203.

Akan tetapi, langkah cerdas telah diambil oleh kedua bank untuk mengantisipasi risiko atas kelemahan dari segi teknologi dan yuridis dengan membuat suatu kebijakan yang disebut *self-regulation.* Pihak bank sendiri secara dini telah mengantisipasi segala kelemahan tersebut dengan membuat suatu ketentuan yang sifatnya sepihak.[43]

Kenyataan ini sangat dirasakan dan dapat dilihat terutama yang berhubungan dengan upaya melindungi data pribadi nasabah dan perubahan teknologi yang berhubungan dengan layanan *internet banking.*

Dari dua situs yaitu www.bankmandiri.co.id dan www.klikbca.com, dapat diuraikan bahwa kedua bank, baik Bank Mandiri dan Bank BCA selaku penyelenggara layanan *internet baking*, ternyata telah membuat suatu kebijakan internal yang berhubungan dengan perlindungan data pribadi nasabah.

Diawali dengan menguraikan kebijakan internal yang ada pada situs www.bankmandiri.co.id terutama pada aspek perlindungan atas data pribadi sekaligus dana nasabah dapat ditemukan pada halaman *webpages* yang terletak pada bagian *electronic banking* yang difokuskan pada kebijakan kerahasiaan nasabah.

Menurut kebijakan kerahasiaan nasabah yang ada pada layanan *internet banking* milik Bank Mandiri dikemukkan bahwa Aplikasi *Internet Banking* Mandiri dijamin kerahasiaan dan keamanannya. Dalam hal ini Bank Mandiri menggunakan teknologi enkripsi *Secure Socket Layer* (SSL) 128 bit yang akan melindungi komunikasi antara komputer nasabah dengan *server* Bank Mandiri. Untuk menambah keamanan digunakan metode *time out session*, maksudnya

---

[43] *Ibid.*

adalah setelah 10 menit tanpa aktivitas nasabah, akses dari komputer nasabah ke *server* Bank Mandiri secara otomatis diputus.[44]

Selain itu, Bank Mandiri akan menjaga kerahasiaan data pengguna *Internet Banking* Mandiri, dan hanya orang tertentu yang berhak untuk mengakses informasi tersebut untuk digunakan sebagaimana mestinya (dalam hal ini Bank Mandiri selalu mengingatkan karyawan akan pentingnya menjaga kerahasiaan data nasabah). Bank Mandiri tidak akan memperlihatkan/menjual data tersebut kepada pihak ketiga.

Bank Mandiri juga tidak secara otomatis mengumpulkan informasi data pengunjung *Internet Banking* Mandiri. Hanya beberapa informasi umum yang akan dikumpulkan dan digunakan antara lain[45] :

a. nama domain yang akan digunakan nasabah untuk mengakses internet;
b. *internet banking* yang digunakan untuk mengakses *website* Bank Mandiri;
c. *browser* yang digunakan;
d. hari, tanggal, dan waktu mengakses internet;
e. pilihan yang ditentukan oleh nasabah untuk memberikan informasi kepada bank, antara lain jenis rekening.

Untuk dapat mengakses *Internet Banking* Mandiri, nasabah harus memasukkan terlebih dahulu *User ID* dan PIN, dan untuk keamanan, nasabah diharuskan memasukkan kembali PIN untuk setiap transaksi yang bersifat finansial.

---

[44] *Ibid.*
[45] *Ibid.*

Mengingat banyaknya variasi internet *browser* yang ada, dan *internet banking* harus mengikuti keamanan masing-masing *browser*. Saat ini Bank Mandiri menyediakan sarana *internet banking* yang lebih cocok diakses dengan menggunakan *Netscape Communicator 4.7* atau *Microsoft Internet Exploler versi 5.01* atau bersi terakhir.[46]

Dari sini dapat diananlisis bahwa sudah ada upaya melindungi data pribadi nasabah dalam layanan *internet banking* milik Bank Mandiri terdiri dari perlindungan data atas data yang dikumpulkan, dimanfaatkan atau digunakan untuk keperluan transaksi dari nasabahnya. Perlindungan atas data pribadi nasabah ini diperketat lagi dengan adanya prasyarat-prasyarat tertentu dalam penggunaan saran teknologi yang akan digunakan untuk bertransaksi dengan menggunakan layanan *internet banking* Bank Mandiri. Hal ini barangkali dilakukan berdasarkan pada suatu kesadaran bahwa tidak semua teknologi punya daya keamanan yang sama dan tidak semua teknologi dikuasai oleh pihak penyelenggara layanan *internet banking*.

Di samping kebijakan secara khusus dalam situs www.bankmandiri.co.id yang terkait dengan kebijakan kerahasiaan nasabah, juga ketika nasabah akan menggunakan layanan *internet banking* Bank Mandiri ini diwajibkan melakukan registrasi. Di dalam bagian registrasi juga diuraikan beberapa petunjuk dan langkah yang kalau ditelaah petunjuk dan langkah itu dimaksudkan untuk melindungi data pribadi nasabah. Petunjuk itu dikemas dalam dua aspek, yakni syarat pendaftaran dan langkah pendaftaran.

---

[46] *Ibid,* hlm 206.

Untuk menjadi pengguna *Internet Banking* Mandiri, cukup ikuti langkah-langkah petunjuk berikut ini :[47]

Syarat Pendaftaran :

a. Memiliki rekening tabungan, giro rupiah dan atau mata uang lainnya,
b. Untuk pendaftaran di ATM, harus memiliki kartu ATM Mandiri sedangkan untuk pendaftaran di cabang harus menunjukkan bukti identitas diri (KTP, SIM, Passport, KIMS) dan bukti kepemilikan rekening (buku tabungan, kartu ATM Mandiri).

Langkah Pendaftaran :

Langkah 1 : Lakukan pendaftaran *Internet Banking* Mandiri dengan salah satu cara di bawah ini, untuk mendapatkan Nomor *Access ID* dan *Access Code*.

a. Datang ke ATM Bank Mandiri. Masuk ke menu utama dan pilih registrasi *e-banking* serta ikuti petunjuk yang ada di layar ATM untuk membuat *Access Code*.

   Sementara itu, untuk nomor *Access ID* digunakan 16 digit nomor kartu ATM Anda.
b. Atau datang ke cabang *Bank Mandiri.* Isi formulir atau aplikasi pendaftaran *Internet Banking* Mandiri yang ada di cabang selanjutnya bank akan mengirim *Access ID* ke alamat *e-mail* anda serta menyerahkan *Access Code* dalam amplop tertutup.

[47] Dikutip dari www.bankmandiri.co.id. Diakses tanggal 28 April 2011

Langkah 2 : Lakukan Pendaftaran *Token* PIN Mandiri

Dapatkan *Token* PIN Mandiri di caban Bank Mandiri terdekat dengan mengisi formulir aplikasi Penggunaan *Token* Mandiri serta ikuti buku petunjuk penggunaan yang terdapat di dalam box.

Catatan :

a. Untuk bisa bertransaksi, Anda diharuskan menggunakan *Token* PIN Mandiri.
b. Tanpa *Token* PIN Mandiri, Anda masih bisa *log in* ke dalam sistem *Internet Banking* Mandiri untuk mendapatkan Informasi Saldo dan mutasi transaksi.

Langkah 3 : Lakukan Aktivasi *Internet Banking* Bank Mandiri

a. Klik tombol aktivasi pada situs www.bankmadiri.co.id , dan masukkan/input *Access ID* dan *Access Code* yang diperoleh dari bank setelah Anda melakukan registrasi di ATM atau cabang Bank Mandiri.
b. Selanjutnya, buat sendiri *User ID* dan PIN *Internet Banking* Mandiri Anda untuk bisa *log in* ke dalam layanan *Internet Banking* Mandiri.

Langkah 4 : Lakukan Aktivasi *Token* PIN Mandiri Anda.

Log in ke *Internet Banking* Mandiri di www.bankmadiri.co.id, masuk ke menu administrasi dan pilih Aktivasi *Token* PIN Mandiri.

Melalui instrumen persyaratan pendaftaran dan langkah pendaftaran pada dasarnya menunjukkan adanya upaya preventif dari penyelenggara layanan *internet banking* Bank Mandiri untuk mencegah atas pelanggaran data pribadi nasabah salah satunya. Kalaupun terjadi pelanggaran, syarat pendaftaran dan langkah-langkah ini dapat saja dijadikan sarana untuk membantu mengidentifikasi pelanggarannya sendiri.[48]

---

[48] *Ibid,* hlm 209.

Selanjutnya, upaya melindungi data pribadi nasabah yang dilakukan oleh layanan *Internet Banking* Bank Mandiri juga diperkuat dengan dihadirkannya *Tips E-Banking*. *Tips E-Banking* dikhususkan bagi nasabah yang memanfaatkan layanan *SMS Banking*.

Setelah diketahui upaya perlindungan atas data pribadi nasabah dalam layanan *internet banking* milik Bank Mandiri melalui pendekatan *self-regulation*, berikutnya akan diuraikan upaya yang sama yang terdapat pada layanan *internet banking* milik Bank BCA.

Upaya perlindungan atas data pribadi nasabah yang dibentuk melalui pendekatan *self-regulation* terdapat pada instrumen *privacy policy*. Didalam instrumen *privacy policy* dinyatakan sebagai berikut :[49]

> BCA menggunakan teknologi enkripsi *Secure Socker Layer* (*SSL*) 128 bit untuk memproteksi komunikasi antara komputer Anda dan server BCA selama Anda mengakses *internet banking* BCA.
>
> Untuk memastikan proteksi Anda, silahkan lakukan hal-hal sebagai berikut:
>
> a. Periksa sertifikat secara teratur untuk memastikan bahwa anda menerima sertifikat yang sah yang telah teregristrasi untuk IBANK.KLIKBCA.COM.
>
> b. Apabila Anda menerima pesan yang menjelaskan bahwa sertifikat tidak sah, dimohon Anda tidak melanjutkan. Pastikan bahwa anda telah mengetik alamat yang benar.

[49] Dikutip dari www.klikbca.com. Diakses tanggal 28 April 2011

c. Pastikan bahwa disebelah bawah *browser* Anda terdapat gambar gembok/kunci yang mengindikasikan bahwa halaman yang Anda akses saat ini dienkripsi menggunakan *SSL*.

Jika Anda tidak melihat gambar gembok/kunci dimohon Anda untuk *log out* dan *log in* kembali.

BCA mewajibkan Anda untuk memasukkan *User ID* dan PIN sebelum Anda diperbolehkan mengakses fasilitas internet banking. Anda juga diwajibkan untuk memasukkan PIN Anda pada saat melakukan transaksi finansial sebagai tanda persetujuan Anda.

Untuk memastikan proteksi Anda, silahkan lakukan hal-hal sebagai berikut:

a. Jagalah kerahasiaan *User ID* dan PIN Anda, jangan diberitahukan kepada orang lain.

b. Jangan beritahukan PIN atau sebagian PIN Anda kepada orang lain, walaupun orang tersebut mengaku sebagai karyawan BCA. BCA tidak pernah menanyakan PIN Anda.

c. Gantilah PIN Anda secara periodik jika Anda tidak yakin terhadap kerahasiaan PIN Anda. Jangan gunakan PIN yang mudah diterka. Jangan menuliskan PIN Anda di tempat dimana orang lain bisa melihatnya.

d. Hubungi Halo BCA jakarta di (021) 52-999-888 jika Anda lupa PIN atau PIN Anda terblokir.

Ikuti instruksi mereka bagaimana cara untuk kembali mengaktifkan fasilitas *internet banking* Anda kembali.

BCA mewajibkan Anda untuk memberikan alamat *email* Anda kepada BCA. BCA akan menggunakan alamat *email* Anda untuk mengirimkan kepada Anda informasi atas transaksi finasial yang telah Anda lakukan melalui *internet banking*. Untuk memastikan proteksi Anda, silahkan lakukan hal-hal berikut :

a. Berikan kepada BCA alamat *email* pribadi Anda. Jangan menggunakan alamat *email* palsu.
b. Ubahlah segera alamat *email* Anda di *internet banking* jika Anda mengganti alamat *email* Anda.
c. Jika Anda menghubungi BCA melalui *email*, jangan krimkan informasi rekening yang sifatnya rahasia atau sensitif.

BCA tidak menjual, menukar atau memperlihatkan segala informasi yang berkaitan dengan nasabah atau pengunjung *wabsite* BCA. BCA tidak melacak pengunjung *website* BCA. Selama Anda *log in* ke *internet banking*, BCA akan menggunakan *cookie* yang akan berakhir pada saat Anda *log out*.

Semua transaksi perbankan Anda dan informasi rekening lainnya disimpan secara rahasia sesuai dengan hukum dan peraturan Bank Indonesia dan kebijakan pengamanan internal BCA.

Di dalam *website* BCA, BCA menyediakan *URL link* ke *website* lain yang tidak dikontrol oleh BCA. BCA tidak bertanggung jawab atas isi dan keamanan dari *website* tersebut. Jika Anda mengakses *website* tersebut, silahkan memeriksa *privacy and security policies* mereka. Dalam hal Anda mengakses *website* atau *internet banking* BCA melalui *URL link* dari

webiste lain, pastikan kebenaran alamat yang Anda akses yaitu, http://www.klikbca.com atau https://ibank.klikbca.com

Karena banyaknya variasi *internet browser* yang ada, sulit untuk menyediakan *internet banking* yang mengikuti keamanan masing-masing *browser*. Saat ini BCA hanya menyediakan sarana *internet banking* yang lebih cocok diakses dendgan menggunakan *Microsoft Internet Exploler versi 5* atau terbaru.

BCA mohon maaf atas ketidaknyamanan ini.

BCA dapat mengubah kebijaksanaan ini setiap saat untuk tetap menyesuaikan dengan situasi dan teknologi terbaru. Anda selalu dapat meninjau kebijakan BCA yang terbaru di http://www/klikbca.com/privacy.html atau Anda dapat memintanya dengan mengirimkan *email* ke klikbca@bca.co.id.

Apabila dianalisis dari kebijakan privasi (*privacy policy*) ini, terlihat bahwa pihak penyelenggara layanan *internet banking*, dalam hal ini Bank BCA, menghendaki ada perlindungan hukum, baik bagi kepentingan nasabah maupun pihak bank sendiri sebagai penyelenggara layanan. Perlindungan hukum dalam kebijakan privasi terkait dengan pemanfaatan data pribadi nasabah guna keperluan transaksi yang menggunakan layanan *internet banking*.[50]

Upaya perlindungan juga dilakukan dengan memberikan informasi di seputar teknologi yang layak diterapkan dalam pemanfaatan layanan *internet banking* ketika nasabah menggunakannya untuk bertransaksi. Di samping itu, dengan kebijakan privasi ini, pihak bank sebagai penyelenggara layanan

[50] Budi Agus Riswandi, *Aspek Hukum Internet Banking, op. cit,* hlm 214

mempunyai hak untuk melakukan perubahan atas kebijakan yang disesuaikan dengan perkembangan teknologi.

Berdasarkan pada uraian upaya perlindungan data pribadi nasabah yang ada pada dua layanan *internet banking* di atas, terlihat bahwa ada persamaan dan ada perbedaannya. Persamaan teridentifikasi pada adanya pembentukan kebijakan internal oleh dua layanan *internet banking* sehubungan dengan perlindungan data pribadi nasabah.

Dalam hal perbedaannya, dua layanan tersebut mempunyai perbedaan dalam memformulasikan kebijakan internalnya dalam mengupayakan perlindungan atas data pribadi nasabah. Di dalam layanan *internet banking* Bank Mandiri, formulasi perlindungan atas data pribadi nasabah dituangkan tidak saja dalam wujud kebijakan seperti kebijakan kerahasiaan nasabah, namun diformulasikan juga dalam wujud proses pendaftaran dan pemberian *tips e-banking*, sedangkan dalam layanan *internet banking* Bank BCA formulasi kebijakan hanyalah dituangkan dalam wujud kebijakan privasi atau lebih dikenal dengan istilah *privacy policy*.

Meskipun keduanya ada persamaan dan perbedaan hal yang lebih penting lagi dalam kaitannya dengan perlindungan data pribadi nasabah dalam dua layanan *internet banking* di atas, ternyata kebijakan-kebijakan tersebut dibentuk dan disusun atas pertimbangan sepihak. Oleh karena itu, dari sudut pandangan hukum sesungguhnya model-model pembentukan dan penyusunan aturan sepihak ini kecenderungan yang terjadi justru kepentingan dari pihak pembentuk dan penyusunlah yang lebih dominan dilindungi.

Bila dicermati bunyi aturan-aturan yang telah diuraikan di atas, kedengarannya akan banyak merugikan pada kepentingan si nasabah. Salah satu bunyi aturan yang dimaksudkan sebagaimana dinyatakan sebagai berikut :

> BCA dapat mengubah kebijaksanaan ini setiap saat untuk tetap menyesuaikan dengan situasi dan teknologi terbaru. Anda dapat selalu meninjau kebijakan BCA yang terbaru di http://klikbca.com/privacy.html atau Anda dapat memintanya dengan mengirimkan *email* ke klikbca@bca.co.id (www.klikbca.com).

Dalam situs www.bankmandiri.co.id juga dinyatakan sebagai berikut :

> Selain itu, Bank Mandiri akan menjaga kerahasiaan data pengguna *internet banking* Mandiri, dan hanya orang tertentu yang berhak untuk mengakses informasi tersebut menggunakan sebagaimana mestinya (dalam hal ini Bank Mandiri akan selalu mengingatkan karyawan akan kepentinganya menjaga kerahasiaan data nasabah). Bank Mandiri tidak akan memperlihatkan/menjual data tersbut kepada pihak ketiga.

Analisis atas bunyi ketentuan pada situs www.klikbca.com terlihat bahwa nasabah tidak pernah diberikan kesempatan untuk mengetahui perubahan kebijakan baru atas privasi. Terlebih lagi, alasan yang didalihkan adalah untuk menyesuaikan dengan situasi dan teknologi terbaru. begitu pula, dalam bunyi ketentuan pada situs www.bankmandiri.co.id, pada ketentuan yang ada di situs ini pun tampaknya nasabah sulit untuk dapat mengetahui kebenaran atas tidak terjadinya penjualan datanya kepada pihak ketiga.

2. Ketentuan Pidana Penggunaan Fasilitas *Internet Banking* yang berkaitan dengan *Cyber Crime*

Didasarkan pada konsep perlindungan hukum yang dikemukakan Philipus M. Hardjon, dimana perlindungan hukum dapat dilakukan dalam wujud preventif. Artinya, pencegahan atas tindakan pelanggaran hukum. Upaya pencegahan ini diimplementasikan dengan membentuk aturan hukum yang sifatnya normatif.

Penelitian dilakukan dengan mercermati Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penetapan Undang-Undang ITE sebagai sumber untuk melakukan penelitian didasarkan pada pertimbangan bahwa Undang-Undang ITE merupakan ketentuan yang dekat dan berhubungan erat dengan masalah diteliti.

Pada dasarnya penyelenggaraan layanan *internet banking* tidak akan terlepas dari Undang-Undang Informasi dan Transaksi Elektroonik (ITE). Hal ini dipertegas oleh Pasal 1 angka 2 Undang-Undang Informasi dan Transaksi Elektronik yang menyatakan :

"Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan atau media elektronik lainnya"

Dalam Pasal 1 Undang-Undang ITE ini tidak membatasi transaksi elektronik hanya sebatas perbuatan hukum yang dilakukan menggunakan komputer dan jaringan komputer saja, tetapi juga menggunakan media elektronik lainnya. Berarti juga mengakomodir kegiatan perbankan diluar penyeleggaraan *internet banking* saja, misalnya : *SMS Banking* atau transaksi melalui mesin ATM.

Dalam perlindungan hukum yang diberikan kepada nasabah selaku pengguna sistem elektronik dapat dicermati dalam ketentuan Pasal 15 Undang-Undang Informasi dan Transaksi Elektronik, yang menyatakan sebagai berikut :

> (1) Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggungjawab terhadap beroperasinya sistem elektronik sebagaimana mestinya;
> (2) Penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya;
> (3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik.

Dari ketentuan diatas, jelas bahwa pihak bank diharuskan menyelenggarakan sistem elektronik secara andal, aman dan bertanggung jawab beroperasi sebagaimana mestinya. Dalam penjelasan Pasal 15 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang dimaksud dengan "Andal" adalah sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. Bank sebagai penyelenggara sistem elektronik dituntut bisa memenuhi kebutuhan pengguna atau nasabah dalam hal penyelenggaraan *internet banking*. Sedangkan yang dimaksud dengan "Aman" adalah sistem elektronik terlindungi secara fisik maupun nonfisik. Selanjutnya maksud kata "beroperasi sebagaimana mestinya" adalah sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. Kemudian dalam penjelasan Pasal 15 ayat (2) terdapat kata "bertanggung jawab" yang berarti ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut. Dalam hal penyelenggaraan layanan *internet banking* tentu bank sebagai subjek hukum bertanggung jawab terhadap penyelenggaraan sistem elektroniknya.

Melalui Pasal 15 ayat (1) dan (2) Undang-Undang Informasi dan Transaksi Elektronik, perlindungan hukum atas data pribadi nasabah yang tersimpan atau ada dalam sistem elektronik suatu bank sudah dilindungi karena bank bertanggung jawab penuh terhadap sistem elektronik yang dikelolanya. Namun tidak menutup kemungkinan pihak penyelenggara atau bank dalam hal ini, tidak bertanggung jawab bila dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. Jadi, pihak pengguna sistem elektronik dalam hal ini nasabah, perlu berhati-hati dalam melakukan transaksi elektronik karena apabila dapat dibuktikan hal yang tersebut diatas, maka pihak penyelenggara sistem elektronik tidak dapat mempertanggungjawabkannya.

Dalam hal perlindungan hukum atas data dan dana nasabah dapat dicermati pula dalam ketentuan Pasal 30 UU Informasi dan Transaksi Elektronik yang menyatakan sebagai berikut :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Dilanjutkan dengan ketentuan Pasal 46 UU Informasi dan Transaksi Elektronik yang menyatakan bahwa :

(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).

(3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

Pasal 30 UU Informasi dan Transaksi Elektronik dapat dijadikan landasan yang cukup kuat untuk melindungi data pribadi sekaligus uang nasabah pengguna fasilitas *internet banking* yang kemungkinan dibobol akunnya oleh pihak yang tidak bertanggungjawab, karena apabila ada pihak yang mencoba mengakses dengan cara melawan hukum akun *internet banking* milik nasabah, maka secara otomatis pelaku telah melanggar Pasal 30 ayat (1) UU Informasi dan Transaksi Elektronik dan ancaman pidananya dalam Pasal 46 ayat (1) UU Informasi dan Transaksi Elektronik yaitu pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah). Sedangkan pada Pasal 30 ayat (2) yang dilindungi adalah Informasi Elektronik dan/atau Dokumen Elektronik. Pasal 1 angka 1 UU Informasi dan Transaksi Elektronik menyebutkan bahwa :

> " Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleteks, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya"

Sedangkan yang Pasal 1 angka 4 UU Informasi dan Transaksi Elektronik menyatakan bahwa :

> "Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat,

ditampilan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu membacanya"

Pasal 30 ayat (2) UU Informasi dan Transaksi Elektornik lebih mengatur mengenai terjadinya pengambilan Informasi Elektronik dan/atau Dokumen Elektronik yang ada di komputer dan/atau sistem elektronik, dengan sengaja dan tanpa hak atau melawan hukum. Apabila dihubungkan dengan kegiatan *internet banking* maka Pasal 30 ayat (2) UU Informasi dan Transaksi Elektronik ini melindungi data-data dan informasi nasabah yang ada didalam komputer atau didalam sistem elektronik yang diselenggarakan oleh bank. Pasal ini tidak hanya melindungi nasabah semata dari pengambilan Informasi Elektronik dan/atau Dokumen Elektronik, namun juga melindungi pihak bank sebagai penyelenggara sistem elektronik yang tentu saja menyimpan banyak Informasi dan Dokumen Elektronik milik nasabahnya. Sementara itu pidana yang diancamkan untuk pelanggaran Pasal 30 ayat (2) UU Informasi dan Transaksi Elektronik, yang diatur di dalam Pasal 46 ayat (2) UU Informasi dan Transaksi Elektronik adalah adalah pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).

Kemudian pada Pasal 30 ayat (3) mengatur mengenai perbuatan melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Bila dihubungkan dengan penyelenggaraan layanan *internet banking*, maka Undang-undang ini melindungi kepentingan nasabah dan juga bank sebagai penyelenggara sistem elektronik. Sistem pengamanan yang dimiliki oleh

penyelenggara sistem elektronik yakni bank, bisa saja dibobol oleh *cracker* yang mungkin memiliki pengetahuan dan teknologi yang canggih. Oleh karena itu, keberadaan Pasal 30 ayat (3) ini dirasa menjadi sangat vital dalam perlindungan penyelenggaraan layanan *internet banking*. Sementara itu pidana yang diancamkan untuk pelanggaran Pasal 30 ayat (3), yang diatur dalam Pasal 46 ayat (3) UU Informasi dan Transaksi Elektronik adalah pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

Dasar hukum lain yang tidak kalah penting dalam perlindungan yang diberikan oleh hukum pidana terhadap keamanan data dan dana nasabah adalah Pasal 31 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik. Pasal 31 Undang-Undang Informasi dan Tranasaksi Elektronik menyatakan sebagai berikut :

> (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektroik milik orang lain;

Dilanjutkan dengan ketentuan pidana Pasal 47 Undang-Undang Informasi dan Transaksi Elektronik yang menyatakan bahwa :

> "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh0 tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah)"

Pasal 31 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik dapat dijadikan landasan untuk melindungi data pribadi nasabah yang kemungkinan disadap aktifitas dunia mayanya oleh pihak yang tidak bertanggungjawab. Penyadapan dilakukan oleh pelaku agar mendapatkan informasi elektronik dan/atau dokumen elektronik yang diakses atau dikirimkan oleh pengguna fasilitas *internet banking*, yang dalam hal ini yang disadap adalah *user name* dan *password* akun *internet banking*. Bila terbukti pelaku melakukan penyadapan dengan sengaja dan tanpa hak atau melawan hukum dalam komputer dan/atau sistem elektronik milik orang lain, maka pelaku melanggar Pasal 31 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik dan ancaman pidananya dalam Pasal 47 Undang-Undang Informasi dan Transaksi Elektronik yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta tupiah).

Kemudian dicermati pula Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik yang menyatakan bahwa :

> "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik"

Dilanjutkan dengan ketentuan pidana Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang menyatakan bahwa :

(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas)

tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah)

Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik merupakan dasar hukum bagi perlindungan data dan dana nasabah yang dikelabui oleh situs *internet banking* palsu yang dibuat oleh pelaku kejahatan *cyber*. Bila terbukti melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, maka pelaku dapat dijerat dengan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik dan ancaman pidananya dalam Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yaitu pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).

Bila dihubungkan dengan sistem penyelenggaraan *internet banking,* maka *hacking* dan *cracking*-lah yang menjadi ancaman utama, karena *hacking* dan *cracking* dapat membobol dan melakukan pencurian terhadap data pribadi dan dana nasabah yag dipercayakan kepada bank. Untuk lebih jelas mengenai cara *cracker* membobol sistem penyelenggaraan *internet banking* atau akun *internet banking* milik nasabah dan kaitannya dengan aturan hukum diatas maka penulis menjabarkannya sebagai berikut :[51]

[51] Dikutip dari www.maubaca.com/cara-cracker-membobol-internet-banking/.html. Diakses tanggal 8 April 2011.

1) Teknik *Session Hijacking*

Dengan *session hijacking, cracker* menempatkan *monitoring/spying* yang dilakukan pengguna komputer yang digunakan oleh pengguna/user untuk mengunjungi situs *internet banking*. Teknik ini menggunakan cara penyadapan terhadap aktifitas dunia maya pengguna fasilitas *internet banking*. Setiap kegiatan yang dilakukan oleh pengguna dapat diketahui oleh *cracker*. Ketika pengguna mengakses *website internet banking,* kemudian menuliskan *username* dan *password* maka akan dengan mudah diketahui oleh *cracker*. Sehingga nantinya *cracker* dengan mudah dapat memasuki akun *internet banking* milik korban. Bila sudah berhasil memasuki akun *internet banking* milik korban, maka *cracker* dapat berbuat sesukanya karena telah terotentikasi sebagai pemilik akun. Dalam hal terjadinya penyadapan dan mengakses dengan tanpa hak akun *internet banking* milik orang lain maka dapat dijerat dengan Pasal 30 ayat (1) dan (2) lalu Pasal 31 ayat (1) dan ketentuan pidananya Pasal 46 ayat (1) dan (2) lalu Pasal 47 Undang-Undang Informasi dan Transaksi Elektronik.

(2) Teknik *Man in the Middle Attack*

Dengan *man in the middle attack* ini cracker melakukan penangkapan paket data atau penyadapan data yang ditransmisikan dari komputer *user* ke *web server internet banking* pada jaringan *internet*. Dalam hal penggunaan fasilitas *internet banking* pelaku melakukan penyadapan data nasabah dikala nasabah sedang melakukan pengiriman data, dengan kata lain *cracker* ikut menunggangi kegiatan transaksi

elektronik yang dilakukan oleh nasabah, hingga memungkinkan terjadinya pengambilan dan pencurian informasi elektronik dan/atau dokumen elektronik oleh pelaku kejahatan *cyber*, baik itu berupa *user name, password,* ataupun data-data lain yang sebenarnya bersifat rahasia. Apabila *cracker* telah mendapatkan *username, password,* atau data penting lainnya, maka ia dapat melakukan transaksi menggunakan akun *internet banking* milik nasabah karena telah terotentifikasi sebagai pangguna layanan yang sah. Masalah *man in the middle attack* ini bisa dihindari dengan melakukan penyadian/enkripsi pada paket data di komputer *user* sebelum dikirimkan melalui media internet ke *web server*. Pelaku yang melakukan penyadapan dan mengakses akun *internet banking* milik nasabah secara sengaja dan tanpa hak atau melawan hukum dapat dijerat dengan Pasal 30 ayat (1) dan (2) lalu Pasal 31 ayat (1) dan ketentuan pidananya Pasal 46 ayat (1) dan (2) lalu Pasal 47 Undang-Undang Informasi dan Transaksi Elektronik.

(3) Teknik *Fake Web*

Pada teknik ini *cracker* berusaha membuat pengguna mengunjungi situs *internet banking* yang salah sehingga pengguna memberikan informasi elektronik rahasia kepada pihak yang tidak berhak. Untuk melancarkan aksinya *cracker* umumnya membuat situs *internet banking* palsu, yang nama, alamat dan tampilannya semirip mungkin dengan nama *server internet banking* yang asli. Misalnya : www.klikbca.com merupakan situs yang asli, maka *cracker* dengan maksud mengelabui pengguna/*user* membuat situs beralamat

www.klickbca.com, www.klikbca.org, www.klikbca.co.id, www.clickbca.com, www.kliikbca.com, dll. Dengan demikian ketika pengguna membuka alamat yang salah, ia akan tetap menduga bahwa ia mengunjungi situs klikbca yang benar. Situs palsu tersebut digunakan oleh pelaku kejahatan untuk merekam *username* dan nomor *password* milik nasabah yang berhasil dikelabui. Nasabah yang berhasil dikelabui akan memasukkan *username* dan *passwordnya* pada situs palsu, kemudian digunakan untuk bertransaksi pada situs yang asli.[52]

Masalah diatas dapat dihindari dengan melengkapi *Digital Certificate*/Sertifikat Digital pada situs asli. Dengan demikian *cracker* dapat membuat nama yang hampir sama namun tidak dapat memalsukan *digital certificate*. Pengguna atau pengunjung situs dapat mengetahui bahwa situs tersebut asli atau tidak, dengan melihat ada tidaknya sertifikat digital pada situs tersebut. Pelaku yang menciptakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik dan kemudian masuk dengan sengaja dan tanpa hak atau melawan hukum mengakses akun *internet banking* milik nasabah dapat dijerat Pasal 30 ayat (1) dan (2) lalu Pasal 35 serta dijerat dengan ketentuan pidana Pasal 46 ayat (1) dan (2) lalu Pasal 51 ayat (1) Undang-Undang Transaksi dan Informasi Elektronik.

[52] Tb. Irman S, *Anatomi Kejahatan Perbankan, op. cit,* hlm 198

(4) Teknik *Website Defacing*

Pada teknik ini *cracker* melakukan serangan terhadap situs *internet banking* yang asli, misalkan situs klikbca.com. *Cracker* kemudian mengganti isi halaman pada *server* tersebut dengan miliknya. Sehingga pengunjung akan mengunjungi alamat dan *server* yang benar namun sebenarnya halaman tersebut buatan *cracker*. Dengan teknik ini *cracker* membobol sistem pertahanan dan pengamanan yang dibuat oleh bank selaku penyelenggara *internet banking*, kemudian memanipulasi informasi elektronik atau dokumen elektronik dengan tujuan informasi elektronik atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, kemudian mendapatkan informasi elektronik yang dibutuhkan dari nasabah yang telah memasukkan informasi elektronik ke halaman *internet banking* hasil manipulasi *cracker,* kemudian dengan data yang diperoleh dari nasabah, *cracker* dapat mengakses akun *internet banking* milik nasabah karena mengetahui *username* dan *passwordnya.* Banyak pasal yang telah dilanggar oleh *cracker* yang melakukan teknik *website defacing* ini.

Ketentuan lain mengenai penambahan pidana pokok adalah Pasal 52 ayat (3) dan (4), yakni :

(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan 37 ditujukan terhadap komputer dan/atau sistem elektronik serta informasi elekronik dan/atau dokumen elektronik milik pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada

lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan, diancam dengan pidana maksimal ancaman pidana pokok masing-masing pasal ditambah dua pertiga.

(4) Dalam hal tindak pidana sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

B. Yang Bertanggungjawab Atas Akibat Hukum Dalam Pelaksanaan Transaksi Elektronik Menurut Undang-Undang Informasi dan Transaksi Elektronik

Bank adalah lembaga kepercayaan, dalam menjalankan kegiatan *elecronic banking* (*e-banking*) harus pula memperhatikan ketentuan maupun prinsip-prinsip kehati-hatian dan manajemen resiko terkait penyelenggaraan *internet banking*, khususnya resiko reputasi dan resiko hukum.

Dalam pelaksanaan *internet banking,* permasalahan hukum akan timbul bila transaksi elektronik yang dilakukan gagal, siapakah yang akan bertanggung jawab terhadap kegagalan transaksi tersebut ? Bentuk tanggung jawab para pelaku yang terkait dengan penyelenggaraan *internet banking* dimulai dari adanya hubungan hukum antara penyedia jasa dan konsumen (nasabah) pada akhirnya melahirkan suatu hak dan kewajiban yang mendasari terjadinya suatu tanggung jawab. Tanggung jawab yang dimaksud disini adalah tanggung jawab perdata.

Mengenai permasalahan pertanggungjawaban, beberapan negara telah mengatur, sebagai berikut :

1. Di Amerika Serikat, *Electronic Fund Transfer Act* 1978 (EFTA), mengatur kerangka dasar penetapan hak, kewajiban dan tanggung

jawab peserta yang terlibat dalam transfer dana elektronik. Istilah "Transfer Dana Elektronik" secara luas meliputi transaksi elektronik yang dimulai melalui terminal, telepon, komputer, atau pita perekam suara yang berisi perintah nasabah pada lembaga keuangan untuk mendebet atau mengkredit rekening konsumen.

2. Di Australia, Kode Etik Transfer Dana Elektronik telah dirilis pada tahun 2002. Kode ini bertujuan untuk perlindungan nasabah dalam bentuk penggunaan teknologi netral untuk penyelenggaraan *e-banking* dan pembayaran produk.
3. Di Denmark, di bawah Undang-Undang Instrumen Pembayaran Tertentu, diatur bahwa dalam hal terjadi pelanggaran/penipuan oleh orang lain yang menyebabkan kerugian bagi pemegang kartu, maka penerbit bertanggung jawab, kecuali karena PIN digunakan oleh orang lain. Sebagaimana diketahui PIN bersifat pribadi dan sangat rahasia sehingga pin menjadi tanggung jawab pemegang kartu.

Di Indonesia, selain perjanjian yang mengatur hubungan keperdataan, hukum positif yang mengatur mengenai tanggung jawab penyelanggaraan elektronik adalah Undang-Undang ITE. Dalam rangka perlindungan nasabah, Undang-Undang Informasi dan Transaksi Elektronik mengatur adanya teknologi netral yang dipergunakan dalam transaksi elektronik, serta mensyaratkan adanya kesepakatan penggunaan elektronik yang dipergunakan. Hal ini tertuang dalam Pasal 3 Undang-Undang Informasi dan Transaksi Elektronik yang berbunyi :

"Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi"

Asas kebebasan memilih teknologi atau netral teknologi berarti asas pemanfaatan teknologi informasi dan transaksi elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang. Pegertian ini ditemui dalam Penjelasan Undang-Undang Informasi dan Transaksi Elektronik Pasal 3.

Selain itu setiap penyelenggara sistem elektronik diwajibkan menyediakan sistem elektronik diwajibkan untuk menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya. Namun demikian hal tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. Hal ini diatur dalam Pasal 15 ayat (1), (2) dan (3) Undang-Undang Informasi dan Transaksi Elektronik.

Dalam Penjelasan Pasal 15 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik dijelaskan bahwa "Andal" artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. Sedangkan "Aman' berarti sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. Dan "Beroperasi sebagaimana mestinya" artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. Kemudian 'Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut. Jadi berdasarkan Undang-Undang ini

membebankan penyelenggara sistem elektronik untuk menyelenggarakan sistem elektroniknya sesuai dengan kebutuhan pengguna dan terlindungi, serta memiliki kemampuan sesuai spesifikasinya dan juga bertangung jawab terhadap penyelenggaraan sistem elektronik tersebut kecuali dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik.

Undang-Undang Informasi dan Transaksi Elektronik pada Pasal 16 ayat (1) juga mengatur bahwa sepanjang tidak ditentukan lain oleh Undang-Undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut :

a. dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;
b. dapat melindungi ketersediaan, keutuhan, keontetikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan
e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Pasal 16 ayat (1) huruf b Undang-Undang Informasi dan Transaksi Elektronik maka penyelenggara sistem elektronik berkewajiban untuk melindungi ketersediaan, keutuhan, kotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut. Penyelenggara sistem elektronik *internet banking* dalam hal ini bank, berkewajiban melindungi hal tersebut diatas. Hal ini dimaksudkan agar bank dapat menjaga sistem elektroniknya agar aman dan tidak diterobos oleh pihak lain yang ingin mengambil keuntungan dengan cara melawan hukum.

Terkait dengan para pihak yang melakukan kegiatan transaksi elektronik diatur dalam Pasal 21 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik bahwa pengirim atau penerima dapat melakukan transaksi elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui agen elektronik. Dalam hal ini berdasarkan Pasal 21 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik, pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik adalah :

a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab pihak yang bertransaksi;
b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab pemberi kuasa;
c. jika dilakukan melalui agen elektronik, segala akibat hukum dalam pelaksanaa transaksi elektronik menjadi tanggung jawab agen elektronik.

Berdasarkan Pasal 1 angka 8 Undang-Undang Informasi dan Transaksi Elektronik yang dimaksud dengan agen elektronik adalah :

> "Perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang"

Kemudian Pasal 21 ayat (3) yang berbunyi :

> "Jika kerugian transaksi elektronik disebabkan gagal beroperasinya agen elektronik akibat tindakan pihak ketiga secara langsung terhadap sistem elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara agen elektronik"

Lalu Pasal 21 ayat (4) yang berbunyi :

> "Jika kerugian transaksi elektronik disebabkan gagal beroperasinya agen elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi yanggung jawab pengguna jasa layanan"

Selanjutnya Pasal 21 ayat (5) meyatakan :

> "Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik"

Jadi, Pasal 21 ayat (1), (2), (3), (4) dan (5) menjelaskan yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik, dalam hal ini *internet banking*. Apabila dapat dibuktikan bahwa kesalahan atau kelalaian

bukan dari pihak pengguna jasa layanan dalam hal ini nasabah, dan dapat dibuktikan bahwa kerugian transaksi elektronik disebabkan kegagalan beroperasinya agen elektronik diakibatkan oleh pihak ketiga atau atau kesalahan penyelenggara agen elektronik sendiri maka segala akibat hukum menjadi tanggung jawab agen elektronik. Akan tetapi, apabila dapat dibuktikan kerugian transaksi disebabkan gagal beroperasinya agen elektronik akibat kelalaian pihak pengguna jasa layanan, maka segala akibat hukum menjadi tanggung jawab pengguna jasa layanan, dalam hal ini nasabah pengguna fasilitas *internet banking*.

Sedangkan dalam ranah pidana, untuk menentukan pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik, terutama dalam transaksi *internet banking*, diperlukan suatu proses pembuktian yang sesuai dengan peraturan perundang-undangan.

Adapun pasal-pasal yang melegitimasi penggunaan alat bukti elektronik dalam pengungkapan kejahatan yang menggunakan media internet yaitu :

a. Pasal 44 Undang-Undang Informasi dan Transaksi Elektronik, menyatakan:

   Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut :

   a) alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan; dan
   b) alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)."

b. Kemudian Pasal 1 angka 1 Undang-Undang Informasi dan Transaksi Elektronik, yang berbunyi :

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan. foto, *eletronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleteks, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu melihatnya.

c. Selanjutnya Pasal 1 angka 4 Undang-Undang Informasi dan Transaksi Elektronik, yang berbunyi :

Dokumen eletronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau prforasi yang memiliki makna atau arti yang dapat dipahami oleh orang yang mampu memahaminya.

d. Kemudian Pasal 5 Undang-Undang Informasi dan Transaksi Elektronik menyatakan bahwa :

(1) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
(2) Informasi elektronik dan/atau dokumen dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.
(3) Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

Pasal-pasal diatas dianggap telah memberikan sebuah panduan kepada para penyidik untuk pengumpulan bukti-bukti elektronik di dalam usaha mereka mengungkap pelaku tindak pidana di internet, khususnya terkait mengenai *cyber crime* yang terjadi pada *internet banking*.

Alat-alat bukti elektronik tersebut biasanya digunakan untuk melengkapi alat-alat bukti yang sebelumnya diatur dalam Pasal 184 KUHAP, dimana diantara alat bukti yang sah dan boleh dipergunakan dalam pembuktian adalah :

1. Keterangan Saksi,
2. Keterangan Ahli,
3. Surat,
4. Petunjuk,
5. Keterangan Terdakwa.

Penjatuhan pidana oleh hakim diharuskan untuk menggunakan sekurang-kurangnya 2 (dua) alat bukti yang sah yang membuatnya memperoleh keyakinan bahwa telah terjadi tindak pidana dan terdakwalah yang melakukan tindak pidana tersebut. (Pasal 183 KUHAP).

Kejahatan terhadap komputer dan program komputer merupakan kejahatan yang sulit dibuktikan, karena dalam Pasal 184 KUHAP telah diberikan pembatasan berbagai alat bukti yang sah yang dapat digunakan sebagai dasar pertimbangan hakim dalam memberikan putusan. Maka pembuktian *cyber crime* terhadap komputer dan program komputer harus mengikuti ketentuan tersebut. Kini menjadi tugas penuntut umum untuk mengajukan alat-alat bukti tersebut kedepan persidangan untuk memberikan keyakinan kepada hakim mengenai

kesalahan terdakwa. Dilihat dari perkembangan teknologi saat ini, alat bukti menurut KUHAP yang dapat digunakan dalam mengadili *cyber crime*, adalah keterangan ahli, surat dan petunjuk. Ketiga alat bukti ini adalah alat-alat bukti paling esensiil memberi pembuktian yang maksimal sehubungan dengan kejahatan *cyber* yang semakin pesat perkembangannya. Tidak berarti keterangan saksi (yaitu saksi korban dan saksi lain) dan keterangan terdakwa bukan merupakan alat bukti penting, hanya saja kurang dapat memberikan pembuktian yang maksimal jika dibandingkan dengan ketiga alat bukti lain. Sebagai contoh dalam pembobolan akun *internet banking* nasabah, umumnya korban tidak menyadari akun sedang dibobol dan uangnya sedang dipindahkan keberadaannya. Biasanya nasabah mengetahui telah menjadi korban ketika nasabah tersebut melakukan pengecekan saldo. Sementara itu bukti-bukti telah terjadinya suatu tindak pidana tidak tampak atau bahkan hilang.

Lebih jauh lagi, dalam tindak pidana terhadap pembobolan akun *internet banking* jarang ditemukan orang yang dapat dijadikan saksi. Misalnya akun salah seorang nasabah dibobol oleh *cracker,* tidak ada orang yang bisa mengetahui telah atau sedang terjadi tindak pidana kecuali secara kebetulan. Padahal saksi menurut Pasal 1 butir 26 KUHAP, haruslah orang yang melihat, mendengar atau mengalami sendiri tindak pidana. Karena itu sulit mengandalkan pembuktian pada keterangan saksi, baik itu saksi korban maupun saksi lain.

Juga bila menggantungkan harapan pada keterangan terdakwa. Terdakwa tidak memberikan keterangan dibawah sumpah, terdakwa dapat berbohong atau dapat menyatakan ia tidak bersalah. Bahkan yang sering terjadi di persidangan adalah, terdakwa menyangkal keterangan yang diberikan di hadapan penyidik

dengan alasan diintimidasi ketika pemeriksaan, sehingga umumnya hakim menyatakan bahwa keterangan yang akan dipakai sebagai alat bukti yang sah adalah keterangan saksi di depan sidang pengadilan (sesuai dengan ketentuan Pasal 185 ayat (1) KUHAP).

Berita Acara Pemeriksaan dari penyidik tidak lagi memiliki kekuatan pembuktian. Sehubungan dengan itu, alat bukti keterangan ahli, surat, dan petunjuk menjadi penting artinya bagi proses pembuktian kejahatan *cyber*. Keterangan ahli merupakan bukti terkuat, dengan dasar pemikiran bahwa penggunaan komputer membutuhkan keahlian khusus. Keahlian khusus seperti memecahkan kode masuk pengaman (*security password*). Untuk membuktikan bahwa terdakwa telah melakukan kejahatan terhadap komputer dalam hal ini penyelenggaraan sistem elektronik *internet banking,* tentu dibutuhkan keterangan ahli komputer di persidangan.[53]

Permintaan keterangan ahli dimungkinkan oleh Pasal 120 KUHAP, yaitu diminta oleh penyidik. Akan tetapi, dalam KUHAP terlihat adanya beberapa kategori ahli, yaitu dokter ahli kedokteran kehakiman, dimana keterangan yang diberikannya disebut keterangan ahli lainnya. Defenisi ahli lainnya ini tidak terdapat dalam KUHAP, sehingga status dan nilai pembuktian keterangan ahli komputer belum jelas. Jadi tergantung kejelian penuntut umum untuk meyakinkan hakim agar menerima ahli komputer dan keterangannya sebagai alat bukti yang sah.

Mengenai alat bukti surat, hal ini berhubungan dengan hasil *print out* komputer. Dalam Pasal 187 KUHAP yang isinya mengenai penggolongan surat,

---

[53] Ninik Suparni, *CYBERSPACE : Problematika dan Antisipasi Pengaturannya,* Sinar Grafika, Jakarta, 2009, hlm 125

tidak disebut mengenai hal ini. Namun didalam Pasal 5 ayat (1) dijelaskan bahwa "informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Dapat penulis simpulkan apabila *print out*/hasil cetak komputer merupakan alat bukti yang sah, maka ia termasuk kedalam alat bukti surat.

Sebelum dibawa kedepan persidangan untuk pembuktian suatu kasus *cybercrime*, bukti elektronik haruslah melalui proses pengolahan terlebih dahulu. Pengolahan ini dilakukan melalui suatu cabang ilmu hukum pidana yang disebut komputer forensik.

Forensik memilik arti "membawa ke pengadilan". Istilah forensik adalah suatu proses ilmiah yang didasari oleh ilmu pengetahuan dalam mengumpulkan, menganalisis, dan menghadirkan barang bukti dalam sidang pengadilan terkait adanya suatu kasus hukum. Kekuatan forensik adalah memungkinkan menganalisa dan mendapatkan kembali fakta dari kejadian dan lingkungan.

Komputer forensik adalah metode pengumpulan, penyelamatan, mengidentifikasi, memelihara, menganalisa, dan mengajukan ke pengadilan bukti digital yang berhubungan dengan komputer, dan sesuai menurut hukum yang berlaku. Metode ini dikembangkan karena kebutuhan eksklusif akibat dari berkembangnya teknologi informasi. [54] Komputer forensik masih jarang digunakan oleh penegak hukum di Indonesia. Alat bukti elektronik dapat berbentuk cetakan atau bahkan digital, disinilah dibutuhkan peran komputer forensik.

---

[54] Feri Sulianto, *Komputer Forensik*, PT. Elex Media Komputindo, Jakarta, 2008, hlm. 150

Komputer forensik mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan juga berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan.

Secara umum komputer forensik dapat digolongkan sebagai berikut :[55]

a. Keperluan investigasi tindak kriminal dan perkara pelanggaran hukum;
b. Rekonstruksi duduk perkara insiden keamanan komputer;
c. Pemulihan-pemulihan kerusakan sistem;
d. *Troubleshooting* (kerusakan) yang melibatkan *hardware* amupun *software.*

Dalam dunia komputer forensik alat bukti elektronik disebut dengan *Digital Evidence*. Beberapa contoh bukti elektronik yang sering dijumpai dalam kehidupan sehari-hari antara lain :

a. *E-mail*, atau alamat *e-mail;*
b. Pesan dalam bentuk SMS (*Short Mesagge Service*);
c. *Wordprocessor/spread sheet files* pada komputer;
d. *Source code* diperangkat lunak;
e. *Files* berbentuk *image* ;
f. *Web browser bookmarks, cookies* pada internet;
g. Kalender, dan *to-do* list pada komputer;
h. dll.

[55] *Ibid,* hlm 3

Pengumpulan bukti elektronik dalam komputer forensik dilakukan melalui komputer dan perangkat elektronik lain yang berhubungan dengannya. Dalam melaksanakan tugas pengumpulan bukti elektronik melalui komputer forensik seorang penyidik atau investigator harus menguasai jenis-jenis kejahatan apa yang sedang ditanganinya, dan bukti elektronik apa yang harus diperiksa oleh investigator tersebut.

Menurut Feri Sulianta, bukti kejahatan komputer meliputi :[56]

a. *Bookmarks;*
b. *Configuration files;*
c. *E-mail,* surat elektronik;
d. *Log* aktivitas di internet;
e. *Internet protocol address* dan *username;*
f. *Internet Relay Chat* (IRC) *logs;*
g. *Source code;*
h. *File teks, (username* dan *password).*

Menurut penulis keberadaan komputer forensik sebagai untuk menganalisa dan mendapatkan kembali fakta dari kejadian atau lingkungan berperan penting dalam pembuktian terhadap kejahatan *cyber crime*, karena dalam era komputer ini pencatatan aktivitas dan kegiatan di dunia maya dilakukan tanpa kertas/*papperless*, kemungkinan data dan fakta telah dihapus oleh pelaku kejahatan *cyber* sangat besar, sehingga menyulitkan penyidik untuk menemukan bukti-bukti yang ada. Dengan adanya komputer forensik ini, data dan fakta yang telah dihapus masih dimungkinkan untuk ditemukan kembali dan dikemukakan

[56] *Ibid,* hlm 10

dimuka pengadilan, sehingga memungkinkan untuk memberi keyakinan pada hakim dalam memutuskan pidana yang akan dijatuhkan. Komputer forensik dapat berperan besar dalam penegakan hukum pidana terhadap pelaku kejahatan *cyber* nantinya.

Dengan telah diberlakukannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka telah secara sah berlaku pula alat bukti elektronik pada tahap penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan. Terutama terkait dengan pembuktian terhadap *cyber crime* yang terjadi dalam penyelenggaraan sistem elektronik *internet banking*. Dengan berlakunya informasi elektronik dan/atau dokumen elektronik atau hasil cetaknya maka semakin terlindungi nasabah, terutama dalam hal memperkuat pertimbangan hakim dalam penjatuhan hukuman terhadap pelaku yang melakukan pembobolan terhadap akun *internet banking* milik nasabah.

BAB IV

PENUTUP

A. Kesimpulan

1. Perlindungan bagi nasabah telah diberikan oleh bank melalui kebijakan internal yang dibuat oleh bank selaku penyelenggara sistem elektronik, namun dalam pembentukan dan penyusunan kebijakan yang sepihak ini cenderung menguntungkan dan melindungi pihak pembentuk dan penyusun sendiri yakni bank. Disinilah fungsi pemerintah sebagai pembentuk undang-undang berkewajiban melindungi nasabah dari tindakan *cyber crime* yang dapat merugikan nasabah sekaligus bank.Penulis tidak menemukan adanya suatu peraturan khusus yang melindungi dan memberikan hak-hak khusus bagi nasabah. Sehubungan dengan *internet banking* merupakan transaksi elektronik maka Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi dasar hukum yang paling dekat karena berkaitan erat dengan dunia maya, terutama dalam hal transaksi elektronik *internet banking* masih memberikan celah terjadinya kejahatan. Oleh karena itu Undang-Undang Informasi dan Transaksi Elektronik mengatur mengenai penggunaan fasilitas *internet banking* yang berkaitan dengan *cyber crime* memberikan perlindungan terhadap nasabah melalui ketentuan pidananya. Perlindungan hukum pidana preventif dapat dicapai karena di dalam Undang-Undang Informasi dan Transaksi Elektronik ancaman pidana penjara dan denda bagi pelaku kejahatan *cyber* yang berat, sehingga membuat orang takut atau tidak berani melakukan *cyber crime*. Sekalipun

terjadi *cyber crime* maka pelaku *cyber crime* akan diancam dengan pidana dan denda yang berat.

2. Berdasarkan Pasal 21 ayat (2) Undang- Undang Informasi dan Transaksi elektronik yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik adalah sebagai berikut : a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab para pihak yang bertransaksi; b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab pemberi kuasa; atau c. jika dilakukan melalui agen elektronik, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab penyelenggara agen elektronik. Untuk melakukan suatu pembuktian Undang-Undang Informasi dan Transaksi Elektronik mengatur bahwa informasi elektronik/dokumen elektronik dan/atau hasil cetaknya merupakan perluasan alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Alat bukti elektronik diakui seperti halnya alat bukti lainnya yang diatur dalam KUHAP. Sebelum dibawa kedepan persidangan untuk pembuktian suatu kasus *cyber crime,* bukti elektronik haruslah melalui proses pengolahan terlebih dahulu. Pengolahan ini dilakukan melalui suatu cabang ilmu hukum yang disebut komputer forensik.

B. Saran

1. Dikarenakan penulis tidak menemukan adanya suatu peraturan perundang-undangan yang khusus dalam pelaksanaan dan perlindungan nasabah pengguna fasilitas *internet banking*, mana penulis menilai perlu adanaya suatu

peraturan perundang-undangan yang mengatur mengenai pelaksanaan dan juga perlindungan bagi nasabah yang menggunakan fasilitas *internet banking.*

2. Perlu segera diupayakan sosialisasi *cyber law* di Indonesia yang akan sangat menunjang pemanfaatan teknologi informasi di berbagai bidang secara bertanggung jawab dan memiliki dasar hukum yang kuat baik dalam landasan hukum maupun penerapan UU Informasi dan Transaksi Elektronik.
3. Perlunya sosialisasi aktif perbankan kepada masyarakat/nasabah dan pegawai perbankan penyedia fasilitas *internet banking* mengenai bentuk-bentuk kejahatan yang dapat terjadi dengan produk/layanan *internet banking* dan memberi penjelasan kepada nasabah mengenai upaya preventif yang dapat nasabah lakukan dan telah pihak bank lakukan sebagai penyelenggara, agar memberikan edukasi kepada nasabah pengguna fasilitas *internet banking.*
4. Masih kurangnya ahli yang berkompeten di bidang telematika, maka penulis menyarakan agar pemerintah memberikan pendidikan dan pengangkatan ahli telematika baru untuk membantu pihak yang berwenang dalam mengungkap kasus-kasus *cyber crime* yang terjadi

DAFTAR PUSTAKA

1. Buku

Al. Wisnusubroto, *Strategi Penanggulangan Kejahatan Telematika,* Yogyakarta: Atma Jaya Yogyakarta, 2010.

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara,* Bandung: PT. Refika Aditama, 2005

Barda Nawawi Arief, *Tindak Pidana Mayantara,* Jakarta: PT. RajaGrafindo Persada, 2007

Budi Agus Riswandi, *Aspek Hukum Internet Banking*, Jakarta: PT. Raja Grafindo Persada, 2005

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law* : *Aspek Hukum Teknologi Informasi*, Bandung: PT. Refika Aditama, 2009

Ermansyah Djaja, *Penyelesaian Sengketa Hukum Teknologi Informasi dan Transaksi Elektronik,* Yogyakarta: Pustaka Timur, 2010

Iman Sjahputra, *Perlindungan Konsumen dalam Transaksi Elektronik,* Bandung: PT. Alumni, 2010.

Muhammad Djumhana, *Hukum Perbankan di Indonesia,* Bandung: PT Citra Aditya Bhakti, 2000.

Mukti Fajar ND dan Yulianto Ahmad, *Dualisme Penelitian Hukum* : *Normatif dan Empiris,* Yogyakarta: Pustaka Pelajar, 2010

Niniek Suparni, *CYBERSPACE : Problematika dan Antisipasi Pengaturannya*, Jakarta: Sinar Grafika, 2009

Ronny Prasetya, *Pembobolan ATM : Tinjauan Hukum Perlindugan Nasabah Korban Kejahatan Perbankan,* Jakarta: Prestasi Pustaka, 2010

Soerdjono Soekanto, *Pengantar Penelitian Hukum,* Jakarta: UI-Press, 1986.

Sutan Remy Syhadeini, *Kejahatan & Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009

Tb. Irman S, *Anatomi Kejahatan Perbankan*, Jakarta: MQS Publishing, 2006

2. Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan Undang-Undnag Nomor 7 Tahun 1992 tentang Perbankan.

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

3. Internet

Hermansyah, *Makalah Tinajaun Yuridis Nasabah Penyimpanan Dana Terhadap Bank Yang Dilikuidasi,* dikutip dari http//:repository.usu.ac.id.bitstream1234.pdf, hlm. 4-5, diakses tanggal 4 Januari 2011

Rezqy Fardj, "Hukum dan *Internet Banking*" dikutip dari *http://rezqy-fardj.blog.friendster.com/2008/04/hukum-dan-internet-banking* diakses tanggal 5 Januari 2011

http://www.republika.co.id/berita/br...ah-rp-255-juta. Diakses tanggal 1 Februari 2011.

www.**maubaca**.com/**cara-cracker-membobol-internet-banking**/.html. Diakses tanggal 8 April 2011

http://keamananinternet.tripod.com/keamanan-internet-banking.html. Diakses tanggal 19 April 2011

http://ekaeldoneris.wordpress.com/2008/12/09/perlindungan-hukum-bagi-nasabah-pengguna-internet-banking/.html. Diakses tanggal 24 April 2011

www.klikbca.com. Diakses tanggal 28 April 2011

www.bankmadiri.co.id. Diakses tanggal 28 April 2011

http://id.m.wikipedia.org/wiki/Kejahatan_dunia_maya diakses tanggal 16 Juni 2011