

**PERLINDUNGAN NASABAH BANK DARI
KEJAHATAN PEMBOBOLAN ATM MENURUT
UU No. 8 TAHUN 1999 TENTANG
PERLINDUNGAN KONSUMEN¹**

Oleh : Megi Mokoginta²

ABSTRAK

Penelitian ini dilakukan dengan tujuan untuk mengetahui bagaimana Perlindungan Hukum Terhadap Nasabah Bank dalam Penggunaan Fasilitas *Internet Banking* Dihubungkan Dengan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen dan bagaimana Modus Operandi Pembobolan ATM Bank dan upaya Perlindungan Terhadap Nasabah Pengguna. Dengan menggunakan metode penelitian yuridis normative disimpulkan: 1. Terdapat beberapa hal yang dapat dilakukan pihak perbankan untuk meningkatkan keamanan *internet banking* misalnya melakukan standarisasi dalam pembuatan aplikasi *internet banking*. Misalnya, 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*. Undang-Undang Nomor 8 tahun 1999 Tentang Perlindungan Konsumen mengatur mengenai perlindungan terhadap nasabah atas kerusakan *electronic banking* yang mensyaratkan adanya keseimbangan perlindungan kepentingan konsumen dan pelaku usaha sehingga tercipta perekonomian yang sehat, dalam konteks ini termasuk dalam hubungan antara bank sebagai pelaku usaha dengan nasabahnya. Apabila terjadi permasalahan atas kerusakan *electronic banking*, maka nasabah selaku konsumen dapat mengajukan pengaduan kepada Bank Indonesia. Tindakan hukum yang dapat dilakukan oleh nasabah apabila yang diajukan ditolak adalah dengan mengajukan gugatan dengan melakukan suatu hal yang dapat membuktikan bahwa pihak penanggung Bank melakukan wanprestasi berdasarkan pasal 1243 KUHPdata karena sudah tidak memenuhi prestasi atas isi dalam perjanjian yang telah dibuat oleh kedua belah pihak. 2. Belakangan

ini semakin canggih saja kejahatan yang dilakukan untuk membobol ATM. Setidaknya ada tiga modus pembobolan ATM yang pernah terjadi di Indonesia. Modus pertama adalah dengan cara membobol *card rider anti vandal* (tempat memasukkan kartu ATM pada mesin). Modus kedua hampir sama dengan sebelumnya, yaitu membuat kartu ATM nasabah tertahan dan tidak bisa dikeluarkan dari mesin ATM. Pelaku juga menempelkan nomor telepon pusat layanan palsu di badan mesin. Berbeda dengan modus pertama, pelaku menggunakan perangkap potongan korek api agar kartu ATM tertahan. Modus ketiga adalah dengan menggunakan kartu ATM palsu. Kata kunci: Nasabah, bank, kejahatan, pembobolan, ATM.

PENDAHULUAN

A. Latar Belakang Masalah

Saat ini semakin marak penyedia layanan jasa *internet banking* di Indonesia. Dengan keluarnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik kini menjadi peraturan perundang-undangan yang dapat menjamin kepastian hukum. *Internet banking* kini bukan lagi istilah yang asing bagi masyarakat Indonesia khususnya yang tinggal di wilayah perkotaan. Hal tersebut disebabkan semakin banyaknya perbankan nasional yang menyelenggarakan layanan tersebut. Di masa mendatang, layanan ini tampaknya sudah bukan lagi sebuah layanan yang akan memberikan keuntungan bagi bank yang menyelenggarakannya, tapi 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 di kemudian hari dapat merugikan masyarakat jika tidak diantisipasi dengan baik.³

Internet banking merupakan salah satu pelayanan perbankan tanpa cabang, yaitu berupa fasilitas yang akan memudahkan nasabah untuk melakukan transaksi perbankan tanpa perlu datang ke kantor cabang. Layanan yang diberikan *internet banking* kepada nasabah berupa transaksi pembayaran tagihan,

¹ Artikel Skripsi. Dosen Pembimbing : Selviani Sambali, SH, MH; Lendy Siar, SH, MH

² Mahasiswa pada Fakultas Hukum Unsrat, NIM. 100711241

³ Silalahi, Darwin. "Banyak Negara Bersiap dengan Ekonomi Berbasis Internet," Harian Kompas, Tanggal 10 April 2000, hlm. 17.

informasi rekening, pemindahbukuan antar rekening, informasi 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 penyetoran maupun pengambilan uang, masih memerlukan layanan ATM.

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 kerahasiaan 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 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.⁴

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 bisnis perbankan pada dasarnya merupakan bisnis yang berisiko tinggi. Terdapat sedikitnya 8 macam risiko utama yang berkaitan dengan aktivitas perbankan, yaitu strategi, reputasi, operasional (termasuk yang disebut risiko transaksi dan legal), kredit, harga, kurs, tingkat bunga, dan likuiditas. Di samping itu, penggunaan Teknologi Sistem Informasi (TSI) terdapat risiko yang bersifat teknis dan khusus, yang berbeda dengan penggunaan sistem manual. Risiko yang dimaksud antara lain risiko kekeliruan pada tahap pengoperasian, risiko akses oleh pihak yang tidak berwenang, risiko 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 faktor 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 risiko.⁵

B. Perumusan Masalah

1. Bagaimanakah Perlindungan Hukum Terhadap Nasabah Bank dalam Penggunaan Fasilitas *Internet Banking* Dihubungkan Dengan Undang-Undang

⁴ Setiawan, Iwan., *Pembobolan ATM Bank*, Gatra, 24 Februari 2010, hlm. 102.

⁵ Next-generation retail banking," <http://zle.nonstop.compad.com/view.asp?IO=INTBKGWP>, diakses 22 Desember 2003.

Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen ?

2. Bagaimanakah Modus Operandi Pembobolan ATM Bank dan upaya Perlindungan Terhadap Nasabah Pengguna?

C. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode deskriptif. Metode deskriptif adalah suatu metode yang dipergunakan untuk memecahkan masalah yang ada pada waktu sekarang, dan pelaksanaannya tidak terbatas hanya sampai pada pengumpulan dan penyusunan data, tetapi meliputi analisa dan interpretasi data itu.

PEMBAHASAN

A. Perlindungan Hukum Terhadap Nasabah Bank Sebagai Pengguna Fasilitas *Internet Banking* (Termasuk ATM) Dihubungkan Dengan UU No 8 Tahun 1999 Tentang Perlindungan Konsumen

Perlindungan hukum terhadap nasabah bank atas kerusakan *electronic banking* dihubungkan dengan Undang-Undang Nomor 8 Tahun 1999 Tentang perlindungan konsumen. Dewasa ini, industri perbankan khususnya di Indonesia dihadapkan pada tingkat persaingan yang ketat. Salah satu upaya agar mampu bersaing, bank harus dapat mengotomatisasi kegiatan kerjanya dari sistem manual menjadi sistem otomatis. Melalui penerapan suatu sistem informasi yang tepat, bank diharapkan dapat memberikan pelayanan yang cepat, teliti dan aman kepada nasabahnya.

Saat ini sebagian besar layanan *electronic banking* terkait langsung dengan rekening bank. Jenis *electronic banking* yang tidak terkait rekening biasanya berbentuk nilai moneter yang tersimpan dalam basis data atau dalam sebuah kartu (*chip* dalam *smart card*) semakin berkembangnya teknologi dan kompleksitas transaksi mengakibatkan berbagai jenis e-banking semakin sulit dibedakan karena fungsi dan fiturnya cenderung terintegrasi atau mengalami konvergensi. Seperti diketahui, kehadiran layanan *electronic banking* telah menawarkan fleksibilitas dan kemudahan dalam melakukan transaksi, baik antara bank dengan nasabahnya, bank dengan merchant, bank dengan bank dan nasabah dengan

nasabah. Namun demikian, kemudahan ini bukanlah berarti tanpa memiliki risiko karena tidak menutup kemungkinan timbul kendala dalam kegiatan transaksi *electronic banking* baik dari segi teknis maupun hukum yang bisa berakibat juga kepada perlindungan nasabah sebagai konsumen. Beberapa permasalahan yang timbul antara lain bagaimana Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen mengatur mengenai perlindungan terhadap nasabah atas kerusakan *electronic banking* dan tindakan hukum apa yang dapat dilakukan oleh para pihak atas kerusakan *electronic banking*.

Dewasa ini, industri perbankan khususnya di Indonesia dihadapkan pada tingkat persaingan yang ketat. Salah satu upaya agar mampu bersaing, bank harus dapat mengotomatisasi kegiatan kerjanya dari sistem manual menjadi sistem otomatis. Melalui penerapan suatu sistem informasi yang tepat, bank diharapkan dapat memberikan pelayanan yang cepat, teliti dan aman kepada nasabahnya. Saat ini sebagian besar layanan *electronic banking* terkait langsung dengan rekening bank. Jenis *electronic banking* yang tidak terkait rekening biasanya berbentuk nilai moneter yang tersimpan dalam basis data atau dalam sebuah kartu (*chip* dalam *smart card*). Semakin berkembangnya teknologi dan kompleksitas transaksi mengakibatkan berbagai jenis e-banking semakin sulit dibedakan karena fungsi dan fiturnya cenderung terintegrasi atau mengalami konvergensi. Seperti diketahui, kehadiran layanan *electronic banking* telah menawarkan fleksibilitas dan kemudahan dalam melakukan transaksi, baik antara bank dengan nasabahnya, bank dengan merchant, bank dengan bank dan nasabah dengan

yang dapat dilakukan oleh para pihak atas kerusakan *electronic banking*.

Undang-Undang Nomor 8 tahun 1999 Tentang Perlindungan Konsumen mengatur mengenai perlindungan terhadap nasabah atas kerusakan *electronic banking* yang mensyaratkan adanya keseimbangan perlindungan kepentingan konsumen dan pelaku usaha sehingga tercipta perekonomian yang sehat, dalam konteks ini termasuk dalam hubungan antara bank sebagai pelaku usaha dengan nasabahnya. Apabila terjadi permasalahan atas kerusakan *electronic banking*, maka nasabah selaku konsumen dapat mengajukan pengaduan kepada Bank. Indonesia hal ini berdasarkan Peraturan Bank Indonesia Nomor 10/10/PBI/2008 tentang perubahan atas Peraturan Bank Indonesia Nomor 7/7/PBI/2005 Tentang Penyelesaian Pengaduan nasabah. Tindakan hukum yang dapat dilakukan terhadap para pihak terkait dalam kerusakan *electronic banking* adalah dengan cara diteruskannya penyelesaian persoalan ke pada pihak ketiga yang secara hukum memiliki wewenang untuk menangani permasalahan yang ada dan diselesaikan secara litigasi/melalui pengadilan atau pun secara non litigasi/di luar pengadilan seperti melalui mediasi, negosiasi, konsiliasi dan arbitrase menurut aturan hukum yang berlaku. Sedangkan tindakan hukum yang dapat dilakukan oleh nasabah apabila yang diajukan ditolak adalah dengan mengajukan gugatan dengan melakukan suatu hal yang dapat membuktikan bahwa pihak penanggung Bank melakukan wanprestasi berdasarkan pasal 1243 KUHPdata karena sudah tidak memenuhi prestasi atas isi dalam perjanjian yang telah dibuat oleh kedua belah pihak.

B. Modus Operandi Pembobolan ATM Bank Dan Upaya Perlindungan Nasabah Pengguna.

1. Kejahatan Perbankan Pembobolan ATM Potensial Sistemik

Aparat penegak hukum dan jajaran pengelola bank harus segera menuntaskan kasus pembobolan anjungan tunai mandiri (ATM) sekarang ini. Jika tidak, keresahan masyarakat bisa kian merebak dan berdampak sistemik terhadap industri perbankan nasional

jika keresahan itu sampai menimbulkan tindak penarikan uang secara besar-besaran (*rush*).

Aparat penegak hukum dan pengelola perbankan harus bertindak cepat. Jangan sampai beberapa kasus pembobolan ATM menimbulkan keresahan dan melunturkan kepercayaan masyarakat terhadap perbankan nasional. Tindakan bank memberikan penggantian terhadap nasabah yang menjadi korban pembobolan ATM memang bagus karena membebaskan korban dari risiko kehilangan dana. Tapi tindakan itu saja tidak cukup bisa meredakan keresahan masyarakat menyangkut keamanan dana mereka di perbankan nasional. Selama aparat berwenang tak bisa segera mengungkap kasus-kasus pembobolan yang sudah terjadi, dan di sisi lain pengelola perbankan tidak bisa meyakinkan masyarakat menyangkut sistem pengamanan dana nasabah, keresahan masyarakat bisa tetap semakin menjadi-jadi dan meluas. Kalau sudah begitu, perbankan nasional harus menanggung risiko dampak sistemik kasus pembobolan ATM. Jadi, kasus-kasus tersebut harus segera ditangani. Jangan biarkan masyarakat dilanda resah, dan jangan pula keresahan itu dibiarkan meluas.

2. Potensi-potensi Kerugian

Bank Indonesia (BI) menerima laporan pembobolan kartu ATM di beberapa bank di Bali 20 Januari 2010 lalu berjumlah Rp. 4,1 miliar. Nilai tersebut terdiri dari 236 rekening nasabah. "Salah satu dari bank yang dibobol tersebut saja berpotensi mengalami kerugian sebesar Rp. 4,1 miliar. Nilai itu terdiri dari 236 rekening nasabah. Dan nilai itu belum termasuk di bank lainnya," terang Deputy Gubernur BI Budi Rochadi, selepas konferensi pers di Gedung BI Jakarta. Hingga saat ini BI telah menerima laporan pembobolan rekening nasabah lewat ATM pada 6 bank yaitu BCA, Bank Mandiri, BNI, BRI, Bank Permata, dan BII. Bahkan beberapa hari ini BI juga seringkali menerima laporan kerugian dari nasabah. Kerugian tersebut berasal dari pengurangan saldo lewat ATM.⁶

Selama ini banyak pihak nasabah yang mengadu ke Polisi dan bank terkait

⁶ *Ibid*, hal. 69

pengurangan saldo. Sehingga untuk menghindari kejadian ini berulang, BI meminta bank untuk lebih mengetatkan pengamanan kartu ATM serta mesin ATM-nya sehingga data-data dari ATM tidak mudah dibobol. PT Bank Central Asia Tbk atau BCA mengakui, ada 200 nasabahnya yang mengalami masalah pengurangan saldo akibat transaksi mencurigakan. Total kerugian yang diderita akibat kasus ini mencapai Rp 5 miliar. Kira-kira ada 200 nasabah. Kerugian Rp 4 miliar sampai Rp 5 miliar.⁷

Sebagian besar kerugian nasabah tersebut telah diganti perseroan. Untuk mengantisipasi masalah ini, BCA telah memasang alat *anti-skimming* di semua ATM BCA. Meski demikian, demi keamanan bertransaksi di ATM, pihak BCA menghimbau agar para nasabah segera mengganti nomor PIN.

Saat ini, BCA juga tengah mempersiapkan penggunaan kartu ATM atau debit dengan *combi card* yang menggunakan teknologi *chip* dan *magnetic*. Namun, ada kendala-kendala kalau pakai kartu *chip*, berarti tidak bisa dipakai di ATM di luar negeri.

3. Modus Pembobolan ATM

Belakangan ini semakin canggih saja kejahatan yang dilakukan untuk membobol ATM. Setidaknya ada tiga modus pembobolan ATM yang pernah terjadi di Indonesia. Modus pertama adalah dengan cara membobol *card rider anti vandal* (tempat memasukkan kartu ATM pada mesin). Cara ini terbongkar setelah aparat menggulung komplotan pembobol di Tangerang dan Tulungagung, Jawa Timur. Setelah membobol *card rider*, tersangka menempelkan plastik mika bening di belakangnya dan mengelemnya supaya tidak lepas. Setelah itu, tersangka memasang kembali tempat kartu itu ke mesin ATM. Mereka kemudian mengawasi korban yang masuk ke ruang ATM. Setelah korban melakukan transaksi, dipastikan kartu tidak bisa keluar karena terganjal mika. Tersangka yang kesulitan mengambil kartu, menelepon ke sebuah nomor keluhan yang sebelumnya ditempelkan komplotan itu di ruang ATM.

Modus kedua hampir sama dengan sebelumnya, yaitu membuat kartu ATM

nasabah tertahan dan tidak bisa dikeluarkan dari mesin ATM. Pelaku juga menempelkan nomor telepon pusat layanan palsu di badan mesin. Berbeda dengan modus pertama, pelaku menggunakan perangkap potongan korek api agar kartu ATM tertahan. Korban yang biasanya panik langsung menelepon nomor pusat layanan fiktif. Petugas fiktif meminta korban menekan tombol tertentu supaya kartu ATM kelaar. Karena tak kunjung keluar, petugas fiktif membujuk korban menyebutkan nomor PIN ATM dengan alasan memblokir rekening. Merasa aman rekening sudah diblokir, korban meninggalkan lokasi ATM. Kesempatan ini dimanfaatkan pembobol untuk menganibil kartu menggunakan gergaji besi. Modus ketiga adalah dengan menggunakan kartu ATM palsu.

4. Perlindungan Nasabah

Jika hal-hal tersebut terjadi, apa kekuatan hukum nasabah? Apakah sudah ada peraturan yang mewadahi (untuk melindungi nasabah. Bukan sekedar mewadahi dan menampung kemudian mengalahkan si nasabah. Bukankah gagainya transaksi karena kesalahan bank? Bukankah bobolnya rekening juga melibatkan lemahnya sistem keamanan bank? Apakah bank dapat menjamin oknum petugas bank, sama seperti malaikat. Apakah oknum petugas, tak mungkin tergiur kongkalikong membocorkan PIN nasabah?

Lalu, jika nasabah didenda karena terlambat membayar cicilan, apakah bank yang telah merugikan nasabah karena transaksinya terhambat dapat didenda? Bagaimana pula dengan potongan saldo beralih biaya administrasi? Lebih kurang masalah itulah kemudian yang menimpa Surianty. Bank berprinsip kehilangan uang melalui ATM itu tanggung jawab si nasabah. Pokcknya argumen apapun yang disampaikan nasabah, semua itu salahnya si nasabah, tanpa berusaha melakukan introspeksi dan restropeksi. Tetapi Surianty punya nyali, pantang untuk menyerah. Gagal dapatkan ganti rugi dari bank, Surianty menempuh upaya hukum melalui Badan Penyelesaian Sengketa Konsumen (BPSK).

Cukup panjang proses untuk menggenggam keadilan itu. Nasabah dan bank sating berargumentasi. Saksi dan bukti diajukan. Untungnya, putusan BPSK rnemang berpihak

⁷ *Ibid*, hal. 72

pada SURIANTY. Bank diwajibkan untuk mengembalikan uang si nasabah.

Apakah bank dapat menerima putusan BPSK itu? Tidak!, masalahnya pihak bank justru keberatan dan menggugat balik si nasabah ke pengadilan. Nasib si nasabah, seperti sudah jatuh tertimpa tangga pula. Posisi nasabah bank begitu rapuh. Sama sekali tiada kebijakan hukum yang dapat melindunginya.

5. Perlindungan Nasabah dalam Bidang Pelayanan Perbankan

Kedudukan nasabah dalam hubungannya dengan pelayanan jasa perbankan, berada pada dua posisi yang dapat bergantian sesuai dengan di sisi mana mereka berada. Dilihat pada sisi pengerahan dana, nasabah yang menyimpan dananya pada bank baik sebagai penabung, deposan maupun pembeli surat berharga (obligasi atau commercial paper), maka pada saat itu nasabah berkedudukan sebagai kreditur bank. Sedangkan pada sisi penyaluran dana, nasabah peminjam berkedudukan sebagai debitur dan bank sebagai kreditur. Dalam pelayanan jasa perbankan lainnya seperti dalam pelayanan bank garansi, penyewaan *save deposit box*, transfer uang, dan pelayanan lainnya, nasabah (konsumen) mempunyai kedudukan yang berbeda pula. Tetapi dari semua kedudukan tersebut pada dasarnya nasabah merupakan konsumen dari pelaku usaha yang menyediakan jasa di sektor usaha perbankan.⁸

Fokus persoalan perlindungan nasabah tertuju pada ketentuan peraturan perundang-undangan serta ketentuan perjanjian yang mengatur hubungan antara bank dengan para nasabahnya. Hubungan hukum yang terjadi antara bank dengan nasabah dapat terwujud dari suatu perjanjian, baik perjanjian yang berbentuk akta di bawah tangan maupun dalam bentuk otentik. Dalam konteks inilah perlu pengamatan yang baik untuk menjaga suatu bentuk perlindungan bagi konsumen namun tidak melemahkan kedudukan posisi bank. Hal demikian perlu mengingat seringnya perjanjian yang dilakukan antara bank dengan

nasabah telah dibekukan dengan sebuah perjanjian baku.

Sisi lain yang menjadi fokus perlindungan konsumen dalam sektor jasa perbankan, yaitu pelayanan di bidang perkreditan. Hal-hal yang menjadi perhatian untuk perlindungan konsumen, yaitu proses yang harus dilalui, dan warkat-warkat yang digunakan dalam pemberian kredit tersebut. Tidak kalah pentingnya pula yaitu saat pengikatan hukum antara bank dengan nasabah dimana secara hukum biasanya menyangkut dua macam pengikatan berupa: perjanjian pokok yakni perjanjian kredit, dan perjanjian tambahan yakni perjanjian mengikuti perjanjian pokok berupa suatu perjanjian penjamin.

6. Perlindungan Keamanan yang Dilakukan Pihak Bank Terhadap Mesin-Mesin ATM-nya

Ada beberapa cara pengamanan yang dilakukan pihak bank terhadap mesin-mesin ATM-nya, yaitu:

- a. Penggunaan kartu khusus elektronik yaitu kartu ATM.
- b. Kode identitas yaitu kode PIN.
- c. Maksimum uang yang dapat diambil pada suatu waktu.

Semua pengamanan ini bisa diatur lewat software. Biasanya software ini dipasang di komputer pusat, host. Terminal-terminal ATM yang biasa kita lihat di bank-bank, swalayan--swalayan atau tempat-tempat lain, hanya merupakan alat input dan output. Semua proses dan pengamanan diatur oleh software khusus pada komputer host. Seandainya ada orang lain yang berhasil mencuri kartu ATM, ia tidak akan bisa mengambil uang dalam rekening nasabah bank tersebut sebelum mengetahui kode PIN. Kalaupun ia berhasil mengetahui kode PIN itu, ATM masih membatasi jumlah maksimum uang yang bisa diambilnya pada satu saat, misalnya Rp.300.000,00. Sehingga walaupun rekening nasabah kebobolan, nasabah tersebut hanya akan rugi Rp.300.000,00. hal ini karena sebelum pencuri sempat mengambil lebih banyak pada pengembalian berikutnya, nasabah sudah keburu melapor ke bank tentang hilangnya kartu ATM sehingga bank bisa mencegah

⁸ Djumhana, Muhammad., *RUU Perbankan Tidak Mengatur Perlindungan Bagi Nasabah*, Suara Pembaharuan, 28 November 2007, hal. 13

kebobolan berikutnya.⁹ Karena ATM juga merupakan jaringan komputer yang terdiri dari terminal-terminal dan komputer host, maka sudah barang tentu tidak lepas dari rongrongan Para hacker. Dari beberapa informasi BBS hacker, dikatakan bahwa hacker dapat saja memasuki dan menyadap jaringan ATM. Dan bahkan dengan menggunakan sebuah personal computer hacker dapat memerintahkan terminal-terminal ATM untuk melakukan hal-hal tertentu. Hal ini terjadi karena sebelum pesan-pesan transaksi yang dikirim *terminal ATM* sampai ke *komputer host*, terlebih dulu sudah diterima oleh personil komputer milik hacker. Kemudian hacker akan mengirim pesan-pesan balasan dan memberi perintah-perintah tertentu untuk melakukan transaksi-transaksi yang diinginkannya. Kelemahan-kelemahan software pada ATM juga merupakan sasaran bagi para hacker. Banyak dari kasus-kasus kejahatan ATM pada masa-masa awal penggunaan ATM di Amerika Serikat disebabkan justru oleh karena kelemahan-kelemahan software ATM tersebut.¹⁰ Untuk lebih memberikan rasa aman pada setiap pemegang kartu ATM, *Mastercard* internasional bekerja sama dengan *Magtec Inc*, kini tengah mengembangkan teknologi anti penggandaan untuk kartu kredit (*credit card*) *Mastercard*.

Penegasan tersebut terungkap dengan telah ditandatangani perjanjian antara *Mastercard International* dengan *Mag-tec Inc*, pemimpin provider internasional untuk produk-produk dan teknologi card reader dalam upaya mengurangi risiko pemalsuan kartu kredit. Dalam perjanjian itu kedua belah pihak sepakat melakukan riset dan mengembangkan solusi dan program yang akan mengurangi risiko penipuan kartu kredit. Program yang dikenal sebagai skimming atau penggandaan pita magnetis di belakang kartu dengan menggunakan property fisik intrinsic dan strip magnetic (yang unik setiap kartu) akan dapat membedakan antara yang asli dengan yang palsu.

⁹ Suyatno, Thomas., *Dasar-dasar Perkreditan*, Cetakan Kedua Edisi Ketiga, Gramedia Pustaka Utama, Jakarta, 1991, hal. 71

¹⁰ Turban, Efraim., et.al, *Electronic Commerce A Manajerial Perspective* (New Jersey: Prentice-Hall, Inc, 2000), hlm.173, hal. 29

Vice President dan Regional Head, Security and Risk Managemant Mastercard International untuk wilayah Asia Pasifik, Esmond Chan, mengatakan: pihaknya terus akan berupaya untuk melindungi para pemegang kartu ATM. Bekerja sama dengan mitra-mitranya seperti *Mag-tec* dalam mengembangkan dan memperkenalkan tidak hanya program pembayaran terancang tetapi juga aman dan melindungi para pemegang kartu kredit *Mastercard*.¹¹

Kombinasi karakteristik strip magnetic yang sangat unik, bersamaan dengan nomor rekening dan data lainnya yang tertera pada *strip* oleh *issuer*, akan membuat setiap *Mastercard* betul-betul unik dan tidak dapat digandakan. *Mastercard* memimpin industri pembayaran dalam pengembangan fitur keamanan seperti panel tanda tangan penggunaan hologram tiga dimensi, kode-kode validasi kartu serta mikroprosesor *smart card*.

PENUTUP

A. Kesimpulan

1. Terdapat beberapa hal yang dapat dilakukan pihak perbankan untuk meningkatkan keamanan *internet banking* misalnya melakukan standarisasi dalam pembuatan aplikasi *internet banking*. Misalnya, 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*.

Undang-Undang Nomor 8 tahun 1999 Tentang Perlindungan Konsumen mengatur mengenai perlindungan terhadap nasabah atas kerusakan *electronic banking* yang mensyaratkan adanya keseimbangan perlindungan kepentingan konsumen dan pelaku usaha sehingga tercipta perekonomian yang sehat, dalam konteks ini termasuk dalam hubungan antara bank sebagai pelaku usaha dengan nasabahnya. Apabila terjadi permasalahan atas kerusakan *electronic banking*, maka nasabah selaku konsumen dapat mengajukan pengaduan

¹¹ "Mastercard Kembangkan Teknologi Anti-Pemalsuan," Surya, 18 Januari 2001, hal. 14, Kolom Bisnis.

kepada Bank Indonesia. Tindakan hukum yang dapat dilakukan oleh nasabah apabila yang diajukan ditolak adalah dengan mengajukan gugatan dengan melakukan suatu hal yang dapat membuktikan bahwa pihak penanggung Bank melakukan wanprestasi berdasarkan pasal 1243 KUHPerdara karena sudah tidak memenuhi prestasi atas isi dalam perjanjian yang telah dibuat oleh kedua belah pihak.

2. Belakangan ini semakin canggih saja kejahatan yang dilakukan untuk membobol ATM. Setidaknya ada tiga modus pembobolan ATM yang pernah terjadi di Indonesia. Modus pertama adalah dengan cara membobol *card rider anti vandal* (tempat memasukkan kartu ATM pada mesin). Modus kedua hampir sama dengan sebelumnya, yaitu membuat kartu ATM nasabah tertahan dan tidak bisa dikeluarkan dari mesin ATM. Pelaku juga menempelkan nomor telepon pusat layanan palsu di badan mesin. Berbeda dengan modus pertama, pelaku menggunakan perangkat potongan korek api agar kartu ATM tertahan. Modus ketiga adalah dengan menggunakan kartu ATM palsu.

B. Saran

Pihak pemerintah dapat membebankan masalah keamanan *internet banking* kepada pihak bank, sehingga bila terjadi masalah kelalaian bank dalam suatu nilai tertentu, *user* dapat mengajukan klaim. Khusus perihal beban pembuktian, perlu dipikirkan kemungkinan untuk menerapkan *omkering van bewijslast* atau pembuktian terbalik untuk kasus-kasus *cybercrime* yang sulit pembuktiannya. Hakikat dari pembuktian terbalik ini adalah terdakwa wajib membuktikan bahwa dia tidak bersalah atas dakwaan yang dituduhkan kepada terdakwa.

DAFTAR PUSTAKA

Aman, Edy Putra The., *Kredit Perbankan Suatu Tinjauan Yuridis*, Liberty, Yogyakarta, 1986.
Caldwell. Kave., "Applying Old Law to New Technology," The Commercenet Newsletter The Public Policy Report. Vol. 2 No. 7

Agustus 2000.

Chandra, Fransisca Haryanti., *Internet : Information Superhighway*. Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah VI di Semarang, 4-8 September 1995.

Djumhana, Muhammad., *RUU Perbankan Tidak Mengatur Perlindungan Bagi Nasabah*, Suara Pembaharuan, 28 November 2007.

Furst, Karen., et.al, "Internet Banking: Development and Prospects;" *Program on Information Resources Policy Harvard University*, April 2002, hlm. 4. Lihat juga Karen Furst, "Who Offers Internet Banking," *Quarterly Journal*, vol. 19 No. 2 June 2000.

Komarrudin, *Kamus Perbankan*, CV Rajawali, Cetakan Pertama, Jakarta, 1984.

Pattiradjawane, Rene L., "Globalisasi dan Teknologi Menuju Keseimbangan Baru," *Harian Kompas*, Tanggal 28 April 2000.

Setiawan, Iwan., *Pembobolan ATM Bank*, Gatra, 24 Februari 2010.

Silalahi, Darwin. "Banyak Negara Bersiap dengan Ekonomi Berbasis Internet," *Harian Kompas*,. Tanggal 10 April 2000.

Simorangkir, O.P., *Dasar-Dasar dan Mekanisme Perbankan*, Aksara Persada Press, Cetakan Ke-5, Jakarta, 1985.

Suyatno, Thomas., *Dasar-dasar Perkreditan*, Cetakan Kedua Edisi Ketiga, Gramedia Pustaka Utama, Jakarta, 1991.

Turban, Efraim., et.el, *Electronic Commerce A Manajerlral Perspective* (New Jersey: Prentice-Hall. Inc, 2000), hlm.173.

Artikel ATM (1) Diposkan oleh Ivan di 17.21 Label: on banking ATM, Setelah Simjian Menemukannya Jumat, 29 Januari 2010.

<http://fakhrurrazypi.wordpress.com/2010/03/25/pembobolan-atm-bank/>.

Mastercard Kembangkan Teknologi Anti-Pemalsuan, Surya, 18 januari 2001, Kolom Bisnis.

Next-generation retail banking," <http://zle.nonstop.com/view.asp?IO=INTBKGWP>, diakses 22 Desember 2003.