BAB IV

ANALISIS HUKUM MENGENAI PENCURIAN DANA NASABAH BANK MELALUI MODUS PENGGANDAAN KARTU ATM (SKIMMER) DIHUBUNGKAN DENGAN PASAL 363 AYAT (5) KITAB UNDANG-UNDANG HUKUM PIDANA (KUHP) JUNCTO UNDANG-UNDANG NO.11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (ITE)

A. Pembuktian Mengenai Pencurian Dana Nasabah Bank melalui Modus Penggandaan Kartu ATM (Skimmer) dihubungkan dengan Pasal 363 ayat (5) kitab Undang-Undang Hukum Pidana (KUHP) Juncto Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Teknologi terus berkembang seiring dengan perkembangan peradaban manusia, kini hampir semua kegiatan industri dan bahkan rumah tangga memanfaatkan kemajuan teknologi. Perkembangan teknologi dan penerapannya ini telah menyusup dan berpengaruh secara kuat dalam kehidupan modern, bahkan sebagian besar kegiatan bisnis telah mempercayakan pada teknologi tersebut, salah satunya industri perbankan. Perkembangan teknologi memberikan kontribusi yang sangat besar bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, namun demikian terdapat pula dampak negatif yang tidak dapat dihindari, seperti pencurian dana nasabah bank melalui penggandaan kartu ATM. Dalam hal pencurian dana nasabah bank melalui penggandaan kartu ATM, pelaku kejahatan biasanya menggunakan teknologi komputer dan memanipulasi

data dengan cara memindahkan data elektronik yang terdapat pada kartu ATM korbannya ke kartu ATM milik pelaku dengan bantuan program komputer, sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil yaitu perbuatan seseorang yang memasuki komputer orang lain tanpa izin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Pencurian dana nasabah bank melalui penggandaan kartu ATM (skimmer) telah menjadi ancaman stabilitas dan rasa aman nasabah bank, sehingga pihak bank sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer.

Kecanggihan teknologi komputer telah memberikan kemudahan-kemudahan, terutama dalam membantu pekerjaan manusia. Selain itu, perkembangan teknologi komputer menyebabkan munculnya jenis kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandi. Penyalahgunaan komputer dalam perkembangannya sangat rumit, terutama kaitannya dengan proses pembuktian tindak pidana. Apalagi penggunaan komputer untuk tindak kejahatan itu memiliki karakteristik tersendiri atau berbeda dengan kejahatan yang dilakukan tanpa menggunakan komputer (konvensional). Perbuatan atau tindakan, pelaku, alat bukti ataupun barang bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer.

Maraknya kejahatan yang terjadi dalam bidang perbankan, seperti pencurian dana nasabah bank melalui modus skimmer, mempengaruhi stabilitas dan rasa aman bagi nasabah bank. Kemajuan teknologi informasi

yang menjadi nilai awal dari keberadaan *cyber crime*, secara yuridis dapat membawa dampak pada hukum yang mengatur tentang hal tersebut.

Berdasarkan Pasal 5 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dinyatakan bahwa :

" 1. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi Elektronik dan/atau 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.
4. Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

   a. Surat yang menurut undang - undang harus dibuat dalam bentuk tertulis; dan
   b. Surat beserta dokumennya yang menurut Undang - undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta."

Pasal 5 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik di atas merupakan perluasan dari alat bukti yang sah sebagaimana diatur dalam pasal 184 KUHAP, yaitu:

1. Keterangan saksi-saksi, dalam Pasal 185 KUHAP ayat (1) disebutkan bahwa keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan dalam persidangan. Penjelasan KUHAP menyatakan bahwa dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain. Pasal 1 angka (27) KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri,

lihat sendiri dan dialami sendiri dengan menyebut alasan dari pengetahuannya itu.

2. Keterangan ahli, Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Selanjutnya penjelasan Pasal 186 KUHAP menyatakan bahwa keterangan ahli ini dapat juga sudah diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam suatu bentuk laporan dan dibuat dengan mengingat sumpah di waktu ia menerima jabatan atau pekerjaan. Menurut teori hukum pidana yang dimaksud dengan keterangan ahli adalah keterangan yang diberikan seseorang berdasarkan ilmu dan pengetahuan yang dikuasainya.
3. Surat, diatur dalam Pasal 187 KUHAP, yang dibedakan atas empat macam surat, yaitu :
    a. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, didengar, dilihat atau dialaminya sendiri, disertai dengan alasan tentang keterangan itu;
    b. Surat yang dibuat menurut peraturan undang-undang atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukan bagi pembuktian sesuatu hal atau keadaan;
    c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau keadaan yang diminta secara resmi dari padanya; dan

d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

4. Petunjuk, Pasal 188 ayat (1) KUHAP memberi definisi petunjuk sebagai perbuatan, kejadian atau keadaan, yang karena penyesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya. Selanjutnya Pasal 188 ayat (3) KUHAP dinyatakan bahwa penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif lagi bijaksana, setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.
5. Keterangan terdakwa, menurut Pasal 189 ayat (1) KUHAP adalah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri dan alami sendiri. Keterangan terdakwa tidak perlu sama dengan pengakuan, karena pengakuan sebagai alat bukti mempunyai syarat, yaitu :
   a. Mengaku ia yang melakukan delik yang didakwakan; dan
   b. Mengaku ia bersalah

Berdasarkan alat bukti yang disebutkan dalam Pasal 184 KUHAP, mengenai alat bukti telah diterangkan bahwa dalam kejahatan dengan menggunakan komputer dapat ditemukan beberapa alat bukti yang tertera di dalam Pasal 184 KUHAP, yaitu alat bukti surat, keterangan ahli, dan petunjuk. Selain itu, berdasarkan Pasal 5 ayat (1) Undang-Undang Nomor 11

Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengenai alat bukti berupa informasi elektronik dan/atau dokumen elektronik, apabila dikaitkan dengan Pasal 184 KUHAP termasuk alat bukti surat, maka dalam hal ini pelaku kejahatan pencurian dana nasabah bank dengan modus skimmer dapat dijerat dengan alat bukti tersebut karena pelaku menggunakan teknologi komputer yang dinamakan skimmer (EDC) untuk memindahkan data elektronik dari kartu ATM milik korbannya dan memindahkan ke kartu ATM milik pelaku untuk keuntungannya. Selama bukti ini dikeluarkan oleh yang berwenang dan sebuah jaringan komputer tersebut dapat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP. *Kedua* keterangan ahli, peran keterangan ahli merupakan untuk memberikan suatu penjelasan di dalam persidangan bahwa dokumen yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum. *Ketiga* alat bukti petunjuk, alat bukti petunjuk dilakukan oleh hakim dengan melihat dari perbuatan dalam hal ini hakim melihat perbuatan pelaku kejahatan dengan modus pencurian dana nasabah bank dengan modus penggandaan kartu ATM telah merugikan pihak bank dan nasabahnya, sehingga hakim dapat memutus perkara dan menjatuhkan hukuman kepada pelaku kejahatan pencurian dana nasabah bank melalui penggandaan kartu ATM dengan peraturan perundang-undangan yang berlaku. selain itu, hakim melihat dari kejadian atau keadaan yang menggambarkan adanya niat dari pelaku kejahatan dengan modus pencurian dana nasabah bank untuk melakukan kejahatan yang dalam aksinya pelaku memindahkan informasi elektronik dan/atau dokumen elektronik dari kartu ATM korbannya, sehingga hakim dapat melihat dari

keadaan tersebut dan memberikan keputusan yang memberatkan atau meringankan pelaku kejahatan dengan modus pencurian dana nasabah bank dengan modus skimmer. Alat bukti yang disebutkan Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dapat menjerat pelaku kejahatan dengan menggunakan teknologi komputer yang mana para tersangka tersebut memiliki informasi elektronik dan/atau dokumen elektronik yang tersimpan dalam pita magnetik di kartu ATM milik korbannya yang kemudian dipindahkan data elektroniknya ke kartu ATM yang baru milik pelaku yang digunakan untuk keuntungannya.

Pada kasus pencurian dana nasabah melalui modus skimmer, pelaku dapat dikenakan atau dijerat dengan 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. Pada Pasal 5 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyebutkan bahwa :

> “Informasi elektronik dan/atau dokumen elektronik merupakan perluasan dari alat bukti yang sesuai dengan hukum acara yang berlaku di Indonesia”

Dengan demikian, proses pembuktian atas tindak pidana pencurian/pembobolan dana pada bank termaksud dalam Pasal 184 KUHP dan Pasal 5 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tersebut bahwa pelaku kejahatan dapat dijerat oleh hukum pidana yang berlaku, dalam hal ini dapat digunakan pasal 363 ayat(5) Kitab Undang-Undang Hukum Pidana dan Pasal 32 ayat (1)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Berdasarkan Pasal 363 ayat (5) KUHP, ditegaskan bahwa :

> “Pencurian yang dilakukan oleh tersalah dengan masuk ketempat kejahatan itu atau dapat mencapai barang untuk diambilnya, dengan jalan membongkar, memecah atau memanjat atau dengan jalan memakai kunci palsu, perintah palsu atau pakaian jabatan palsu”

Unsur-unsur dalam Pasal 363 ayat (5) Kitab Undang-Undang Hukum Pidana (KUHP) tersebut terdiri dari :

1. Unsur subjektif:

   Dengan maksud untuk menguasai secara melawan hukum

2. Unsur objektif :
   a. Barang siapa;
   b. Mengambil, yaitu setiap tindakan yang membuat sebagian harta kekayaan orang lain menjadi berada dalam penguasaannya tanpa bantuan atau tanpa izin orang lain tersebut, ataupun untuk memutuskan hubungan yang masih ada antara orang lain itu dengan bagian harta kekayaan yang dimaksud;
   c. Sesuatu benda;
   d. Yang sebagian atau seluruhnya kepunyaan orang lain.

Pasal 363 ayat (5) KUHP dapat diterapkan pada telah pelaku pencurian dana nasabah bak melalui penggandaan kartu ATM karena telah memenuhi unsur-unsur yang terdapat pada pasal tersebut. Pasal 363 ayat (5) KUHP 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 dalam tindak pidana pencurian dana nasabah bank dengan modus penggandaan kartu ATM (skimmer).

Pasal 32 ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) dapat diakomodasi sebagai upaya hukum dalam kejahatan dengan modus pencurian dana nasabah bank dengan modus skimmer, yang berbunyi:

> “ Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan tranmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik “

Tindak pidana pencurian dalam bentuk pokok seperti yang diatur dalam Pasal 32 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik diatas, terdiri dari unsur subjektif dan unsur objektif, yakni sebagai berikut :

1. Unsur subjektif :
    a. Dengan sengaja;
    b. Tanpa hak;
    c. Secara melawan hukum.

2. Unsur objektif :
    a. Setiap orang;
    b. Mengubah, menambah, mengurangi, melakukan tranmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik;
    c. Milik orang lain atau publik.

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. Dalam melakukan kejahatannya, pelaku skimmer dengan sengaja memindahkan informasi elektronik yang terdapat pada pita magnetik kartu ATM korbannya ke dalam pita magnetik pada kartu ATM milik pelaku untuk kemudian diakses dan digunakan oleh pelaku untuk mengambil uang korbannya melalui mesin ATM. Dengan demikian Pasal 32 ayat (1) Undang-Undang no.11 tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diakomodasikan dalam mengatasi kasus pencurian dana nasabah bank melalui penggandaan kartu ATM (skimmer).

Berdasarkan hal-hal di atas, sangat sulit untuk membuktikan pelaku kejahatan yang modus operandinya di bidang informasi dan teknologi seperti kejahatan pencurian dana nasabah bank dengan modus skimmer. Pasal 5 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi

Elektronik menyatakan bahwa informasi, dokumen, dan tanda tangan elektronik merupakan alat bukti hukum yang sah yang dapat diakomodasi sebagai upaya hukum dalam mengatasi kasus tersebut. Pencurian dana nasabah bank melalui penggandaan kartu ATM telah banyak memakan korban yaitu nasabah bank, dan bank itu sendiri. Para nasabah bank umumnya adalah orang-orang yang biasa menggunakan fasilitas mesin ATM. Kondisi ini dimanfaatkan oleh pelaku kejahatan untuk mencuri data dan membobol dana yang dimiliki oleh nasabah bank tersebut.

Sistem pembuktian di era teknologi informasi sekarang ini menghadapi tantangan besar yang memerlukan penanganan serius, khususnya dalam kaitan dengan upaya pemberantasan kejahatan dengan teknologi komputer. Hal ini muncul karena bagi sebagian jenis-jenis alat bukti yang selama ini dipakai untuk menjerat pelaku tindak pidana tidak mampu lagi dipergunakan dalam menjerat pelaku-pelaku dalam kejahatan dunia maya. Setelah disahkannya Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE), para tersangka pun dapat dikenakan atau dijerat dengan menggunakan pasal 32 ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE), yang mana para tersangka tersebut memiliki informasi elektronik dan/atau dokumen elektronik berupa data yang tersimpan dalam pita magnetik kartu ATM korbannya yang kemudian dipindahkan ke kartu ATM milik pelaku, untuk keuntungan dirinya. Kasus pencurian dana nasabah bank melalui penggandaan kartu ATM dapat dijerat Pasal 363 ayat (5) KUHP, selain itu pelaku kejahatan skimmer dapat juga dikenakan Pasal 32 ayat (1)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dapat diakomodasi sebagai menutup kekosongan hukum.

Pasal-pasal tersebut dapat dijadikan dasar hukum bagi para penegak hukum, hal ini dikarenakan pelaku kejahatan dengan modus operandi pencurian dana nasabah bank melalui penggandaan kartu ATM memenuhi unsur-unsur yang terdapat dalam ketentuan yang berlaku, Penggunaan sistem pembuktian dan alat-alat bukti berdasarkan Pasal 184 KUHAP mampu menjangkau pembuktian untuk kejahatan dengan menyalahgunakan kecanggihan teknologi yang tergolong tindak pidana baru. Penelusuran terhadap alat-alat bukti konvensional seperti keterangan saksi dan saksi ahli, juga pergeseran surat dan petunjuk dari konvensional menuju alat-alat elektronik yang digunakan pelaku kejahatan akan mampu menjerat pelaku kejahatan tersebut. Kasus-kasus yang terjadi mengenai tindak pidana pencurian dana nasabah bank melalui penggandaan kartu ATM di Indonesia sangat jelas telah menimbulkan kerugian yang tidak sedikit, oleh karena itu, harus mendapat perhatian dan tindakan yang sungguh-sungguh dan tegas agar terciptanya kenyaman dan keamanan dalam melaksanakan kegiatan perbankan.

Alat bukti sebagaimana diatur dalam Pasal 83 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan barang bukti seperti diatur dalam Pasal 39 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) masih bersifat terbatas/kuantatif, karena Indonesia menganut sistem pembuktian terbalik (*Negatief Wettelijk Stelsel*) yaitu salah tidaknya seorang terdakwa ditentukan oleh keyakinan hakim yang didasarkan pada cara dan dengan alat bukti yang sah menurut undang-undang. Pada dasarnya setiap orang tidak dapat

dikatakan bersalah sebelum ada putusan hakim yang memiliki kekuatan hukum yang tetap dan pasti. Pengertian ini merupakan asas yang biasa disebut dengan istilah praduga tak bersalah. Untuk menyatakan salah terhadap seseorang harus dibuktikan bahwa seseorang tersebut bersalah, artinya benar melakukan kejahatan yang didakwakan terhadapnya, dalam hal inilah hukum pembuktian memegang peranan penting.

Pada proses persidangan, hakim harus berpegang pada Pasal 10 ayat (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman, yaitu:

> ” Pengadilan dilarang menolak untuk memeriksa, mengadili, dan memutus suatu perkara yang diajukan dengan dalih bahwa hukum tidak ada atau kurang jelas, melainkan wajib untuk memeriksa dan mengadilinya.”

Dalam hal ini, hakim tidak hanya berpegang berdasarkan Pasal 10 Ayat (1) Undang-Undang Nomor 4 Tahun 2004 Tentang Kekuasaan Kehakiman, tetapi hakim juga harus berpegang pada Pasal 5 ayat (1) Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman, yaitu:

> “Hakim dan hakim konstitusi wajib menggali, mengikuti, dan memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat.”

Hakim dalam hal ini tidak boleh menolak suatu kasus yang telah masuk dalam pengadilan, dengan alasan belum ada aturan hukum tertulis

yang mengatur tentang kasus atau perkara yang masuk ke Pengadilan. Di sini hakim memiliki kewajiban menyelesaikan kasus yang ada dengan menggali, mengikuti, dan memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat, serta memperhatikan kebiasaan-kebiasaan yang terjadi di masyarakat, agar tidak terjadi kekosongan hukum dan tercapainya kepastian hukum yang tetap (*inkracht*).

Berdasarkan penjelasan diatas, untuk melakukan pembuktian terhadap tindak pidana pencurian/pembobolan dana pada bank, penyidik atau penuntut umum dapat melakukan penyelidikan, yang dapat diperoleh dengan meminta keterangan lebih lanjut dan kerja sama kepada bank, karena dalam hal ini bank memiliki kaitan yang erat.

Penyidik harus dengan cermat dan tepat menggunakan definisi Informasi dan transaksi elektronik yang dapat diterima sebagai alat bukti, penemuan alat bukti yang kuat, dapat menjerat pelaku tindak pidana pencurian dana nasabah bank melalui penggandaan kartu ATM. Sehingga dapat dijatuhkan pidana dengan cukup 2 alat bukti saja sebagaimana diatur dalam Pasal 183 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), serta memenuhi unsur objektif dan subjektif dari Pasal 363 ayat(5) Kitab Undang-Undang Hukum Pidana (KUHP) dan didukung oleh alat bukti yang sah sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

B. Tindakan Hukum Terhadap Pelaku Pencurian Dana Nasabah Bank melalui Modus Penggandaan Kartu ATM (Skimmer) dihubungkan dengan Pasal 363 ayat (5) kitab Undang-Undang Hukum Pidana (KUHP) Juncto Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Dewasa ini, kejahatan dengan menyalahgunakan kecanggihan teknologi semakin marak terjadi, dengan adanya kemajuan teknologi komputer tidaklah menyebabkan kejahatan itu semakin berkurang tapi justru sebaliknya. Kejahatan yang dilakukan semakin canggih dan rumit, tidak sesederhana yang kita bayangkan. Pada kejahatan perbankan, yang mana sebagian besar bank pada saat ini mengandalkan teknologi informasi dan media elektronik sebagai basis layanannya justru menjadi celah bagi para pelaku kejahatan untuk melakukan aksinya, salah satu bentuk kejahatan tersebut yaitu pencurian dana nasabah melalui penggandaan kartu ATM.

Internet banking, selain memiliki kelebihan berupa kemudahan dan manfaat luas yang meningkatkan kualitas kehidupan manusia, maka layanan perbankan elektronik juga memiliki banyak kelemahan yang patut diwaspadai dan diantisipasi, sehingga, teknologi tersebut tetap dapat dipakai, manfaatnya terus dinikmati oleh nasabahnya, 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) karena masalah keamanan adalah tanggung jawab bersama, semua pihak harus turut serta berperan aktif dalam upaya pengamanan.

Untuk itu, bank dalam menyajikan fasilitas layanannya, harus menciptakan sistem keamanan agar tidak terjadi hal yang merugikan kepada nasabah. Keamanan memang faktor utama dalam penggunaan ATM. Karena sebagaimana kejahatan yang berkembang di Indonesia, transaksi di ATM juga rawan terhadap pengintaian dan penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab. Sebuah mesin ATM selayaknya dilengkapi standar keamanan yang lengkap untuk menjamin bahwa fungsi yang disediakan di mesin ATM hanya dimanfaatkan oleh mereka yang betul-betul berhak.

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi, sebuah informasi umumnya hanya ditunjukan bagi segolongan tertentu. Oleh karena itu, sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah :

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja;
2. Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang;

3. Otentikasi (*authentication*) merupakan layanan yang terkait dengan identifikasi terhadap pihak-pihak yang ingin mengakses sistem informasi (*entity authentication*) maupun keaslian data dari sistem informasi itu sendiri (*data origin authentication*);
4. Ketiadaan penyangkalan (*non-repudiation*) adalah layanan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku sistem informasi.

kejahatan dengan menggunakan teknologi komputer adalah kejahatan yang berdampak sangat nyata. Terdapat 3 (tiga) pendekatan yang dapat dilakukan sebagai upaya pencegahan dan penanggulangan kejahatan teknologi maupun dunia maya, yaitu :

1. Pendekatan teknologi, diantaranya:
    a. Untuk transaksi *internet banking,* bank harus memastikan bahwa *website* bank telah menyediakan informasi yang memungkinkan calon nasabah memperoleh informasi yang tepat mengenai identitas dan status hukum bank sebelum melakukan transaksi. Informasi tersebut mencakup namun tidak terbatas pada : nama dan tempat kedudukan Bank, identitas otoritas pengawasan bank, tata cara nasabah mengakses unit pelayanan nasabah (*call center*) dan tata cara bagi nasabah untuk mengajukan pengaduan;
    b. Dalam penyelenggaraan layanan *internet banking* yang menyediakan sarana fisik seperti ATM, bank harus melakukan pengendalian pengamanan fisik terhadap peralatan dan

ruangan yang digunakan terhadap bahaya pencurian, perusakan dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Bank harus melakukan pemantauan secara rutin untuk menjamin keamanan dan kenyamanan bagi nasabah pengguna jasa *e-banking*;

c. Bank harus memastikan adanya pengamanan atas aspek transmisi data antara Terminal *Electronic Fund Transfer* (EFT) dengan *Host Computer*, terhadap risiko kesalahan transmisi, gangguan jaringan, akses oleh pihak yang tidak bertanggung jawab, dan lain-lain. Pengamanan mencakup pengendalian terhadap peralatan yang digunakan, pemantauan kualitas serta akurasi kinerja perangkat jaringan dan saluran transmisi, pemantauan terhadap akses perangkat lunak *Controller* (*Host-Front End*);

2. Pendekatan sosial budaya, diantaranya :

a. Pihak bank melakukan penyuluhan kepada masyarakat agar tidak memberikan nomor PIN kepada siapa saja, karena Nomor PIN bersifat rahasia dan seharusnya hanya diketahui oleh nasabah yang bersangkutan saja.

b. Pihak bank memberikan himbauan kepada masyarakat tentang bahaya kejahatan terhadap pencurian dana, baik melalui media elektronik maupun media non elektronik.

c. Berhati-hati pada saat melakukan transaksi di ATM maupun di merchant di mana pun, sehingga tidak ada kesempatan bagi

para pelaku untuk mengingat ataupun mencatat nomor seri kartu kredit (*credit card*).

d. Para nasabah tidak seenaknya membuang struk transaksi kartu kredit (*credit card*) yang telah digunakan, karena dari struk transaksi kartu kredit (*credit card*) terdapat data-data yang dapat dilacak untuk digunakan dalam tindak pidana pencurian dana.

3. Pendekatan hukum :

   Dengan adanya aturan dan sanksi yang tegas kepada para pelaku tindak pidana pencurian/pembobolan dana pada bank, dengan tujuan agar masyarakat/pelaku takut dan tidak akan melakukan tindak pencurian dana nasabah dengan modus skimmer tersebut dan sebagai efek jera. Saat ini Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) dapat diakomodasi sebagai dasar hukum terhadap pelaku tindak pidana pencurian dana nasabah bank melalui modus skimmer.

Ketiga pendekatan tersebut untuk mengatasi tindak kejahatan khususnya tindak kejahatan dengan modus pencurian dana nasabah bank dengan modus skimmer. Dalam hal ini, terhadap tindak pidana pencurian dana nasabah bank melalui penggandaan kartu ATM harus dilakukan upaya reperesif/tindakan hukum. Upaya reperesif /tindakan hukum yang dilakukan oleh polisi atau penyidik dilaksanakan sesuai dengan peraturan perundang-undangan yang berlaku. Tindakan hukum atau upaya reperesif yang dapat dilakukan terhadap tindak pencurian/pembobolan dana pada bank

diantaranya dengan menerapkan Pasal 363 ayat (5) KUHP dan pasal 32 ayat (1) Undang-Undang no.11 tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menjerat pelaku pencurian dana nasabah bank melalui modus skimmer. Disamping itu, pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak. Transaksi melalui mesin ATM merupakan kemudahan yang diberikan oleh bank kepada nasabahnya, karena melalui fasilitas inilah nasabah dapat menghemat waktu, jarak, dan biaya. Namun di balik kemudahan-kemudahan tersebut celah kejahatan dapat terjadi, salah satunya pencurian dana nasabah bank melalui modus penggandaan kartu ATM, yang mana korbannya merupakan nasabah pengguna fasilitas mesin ATM itu sendiri.

Saat ini, para pelaku tindak pidana pencurian dana nasabah bank melalui modus skimmer dapat dikenakan atau dijerat Pasal 32 ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE). Unsur subjektif Pasal 32 ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yaitu dengan sengaja, artinya para tersangka dengan sengaja melakukan suatu perbuatan dengan cara mencuri data. Unsur objektifnya yaitu melakukan tranmisi, 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. Dengan demikian, perkembangan teknologi dan informasi membutuhkan kecermatan para penegak hukum dalam menggunakannya untuk kemudian dapat diajukan dan diterima oleh hakim.

Ketentuan dalam hukum acara pidana (KUHAP) khususnya mengenai alat bukti dan barang bukti yang secara jelas disebutkan, dapat diterapkan terhadap pelaku kejahatan dengan modus pencurian dana nasabah bank melalui modus skimmer. Kehadiran alat-alat bukti dan barang bukti dalam kejahatan komputer ini berbeda karakteristik dengan kejahatan biasa mengakibatkan sulitnya dalam menangani kejahatan ini. Diperlukan peningkatan kualitas penegak hukum (polisi, penyidik, jaksa, dan hakim) dalam menangani kejahatan komputer ini, mengingat modus operandi dalam kejahatan penggandaan kartu ATM ini berbeda dengan kejahatan konvensional.

Pelaku pencurian dana nasabah bank melalui modus skimmer dapat dijerat atau 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, juncto Pasal 32 ayat (1) Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), tentang memindahkan informasi elektronik dan atau dokumen elektronik milik orang lain atau milik publik, yang mana ketentuan pidananya diatur Pasal 48 ayat (1) UU ITE dengan ancaman hukuman penjara paling lama delapan tahun dan/atau denda paling banyak dua miliar rupiah.