BAB III

PENCURIAN DANA NASABAH BANK MELALUI MODUS PENGGANDAAN KARTU ATM (SKIMMER)

A. Pihak-Pihak Yang Terkait Pencurian Dana Nasabah Bank Melalui Modus Skimmer

Masyarakat kini telah semakin banyak memanfaatkan Teknologi secara intensif di dalam setiap aspek kehidupannya. Pemanfaatan ini bukan hanya dilakukan oleh masyarakat perkotaan dan kelas sosial menengah ke atas tetapi untuk jenis teknologi dan media elektronik tertentu juga telah meluas hingga ke masyarakat pedesaan dan kelas sosial menengah ke bawah. Media elektronik sebagai salah satu sarana Teknologi Informasi, tidak digunakan untuk penyebaran informasi yang bersifat satu arah saja, namun kini juga menjadi sarana transformasi informasi dan data yang bersifat interaktif sehingga transaksi ekonomi pun dapat dilakukan melalui media elektronik, misalnya terjadi pada teknologi telepon, internet, dan sebagainya.

Industri perbankan adalah salah satu bidang jasa yang secara intensif menyelenggarakan layanan dengan memanfaatkan media elektronik (*electronic banking*). Sebagian besar bank pada saat ini bahkan mengandalkan teknologi informasi dan media elektronik sebagai basis layanannya, sehingga layanan perbankan yang diselenggarakannya kini menawarkan berbagai kemudahan

yang dapat dimanfaatkan masyarakat setiap saat dan dimana saja, tidak dibatasi jarak, ruang dan waktu.

Segala layanan sistem informasi bank yang dinikmati nasabah memerlukan proses yang panjang. Tahap-tahap yang harus dilalui sebelum bentuk layanan tersedia kepada nasabah. Tahapan-tahapan layanan perbankan tersebut adalah sebagai berikut :[17]

1. Mengetahui kebutuhan atau keinginan nasabah yaitu dengan cara melakukan penelitian, baik kepada nasabah maupun pesaing, apa yang telah dapat diakses kepada nasabahnya atau apakah ada produk baru yang belum ada di pasaran, serta hal-hal lain yang berkaitan dengan perkembangan teknologi komputer serta produk-produk bank.
2. Memperhitungkan kemampuan yang dimiliki pada saat itu, meliputi tersedianya sarana pendukung (perangkat keras, perangkat lunak, biaya) serta tingkat urgensi kebutuhan nasabah dibandingkan dengan kemampuan yang dimiliki. Apabila ternyata setelah dianalisa belum dimungkinkan untuk melakukan komputerisasi maka tahapan tersebut bisa langsung dihentikan, namun, apabila dimungkinkan maka bisa langsung melanjutkan ke tahapan berikutnya.

[17] Kotrik Sudarno, *Pelayanan Jasa Perbankan Melalui Komputer,* September-Oktober, vol. 55, hlm. 18

3. Menjabarkan kebutuhan nasabah secara rinci dalam bentuk *User Requirements,* untuk mengetahui tingkat kompleksitasnya serta hubungannya dengan produk pelayanan yang telah ada.
4. Menyusun program aplikasi untuk diproses dalam komputer atau membeli paket perangkat lunak yang sesuai kebutuhan.
5. Melakukan sistem *testing* untuk meyakini bahwa proses komputerisasi tersebut akan berhasil baik.
6. Melakukan uji coba produksi di salah satu cabang bank dan apabila telah berhasil baru dilakukan implementasi secara menyeluruh, sehingga seluruh nasabah dapat menikmati bentuk layanan baru tersebut.
7. melakukan evaluasi untuk penyempurnaan lebih lanjut.

Semua bank nasional pada saat ini telah terhubung secara *online* dan ada yang bergabung dengan jaringan kerjasama layanan *e-banking* lokal maupun internasional untuk memperluas jaringan dan meningkatkan efisiensi layanan serta sekaligus meminimalisir biaya operasional dan perawatan, misalnya untuk layanan ATM yang kini paling banyak digunakan oleh nasabah perbankan, pihak bank tidak hanya menyediakan layanan ini melalui jaringan mesin ATM yang dimiliki sendiri[18] (seperti BCA 6.000 ATM, Mandiri 3.000 ATM, BNI 3.000 ATM, BRI 4.000 ATM) melainkan juga bergabung dengan jaringan

[18] *Ibid.*

mesin ATM yang diselenggarakan oleh pihak lain baik itu lokal (ATM Bersama, 11.000 ATM) dan internasional (Plus, Cirrus, Alto, Link dll. yang memiliki jutaan ATM di seluruh dunia).

Nasabah pengguna kartu ATM tidak harus tergantung dan melakukan transaksi dari mesin ATM bank yang bersangkutan, nasabah bank dapat menggunakan ATM lain yang memiliki kerjasama dengan bank penerbit asalnya. Biasanya logo jaringan ATM yang didukung tertera di setiap kartu ATM. Sehingga pengguna bisa memilih. Semua bank nasional kini menerbitkan kartu ATM, bahkan beberapa bank nasional secara otomatis akan memberikan kartu ATM kepada nasabah untuk setiap pembukaan rekening baru. Diperkirakan pada akhir tahun 2009 di Indonesia ada sekitar 50 juta pengguna kartu ATM aktif[19] dimana sebagian besar dari kartu ATM tersebut juga berfungsi sebagai kartu debit (dapat digunakan sebagai media pembayaran elektronik di *merchant* pembelanjaan yang memiliki kerjasama dengan bank).

Semakin luasnya pemanfaatan kartu ATM dan kartu kredit sebagai alat pembayaran mendorong tumbuhnya layanan perbankan lain yang ditujukan kepada merchant pembayaran yaitu sistem (*electronic data capture*) atau EDC. Saat ini di seluruh dunia sistem EDC telah digunakan jutaan counter merchant yang meliputi hampir seluruh jenis transaksi ekonomi yang bersifat konsumsi baik itu barang maupun jasa. Sistem EDC selain memiliki kelebihan berupa kemudahan dan manfaat luas yang meningkatkan kualitas kehidupan manusia,

[19] *Ibid.*

maka layanan perbankan elektronik juga memiliki banyak kelemahan yang patut diwaspadai dan diantisipasi, sehingga teknologi tersebut tetap dapat dipakai, manfaatnya terus dinikmati oleh umat manusia namun juga harus ada tanggung jawab, pengawasan dan upaya untuk memperbaiki kelemahan, menanggulangi permasalahan yang mungkin timbul serta yang paling penting adalah meningkatkan kesadaran dan menanamkan pemahaman tentang resiko dari pemanfaatan teknologi yang digunakan oleh layanan perbankan itu terutama kepada masyarakat luas, pengguna/nasabah, pemerintah/regulator, aparat penegak hukum dan penyelenggara layanan itu sendiri (bank, merchant).

Kerawanan prosedur perbankan yang paling menonjol adalah lemahnya proses identifikasi dan validasi calon nasabah[20]. Masalah ini bukan sepenuhnya kesalahan bank, karena di Indonesia belum diterapkan Single Identity Number (SIM) yang terintegrasi antar departemen terkait pelaksanaan pelayanan publik, sehingga mudah sekali untuk melakukan pemalsuan identitas dan mengecoh sistem validasi bank sehingga akhirnya akan berakibat pada penyalahgunaan rekening, fasilitas dan layanan terkait dengan nasabah seperti kartu ATM/debit untuk kegiatan kejahatan mulai penipuan, pencurian hingga ke pencucian uang. Kecenderungannya para pelaku kejahatan akan memilih untuk sejauh mungkin hanya menggunakan layanan elektronik saja, menghindari transaksi dan kontak fisik baik dengan petugas bank maupun korban. Hal yang paling mengkhawatirkan dan terbukti paling sering dieksploitasi oleh pelaku kejahatan adalah kerawanan prosedur pada mesin ATM dan mesin EDC.

[20] *Ibid.*

Masalahnya adalah minimnya upaya pengawasan bank terhadap dua sistem tsb. Sehingga nasabah dituntut untuk lebih berhati-hati/waspada saat bertransaksi di ATM dan EDC. Bukan hanya modus eksploitasi yang melibatkan teknologi seperti skimming namun juga yang konvensional seperti hipnotis serta aneka penipuan via SMS, undian berhadiah dan lain-lain. Sangat jarang dijumpai pesan peringatan (reminder) kepada nasabah maupun upaya peningkatan sistem pengamanan yang memadai dengan misalnya memasang kamera pengawas di semua ATM.

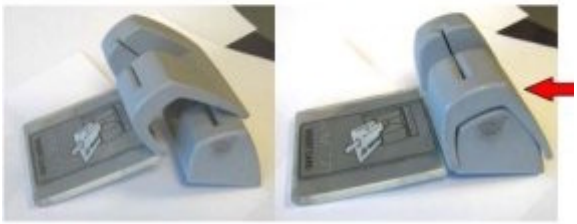
Sebagian besar kartu ATM yang digunakan bank saat ini jenisnya *magnetic stripe card* yang tidak dilengkapi pengaman chip (*smart card*). Kartu jenis ini sangat mudah digandakan. Perangkat penggandaan dan bahan baku kartu magnetic ini dapat dengan mudah dijumpai di pasaran dengan harga yang sangat murah. Pelaku kejahatan menyalahgunakan kemajuan teknologi sedemikian rupa sehingga modus-modus tersebut berkembang, salah satu contohnya kejahatan ekonomi di bidang perbankan yang mengakibatkan timbulnya korban, korban akibat dari kejahatan ekonomi di bidang perbankan meliputi nasabah penyimpan dana, dan pihak bank.

Teknologi informasi merupakan sesuatu yang bersifat netral, teknologi diartikan bebas nilai. Teknologi tidak dapat dilekati sifat baik dan jahat, akan tetapi pada perkembangannya kehadiran teknologi memberi peluang pihak-pihak yang berniat jahat untuk menyalahgunakannya. Bermacam-macam jenis kejahatan yang dapat dilakukan, salah satu jenis kejahatan teknologi di bidang

perbankan yang marak terjadi beberapa waktu lalu, yaitu pencurian dana nasabah bank melalui modus penggandaan kartu ATM (*skimmer*). Kasus ini sebetulnya telah lama diketahui bersama dan telah banyak kasus yang terjadi. kejadian pun terulang kembali sampai berita tentang pencurian dana 200 nasabah BCA diketahui masyarakat, wakil direktur utama Bank Central Asia, Jahja Setiaatmadja mengatakan kerugian akibat pencurian dengan modus skimmer mencapai lima milyar rupiah, bank yang terkena pencurian selain Bank BCA adalah Bank BRI, Bank Mandiri, Bank BNI, Bank Permata, dan Bank BII.



The real card reader slot. The capture device



The side cut out is not visible when on the ATM.

1. gambar *Electronic Data Capture* atau *Skimmer*



2. gambar mesin ATM yang sudah dipasang Skimmer



3. gambar mesin ATM yang dipasangi kamera oleh pelaku *Skimmer*

Saat ini baru kartu kredit saja yang telah diganti dengan jenis smart card sejak Januari 2010 sesuai ketentuan Bank Indonesia[21]. Seharusnya penggantian jenis kartu dan peningkatan teknologi yang digunakan harus lebih

[21] *ibid.*

sering dilakukan karena modus kejahatan pun semakin cepat mengalami perubahan. Selain jenis *smart card*, sekarang juga sudah dikembangkan jenis kartu lain (*next generation*) yang lebih kuat teknologi pengamanannya. Standar pengamanan mesin ATM dan EDC juga masih sangat kurang. Seharusnya mesin ATM dilengkapi dengan sensor, alarm, kamera pengawas dan berbagai mekanisme pengamanan lainnya, misalnya penggunaan *privacy screen* dengan sudut penglihatan yang sempit, cover untuk melindungi *numeric keypad*, hinga anti *skimming card reader hole*. melihat teknologi yang kini tersedia, semua fasilitas pengamanan itu dapat diselenggarakan dengan biaya yang murah.

Sehubungan dengan tindak kejahatan pencurian dana nasabah bank melalui modus penggandaan kartu ATM (skimmer), terdapat pihak-pihak terkait, yaitu:

1. Pelaku kejahatan Skimer, yaitu orang-orang yang memanfaatkan kelemahan dari keamanan sistem elektronik perbankan, dan menyalahgunakan perkembangan teknologi informasi sebagai sarana untuk melakukan pencurian dana nasabah bank. Pelaku Skimmer mencari target sasarannya pada mesin ATM yang lemah, misalkan pada ATM yang tidak dilengkapi penjagaan pengamanan, sepi dan tidak ada kamera keamanannya (CCTV).
2. Nasabah bank, sebagai pihak yang menggunakan jasa bank harus memiliki pemahaman mengenai kemungkinan risiko kerawanan dan kelemahan pada sistem elektronik yang digunakan dan mendapatkan update informasi

tentang masalah keamanan di dunia perbankan bahkan bila diperlukan bank harus melakukan kampanye secara umum agar nasabah paham adanya ancaman bahaya. Misalnya, harus dijelaskan kondisi di sekitar mesin ATM dan prosedur serta etika yang sebaiknya diterapkan ketika memanfaatkan layanan tsb. Contoh: perlunya jarak antrian dalam batas yang aman agar orang tidak mudah mengintip. Layanan peringatan (reminder, misalnya via SMS) berupa anjuran untuk mengganti PIN dan password secara rutin, pesan kewaspadaan terhadap aneka modus penipuan, termasuk praktek skimming.

3. Bank, sebagai suatu lembaga keuangan yang eksistensinya tergantung mutlak pada kepercayaan dari pada nasabahnya yang mempercayakan dana dan jasa-jasa lain yang mereka lakukan melalui bank pada khususnya, dan dari masyarakat luas pada umunya. Oleh karena itu, bank sangat berkepentingan menjaga agar kepercayaan masyarakat terpelihara dengan baik. Mengingat bank adalah bagian dari sistem keuangan dan pembayaran, yang masyarakat luas berkepentingan atas kesehatan dari sistem-sistem tersebut, sedangkan kepercayaan masyarakat kepada bank merupakan unsur paling pokok dari eksistensi suatu bank, maka terpeliharanya kepercayaan masyarakat kepada perbankan adalah juga menjadi kepentingan masyarakat banyak[22]. Pada kasus Pencurian dana nasabah melalui modus *Skimmer* bank harus menjadi pihak yang

[22] Diktat Mata Kuliah Hukum Perbankan, Budi Fitriadi, Fakultas Hukum, Universitas Komputer Indonesia, 2007

bertanggung jawab karena posisi sebagai sistem penyelenggara layanan transaksi elektronik.

Di negara lain, misalnya Jepang[23], pemerintah menerapkan aturan yang mengubah cara berfikir dunia perbankan di dalam mensikapi terjadinya insiden keamanan. Pemerintah Jepang justru mewajibkan kepada pihak bank yang mengalami insiden/serangan untuk membuka informasi secara detail bukan hanya kepada nasabah melainkan juga kepada publik sehingga terjadi proses pembelajaran dan terbentuk kesadaran terhadap aspek keamanan dan pengamanan. Sehingga bank lain dapat secepatnya melakukan antisipasi seandainya memiliki kelemahan serupa.

Masyarakat pada umumnya dan nasabah pada khususnya harus terus mendapatkan informasi terkini, informasi tentang masalah keamanan di dunia perbankan bahkan bila diperlukan sarana untuk mengamankan diri. Bank harus melakukan kampanye secara umum agar masyarakat dan nasabah paham adanya ancaman bahaya. Misalnya, harus dijelaskan kondisi di sekitar mesin ATM dan prosedur serta etika yang sebaiknya diterapkan ketika memanfaatkan layanan tersebut.

[23] http://www.idsirtii.or.id diakses selasa 1 juni 2010 pukul 23.00 WIB

B. Akibat Hukum Yang Timbul Dari Tindak Pidana Pencurian Melalui Modus Skimmer

Perkembangan ilmu pengetahuan dan teknologi khususnya teknologi informasi dan komunikasi telah menimbulkan pengaruh hampir dalam seluruh aspek kehidupan manusia dan kegiatannya di masyarakat termasuk di bidang perbankan. Kemajuan teknologi informasi dan komunikasi di perbankan nasional memberikan kemudahan bagi nasabah bank, sebagian besar bank pada saat ini bahkan mengandalkan teknologi informasi dan media elektronik sebagai dasar pelayanannya, seiring dengan kemudahan untuk melakukan transformasi secara cepat melalui pemanfaatan teknologi ternyata dari segi hukum membawa konsekuensi tersendiri. Konsekuensi hukum yang terlihat, yakni bentuk kejahatan hukum yang mengarah kepada suatu perbuatan kriminal[24].

Sejalan dengan kemajuan teknologi informasi, telah muncul beberapa kejahatan yaitu kejahatan yang timbul sebagai akibat penyalahgunaan perkembangan teknologi, yang membentuk *cyber space.* Kejahatan ini sering dipersepsikan sebagai kejahatan yang dilakukan dalam ruang atau wilayah *cyber.* Kejahatan pada saat ini terus berkembang modus operandinya dapat diambil salah satu contoh kasus adalah pencurian dana nasabah bank melalui penggandaan kartu ATM.

Perbankan merupakan suatu lembaga kepercayaan masyarakat, kemajuan teknologi, informasi, komunikasi dan ilmu pengetahuan. Sementara

[24] Budi Agus Riswandi, *Aspek Hukum Internet Banking,* Rajawali Pers, Jakarta. 2005, hlm. 188

itu, sistem kontrol dan pengawasan internal perbankan sendiri belum cukup memadai, sehingga potensi terjadinya pelanggaran terhadap aturan perbankan akan membuka peluang terjadinya kejahatan. Sektor perbankan menempati posisi sangat strategis dalam perekonomian nasional. Lembaga perbankan sangat penting dalam menunjang sistem keuangan nasional, sekaligus sebagai lembaga intermedisasi. Lembaga perbankan nasional di Indonesia berada dalam tanggung jawab Bank Indonesia. Lembaga perbankan yang dimaksud adalah menyangkut tentang bank, baik kelembagaan, kegiatan usaha maupun cara dan proses dalam melaksanakan kegiatan usahanya.

Lembaga perbankan selalu memanfaatkan kemajuan teknologi informasi dan komunikasi yang modern untuk melakukan setiap transaksi keuangannya. Akan tetapi, *risk management* dan *internal control sistem* di lingkungan perbankan sendiri masih belum memadai, sehingga potensi terjadinya tindak kejahatan di lingkungan perbankan menjadi sangat besar. Kegiatan operasional suatu bank bertumpu pada ketersediaan sumber dana dan pengelolaan sumber dana. Apabila salah dalam mengurus pengelolaan dana, pasti akan menimbulkan permasalahan pada bank.

Pesatnya perkembangan ilmu pengetahuan dan teknologi melahirkan berbagai dampak, baik dampak positif maupun dampak yang negatif. Dampak positif merupakan hal yang diharapkan dapat bermanfaat bagi kehidupan manusia di dunia termasuk di negara Indonesia sebagai negara berkembang, yang mana hasil dari kemajuan ilmu pengetahuan dan teknologi ini dibuat dalam berbagai bentuk sehingga dapat dimanfaatkan oleh masyarakat.

Dampak negatif yang timbul dari kejahatan dalam bidang perbankan yang dalam hal ini berupa pencurian dana nasabah bank melalui modus penggandaan kartu ATM melahirkan timbulnya akibat hukum karena hal tersebut dapat mengakibatkan kerugian bagi banyak pihak, terutama pihak bank dan nasabahnya.

Teknologi informasi menyentuh setiap aspek kehidupan manusia yang dapat menimbulkan kejahatan, baik kejahatan itu dilakukan dengan menggunakan sarana-sarana dari sistem atau jaringan komputer, di dalam sistem atau jaringan komputer, dan terhadap sistem atau jaringan komputer[25]. Dalam kejahatan pencurian dana nasabah bank melalui penggandaan kartu ATM, tindak kejahatan tersebut dilakukan dengan menggunakan sarana dari sistem komputer dan terhadap sistem atau jaringan komputer, yaitu dengan mengambil data elektronik yang terdapat dalam kartu ATM korbannya dan memindahkan data elektronik tersebut pada pita magnetik kartu ATM yang baru, dengan demikian pelaku dapat dengan leluasa menggunaan kartu ATM tersebut dan mengambil uang korbannya melalui mesin ATM. Pada Kitab Undang-Undang Hukum Pidana (KUHP) tindak pidana pencurian dimuat dalam Pasal 362, sedang penggolongannya diatur dalam Pasal 363 (pencurian dengan pemberatan), Pasal 364 (pencurian ringan), Pasal 365 (pencurian yang disertai dengan kekerasan/ancaman kekerasan, Pasal 367 (pencurian di lingkungan keluarga). Pada pencurian dana nasabah bank melalui modus penggadaan kartu ATM (*Skimmer*) dapat diterapkan Pasal 363 ayat (5) KUHP, Pasal tersebut

[25] Barda Nawawi Arief, *Masalah Penegakan Hukum Dan kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan,* Kencana, Jakarta. 2007, Hlm 243.

memperluas pengertian kunci palsu dan perintah palsu sehingga kartu ATM yang telah digandakan dan nomor Pin ATM korban yang diketahui pelaku *skimmer* yang digunakan dalam pencurian tersebut termasuk di dalamnya artinya Pasal 363 ayat (5) KUHP dapat diakomodasi menjadi acuan tindak pidana pencurian dana nasabah bank dengan modus penggandaan kartu ATM (skimmer).

Pada Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) pelaku kejahatan yang menyalahgunakan teknologi perbankan dengan melakukan pencurian dana nasabah bank melalui modus skimmer dapat dijerat dengan pasal 30 ayat (3) UU ITE yang menyebutkan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Pasal 32 ayat (1) UU ITE juga merupakan ketentuan yang dapat diakomodasikan dalam pencurian dana nasabah bank melalui skimmer, pasal tersebut menyebutkan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan atau dokumen elektronik milik orang lain atau milik publik.

Kejahatan perbankan dengan menggunakan teknologi komputer ini telah menyebabkan kerugian besar terhadap banyak pihak, kerugian yang ditimbulkan akibat pencurian dana nasabah bank melalui penggandaan kartu

ATM melahirkan akibat hukum, karena hal tersebut mengakibatkan kerugian secara materil maupun immateril. Dalam hal ini korban dari pencurian melalui modus *skimmer* mengalami kerugian akibat tindakan pelaku kejahatan yang mencuri informasi personal seperti *Personal Identification Number* (PIN) dan data elektronik dalam kartu ATM untuk keuntungan dirinya. Kemajuan teknologi komputer, teknologi informasi dan teknologi komunikasi menimbulkan suatu tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan tersebut tidak terlepas dari sifatnya yang khas sehingga membawa persoalan baru yang rumit untuk dipecahkan, berkenaan dengan masalah penanggulangannya.

Kejahatan perbankan pencurian dana nasabah melalui penggandaan kartu ATM juga menimbulkan akibat hukum bagi pelakunya, meskipun dalam melakukan kejahatannya pelaku menggunakan alat-alat teknologi komputer, namun tetap dikategorikan sebagai tindakan atau perbuatan hukum yang nyata, dalam hal ini pelaku dapat dikenakan pasal 363 ayat (5) KUHP, yaitu pencurian dengan menggunakan kunci palsu, perintah palsu atau pakaian jabatan palsu, dengan ancaman hukuman penjara selama-lamanya tujuh tahun, dan juga pelaku dapat dikenakan pasal 32 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik, tentang memindahkan informasi elektronik dan atau dokumen elektronik milik orang lain atau milik publik dengan ancaman hukuman penjara paling lama delapan tahun dan/atau denda paling banyak dua miliar rupiah.

Alat bukti kejahatan teknologi biasanya berupa komputer, *laptop*, atau alat elektronik lainnya, alat bukti dalam kejahatan perbankan menjadi suatu kendala lain, karena pada saat pembuktian pada alat bukti tidak dapat digunakan karena dalam Kitab Undang-Undang Hukum Acara Pidana tidak diatur mengenai alat bukti elektronik. Namun dengan adanya Undang-Undang no.11 tahun 2008 tentang Informasi dan Transaksi Elektronik, maka alat bukti telah diatur undang-undang tersebut. Pada pasal 5 ayat (1) UU ITE dijelaskan bahwa informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti yang sah. Oleh karena itu apabila terjadi kejahatan teknologi elektronik dapat segera dilakukan proses penyelidikan dan penyidikan sebagaimana yang terdapat dalam pasal 44 Undang-Undang tentang Informasi dan Transaksi Elektronik mengenai alat bukti dalam proses penyelidikan, penyidikan dan dalam sidang pengadilan. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang terbuat dari kertas. Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, terutama di bidang perbankan, agar dapat dimanfaatkan secara optimal baik oleh pihak bank maupun nasabahnya.