Jurist-Diction
Volume 2 No. 2, Maret 2019
Histori artikel: Submit 1 Februari 2019; Diterima 15 Februari 2019; Diterbitkan online 1 Maret 2019.

Pembobolan ATM Menggunakan Teknik *Skimming* Kaitannya Dangan Pengajuan Restitusi

Michael Enrick
mail.enrick@gmail.com
Universitas Airlangga

Abstract
This research was conducted with the aim to find out Modus Operandi used in bank burglary using Skimming techniques and knowing the victims and positions of victims in criminal acts on ATM burglary using Skimming techniques and legal remedies that can be taken by victims in criminal acts on ATM burglary using Skimming technique. In this study, it was done by using a normative juridical research method. It is concluded: 1. Burglary of ATM using the Skimming technique is a sophisticated modus operandi in bank burglary that violates several criminal rules in UU ITE and KUHP. 2. There is a variation of victims caused ATM burglary uses Skimming techniques between banks and customers depending on the factor of proof of transactions with Skimming techniques. With regard to the possibility of variations, each of the victims have the right to file restitution as compensation by the perpetrators.
Keywords: *Skimming; Banking crime; Victim; Restitution.*

Abstrak
Penelitian ini dilakukan dengan tujuan untuk mengetahui terkait Modus Operandi yang digunakan dalam "pembobolan bank" menggunakan teknik Skimming dan mengetahui terkait korban dan kedudukan korban dalam tindak pidana pada pembobolan ATM dengan menggunakan teknik Skimming serta upaya hukum yang dapat ditempuh oleh korban dalam tindak pidana pada pembobolan ATM dengan menggunakan teknik Skimming. Pada penelitian ini dialkukan dengan menggunakan metode penelitian yuridis normatif. Pada penelitian ini disimpulkan: 1. Pembobolan ATM menggunakan teknik Skimming merupakan modus operandi canggih dalam "pembobolan bank" yang melanggar beberapa aturan pidana dalam UU ITE dan KUHP. 2. Terdapat variasi korban yang ditimbulkan Pembobolan ATM menggunakan teknik Skimming antara bank dan nasabah bergantung terhadap faktor pembuktian transaksi dengan teknik Skimming. Terhadap kemungkinan variasi korban tersebut masing-masing memiliki hak untuk mengajukan restitusi sebagai upaya ganti rugi oleh pelaku.
Kata Kunci: *Skimming*; Kejahatan perbankan; Korban; Restitusi.

Pendahuluan

Pada tahun 1980-an, era baru yang disebut globalisasi dimulai oleh negara-negara dengan perekonomian maju seperti Amerika Serikat dan negara-negara anggota Uni-Eropa.[1] Pada era ini pemikiran orang-orang didunia adalah bukan lagi terbatas pada pemikiran kapitalisme moderen, namun untuk menciptakan

[1] Romli Atmasasmita, *Hukum Kejahatan Bisnis Teori & Praktik di Era Globalisasi* (Prenada Media 2016).[25].

perdagangan yang sifatnya internasional.[2] Sebagai dampak dari era globalisasi, teknologi yang pada mulanya disebut sebagai ARPANET yang merupakan jaringan penghubung satu komputer dengan komputer lain yang pada tahun 1975 hanya digunakan sebagai komunikasi pasukan tempur Amerika Serikat, pada tahun 1995 dibuka untuk penggunaan privat dan hingga sekarang di kenal sebagai internet.[3]

Internet dalam dunia perbankan memungkinkan setiap orang untuk melakukan transaksi perbankan dengan mudah dan cepat. Untuk transfer dana tidak perlu lagi datang ke teller bank seperti cara konfensional, namun cukup dengan menggunakan gawai seperti telepon genggam atau komputer dengan jaringan internet. Sedangkan untuk penarikan tunai ataupun pembayaran mengacu pada Peraturan Bank Indonesia Nomor 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu sebagaimana telah diubah dengan Peraturan Bank Indonesia Nomor: 14 / 2 /PBI/ 2012 Tentang Perubahan Atas Peraturan Bank Indonesia Nomor 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu, dapat dilakukan dengan memanfaatkan media internet yakni secara elektronik menggunakan kartu elektronik, baik itu kartu *automated teller machine* (selanjutnya disebut kartu ATM), kartu Debet, dan/atau kartu kredit.

Terhadap kemajuan teknologi yang begitu pesat di dunia perbankan sendiri sebenarnya kurang begitu terdukung dengan peraturan perundang-undangan terkait perbankan yang ada sekarang. Adapun tindak pidana yang diatur dalam dalam Undang-Undang Republik Indonesia Nomor 7 Tahun 1992 Tentang Perbankan, Lembaran Negara Republik Indonesia Tahun 1992 Nomor 32, Tambahan Lembaran Negara Republik Indonesia Nomor 3473, sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan

---

[2] *ibid.*

[3] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (OUP Oxford 2002).[11-12].

Lembaran Negara Republik Indonesia Nomor 3790 (selanjutnya disebut Undang-Undang Perbankan) dan Undang-Undang No.21 Tahun 2008 tentang Perbankan Syariah, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 94, Tambahan Lembaran Negara Republik Indonesia Nomor 4867 (selanjutnya disebut Undang-Undang Perbankan Syariah) adalah:

a. Tindak pidana berkaitan dengan perizinan;
b. Tindak pidana berkaitan dengan rahasia bank;
c. Tindak pidana berkaitan dengan pengawasan bank;
d. Tindak pidana berkaitan dengan kegiatan usaha bank;
e. Tindak pidana berkaitan dengan pihak terafiliasi;
f. Tindak pidana berkaitan dengan pemegang saham;
g. Tindak pidana berkaitan dengan ketaatan terhadap ketentuan. [4]

Pengaturan terkait pidana tersebut hanya mengatur terkait perbuatan-perbuatan yang dilakukan oleh pihak bank atau pihak terafiliasi. Yang diaksud Pihak Terafiliasi menurut Pasal 1 angka 22 Undang-Undang Perbankan adalah anggota dewan komisaris, pengawas, direksi atau kuasanya, pejabat, atau karyawan bank; anggota pengurus, pengawas, pengelola atau kuasanya, pejabat, atau karyawan bank, khusus bagi bank yang berbentuk hukum koperasi sesuai dengan peraturan perundangundangan yang berlaku; pihak yang memberikan jasanya kepada bank, antara lain akuntan publik, penilai, konsultan hukum dan konsultan lainnya; dan pihak yang menurut penilaian Bank Indonesia (saat ini OJK) turut serta mempengaruhi pengelolaan bank, antara lain pemegang saham dan keluarganya, keluarga komisaris, keluarga pengawas, keluarga direksi, keluarga pengurus. Pemikiran dari pembentukan ketentuan pidana terkesan hanya memikirkan bank dan pihak terafiliasinya sebagai subjek pada posisi yang dominan tanpa memikirkan bahwa bank dapat pula mengalami kerugian diakibatkan oleh tindak pidana, sebagai contoh dapat terjadi "pembobolan bank".

Pada saat penulisan penelitian ini, kejahatan terkait perbankan yang sedang ramai dibicarakan adalah *Skimming*, mengingat kasus *Skimming* bank BRI. Dalam modus operandi "pembobolan bank" dengan cara *Skimming* dilakukan

[4] Otoritas Jasa Keuangan, *Pahami dan Hindari: Buku Memahami dan Menghindari Tindak Pidana Perbankan* (OJK 2016).[9-10].

dengan mekanisme mencuri data nasabah yang tersimpan dalam magnetik strip pada kartu ATM dan dikirim secara nirakabel. Cara pencurian data ini dilakukan dengan beberapa langkah, yaitu umumnya pertama-tama pelaku memasang alat *skimmer*(*electronic data capture*) pada mulut mesin ATM, lalu pelaku memasang kamera tersembunyi untuk menangkap gerakan jari nasabah saat menekan pin ATM yang ditutupi, misalnya dengan kotak brosur. Selain itu, pelaku juga mengkondisikan ATM untuk mengeluarkan pesan isi dari ATM sedang habis padahal sudah memasukkan pin dan kartu, selanjutnya setelah pelaku mendapat data nasabah maka pelaku menyalindata tersebut kedalam kartu palsu. Dalam beberapa kasus pelaku tidak memasang kamera tersembunyi namun hanya dengan mengintip dari balik bahu nasabah.[5] Pada perkembangannya pelaku *Skimming* tidak lagi perlu menggunakan kamera tersembunyi atau dengan mengintip dari balik bahu nasabah, namun menggunakan *keypad*/papan tombol palsu pada mesin ATM untuk merekam pin nasabah secara otomatis.[6]

Terlepas dari modus operandi yang digunakan, tindakan *Skimming* dan mendapatkan pin ATM pada akhirnya akan diikuti dengan perbuatan memindahkan data yang didapatnya kedalam kartu ATM palsu. Kartu ATM palsu tersebut selanjutnya digunakan untuk mengambil uang menggunakan mesin ATM. Sistem mesin ATM yang bekerja secara *Real Time Online* menggunakan jaringan internet, maka penarikan maupaun pemindahan (*Transfer*) dana akan dibebankan terhadap simpanan nasabah dan secara otomatis sistem ATM akan melakukan pengurangan jumlah simpanan nasabah pada bank.

Perbuatan mengambil dana menggunakan kartu palsu yang menimpa nasabah sering dipandang sebagai pencurian uang pada rekening, seperti pada putusan Pengadilan Negeri Denpasar Nomor 687/Pid.B/2012/PN.DPS, dimana pada amarnya menyatakan terdakwa FIRDAUS THEODY alias IRDA FIRDAUS alias WAHYUDI terbukti secara sah dan meyakinkan bersalah melakukan tindak

[5] R. Toto Sugiharto, *Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya* (Media Pressindo 2010).[88, 140-141].

[6] *Ibid* [126-127].

pidana "Pencurian dalam keadaan memberatkan dan Pencucian uang". Pandangan demikian ditimbulkan oleh berkurangnya saldo simpanan nasabah yang ditampilkan pada sistem milik bank. Namun pada khasus *Skimming* bank BRI (Bank Rakyat Indonesia) pada hari Senin 12 Maret 2018 pihak bank memberikan dana pengganti uang simpanan nasabah yang berkurang akibat praktik *Skimming*. Adanya pemulihan dana oleh bank membuat seakan-akan kerugian diambil alih atau bahkan bank benar-benar menjadi subjek yang menerima kerugian akibat praktik *Skimming*, sedangkan nasabah tidak lagi terdampak oleh kerugian yang ditimbulkan oleh penarikan dana menggunakan kartu palsu hasil *Skimming*.

Pada satu sisi dengan adanya sikap perbankan yang mengambil alih kerugian yang diakibatkan penarikan dana menggunakan kartu palsu hasil *Skimming* membuat kepentingan nasabah menjadi terlayani, namun di sisi yang lain menimbulkan kekaburan terhadap bentuk kerugian yang ditimbulkan oleh praktik *Skimming*. Kekaburan tersebut menjadi titik anjak dari beberapa pertanyaan seperti "Siapa sebenarnya korban tindak pidana *Skimming* dan penarikan dana menggunakan kartu palsu hasil *Skimming*?", dan lebih lanjut mengingat kerugian yang timbul "Apa mungkin bank diapandang sebagai korban tindak pidana dan dapat mengajukan restitusi?".

Modus Pembobolan Atm Dengan Menggunakan Teknik Skimming

Pembobolan bank dapat dibagi menjadi dua jenis, yaitu:

A. Error Omission

Yaitu "pembobolan bank" dengan melakukan pelanggaran terhadap sistem atau prosedur yang sifatnya pasif atau tidak melakukan sesuatu yang seharusnya dilakukan. Prosedur yang sifatnya pasif disini mengacu pada prosedur dan prinsip *accounting*, yaitu pada fungsi operasi klerikal, pencatatan transaksi, dan penjurnalan.[7] Pelanggaran ini memiliki bentuk aturan yang jelas dan juga sanksi

[7] Razmy Humris, *Memahami Motif & Mengantisipasi Penyalahgunaan Wewenang* (Gramedia Pustaka Utama 2015).[74].

yang jelas, umumnya sanksi administratif;[8] dan

B. Error Commission

Yaitu "pembobolan bank" yang dilakukan secara aktif dengan melaukan perbuatan yang salah, tetapi karena tidak tertulis dalam sistem dan prosedur maka dilakukan. Pelanggaran ini sangat berkenaan dengan integeritas dari orang-orang pada bank itu sendiri.[9] Pelanggaran ini akan dikenai sanksi yang sifatnya normatif, namun biasanya diatur dalam *code of conduct* (kode etik).[10] [11]

Hal kejahatan "pembobolan bank" sendiri seiring dengan perkembangan teknologi yang ada maka timbul perkembangan terkait dengan Modus Operandi yang digunakan. Adapun beberapa jenis Modus Operandi yang kerap dilakukan adalah:[12]

a. Pemalsuan Dokumen;
b. Pembukuan ganda;
c. Penggelapan uang nasabah;
d. Mekanisme transfer dana;
e. Pembobolan dengan menggunakan L/C; [13]
f. Phishing (*Password harvesting fishing*); [14]
g. Cyber Malware;[15]
h. Skimming.

Skimming dilakukan dengan mencuri data digital yang tersimpan pada kartu ATM dengan menggunakan alat berupa *electronic data capture* yang disebut *skimmer*. *Skimmer* bekerja dengan cara menyalin data pada *magnetic* strip/ pita magnetik yang

[8] Adityah Pontoh, 'Pertanggungjawaban Korporasi Terhadap Tindak Pidana Pembobolan Rekening Nasabah Bank' (2018) VI *Lex Privatum*.[93] dikutip dari K. Wantjik Saleh, *Tindak Pidana Korupsi dan Suap* (Ghalia Indonesia 1971).[51].

[9] Razmy Humris. *Loc.Cit.*

[10] Adityah Pontoh. *Loc.Cit.*

[11] Frilly Margaret Wurangian, 'Pertanggungjawaban Pidana Terhadap Korporasi Perbankan Akibat Dari Tindak Pidana pembobolan bank' (2015) 4 *Lex Crimen* [136] dikutip dari Krisna Wijaya, *Kejahatan Perbankan dalam Perbankan Nasional Catatan Kolom Demi Kolom, cet. Ke dua* (Kompas Media Nusantara 2002)(selanjutnya disebut Krisna Wijaya I).[38].

[12] Krisna Wijaya I. *Op.Cit.*[136-137].

[13] Sarah D.L. Roeroe, 'Perlindungan Terhadap Bank Dalam Transaksi Perdagangan Dengan Menggunakan Sarana Letter Of Credit / LC' (2013) XXI *Jurnal Hukum UNSRAT* [25].

[14] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding* (CV Andi Offset 2013).[214].

[15] Ferry Satya Nugraha [ed.,al.], 'Perlindungan Hukum Terhadap Nasabah Bank dalam Pembobolan *Internet Banking* Melalui metode *Malware*' (2016) 5 *Diponegoro Law Jurnal* [11].

menyimpan data pribadi nasabah yang digunakan dalam sistem perbankan untuk mengidentifikasi nasabah yang hendak melakukan transaksi di mesin ATM.

Skimming dapat dilakukan dengan merekrut orang-orang yang bekerja sebagai pelayan restoran dengan memberikan *Skimmer* berukuran kecil. *Skimmer* tersebut digunakan untuk menggesek kartu saat ada pelanggan restoran yang hendak melakukan pembayaran dengan menggunakan kartu, prosesnya hanya memakan waktu beberapa detik dan dilakukan saat pemilik kartu tidak melihat sehingga proses *Skimming* susah untuk disadari.[16] Selain digunakan dengan merekrut orang, *skimmer* biasanya dipasang pada mesin ATM, *Skimmer* dipasang sehingga seolah-olah seperti bagian dari mesin ATM dengan tujuan agar nasabah selaku pemilik kartu ATM secara sukarela memasukkan kartu ATM milikknya.[17]

Pada awalnya *skimmer* berukuran besar dan tidak terlihat seperti bagian dari mesin ATM, namun seiring perkembangannya *Skimmer* berukuran kecil dan bekerja cukup dengan menggunakan baterai, umumnya dipasang pada tempat memasukkan kartu ATM dengan menggunakan selotip dua sisi sehingga kartu ATM nasabah akan masuk melewati *Skimmer* saat nasabah hendak melakukan transaksi.[18] Data yang diperoleh melalui *skimmer* selanjutnya dimasukkan kedalam kartu palsu yang juga memiliki *magnetic strip/*pita magnetik agar dapat dipergunakan pada mesin ATM seperti nasabah menggunakan kartu ATM.

Berbeda dengan *Phishing* dan *Cyber Mallware* yang langsung mendapat seluruh data nasabah, pada *Skimming*, proses pembobolan juga melibatkan proses memperoleh nomor pin nasabah agar pelaku *Skimming* dapat mengakses mesin ATM menggunakan data nasabah dengan. Untuk memperoleh pin nasabah dapat dilakukan dengan beberapa cara, yang paling sederhana adalah dengan mengintip melalui belakang bahu nasabah saat nasabah memasukkan pin, selain itu dapat dilakukan dengan memasang kamera untuk merekam gerakan jari nasabah saat

[16] Detective K. A. Farner, *Stealing You Blind: Tricks of the Fraud Trade* (iUniverse 2009). [30].

[17] R. Toto Sugiharto. *Op.Cit.*[140-141].

[18] Detective K. A. Farner. *Op.Cit.*[30; 61-62].

memasukkan pin atau lebih canggih lagi dilakukan penggantian papan tombol pada mesin ATM oleh pelaku sehingga pin nasabah akan terekam secara otomatis saat nasabah menekan papan tombol.[19] Setelah pelaku memperoleh data nasabah yang telah dimasukkan kedalam kartu palsu dan pin nasabah maka pelaku *Skimming* dapat melakukan transaksi menggunakan kartu ATM baik penarikan tunai, transfer dana, maupun transaksi debet.

Dalam "pembobolan bank" umumnya melibatkan pihak dalam bank, karena pihak tersebut memiliki pengetahuan dan akses terkait seluk beluk, mekanisme dan sistem kemanan bank yang hendak dibobol.[20] Namun keterlibatan orang dalam bank bukanlah menjadi syarat mutlak bagi suatu operasi "pembobolan bank". Kedelapan Modus Operandi dalam "pembobolan bank" yang telah dijabarkan diatas menunjukkan adanya keragaman dalam hal pelaku pembobolannya (*dader*-nya). Terhadap keragaman pelaku "pembobolan bank" secara umum dapat dikelompokkan menjadi tiga kelompok, yaitu:

1. "pembobolan bank" oleh orang dalam bank (interen) dan murni atas inisiatifnya sendiri;
2. "pembobolan bank" oleh pihak diluar bank (eksteren); dan
3. "pembobolan bank" oleh kolaborasi antara orang dalam bank dengan pihak luar bank (kombinasi). [21]

Dikaitkan dengan pembagian terkait pelaku/*dader* "pembobolan bank", modus-modus "pembobolan bank" juga memiliki perbedaan dari bentuk perbutan atau cara untuk melakukan "pembobolan bank" itu sendiri dan juga sumber perolehan uang dalam Modus Operandi itu sendiri. Berdasarkan kedelapan Modus Operandi yang sebelumnya telah dipaparkan maka bentuk-bentuk perbuatan dalam Modus Operandi sendiri meliputi pemalsuan, manipulasi, penggelapan, dan memperoleh data pribadi nasabah untuk melakukan transaksi atas nama nasabah. Sedangkan

[19] R. Toto Sugiharto. *Op.Cit.*[126-127].
[20] Adityah Pontoh. *Op.Cit.*[91].
[21] *Ibid.* dikutip dari Sutan Remy Sjahdeini, *Himpunan Tulisan Kapita Selekta Hukum Perbankan, jilid 1*(UI Press 2006).[20].

Sumber perolehan uang dalam "pembobolan bank" pun meliputi kredit fiktif, pencairan surat berharga fiktif, L/C, dan secara langsung dari rekening nasabah. Secara sederhana dapat digambarkan dengan matriks sebagai berikut:

Tabel 1. Perbandingan Pembobolan Bank[22]

No	Modus Operandi	Pelaku/ *Dader*			Perbuatan	Perolehan uang
		Interen	Eksteren	Kombinasi		
1	Pemalsuan Dokumen	Tidak	Tidak	Ya	Pemalsuan	Kredit fiktif; Pencairan surat berharga fiktif
2	Pembukuan Ganda	Ya	Tidak	Tidak	Pemalsuan; Manipulasi; Penggelapan	Rekening Nasabah
3	Penggelapan Uang Nasabah	Ya	Tidak	Tidak	Penggelapan	Rekening Nasabah
4	Mekanisme Transfer Dana	Ya	Tidak	Tidak	Manipulasi; Penggelapan	Rekening Nasabah
5	Latter of Credit (L/C)	Tidak	Tidak	Ya	Pemalsuan; Manipulasi	Latter of Credit (L/C)
6	*Password Harvesting Fishing (Phishing)*	Tidak	Ya	Tidak	Mengambil data pribadi nasabah (dengan penipuan secara online/ *cyber fraud);* Transaksi atas nama nasabah	Rekening Nasabah

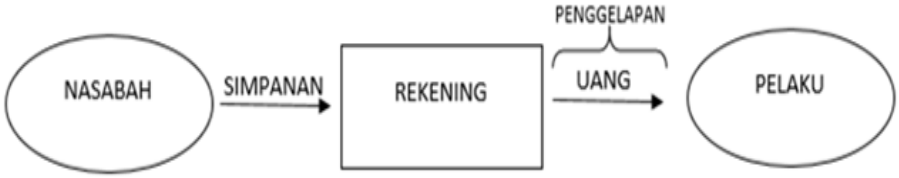
[22] Dibuat berdasarkan beberpa sumber: Krisna Wijaya I. *Op.Cit.*[136-137]. Sarah D.L. Roeroe. *Loc.Cit.* Vyctoria..*Loc.Cit.* Ferry Satya Nugraha [ed.,al.]. *Loc.Cit.* Detective K. A. Farner. *Loc. Cit.* R. Toto Sugiharto. *Loc.Cit.*

7	*Cyber Malware*	Tidak	Ya	Tidak	Mengambil data pribadi nasabah (dengan menggunakan program komputer); Transaksi atas nama nasabah	Rekening Nasabah
8	*Skimming*	Tidak	Ya	Tidak	Mengambil data pribadi nasabah (dengan Menyalin data pada kartu ATM nasabah); perolehan pin nasabah; Transaksi atas nama nasabah	Rekening Nasabah

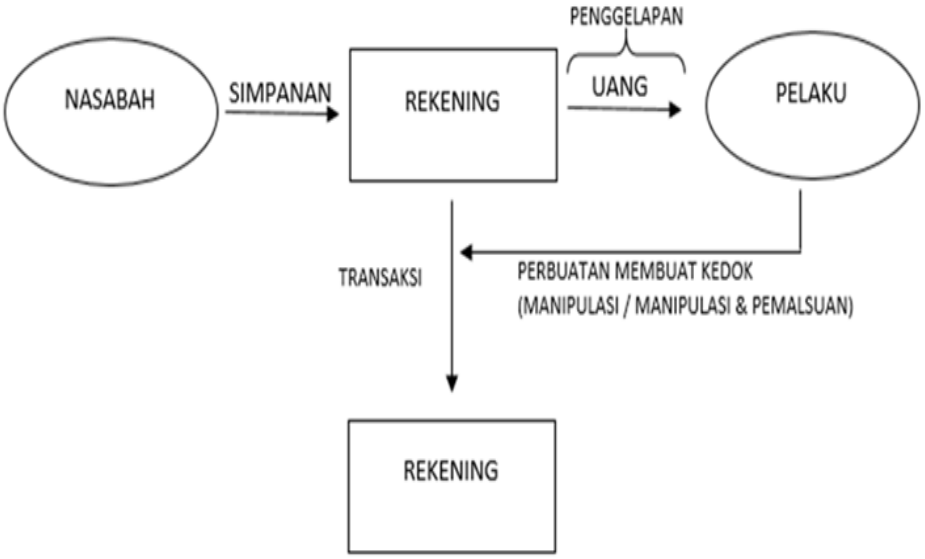
Berdasarkan matriks tersebut, "pembobolan bank" oleh orang dalam bank (interen) meliputi Modus Pembukuan Ganda, Penggelapan Uang Nasabah, dan Mekanisme Transfer Dana, "pembobolan bank" oleh pihak diluar bank (eksteren) meliputi Modus *Phishing, Cyber Malwere,* dan *Skimming*, sedangkan "pembobolan bank" oleh kolaborasi antara orang dalam bank dengan pihak luar bank (kombinasi) meliputi Modus Pemalsuan Dokuman dan Pembobolan dengan Menggunakan L/C. Secara umum setiap kelompok Modus Operandi memiliki ciri-ciri khusus, baik itu "pembobolan bank" oleh orang dalam bank, "pembobolan bank" oleh pihak diluar bank, maupun "pembobolan bank" oleh kolaborasi antara orang dalam bank dengan pihak luar bank.

Pada "pembobolan bank" oleh orang dalam bank, Secara sederhana dapat digambarkan dalam dua buah skema sebagai berikut:

Skema 1. "pembobolan bank" Oleh Orang Dalam Pada Rekening Pasif[23]

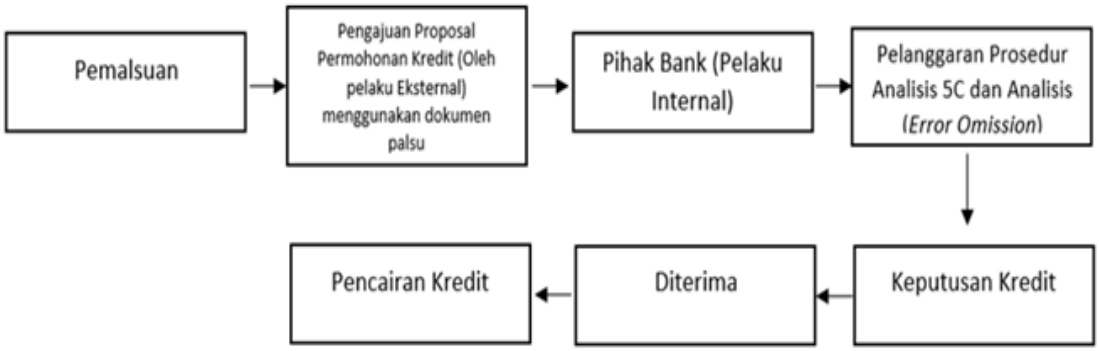


Skema 2. "pembobolan bank" Oleh Orang Dalam Pada Rekening Aktif[24]



"Pembobolan bank" oleh kolaborasi antara orang dalam bank dengan pihak luar bank (kombinasi) dapat digambarkan dalam skema sebagai berikut:

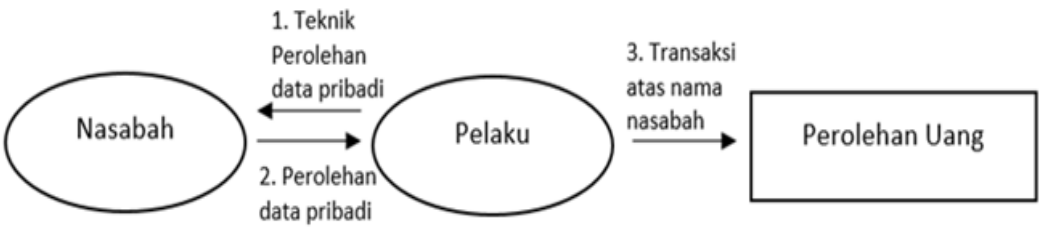
Skema 3. "pembobolan bank" oleh Kombinasi Pihak Dalam dan Luar Bank[25]



[23] Krisna Wijaya I. *Loc.Cit.*
[24] *Ibid*.
[25] Dibuat berdasarkan beberpa sumber: Krisna Wijaya I.*Loc.Cit.* Sarah D.L. Roeroe.*Loc.Cit.*

Seperti sebelumnya telah dibahas, walaupun umumnya melibatkan pihak dalam bank, namun "pembobolan bank" dapat dilakukan dengan oleh pihak diluar bank. Terhadap "pembobolan bank" oleh pihak luar bank maka secara umum dapat digambarkan melalui skema sebagai berikut:

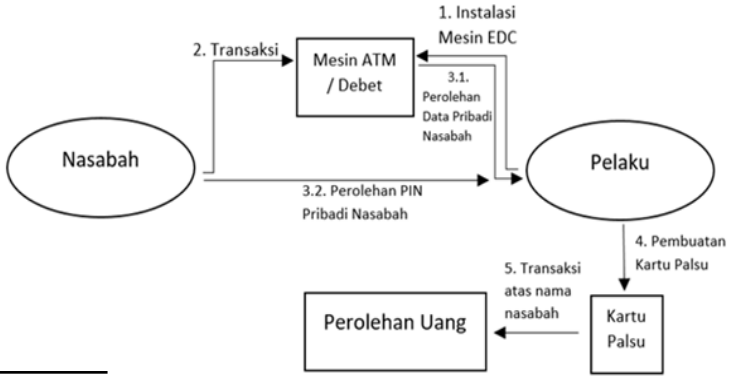
Skema 4. "pembobolan bank" Oleh Pihak Di Luar Bank[26]



Pada skema tersebut dalam hal dikaitkan dengan teknik *Phishing* dan *Cyber Malwere* memang cukup mudah untuk dipahami, karena prosesnya yang sederhana. Pada *Phishing* cukup dengan penipuan melalui media email dan *website* palsu, sedangkan pada *Cyber Malwere* dilakukan secara otomatis menggunakan aplikasi computer secara digital. Berbeda dengan *Phishing* dan *Cyber Malwere* yang cukup sederhana, pada modus *Skimming* memiliki tingkat kerumitan yang lebih tinggi dimana perlu melibatkan perbuatan memasang *Electronic Data Capture*, memperoleh pin nasabah dan pembuatan kartu elektronik palsu.[27]

Secara spesifik dalam "pembobolan bank" menggunakan teknik *Skimming* maka dapat di digambarkan lebih jelas berdasarkan skema sebagai berikut:

Skema 5. "pembobolan bank" Dengan Modus *Skimming*[28]



[26] Dibuat berdasarkan beberpa sumber: Vyctoria. *Loc.Cit.* Ferry Satya Nugraha [ed.,al.]. *Loc. Cit.* Detective K. A. Farner. *Lo.,Cit.* R. Toto Sugiharto. *Loc.Cit.*

[27] R. Toto Sugiharto.*Op.Cit.*[126-127].

[28] Dibuat berdasarkan beberpa sumber: Detective K. A. Farner. *Loc.Cit.* R. Toto Sugiharto. *Loc.Cit.*

Pada proses nomor 3.2 dapat dilakukan dengan beberapa cara diantaranya:

1. Mengintip saat nasabah memasukkan kombinasi pin di mesin ATM atau mesin Debet;
2. Memasang kamera tersembunyi pada mesin ATM untuk merekam pergerakan tangan nasabah saat memasukkan kombinasi pin; atau
3. Memasang Papan tombol palsu yang berfungsi untuk merekam kombinasi pin yang dimasukkan oleh nasabah. [29]

Selanjutnya setelah memperoleh data nasabah dan pin nasabah maka selanjutnya pada proses nomor 4 pelaku membuat kartu elektronik palsu yang ia buat sendiri dengan memasukkan data nasabah yang sebelumnya telah didapatkan. Pada pembuatan kartu elektronik palsu ini dimungkinkan dilakukan dengan tiga cara yaitu:

1. Cara *Altered Card*

   Yaitu dilakukan dengan menggunakan kartu elektronik asli yang diubah datanya. Cara ini dilakukan dengan memanaskan *relief* pada kartu elektronik (*reembossed*) dan selanjutnya diisi dengan data pribadi nasabah (*re-encoded*).[30]

2. Cara *Totally Counterfeit*

   Yaitu pembuatan kartu elektronik yang seluruhnya palsu. Cara ini menuntut pelaku untuk mencetak kartu yang serupa dengan kartu elektronik asli dengan mencantumkan gambar, logo, dan nomor hingga seolah-olah kartu elektronik yang asli. Pembuatannya melibatkan proses *embossing* dan *encoding*.[31]

3. Cara *White Plastic Card*

   Yaitu pembuatan kartu elektronik menggunakan kartu plastik putih polos. Cara ini hanya melibatkan proses *encoding* karena kartu palsu tersebut hanya dilakukan dengan melibatkan data tanpa melakukan pemalsuan pada fisik kartu.[32]

---

[29] R. Toto Sugiharto. *Op.Cit.*[126-127].

[30] Lexy Fatharany Kurniawan, "*Penegakan Hukum Tindak Pidana Kartu Kredit"*. **Skripsi**. Fakultas Hukum Universitas Airlangga. 2006.[30-31].

[31] *Ibid.*

[32] *Ibid.*

Kartu elektronik paslu ini dapat dibaca dan digunakan pada mesin ATM maupun mesin Debet layaknya kartu ATM. Pada akhir rangkaian proses tersebut maka pelaku *Skimming* akan menggunakan kartu palsu yang ia buat menggunakana data nasabah untuk melakukan transaksi perbankan. Karena transaksi perbankan dilakukan pelaku dengan menggunakan jaringan komputer yang aksesnya menggunakan data nasabah, maka sistem secara otomatis akan mengenali transaksi tersebut sebagai transaksi atas nama nasabah.

Tindak Pidana Pada Pembobolan Bank Menggunakan Teknik *Skimming*

*"*Pembobolan bank" dengan teknik *Skimming* dapat dibagi kedalam segmen sebagai berikut:

A. Memperoleh data nasabah;
B. Membuat kartu elektronik palsu; dan
C. Melakukan transaksi dengan menggunakan kartu elektronik palsu.

Perbuatan memperoleh data nasabah dengan menggunakan *Skimmer* sesuai dengan Pasal 46 ayat (2) UU ITE yang berbunyi sebagai berikut: "(2). Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)".

Pasal 46 ayat (2) UU ITE tersebut menjelaskan perbuatan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik berbunyi sebagai berikut: "(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".

Perbuatan yang diuraikan dalam Pasal 30 ayat (2) UU ITEtersebut dapat dijabarkan kedalam unsur-unsur sebagai berikut:

1. Sengaja;
2. Tanpa hak atau melawan hukum;
3. Mengakses Komputer dan/atau Sistem Elektronik; dan
4. Tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Terkait dengan unsur kesengajaan sebenarnya menjelaskan terkait dengan bentuk kesalahan pada delik yang diatur. Pengaturan terhadap bentuk kesalahan secara jelas ini berarti pembentukan pasal ini dilakukan dengan padangan monistis, dimana dalam perbuatan pidana (*Strafbaar feit*) unsur perbuatan dan unsur kesalahan merupakan satu kesatuan.[33] Kesalahan sendiri harus lah memiliki kesengajaan (*Dolus*) atau kealpaan (*Culpa*).[34]

Terhadap kesengajaan tersebut pemenuhannya dijelaskan berdasarkan dua teori, yaitu Teori Pengetahuan (*Voorstellings Theorie*) dan Teori Kehendak (*Wills Theorie*). Teori Pengetahuan (*Voorstellings Theorie*) memandang bahwa kesengajaan terhadap suatu akibat tidak dapat direncanakan, namun terhadap suatu akibat dapat dibayangkan (*Voorstellen*) saat akan melakukan suatu perbuatan, sehingga titik beratnya adalah pengetahuan akan suatu akibat dari tindak pidana yang dilakukan.[35] Teori Kehendak (*Wills Theorie*) memandang bahwa kesengajaan ditimbulkan oleh perbuatan dan kehendak terhadap suatu tindak pidana serta siap menanggung akibatnya.[36] Pada *Memorie van Toelichting* (M.v.T) *Wetboek van Strafrecht* (W.v.S) Belanda dijelaskan "pidana pada umumnya hendaknya dijatuhkan hanya pada barang siapa melakukan perbuatan yang dilarang dan dikehendaki (*Willens*) dan diketahui (*Wetens*)".[37]

Kesengajaan tersebut dapat dibedakan menjadi tiga:

A. Kesengajaan sebagai maksud (*Dolus als oogmerk*);
B. Kesengajaan dengan Kepastian (*zekenheids bewustzijn*);
C. Kesengajaan dengan Kemungkinan (*Dolus eventualis / In Kauf Nehmen*).[38]

Pada perbuatan memperoleh data nasabah dengan *Skimmer* jelas memiliki berupa Kesengajaan sebagai maksud (*opzet als oogmerk*) untuk memperoleh data nasabah itu sendiri.

---

[33] *Ibid* [43].
[34] *Ibid* [63].
[35] *Ibid* [70].
[36] *Ibid* [69].
[37] Liza Agnesta Krisna, *Hukum Perlindungan Anak: Panduan Memahami Anak yang Berkonflik dengan Hukum* (Deepublish 2018).[66].
[38] Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Perss 2014).[70-71].

Unsur tanpa hak atau melawan hukum menjelaskan terkait dengan sifat dari tindak pidana tersebut mewajibkan bahwa tindak pidana tersebut hanya dilanggar bila dilakukan tanpa hak atas akses komputer dan/atau Sistem Elektronik atau dilakukan dengan melawan hukum. Pada *Skimming*, perbuatan memperoleh data pribadi nasabah memiliki sifat melawan hukum yang jelas dimana melanggar ketentuan peraturan perundang-undangan. Pelanggaran yang menimbulkan sifat melawan hukum tersebut perlu diperhatikan Pasal 26 ayat (1) UU ITE yang berbunyi: "(1). Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan". Sehingga jelas bahwa pada perolehan data nasabah dilakukan secara tanpa hak dan juga melawan hukum.

Unsur mengakses Komputer dan/atau Sistem Elektronik merupakan unsur perbuatan dalam tindak pidana yang diatur. Pasal 1 angka 14 UU ITE mendefinisikan "Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan". Pasal 1 angka 5 UU ITE "Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik".

Dalam memperoleh data nasabah, pelaku menggunakan alat *Skimmer* untuk mengakses data nasabah. Akses yang dilakukan oleh pelaku ditujukan pada kartu elektronik yang berisi data nasabah. Berdasarkan definisi Informasi Elektronik maka pada dasarnya adalah data elektronik secara luas dengan bentuk yang tidak terbatas pada apa yang dijelaskan pada definisi tersebut. Terkait dengan konten atau isi dari data elektronik tidak disyaratkan sehingga bukan merupakan persoalan.

Dikaitkan dengan analisa terkait perolehandata pribadi nasabah sebagai Informasi Elektronik maka unsur tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik jelas terpenuhi.

Selanjutnya, berdasarkan Modus Operandi, pembuatan kartu elektronik palsu terdapat dua dimensi yang dapat dikatakan palus, yaitu yang pertama adalah data

dalam kartu elektronik dengan *encoding* dan yang kedua adalah fisik dari kartu palsu tersebut dengan *embossing*. Mengingat kartu elektronik dalam hal ini adalah APMK maka kartu elektronik tersebut merupakan surat berharga berdasarkan Kitab Undang-Undang Hukum Dagang,[39] hal ini mengindikasikan jelas bahwa hal dilakukan pemalsuan fisik kartu elektronik pada "pembobolan bank" menggunakan teknik *Skimming* merupakan tindak pidana (Delik) dalam Pasal 263 Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHAP). Terkait pemalusan data pada kartu palsu merupakan pemalsuan yang terkait dengan komputer sehingga menggunakan Pasal 51 ayat (1) UU ITE

Selanjutnya terkait dengan perbuatan segmen ketiga pada "pembobolan bank" menggunakan teknik *Skimming* yaitu melakukan transaksi dengan menggunakan kartu elektronik palsu. Telah dijelaskan sebelumnya pada bagian Modus Operandi bahwa tansaksi disini merupakan transaksi atas nama terdakwa dengan menggunakan data nasabah yang diperoleh melalui tindak pidana pada segmen pertama. Perbuatan pelaku melakukan transaksi menggunakan data pribadi nasabah memiliki indikasi terhadap adanya penggunaan identitas palsu, yakni pelaku bertindak seolah-oleh ia adalah nasabah yang data pribadinya digunakan. Kaitannya dengan tindak pidana sendiri penggunaan identitas palsu erat kaitannya dengan perbuatan curang (*Bedrog*).

Adapun unsur-unsur dari pasal 378 KUHP tersebut dikelompokkan berdasarkan sifatnya maka terdapat unsur subjektif dan unsur objektif. Unsur maksud untuk menguntungkan diri sendiri atau orang lain dan juga unsur melawan hukum merupakan unsur subjektif. Sedangkan unsur menggunakan nama palsu atau martabat palsu, dengan tipu muslihat, atau rangkaian kebohongan dan unsur menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang merupakan unsur objektif.[40]

---

[39] Sri Yunengsih Utama. "Perlindungan Hukum Terhadap Pemegang Kartu Kredit Sebagai Akibat Penyalahgunaan Kartu Kredit Dalam Transaksi Perdagangan". **Thesis**. Fakultas Hukum Universitas Pasundan. 2013. [2].

[40] Jonaedi Effendi, *Cepat & Mudah Memahami Hukum Pidana* (Kencana 2016).[144-145].

Terkait unsur-unsur subjektif pada perbuatan melakukan transaksi atas nama nasabah menggunakan kartu elektronik palsu jelas terpenuhi. Unsur maksud untuk menguntungkan diri sendiri atau orang lain, jelas telihat dari rangkaian perbuatan yang telah dijelaskan pada bagian Modus Operandi yakni tujuan perolehan uang sebagai tujuan akhir dari "pembobolan bank" itu sendiri. Sedangkan unsur secara melawan hukum terlihat dari penggunaan kartu elekrtonik palsu yang berisi data nasabah yang telah diperoleh yang merupakan hasil dari tindak pidana.

Unsur menggunakan nama palsu, atau martabat palsu, atau tipu muslihat, atau rangkaian kebohongan merupakan unsur perbuatan. Pada unsur ini perbuatan yang disayaratkan disusun secara alternatif, pemenuhan salah satu perbuatan saja cukup untuk memenuhi unsur tersebut. Pada transaksi atas nama nasabah menggunakan kartu elektronik palsu melibatkan baik mesin ATM ataupun mesin debet, yang mana dapat diartikan sebagai Komputer, jaringan Komputer, dan/atau media elektronik lainnya dalam definisi transaksi elektronik dalam Pasal 1 angka 2 Undang-Undang Informasi dan Transaksi Elektronik. Karena tansaksi tersebut merupakan Transaksi Elektronik, maka cara transaksi dilakukan merupakan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana diatur dalam Pasal 17 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Dengan terbatasnya interaksi dalam Transaksi Elektronik pada Informasi Elektronik dan/atau Dokumen Elektronik, maka pada transaksi atas nama nasabah menggunakan kartu elektronik palsu, penggunaan Informasi Elektronik berupa data pribadi nasabah oleh pelaku merupakan bentuk dari nama palsu dan martabat palsu.

Unsur menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang berarti ada orang yang terbujuk untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang. Pada transaksi dengan kartu palsu, secara fisik yang bertemu adalah pelaku dengan mesin. Mesin ATM adalah mesin/komputer yang digunakan oleh bank untuk melakukan kegiatan-kegiatan penyetoran uang, pengambilan uang, pengecekan saldo, transfer antar rekening, dan transaksi

keuangan lain yang dilakukan secara elektronik.[41] Sehingga transaksi dengan mesin ATM yang terjadi bukanlah antara pelaku dengan mesin karena transaksi tersebut merupakan Transaksi Elektronik, kedudukan mesin dalam transaksi tersebut merupakan Sistem Elektronik dan bukan merupakan subjek hukum sehingga dalam hal penarikan tunai pada mesin ATM menggunakan kartu elektronik palsu bukan berarti pelaku menggerakkan mesin ATM untuk menyerahkan sejumlah uang. Bila mengacu pada Pasal 1 angka 3, 4, 5, dan 6 PBI Penyelenggaraan APMK maka sebenarnya perbuatan hukum yang timbul dalam Transaksi Elektronik menggunakan APMK adalah dengan Prinsipal. Pasal 1 angka 8 PBI Penyelenggaraan APMK mendefinisikan mengenai prinsipal sebagai berikut:

"Prinsipal adalah Bank atau Lembaga Selain Bank yang bertanggung jawab atas pengelolaan sistem dan/atau jaringan antar anggotanya, baik yang berperan sebagai penerbit dan/atau acquirer, dalam transaksi APMK yang kerjasama dengan anggotanya didasarkan atas suatu perjanjian tertulis".

Penyerahan uang melalui mesin ATM pada transaksi menggunakan kartu elektronik palsu merupakan Transaksi Elektronik antara pelaku (dengan mengatasnamakan nasabah yang data pribadinya digunakan) dengan bank selaku Prinsipal. Unsur menggerakkan orang lain dalam hal ini mengacu pada bank sebagai subjek hukum dalam hubungan hukum yang timbul saat Transaksi Elektronik terjadi. Demikian unsur menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang telah terpenuhi, sehingga transaksi menggunakan kartu elektronik palsu pada "pembobolan bank" dengan teknik *Skimming* merupakan tindak pidana (Delik) dalam Pasal 378 KUHP.

Korban Tindak Pidana Pembobolan Atm Dengan Menggunakan Teknik Skimming Terkait Dengan Pengajuan Restitusi

Menentukan korban suatu tindak pidana menjadi penting dalam menentukan

[41] Ronny Prasetya, *Pembobolan ATM Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan* (Prestasi Pustaka 2010).[12].

siapa yang berhak atas hak-hak tertentu yang diberikan oleh undang-undang. Menurut Pasal 1 angka 3 UU Perlindungan Saksi dan Korban, Korban adalah "orang yang mengalami penderitaan fisik, mental, dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana"

Pemikiaran-pemikiran diatas terkesan mengartikan korban adalah individu saja. Namun, penimbulan korban dalam "pembobolan bank" menggunakan teknik *Skimming* merupakan penimbulan korban pada modus operandi canggih, sehingga korbannya bukan saja individu konkrit namun juga subjek yang masal dan abstrak.[42] Penderitaan yang ditimbulkan dalam "pembobolan bank" dengan teknik *Skimming* sendiri juga tidak lagi penderitaan fisik seperti pada penimbulan korban yang sifatnya konvensional, namun juga penderitaan moril dan psikologis yang bersifat struktural dan non-struktural.[43]

Barsama dengan perkembangan kejahatan, memang korban tidak lagi terbatas pada perseorangan, namun meluas dan kompleks.

Sellin dan Wolfgang berpendapat pula dalam teorinya mengenai tipologi korban, yaitu korban dapat dibagi menjadi:

1. *Primary victimization*, yaitu korban berupa individu perorangan yang secara langsung dilukai atau dirugikan.
2. *Secondary victimization*, yaitu korban kelompok dalam arti tidak personal, kolektif, dan komersial.
3. *Tertiary victimization*, yaitu korban masyarakat dalam arti yang sangat luas dan tidak termasuk dalam *Primary victimization* dan *Secondary victimization* .
4. *Mutual victimiazation*, yaitu korban yang terlibat dalam kondisi yang bersifat timbal balik.
5. *No victimization*, umumnya digunakan dalam mengkategorikan dalam kenakalan anak. [44]

Dalam UU Perlindungan Saksi dan Korban, pada pasal 1 angka 9 pun mengakui bahwa subjek setiap orang yang diatur di dalamnya tidak terbatas pada individu, namun termasuk pula korporasi. Lebih lanjut di dalam penjelasan

---

[42] Koesparmono Irsan, 'Korban Kejahatan Perbankan', dalam J. E. Sahetapy, (ed) (*Bunga Rampai Viktimisasi*, Eresco 1995).[20].

[43] *Ibid.*

[44] Marvin E. Wolfgang dan Simon I. Singer, 'Victim Categories of Crime' (1978) 69 *Journal of Criminal Law and Criminology* [384-385].

umum UU Perlindungan Saksi dan Korban dijelaskan pula "Ketentuan mengenai subjek hukum yang dilindungi dalam UndangUndang ini diperluas selaras dengan perkembangan hukum di masyarakat." Sehingga menjadi jelaslah bahwa sebenarnya yang dapat disebut sebagai korban tidak hanya terbatas pada individu.

Pasal 378 KUHP untuk transaksi menggunakan kartu palsu sendiri seperti yang telah dijelaskan pada sub sebelumnya mengakibatkan bank selaku badan hukum menyerahkan sejumlah uang kepada pelaku "pembobolan bank". Jelas bahwa penderitaan yang timbul adalah kerugian ekonomi, yaitu sejumlah uang. Perlu dipahami pula bahwa uang yang ada dalam mesin ATM merupakan simpanan nasabah, dimana simpanan timbul berdasarkan perjanjian penyimpanan dana yang bersifat riil, dimana penyerhannya dilakukan secara nyata dan uang yang telah diserahkan kepada bank menjadi milik bank dan penggunaannya jadi wewenang penuh bank.[45] Hal penyerahan uang oleh bank didasarkan penggunaan kartu palsu hasil *Skimming* maka sebenarnya secara yuridis kerugian ada pada bank.

Manjadi persoalan juga terkait dengan penentuan teransaksi mana yang benar-benar dilakukan oleh nasabah dan transaksi mana yang dilakukan oleh pelaku pembobolan. Terkait hal tersebut Direktur Perencanaan Strategis dan Humas Bank Indonesia, Dyah Ni Makhijani menjelaskan bahwa dana nasabah akan diganti oleh bank dengan mekanisme nasabah melapor dengan membawa bukti kepemilikan rekening, bukti bahwa bukan yang bersangkutan yang melakukan transaksi dan merupakan akibat pembobolan dan akan di *verivikasi* terlebih dahulu.[46] Dikaitkan dengan mekanisme tersebut sebenarnya menimbulkan ketidak pastian terkait penimbulan korbannya, karena bank menganggap transaksi yang dilakukan menggunakan data nasabah adalah oleh nasabah itu sendiri sampai terbukti sebaliknya. Bank memberikan kewajiban pembuktian kepada nasabah agar kegiatan bank berjalan mulus dan kerugian tidak ada pada pihak bank.[47] Bank dalam hal tersebut mendasarkan pada 2 teori, yaitu Teori *Statement of Account*, yaitu

[45] Trisadini P. Usanti dan Abd. Somad, *Hukum Perbankan* (Kencana 2016).[39].
[46] Ronny Prasetya. *Op.Cit.* [41-42].
[47] *Ibid* [56].

kewajiban nasabah untuk memeriksa dan memberitahukan pada bank ketimpangan rekeningnya, dalam hal tidak diberitahu maka *statement of account* dianggap benar dan Teori *Contributory Negligence*, diaman laporan berkala saja sudah menggambarkan keadaan sebenarnya sampai nasabah membuktikan sebaliknya.[48]

Penerapan teori-teori tersebut oleh bank menimbulkan dua kemungkinan dalam penggantian uang nasabah. Dua Kemungkinan tersebut dapat dibandingkan dari kasus atas nama terdakwa Tumino alias Petruk bin Sarimin dalam Putusan Pengadilan Negeri Semarang Nomor 600/Pid.B/2014/PN Smg. Pada keterangan saksi-saksinya menunjukkan bahwa Saksi Irene Ludang Nurhayati dan Saksi Andi Susilo bin Mudjtahidin mendapat penggantian uang dari Bank BNI, sedangkan Saksi Risdianto Dwi Purnama Putra, S.Ked dikatakan "belum ada penggantian". Terhadap kasus tersebut dapat disimpulkan terdapat kemungkinan dilakukan penggantian dan kemungkinan tidak dilakukan penggantian oleh bank.

Nasabah yang tidak mampu membuktikan rekeningnya menjadi korban pembobolan namun mengalami kerugian sendiri merupakan korban yang terdampak secara tidak langsung oleh "pembobolan bank" menggunakan teknik *Skimming*, akibat dari kebijakan yang diambil oleh bank. Kebijakan yang diambil oleh bank tidak bersifat melawan hukum, namun nasabah menjadi dirugikan. Pada transaksi menggunakan kartu palsu, nasabah menjadi korban secara *vicarious*, dimana yang dialamai adalah *vicarious victimization*, dimana seorang menjadi korban atas kerugian yang dialami akibat viktimisasi terhadap subjek lain.[49]

Damikian, jelasalah bahwa korban yang timbul dalam pembobolan ATM menggunakan teknik *Skimming* bergantung pada bank dan nasabah. Kondisi yang pertama adalah nasabah mampu membuktikan adanya transaksi oleh pihak lain sehingga bank memulihkan rekening nasabah dan kerugian berada pada pihak bank. Kondisi yang kedua adalah nasabah tidak mampu membuktikan adanya transaksi oleh pihak lain sehingga bank menolak untuk memulihkan rekeningnya

[48] *Ibid* [60].

[49] Bonnie S. Fisher dan Steven P. Lab, ed., *Encyclopedia of Victimology and Crime Prevention* (Sage Publications 2010).[962].

dan kerugian berada pada pihak nasabah. Sebagai implikasi dari dua kondisi yang ada maka terdapat variasi terhadap korban yang timbul, dalam hal terjadi kondisi yang pertama maka yang menjadi korban adalah bank, sedangkan pada kondisi yang kedua yang menjadi korban adalah nasabah.

Bank maupun nasabah sebagai korban pada pembobolan ATM menggunakan teknik *Skimming* memiliki hak untuk memperoleh ganti kerugian yang diakibatkan oleh perbuatan pelaku. Ganti rugi dalam bentuk restitusi ini berbeda dari kompensasi yang hanya dibatasi untuk korban tindak pidana yang merupakan pelanggaran hak asasi manusia yang berat dan tindak pidana terorisme saja, pada restitusi tidak ditentukan secara spesifik mengenai tindak pidana apa saja yang dapat dimintakan restitusi.

Terkait *legal standing* korban untuk mengajukan restitusi tentunya harus memenuhi kualifikasi sebagai korban atau ahli waris korban dalam hal korban meninggal dunia, dan selanjutnya memenuhi persyaratan pada Pasal 7A ayat (2) UU Perlindungan Saksi dan Korban, yaitu tindak pidana sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan LPSK. Pada "pembobolan bank" menggunakan teknik *Skimming* maka terdapat dua subjek korban yang dimungkinkan untuk memperoleh restitusi, yaitu bank atau nasabah.

Hal restitusi kerugian yang timbul menimbulkan keuntungan bagi pihak pelaku dengan jumlah yang setara dengan kerugian yang ditimbulkan, sehingga patut dan layak bila pengembalian kerugian dalam hal restitusi dibebankan terhadap pelaku. Namun, lain halnya bila uang yang diperoleh pelaku disita sebagai barang bukti, tentu pada putusan akan secara otomatis dikembalikan pada korban selaku pemilik sehingga kondisi semula telah tercapai dan restitusi tidak perlu diajukan. Hal memang uang yang diperoleh pelaku telah ditransaksikan maka barulah perlu dimohonkan restitusi. Pembebanan kerugian terhadap pelaku ini diharapkan dapat memulihkan keadaan sesuai dengan tujuan dari restitusi sendiri.

Hal nasabah yang memang dirugikan dan pelaku tidak dapat mengganti kerugian tersebut maka berdasarkan Pasal 1 angka 5 Peraturan Pemerintah Pemberian Kompensasi, Restitusi, dan Bantuan Kepada Saksi Korban, restitusi

dapat diberikan oleh pihak ketiga. Mengingat andil bank dalam viktimisasi yang diterima nasabah, seyogyanya bila pelaku tidak mampu mengganti uang nasabah, maka bank lah yang dibebani pembayaran restitusi tersebut. Dengan pengajuan restitusi yang dibebankan kepada bank maka memberi solusi bagi nasabah yang menjadi korban karena tidak mampu membuktikan ia tidak melakukan transaksi. Beban pembuktian yang tadinya dibebankan bank kepada nasabah, melalui mekanisme restitusi dipermudah, menjadi cukup dengan pembuktian oleh penuntut umum di muka persidangan, pun penyimpangan terhadap kebijakan yang dibuat oleh bank nantinya akan didasarkan pada putusan yang berkekuatan hukum tetap.

Kesimpulan

Teknik *Skimming* merupakan modus opernadi canggih yang dilakukan oleh pihak luar bank dalam melakukan "pembobolan bank. Perbuatan memperoleh data nasabah melanggar Pasal 46 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Perbuatan membuat kartu elektronik palsu melanggar Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik. Perbuatan melakukan transaksi atas nama nasabah menggunakan kartu elektronik palsu berisi data nasabahmelanggar Pasal 378 KUHP. Pelanggaran beberapa aturan pidana tersebut berdiri sendiri-sendiri dan terhadap kesemuanya tentu akan diadili sekaligus, sehingga berlaku konkursus realis (*Meerdaadse Samenloop*).

Penentuan korban yang berhak mengajukan restitusi pada pembobolan ATM dengan menggunakan teknik *Skimming* menjadi sangat kondisional berdasarkan dengan siapa yang menjadi korban antara bank dan nasabah.

Daftar Bacaan

Buku

Bonnie S. Fisher dan Steven P. Lab, ed., Encyclopedia of Victimology and Crime Prevention (Sage Publications 2010).

Detective K. A. Farner, Stealing You Blind: Tricks of the Fraud Trade (iUniverse 2009).

Didik Endro Purwoleksono, Hukum Pidana (Airlangga University Perss 2014).

Jonaedi Effendi, Cepat & Mudah Memahami Hukum Pidana (Kencana 2016).

Liza Agnesta Krisna, Hukum Perlindungan Anak: Panduan Memahami Anak yang Berkonflik dengan Hukum (Deepublish 2018).

Manuel Castells, The Internet Galaxy: Reflections on the Internet, Business, and Society (OUP Oxford 2002).

Otoritas Jasa Keuangan, Pahami dan Hindari: Buku Memahami dan Menghindari Tindak Pidana Perbankan (OJK 2016).

R. Toto Sugiharto, Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya (Media Pressindo 2010).[88, 140-141].

Razmy Humris, Memahami Motif & Mengantisipasi Penyalahgunaan Wewenang (Gramedia Pustaka Utama 2015).

Romli Atmasasmita, Hukum Kejahatan Bisnis Teori & Praktik di Era Globalisasi (Prenada Media 2016).

Ronny Prasetya, Pembobolan ATM Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan (Prestasi Pustaka 2010).

Trisadini P. Usanti dan Abd. Somad, Hukum Perbankan (Kencana 2016).

Vyctoria, Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding (CV Andi Offset 2013).

Jurnal

Adityah Pontoh, ‘Pertanggungjawaban Korporasi Terhadap Tindak Pidana Pembobolan Rekening Nasabah Bank’ (2018) VI Lex Privatum.

Ferry Satya Nugraha [ed.,al.], ‘Perlindungan Hukum Terhadap Nasabah Bank dalam Pembobolan Internet Banking Melalui metode Malware’ (2016) 5 Diponegoro Law Jurnal.

Frilly Margaret Wurangian, ‘Pertanggungjawaban Pidana Terhadap Korporasi Perbankan Akibat Dari Tindak Pidana pembobolan bank’ (2015) 4 Lex Crimen.

Koesparmono Irsan, ‘Korban Kejahatan Perbankan’, dalam J. E. Sahetapy, (ed). (

Bunga Rampai Viktimisasi, Eresco 1995).

Marvin E. Wolfgang dan Simon I. Singer, 'Victim Categories of Crime' (1978) 69 Journal of Criminal Law and Criminology.

Sarah D.L. Roeroe, 'Perlindungan Terhadap Bank Dalam Transaksi Perdagangan Dengan Menggunakan Sarana Letter Of Credit / LC' (2013) XXI Jurnal Hukum UNSRAT.

Karya Ilmiah

Lexy Fatharany Kurniawan, "*Penegakan Hukum Tindak Pidana Kartu Kredit"*. Skripsi. Fakultas Hukum Universitas Airlangga. 2006.

Sri Yunengsih Utama. "Perlindungan Hukum Terhadap Pemegang Kartu Kredit Sebagai Akibat Penyalahgunaan Kartu Kredit Dalam Transaksi Perdagangan". Thesis. Fakultas Hukum Universitas Pasundan. 2013.

HOW TO CITE: Michael Enrick, 'Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dangan Pengajuan Restitusi' (2019) Vol. 2 No. 2 Jurist-Diction