ERA HUKUM
Jurnal Ilmiah Ilmu Hukum
Volume 16, No. 2, Oktober 2018
ISSN 0854-8242 | e-ISSN 2581-0359
Fakultas Hukum - Universitas Tarumanagara
Open Access at: www.journal.untar.ac.id/index.php/hukum

PERKEMBANGAN MODUS OPERANDI KEJAHATAN *SKIMMING* DALAM PEMBOBOLAN MESIN ATM BANK SEBAGAI BENTUK KEJAHATAN DUNIA MAYA (*CYBERCRIME*)

Dian Alan Setiawan
(Dosen Hukum Pidana pada Program Studi Ilmu Hukum Fakultas Hukum Universitas Islam Bandung, Meraih Sarjana Hukum (S.H) pada Fakultas Hukum Universitas Mataram (2010); Magister Hukum (M.H) pada Program Studi Magister Hukum Universitas Airlangga (2011)
(E-mail: dianalan.setia@yahoo.com)

Received: 27 April 2018; *Accepted*:18 Juni 2019; *Published*: 30 Juni 2019

Abstract:

The development of technology and the internet does not always produce positive things. Negative things that are side effects include the crime of skimming (theft of customer data) which is one type of crime in cyberspace. Lately Indonesia is enlivened with breaking ATM news that occurred in various regions in Indonesia. The customers suddenly lose their account balance due to being burglarized by irresponsible people. ATM piercing technique is known as ATM Skimmer Scan technique. ATM machine piercing (Automated Teller Machine) using Skimmer, which is a customer data thieves. The modus operandi of bank breakers is installing skimmer in ATM mouth. After the customer data obtained, the perpetrator just insert into the ATM card. burglars will freely drain the customer's money. Problems that arise is the development of modus operandi crime skimming in the case of bank burglary bank as a form of cybercrime (cybercrime) And Efforts / Legal Steps in Tackling Crime Use of Information Systems and Electronic Transactions. This research is legal research using conceptual approach and statue approach which will review Law Number 11 Year 2008 regarding Information and Electronic Transaction. Based on the method used, it is known that the modus operandi of criminal skimming in ATM bankruptcy as a form of cyber crime and the application of article in Law Number 11 Year 2008 regarding Information and Electronic Transaction as an effort / step in tackling the crime of Information System Use and Electronic Transactions.

Keywords: *Crime, Skimming, ATM burglary*

I. Pendahuluan

A. Latar Belakang

Perkembangan Teknologi Informasi dan Komputer (TIK) telah mengalami kemajuan yang sangat pesat, terutama setelah diketemukannya teknologi yang menghubungkan antar komputer (*Networking*) dan Internet. Namun demikian, berbagai kemajuan tersebut ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan. Istilah ini kemudian dikenal dengan *cybercrime*. Indonesia selama ini dianggap sebagai surga kejahatan *cyber*[1]. Betapa tidak, pada 2016 setidaknya 6.000 lebih warga asing dideportasi akibat pelanggaran perizinan

[1]Pratama Persadha, artikel dalam harian Sindo 26 Agustus 2016, sebagaimana diakses dalam https://www.cissrec.org/publications/detail/38/Indonesia-Surga-Kejahatan-Cyber.html diakses tanggal 12 April 2018

dan tindak kejahatan, sebagian di antaranya pelaku kejahatan *cyber*. Belum lama ini Kepolisian RI kembali menangkap 31 orang asal China yang ditenggarai melakukan tindak kejahatan *cyber*.

Modusnya mereka menargetkan korban warga negara di tempat asalnya. Para pelaku ini melakukan pendekatan dan menjebak korban untuk melakukan pencucian uang. Lalu di tengah jalan para pelaku mengaku sebagai polisi dan meretas para korbannya. Ada lagi modus penipuan kartu kredit. Para pelaku ini mendapatkan suplai informasi dari tim yang ada di negara asalnya. Dengan data yang ada, mereka melakukan penipuan dengan menyamar sebagai pihak bank. Akhirnya banyak yang tertipu dan memberikan tiga nomor CVV (*card verification value*) yang ada pada kartu kredit. Ada lagi di Bali sekelompok warga negara Eropa Timur melakukan pencurian rekening dan kartu kredit nasabah asal Eropa dan Amerika. Lalu pertanyaannya, mengapa untuk menipu sesama warga negara sendiri harus jauh-jauh dilakukan di Indonesia?

Untuk kasus warga asing asal Eropa Timur yang melakukan pembobolan mesin ATM di Bali tahun lalu, bisa dipastikan mereka memanfaatkan kelemahan ATM yang ada di Tanah Air. Lebih dari 80% mesin ATM di Tanah Air ini masih menggunakan sistem operasi Windows XP yang Microsoft sendiri sebagai pembuatnya sudah menghentikan dukungan terhadap produk tersebut, termasuk dari segi keamanan. Kondisi itu jelas menjadi kesempatan yang bisa dimanfaatkan. Bahkan para pelaku rela mengeluarkan uang yang tidak sedikit untuk pergi ke lndonesia, belum Iagi membeli alat *scammer* (peranti keras yang ditanam di mulut ATM untuk menyedot data elektronik nasabah dan semacamnya). Mereka menilai melakukan pencurian data kartu nasabah lewat ATM di Indonesia jauh lebih mudah daripada harus melakukannya di negara mereka sendiri.

Berbeda lagi dengan warga negara China dan Taiwan yang ditangkap pihak kepolisian. Rata-rata mereka dituduh melakukan tindak kejahatan penipuan *online* dengan modus memeras maupun menguras kartu kredit korban. Kejahatan itu dilakukan oleh kelompok terorganisasi. Ada yang bertugas mengumpulkan data calon korban di negara asal. Ada juga yang mengoordinasi para operator lapangan yang ditempatkan di Indonesia. Lalu kenapa tidak mereka lakukan kejahatan ini di China ataupun Taiwan? Jawabannya sama, karena melakukannya di Indonesia jauh lebih mudah. Banyak faktor, dari mudahnya

mendapatkan layanan komunikasi di lndonesia sampai pada banyaknya jumlah *provider* internet yang mencapai lebih dari 400 perusahaan. Ini membuat pengawasan dan peringatan dini menjadi sulit dilakukan. Coba bandingkan dengan China yang hanya ada dua *provider* internet, pengawasan yang dilakukan jadi lebih mudah. Para pelaku ini menyadari, di Indonesia mereka bisa mendapatkan layanan telepon dan internet dengan sangat mudah tanpa harus registrasi, kalau pun perlu registrasi, dengan identitas fiktif pun bisa.

Setidaknya ada tiga hal yang perlu dicatat, yaitu masalah imigrasi, lembaga badan *cyber*, dan revisi UU Informasi dan Transaksi Elektronik (ITE). Untuk masalah imigrasi, memang menjadi sangat sulit. Karena para pelaku ini semuanya menggunakan visa wisata ke Indonesia. Nyatanya mereka malah melakukan tindak kejahatan *online*. Tercatat tahun 2015 ada lebih dari 600 kasus kejahatan yang dilakukan warga negara asing di Indonesia. Sampai pertengahan 2016, Direktorat Jenderal Imigrasi mencatat sudah 100 lebih kasus yang masuk. Sebagian besar dengan modus serupa, visa wisata dimanfaatkan untuk kegiatan kejahatan *cyber* yang menyasar korban negara asalnya. Lalu mengenai Badan Cyber Nasional (BCN). Keberadaannya sangat dibutuhkan. Dalam kasus ini bila BCN nanti sudah ada, mereka bisa membantu pihak kepolisian lewat divisi *cybercrime* dan Imigrasi. Supervisi dan koordinasi dari BCN ini sebenarnya sangat penting dan diperlukan semua instansi nantinya. Karena saat ini dan ke depan masyarakat, dunia usaha, dan pemerintah semakin besar ketergantungannya pada dunia digital. Mau tidak mau kemampuan dan kewaspadaan pemerintah di wilayah *cyber* harus ditingkatkan.

Awareness setiap aparat, pelaku usaha, dan masyarakat harus ada. BCN mendorong setiap kebijakan instansi, termasuk Imigrasi dan Kominfo, untuk memperhatikan aspek keamanan *cyber*. Misalnya tentang penjualan kartu perdana yang sampai saat ini masih bebas dan menjadi pintu masuk penipuan lewat SMS maupun internet. Yang tidak kalah penting adalah UU ITE. Selama ini UU ITE cenderung terkenal dan dikenal masyarakat karena berhasil menjebloskan para netizen dan pemakai media sosial. Hal tersebut karena UU yang disahkan tahun 2008 tersebut memang jangkauannya masih "sempit". Padahal dengan era digital seperti sekarang, *coverage cybercrime* bertambah luas, satu di antaranya beririsan dengan pihak Imigrasi. Salah satu alasan para

pelaku ini mengincar nasabah perbankan dan kartu kredit adalah karena kelemahan sistem perbankan, tidak hanya di Indonesia. Misalnya bagaimana data nasabah bisa berpindah tangan dengan berbagai modus. Bagaimana dengan di Indonesia? Tindak penipuan *online* seperti yang dilakukan WNA juga banyak dilakukan orang Indonesia yang menyasar sesama WNI. Lemahnya pengamanan sistem dan data para nasabah membuat pelaku kejahatan bisa mengeksploitasi korban.

Pembobolan lewat ATM, *carding* dan *social engineering* menjadikan korban semakin banyak dari waktu ke waktu. Menurut data dari Microsoft misalnya, selama 2015 kejahatan *cyber* di Tanah Air menyebabkan kerugian sebesar Rp33 miliar lebih. Angka ini sebenarnya masih bisa bertambah karena banyaknya kejadian yang tidak dilaporkan oleh nasabah. Enggannya nasabah melapor karena mereka sering disalahkan oleh perbankan, di anggap melakukan kelalaian. UU ITE maupun UU yang mengatur hak konsumen harus menjamin bahwa pihak perbankan wajib mengamankan sistem yang mereka miliki sehingga pihak nasabah tidak selalu disalahkan. Bila hal itu terwujud, rasanya pemerintah bisa memperbaiki dan menekan angka kejahatan *cyber*. Perlu dicatat, ada 169 negara yang bebas visa ke Indonesia. Artinya kemungkinan mereka melakukan kejahatan maupun menjadikan Indonesia sebagai markas kejahatan cyber semakin besar. Belum lagi bila WNA ini malah melakukan pengaderan kepada WNI di Tanah Air. Jadi pemerintah harus siap dan gesit menghadapi kemungkinan terburuk.

B. Rumusan Masalah

Beranjak dari latar belakang sebagaimana diuraikan di atas, maka dapat dirumuskan isu hukum dan permasalahan antara lain sebagai berikut :

1) Bagaimana perkembangan modus operandi kejahatan skimming dalam kasus pembobolan ATM bank sebagai bentuk kejahatan dunia maya (*cybercrime)*?
2) Apakah Upaya/Langkah Hukum Dalam Menanggulangi Kejahatan Penggunaan Sistem Informasi dan Transaksi Elektronik?

C. Hasil Penelitian

1. Perkembangan Modus Operandi Kejahatan Skimming Dalam Kasus Pembobolan ATM Bank Sebagai

Bentuk Kejahatan Dunia Maya (*cybercrime*)

Bank merupakan suatu lembaga yang sangat penting di dalam masyarakat, karena bank sebagai salah satu sarana berjalannya perekonomian yang ada di masyarakat. Sektor perbankan merupakan salah satu sektor yang mempunyai peranan penting dalam pembangunan nasional, karena perbankan berfungsi sebagai perantara antara sektor defisit dengan sektor surplus dalam masyarakat maupun sebagai agen pembangunan Beranjak dari peran perbankan yang sangat strategis dalam mendorong kelancaran pembangunan nasional, maka dalam menjalankan usahanya perlu senantiasa mengembangkan profesionalisme yang kokoh agar lembaga perbankan mampu berfungsi secara efisien, sehat, wajar dan mampu menghadapi persaingan global [2].

Berdasarkan *Encyclopedia of Banking and Finance*, sistem elektronik perbankan adalah segala macam transfer dan pemrosesan data dengan menggunakan sistem dan peralatan elektronik yang meliputi transaksi intern dan ekstern suatu bank[3]. Kegiatan transfer dana dengan menggunakan sistem dan peralatan elektronik tersebut kita kenaI dengan istilah *Electronic Fund. Transfer* atau Transfer Dana Elektronik. Sistem dan peralatan elektronik yang dipergunakan dalam transfer dana tersebut dapat berupa telepon, komputer, pita magnetis, dan lain-lain. Penggunaan teknologi informasi dan komunikasi di perbankan nasional relatif lebih maju dibandingkan sektor lainnya. Seiring perkembangan teknologi perbankan, dimulai ketika nasabah melakukan transaksi secara manual yaitu berhadapan dengan *teller*, hingga berkembangnya teknologi yang memberikan kemudahan bagi nasabah melakukan transaksi dimana saja dan kapan saja, salah satunya menggunakan sistem elektronik yang lebih terjangkau seperti melalui jasa mesin pembayaran yang disebut dengan ATM (*Automatic Teller Machine*) atau umumnya disebut juga Anjungan Tunai Mandiri.

Perkembangan teknologi telah memberikan pengaruhnya ke segala aspek, termasuk perkembangan teknologi

[2] Synthiana Rachmie, Penegakan Hukum Pidana Terhadap Pelaku Kejahatan Penggunaan Sistem Elektronik Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.Thesis(S2) thesis, Unpas. http://repository.unpas.ac.id/28343/1 Jurnal Synthiana Rachmie 148040018 150517.docx, diakses tanggal 23 April 2018 : 1

[3] Bambang Setijoprodjo. Majalah Hukum, Permasalahan Hukum dalam Transfer Dana Elektronik. (Semarang: Universitas Diponegoro) 2000

perbankan yang tujuannya memberikan pelayanan yang baik kepada nasabah dan memberikan kemudahan dalam melakukan transaksi. Seiring perkembangan waktu, dimana terjadi perkembangan transaksi ekonomi, maka kebutuhan nasabah akan kemudahan melakukan transaksi semakin meningkat, untuk menunjang kebutuhan nasabah tersebut maka pihak bank mengeluarkan produk-produk perbankan kepada nasabah (baik nasabah dari bank tersebut maupun dari bank lain) untuk melakukan transaksi perbankan melalui media elektronik. Media elektronik yang digunakan adalah mesin ATM, internet banking, maupun *handphone*.

Kemajuan zaman dan perkembangan teknologi merupakan dua hal yang saling berbanding lurus. Artinya semakin maju suatu zaman, semakin berkembang pula teknologi yang digunakan dizaman tersebut. Kemajuan ini berpengaruh terhadap berbagai aspek kehidupan, disebutkan juga oleh pakar hukum pidana Andi Hamzah [4], bahwa perkembangan teknologi itu sangat berpengaruh terhadap sikap tindak dan sikap mental setiap masyarakat. Kemajuan yang dicapai di bidang teknologi akan mempengaruhi pula perubahan di dalam kehidupan masyarakat. Kemajuan teknologi dan industri yang merupakan hasil dari budaya manusia di samping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia serta membawa dampak negatif terhadap perkembangan dari peradaban manusia itu sendiri.

Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J.E Sahetapy menyatakan dalam tulisannya, bahwa kejahatan serta kaitannya dengan perkembangan masyarakat. Semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju. Kejahatan juga menjadi sebagian dari hasil budaya itu sendiri. Hal ini berarti semakin tinggi tingkat budaya dan hasil semakin modern suatu bangsa, semakin modern pula kejahatan itu dalam bentuk , sifat dan cara pelaksanaannya.[5] Belakangan ini banyak terungkap kasus-kasus kejahatan perbankan, Bank Indonesia sudah mengidentifikasi sedikitnya tiga modus kejahatan perbankan yang marak adalah kejahatan perbankan yang berbasis Teknolgi Informasi salah satunya yang menyerang sistem perbankan Indonesia adalah Modus kejahatan perbankan

[4] Andi Hamzah, *Hukum Acara Pidana Indonesia* (Sinar Grafika : Jakarta,2011) hlm. 19

[5] Abdul Wahid, *Kriminologi Dan Kejahatan Kontemporer*, (Lembaga Penerbitan Fakultas Hukum Unisma, Malang, 2003)

umumnya berupa *skimming*, *phishing*, dan *malware*. 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.

Terkait dengan hal tersebut Direktur Tindak Pidana Ekonomi Khusus Mabes Polri Brigadir Jenderal Victor Panggabean menuturkan sejak 2012 hingga 2015 telah terjadi kerugian sebesar 33 Miliar akibat kejahatan perbankan. Ia menyebutkan modus terbesar yang digunakan ialah skimming[6]. Berdasarkan data yang diperoleh terkait kejahatan skimming tersebut dalam tiga tahun terakhir tercatat sebanyak 5.500 kejahatan skimming ATM terjadi di dunia. Dari jumlah itu, 1.549 atau sepertiga diantara kasus tersebut ada di Indonesia. Peningkatan kejahatan tersebut diakibatkan karena adanya kelemahan dalam hal penegakan hukum atas kejahatan tersebut. Berdasarkan hal tersebut, terdapat beberapa faktor penyebab[7] meningkatnya kejahatan dalam penggunaan sistem elektronik dengan modus operandi *skimming*, antara lain yaitu :

a. Faktor Perbankan

Dalam penyelenggaraan layanan *internet banking* yang menyediakan sarana fisik seperti ATM, bank kurang melakukan pengendalian pengamanan fisik terhadap peralatan dan ruangan yang digunakan terhadap bahaya pencurian, perusakan dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Bank juga kurang melakukan pemantauan secara rutin untuk menjamin keamanan dan kenyamanan bagi nasabah pengguna jasa *e-banking*.

b. Faktor Hukum

1) Ketentuan yang berlaku

Terkait dengan pengaturan kejahatan

[6]Tempo, Waspada Modus Kejahatan Perbankan yang Lagi Marak, https://bisnis.tempo.co/read/news/2015/04/29/087661869/waspada-modus-kejahatan-perbankan-yang-lagi-marak, diakses tanggal 21 Agustus 2016

[7] Dikdik M. Arief Mansur, *Cyber Law Aspek Hukum Teknologi Informasi*, (Refika Aditama Bandung, 2005) hal 89

pencurian dana nasabah melalui modus operandi tersebut sebenarnya telah dilakukan pengaturan secara khusus yang diatur dalam Undang-undang mengenai Informasi dan Transaksi Elektronik, namun terkait dengan penjatuhan pidana yang dilakukan para penegak hukum belum maksimal dimana masih terdapat beberapa kasus yang menggunakan penjatuhan pidana tersebut menggunakan KUHP sehingga dampak yang ditimbulkan dari penjatuhan pidana tersebut belum maksimal dan tidak menimbulkan efek jera terhadap para pelaku kejahatan tersebut.

2) Penegakan Hukum

Faktor penegak hukum sering menjadi penyebab maraknya kejahatan dalam penggunaan sistem elektronik, hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi/internet, sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dipakai menjerat pelaku terleih apabila kejahatan yang dilakukan memiliki sistem pengoperasian sangat rumit. Selain itu juga aparat penegak hukum di daerah pun belum siap megantisipasi maraknya kejahatan dalam penggunaan sistem elektronik karena masih banyak institusi kepolisian yang belum dilengkapi dengan jaringan internet.

c. Faktor Teknologi

Faktor teknologi menjadi salah satu faktor pendukung peningkatan kejahatan pada sistem elektronik diantaranya yaitu terdapat kelemahan kondisi mesin ATM dan/atau mesin EDC untuk bertransaksi, kurangnya pengamanan serta kartu debit/kredit yang masih menggunakan *magnetic stripe* yang rentan terhadap pencurian data nasabah.

Secara khusus disebutkan kejahatan tersebut merupakan kejahatan skimming dimana skimming adalah aktivitas menggandakan informasi yang terdapat dalam pita magnetik (*magnetic stripe*) yang terdapat pada kartu kredit maupun ATM/debit secara illegal. Berdasarkan hal tersebut, kasus skimming atau kejahatan penggunaan sistem elektronik dengan modus operandi *skimming* melalui mesin skimmer menjadi hal utama yang akan dilakukan pembahasan oleh penulis, kasus skimming tersebut berdampak signifikan bagi para pengguna layanan bank maupun bagi banknya itu sendiri.

Baru-baru ini terjadi pembobolan mesin ATM (Anjungan Tunai Mandiri) di Bali dengan menggunakan Skimmer, yaitu

sebuah alat pencuri data nasabah[8]. Modus operasi para pembobol bank yaitu memasang skimmer di mulut ATM. Setelah data nasabah didapat, pelaku tinggal memasukkan kedalam kartu ATM nya. Yang nantinya pembobol akan dengan leluasa menguras uang nasabah. Satu skrimmer bisa menyimpan data sampai 2000 kartu dan ironinya skrimmer ternyata dijual bebas disejumlah pertokoan dengan harga Rp 1,5 juta. Selain itu ada cara lain untuk memancing nasabah yaitu dengan Fishing yaitu dengan membuat situs palsu untuk memancing nasabah pengguna layanan internet banking. Dengan mengirim pesan elektronik (e-mail) yang seakan-akan dari operator bank. Isinya meminta nasabah mengisi data kembali dengan alasan ada perbaikan sistem keamanan. Kejahatan teknologi informasi atau kejahatan dunia maya *(Cyber Crime)* merupakan permasalahan yang harus ditangani secara serius, karena akibatnya sangat luas. Dan jika tidak ditanggulangi dan tidak terkendali akan sangat fatal bagi kehidupan masyarakat, khususnya bagi pengguna teknologi.

Belakangan ini semakin canggih saja kejahatan yang dilakukan untuk membobol ATM [9]. 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

[8]Dewi Mastari, Cyber Crime : Penggunaan Skimmer Terhadap Pembobolan ATM, journal.lppmunindra.ac.id/index.php/Faktor_Exacta /article/viewFile/326/307 diakses tanggal 14 April 2018 : 261

[9]Megi Mokoginta, Perlindungan Nasabah Bank Dari Kejahatan Pembobolan Atm Menurut Uu No. 8 Tahun 1999 Tentang Perlindungan Konsumen, Jurnal Lex Privatum Vol. IV/No. 6/Juli/2016 : 104

palsu d dengan modus unakan perangk r kartu ATM t asanya panik langsung menelepon nomor pusat layanan fiktif. Petugas fiktif meminta korban menekan tombol tertentu supaya kartu ATM keluar. 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 mengambil kartu menggunakan gergaji besi. Modus ketiga adalah dengan menggunakan kartu ATM palsu.

Skimmer atau ATM *Skimmer*, merupakan alat pencuri data nasabah yang dipasang di mulut ATM, alat ini akan menyalin data si korban jika ia memasukan kartu ATM melalui skimmer ini, setelah itu maka si penjahat yang menempatakn Skimmer pada lobang ATM akan memiliki data nasabah pemilik ATM. Skimmer berarti alat yang bisa digunakan untuk aktivitas pencurian informasi yang dilakukan dari kartu nasabah, baik dari kartu ATM maupun kartu kredit. Dengan memasang alat ini di mulut ATM, pelaku bisa mendapatkan data di kartu nasabah. Kemudian tinggal memasukannya ke dalam kartu ATM bodong. Sementara untuk pin, pelaku menggunakan kamera pengintai mungil.

a. Metode

Metode yang digunakan oleh pembobol untuk membobol ATM nasabah yaitu[10]: 1. Teknik Skimming Pada ATM Pada saat kita memasukan kartu ATM ke mesin ATM, sang mesin ATM akan membaca informasi pada kartu ATM anda untuk digunakan sebagai KUNCI mengakses fasilitas perbankan anda. Salah satu jalan termudah untuk mencuri data informasi pada Kartu ATM anda di mesin ATM yaitu dengan memasang alat tambahan (*skimmer*) di depan mulut tempat anda memasukan kartu ATM. Proses pemasangan *Skimmer*.

Gambar 1. Proses pemasangan Skimmer

Dengan terpasangnya *SKIMMER* pada mulut atm, setiap yang nasabah datang

[10]Dewi Mastari, Op., Cit.

melakukan transaksi dengan memasukan kartunya ke atm, sebelum data tersebut dibaca oleh mesin ATM, alat *skimmer* pun telah membaca dan merekam data kartu anda untuk selanjutnya akan di-copy-kan ke kartu magnetik lainnya (bodong). Selanjutnya sang pencuri tinggal mengambil alat *skimmer*nya, dan menduplikasi kartu-kartu ATM milik nasabah-nasabah yang sempat mengakses ATM tersebut.

Gambar 2. Kamera Merekam Aktifitas

b. Cara mengetahui PIN nasabah

Para pencuri tersebut memasang hidden camera untuk merekam moment saat kita menekan nomor PIN di ATM tersebut. Camera tersebut bentuknya sangat kecil, dan memiliki internal memory yang cukup besar. Saat ini sangat mudah sekali mendapatkan camera seperti ini di Internet. pemasangan Camera untuk merekam aktifitas pemasukan PIN ATM.

c. Pembuatan Kartu Magnetik Palsu

Saat sang pencuri mengambil kembali skimmer & camera miliknya, dia sudah mendapatkan data-data kartu kita lengkap dengan nomor PIN. Selanjutnya, sang pencuri tinggal membuat kartu magnetik baru dengan data-data kartu kita didalamnya dengan alat yang umum seperti gambar dibawah ini:

Gambar 3. Kartu Magnetik

Selanjutnya sang pencuri memiliki akses penuh selayaknya pemilik rekening yang dicuri. Untuk meminimasi resiko biasanya sang pencuri memilih ATM yang tidak ada ebab itu tidak her saksi yg dilakuka M bank lain yang tidak memiliki CCTV (*switching*).

d. Mengenali bentuk-bentuk *Skimmer*

Gambar 4. Bentuk-bentuk *Skimmer*

2. Upaya/Langkah Hukum Dalam Menanggulangi Kejahatan Penggunaan Sistem Informasi dan Transaksi Elektronik

Penanggulangan kejahatan dengan menggunakan hukum pidana merupakan bagian dari kebijakan criminal. Penanggulangan kejahatan tersebut adalah dalam rangka untuk mencapai tujuan akhir dari kebijakan kriminal itu sendiri yaitu memberikan perlindungan masyarakat dalam rangka untuk mencapai kesejahteraan bagi masyarakat.

Salah satu usaha untuk mencegah dan menanggulangi masalah kejahatan adalah dengan menggunakan hukum pidana (*penal policy*). Masalah kebijakan hukum pidana tidak hanya sebatas membuat atau menciptakan suatu peraturan perundang-undangan yang mengatur hal-hal tertentu.

Lebih dari itu, kebijakan hukum pidana memerlukan pendekatan yang menyeluruh yang melibatkan berbagai disiplin ilmu hukum selain ilmu hukum pidana serta kenyataan di dalam masyarakat sehingga kebijakan hukum pidana yang digunakan tidak keluar dari konsep yang lebih luas yaitu kebijakan sosial dan rencana pembangunan nasional dalam rangka mewujudkan kesejahteraan masyarakat. Namun dalam hal ini, terdapat pendekatan yang digunakan dalam rangka upaya melakukan penanggulangan kejahatan melalui sarana pendekatan kriminal dapat menggunakan 2 (dua) sarana, yaitu sarana penal dan non penal.

Kebijakan dengan sarana penal adalah upaya penanggulangan kejahatan dengan menggunakan sarana pidana. Dalam hal ini telah terjadi semacam perumusan pidana dan pemidanaan yang telah dilegalkan melalui perundang-undangan. Sehingga, telah ada kepastian hukum dalam melakukan penanggulangan maupun pemecahan terhadap pelanggaran atau kejahatan yang dilakukan oleh para pelaku kejahatan Sedangkan kebijakan kriminal dengan sarana non penal artinya upaya penanggulangan kejahatan dengan tidak melakukan hukum pidana. Upaya non penal dapat juga diartikan sebagai upaya yang bersifat preventif, misalnya memperbaiki kondisi-kondisi tertentu dalam masyarakat atau melakukan pengawasan tertantu sebagai upaya prevensi terhadap kejahatan. Selain itu, dapat juga berbentuk sosialisasi terhadap suatu perundang-undangan yang baru, yang didalamnya mencangkup suatu kriminalisasi perbuatan tertentu yang menjadi gejala sosial dalam masyarakat modern.

Berdasarkan hal tersebut diatas maka penanggulangan terkait kejahatan

skimming tersebut dapat dilakukan melalui sarana non penal yang mencakup antara lain:

a. Upaya Penanggulangan oleh Pihak Perbankan

Upaya yang dilakukan oleh pihak perbankan terhadap penanggulanagan kejahatan skimming ini yaitu segera menyelesaikan pengaduan dari nasabah apabila terdapat nasabah yang menjadi korban kejahatan skimming, melakukan edukasi kepada nasabah agar berhati-hati pada saat melakukan transaksi di ATM maupun mesin EDC merchant di mana pun, sehingga tidak ada kesempatan bagi para pelaku untuk mengingat ataupun mencatat nomor seri kartu debit/kredit nasabah serta melakukan peningkatan keamanan pada sekitar mesin ATM melalui sekuriti maupun CCTV untuk dapat meminimalisir kejahatan serupa, serta perbaikan sistem dan infrastruktur mesin-mesinmaupun sistem perbankan menjadi lebih canggih dan rentan terhadap kejahatan nasabah.

b. Upaya Penanggulangan oleh Pihak Nasabah

Himbauan dan kesadaran yang diperlukan dari para nasabah agar tidak sembarangan membuang struk transaksi kartu kredit/debit yang telah digunakan, karena dari struk transaksi kartu kredit/debit terdapat data-data yang dapat dilacak untuk digunakan dalam tindak pidana pencurian dana serta pengembangan pengetahuan untuk para masyarakat umum terkait dengan jenis-jenis kejahatan perbankan dan modus operandi pelaku kejahatan skimming tersebut;

c. Upaya Penanggulangan oleh Pemerintah/ Penegak Hukum

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. Banyak sekali kasus-kasus yang terjadi akibat imbas dari Undang-undang Informasi dan Transaksi Elektronik yang banyak dipertanyakan oleh para ahli. Sehingga akhirnya terjadilah revisi Undang-undang Informasi dan Transaksi Elektronik pada bulan oktober 2016. Perubahan Undang-undang Informasi dan Transaksi Elektronik telah disahkan menjadi Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Informasi dan Transaksi Elektronik Naskah Undang-Undang tersebut tercatat dalam Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251 dan Tambahan Lembaran Negara

Nomor 5952. Maka ditinjau dari modus operandi yang dilakukan oleh para pelaku kejahatan kejahatan penggunaan sistem elektronik dengan modus operandi skimming menggunakan alat skimer tersebut juga dapat dikategorikan dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang terdapat dalam:

Pasal 30 :

(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.

Pasal 32 :

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik;
(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak;
(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33:

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau

mengaibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya"

Pasal 36:

"Setiap orang dengan sengaja dan tanpa haka tau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain"

Namun apabila dianalisa lebih dalam lagi terkait dengan ketentuan-ketentuan yang telah disebutkan diatas masih terdapat kekurangan-kekurangan dengan ketidakjelasan rumuan unsur-unsur yang terdapat dalam beberapa pasal tersebut. Serta pelaksanaannya terkait dengan kasus skimming belum menjadi perhatian masyarakat, pemerintah maupun pihak bank itu sendiri. Karena masih terdapat beberapa bank yang menerima kasus tersebut menjadi kerugian bank itu sendiri, sedangkan apabila dianalisa lebih lanjut seharusnya pelaku itu sendiri dapat diadili sesuai dengan ketentuan yang berlaku di Indonesia.

Tindakan hukum atau upaya reperesif yang dapat dilakukan terhadap tindak pencurian/pembobolan dana pada bank diantaranya dengan menerapkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menjerat pelaku pencurian dana nasabah bank melalui modus skimmer. Hal tersebut menandakan bahwa harus terdapat 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.

D. Penutup

1. Simpulan

a. Kejahatan perbankan yang berbasis Teknologi Informasi salah satunya yang menyerang sistem perbankan Indonesia adalah Modus kejahatan perbankan umumnya berupa *skimming*, *phishing*, dan *malware*. 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. Faktor penyebab meningkatnya kejahatan dalam penggunaan sistem elektronik dengan modus operandi *skimming*, adalah (1) Faktor Perbankan; (2) Faktor Hukum ; dan (3) Faktor Teknologi

b. Penanggulangan kejahatan melalui sarana pendekatan kriminal dapat menggunakan 2 (dua) sarana, yaitu sarana penal dan non penal. Kebijakan dengan sarana penal adalah upaya penanggulangan kejahatan dengan menggunakan sarana pidana. Dalam hal ini telah terjadi semacam perumusan pidana dan pemidanaan yang telah dilegalkan melalui perundang-undangan. Sedangkan kebijakan kriminal dengan sarana non penal artinya upaya penanggulangan kejahatan dengan tidak melakukan hukum pidana. Upaya non penal dapat juga diartikan sebagai upaya yang bersifat preventif, Berdasarkan hal tersebut diatas maka penanggulangan terkait kejahatan skimming tersebut dapat dilakukan melalui sarana non penal yaitu : upaya penanggulangan oleh pihak perbankan dan nasabah dan upaya penanggulangan oleh pihak pemerintah / penegak hukum .

2. **Saran**

a. Bank dalam hal ini harus melakukan pengendalian pengamanan fisik terhadap peralatan dan ruangan yang digunakan terhadap bahaya pencurian, perusakan dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Selain itu, Bank juga harus melakukan pemantauan secara rutin untuk menjamin keamanan dan kenyamanan bagi nasabah pengguna jasa *e-banking* seperti, peningkatan keamanan pada sistem elektronik diantaranya yaitu pada kondisi mesin ATM dan/atau mesin EDC untuk bertransaksi, serta kartu debit/kredit yang masih menggunakan *magnetic stripe* yang rentan terhadap pencurian data nasabah.

b. Pemerintah harus melakukan

tindakan hukum atau upaya reperesif yang dapat dilakukan terhadap tindak pencurian/pembobolan dana pada bank diantaranya dengan menerapkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menjerat pelaku pencurian dana nasabah bank melalui modus skimmer. Hal tersebut menandakan bahwa harus terdapat 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.

Daftar Pustaka

A. Buku

Abdul Wahid, *Kriminologi Dan Kejahatan Kontemporer*, Lembaga Penerbitan Fakultas Hukum Unisma, Malang, 2003

Andi Hamzah, Hukum Acara Pidana Indonesia, Sinar Grafika : Jakarta, 2011

Bambang Setijoprodjo. Majalah Hukum, Permasalahan Hukum dalam Transfer Dana Elektronik. Semarang: Universitas Diponegoro. 2000

Dikdik M. Arief Mansur, Cyber Law Aspek Hukum Teknologi Informasi, Refika Aditama Bandung, 2005

Peter Mahmud Marzuki, *Perlunya Undang-undang Tentang Macam dan Harga Mata Uang (Penelitian)* Kerjasama dengan Bank Indonesia, Hal 2. Lihat juga Peter Mahmud Marzuki, *Penelitian Hukum*, Yuridika, Volume 16 No. 2, Maret *2001*,

---------- *Penelitian Hukum*, (Jakarta : kencana Prenada Media group,Cet 6, 2005)

B. Peraturan Perundang-undangan

Indonesia. Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

C. Jurnal

Dewi Mustari, Cyber Crime : Penggunaan Skimmer Terhadap Pembobolan ATM, journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/viewFile/326/307 hal 261-265

Megi Mokoginta, Perlindungan Nasabah Bank Dari Kejahatan Pembobolan Atm Menurut Uu No. 8 Tahun 1999 Tentang Perlindungan Konsumen, Jurnal Lex Privatum Vol. IV/No. 6/Juli/2016 :100-107

D. Website

Pratama Persadha, artikel dalam harian Sindo 26 Agustus 2016, sebagaimana diakses dalam https://www.cissrec.org/publicaons/detail/38/Indonesia-Surga-Kejahatan-Cyber.html

Synthiana Rachmie, Penegakan Hukum Pidana Terhadap Pelaku Kejahatan Penggunaan Sistem Elektronik Dihubungkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.Thesis(S2) thesis, Unpas. http://repository.unpas.ac.id/28343/1 Jurnal Synthiana Rachmie 148040018 150517.docx, diakses tanggal 23 April 2018 :1-8

Tempo, Waspada Modus Kejahatan Perbankan yang Lagi Marak, https://bisnis.tempo.co/read/news/2015/04/29/087661869/waspada-modus-kejahatan-perbankan-yang-lagi-marak