Volume 1, Issue 2, Desember 2018 **ISSN Online : 2622-7045**
ISSN Cetak : 2654-3605

PERLINDUNGAN HUKUM TERHADAP NASABAH BANK YANG DIRUGIKAN AKIBAT KEJAHATAN SKIMMING DITINJAU DARI PERSPEKTIF TEKNOLOGI INFORMASI DAN PERBANKAN

Dian Ekawati
Fakultas Ilmu Hukum, Universitas Pamulang
Email: mrs.dianeka@gmail.com

ABSTRACT

The progress of the banking system cannot be separated from the role of information technology. In addition to facilitating the company's internal operations, technology tools also aim to facilitate service to bank customers. One side of Information Technology provides not a few benefits to improving services both public services and internal services. On the other hand Information Technology is used by people who are not responsible by committing acts that are against the law, which attacks various legal interests of the people, society, and the state. This study aims to get information about banking crimes that use the skimming method and about legal protection for customers who are victims of skimming crime. The research method is juridical normative, namely obtaining and combining and analyzing data obtained from books, articles and journals and related legislation. The results obtained are that crime skimming is an old mode of customer money burglary which is done by stealing customer data at the customer's ATM with skimmer techniques. Legal protection against customers who are harmed due to the crime of skimming can be carried out by criminal means, namely reporting to the police and the police's duty to arrest the perpetrators. Legal protection through civil law by way of the bank replacing the customer's money after clarifying the transaction against the customer's account.

Keywords: *Licensing, Primary Clinic, Disruption Permit, Clinic Establishment Permit, Clinic Operational Permit*

PENDAHULUAN

Indonesia sebagai negara hukum, sudah semestinya jika setiap aspek kehidupan antara warga negara yang satu dengan yang lainnya diatur oleh hukum, karena masalah hukum senantiasa akan dihadapi oleh manusia baik sebagai individu maupun sebagai warga negara. Setiap manusia juga pasti mendambakan hidup yang damai, aman dan sejahtera. Akan tetapi, seiring dengan perkembangan hukum dan modernisasi dalam segala aspek kehidupan, tindak kejahatan di tengah masyarakat juga semakin meningkat, termasuk di Indonesia.

Setiap perbuatan yang bertentangan dengan kesusilaan, melanggar norma, mengacaukan, dan menimbulkan ketidak tenangan dalam kehidupan masyarakat dapat dikategorikan sebagai kejahatan. Kejahatan tidak hanya mengandung perbuatan melanggar hukum, tetapi juga melanggar hak-hak sosial, ekonomi dan lain sebagainya. Pelanggaran hukum berkaitan juga dengan pelanggaran dan penyalahgunaan

perkembangan teknologi tinggi (*hi tech*). Perkembangan kejahatan yang berkaitan dengan teknologi ini sering dikatakan sebagai bentuk kejahatan *cyber crime* (kejahatan dunia maya). Kejahatan siber (*Cyber* Crime) dapat terjadi tanpa mengenal ruang dan waktu, serta dapat dilakukan oleh siapa saja. Kejahatan dunia maya tersebut berkembang seiring perubahan masyarakat global yang tingkat perkembangannya melebihi eksistensi hukum.

Kejahatan *cyber crime*, disebut juga kejahatan *cyber space* merupakan cerminan dari kondisi masyarakat yang selalu berpacu antara keinginan dengan tarikan pengaruh global yang tidak sedikit menawarkan perubahan yang menimbulkan kerugian. Misalnya menjadikan teknologi sebagai alat memenuhi perkembangan dan dasar pengembangan sistem transaksi pada perbankan, tetapi masih seringkali gagal menolak dampak destruktifnya.

Seiring perkembangan zaman dan semakin canggihnya teknologi, kejahatan siber (*cyber crime*) berevolusi menjadi berbagai macam jenis kejahatan baru dengan modus operandi yang baru pula.Bentuk kejahatan siber (*cyber crime*) terus berkembang, mulai dari yang dikenal umum seperti *hacking, cracking, carding* hingga yang lebih spesifik lagi seperti: *probe* (usaha untuk memperoleh akses kedalam suatu sistem); *scan* (probe dalam jumlah besar); *account compromise* (penggunaan account secara illegal); *root compromise* (account compromise dengan *previlege* bagi si penyusup); *danial of service* atau *dos* (membuat jaringan tidak berfungsi karena kebanjiran traffic); penyalahgunaan *domain name*, dan lain-lain.[1]

Singkat kata, perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, nilai-nilai, wujud benda, logika berfikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi komputerisasi / digital. Hal tersebut telah berpengaruh terhadap bentuk, cara, sasaran hingga akibat dari kejahatan berbasis teknologi. Perubahan paradigm tersebut pada kenyataannya semakin sulit untuk diikuti oleh hukum sebagai sarana penertib sosial. Hukum berfungsi sebagai perlindungan kepentingan manusia. Agar kepentingan manusia terlindungi, hukum harus dilaksanakan. Jadi perlindungan hukum merupakan perlindungan yang diberikan oleh hukum maupun undang-undang untuk melindungi kepentingan manusia agar kehidupan manusia dapat berlangsung normal, tentram dan damai.

Negara selaku penyelenggara pemerintahan dan pelaksana sistem hukum harus berperan aktif menyikapi setiap permasalahan hukum yang berkaitan dengan perkembangan kejahatan *cyber crime*.

[1]Mahesa Jati Kusuma, *Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE di Bidang Perbankan*, Nusa Media, Bandung, 2012, hlm. 2.

Terutama pengembangan dan kajian ilmiah yang berkaitan dengan sistem hukum pidana nasional, khususnya Undang-Undang Informasi dan Transaksi Elektronik.

Permasalahan secara yuridis untuk menjerat pelaku kejahatan ini biasanya dikaitkan dengan berbagai persoalan yang berhubungan dengan beberapa karakteristik kejahatan *cyber crime*. Mengingat kejahatan ini melintasi batas territorial atau *borderless territory*, atau bahkan bisa dikatakan di luar territorial negara, yang pada akhirnya berkaitan dengan yuridiksi mana yang berhak melakukan proses peradilan. Tetapi dalam kajian ini, lebih memfokuskan pada tindak kejahatan *cyber crime* di wilayah Teritorial Nasional Indonesia.

Peran teknologi informasi disemua sektor kehidupan manusia sangat penting tak terkecuali dalam dunia perbankan.Kemajuan sistem perbankan tidak dapat dipisahkan dengan peranan teknologi informasi. Semakin berkembang dan kompleks fasilitas yang diterapkan perbankan untuk memudahkan pelayanan, semakin beragam dan kompleks pula adopsi teknologi yang dimiliki oleh suatu bank. Selain untuk memudahkan operasional internal perusahaan, perangkat teknologi juga bertujuan untuk memudahkan pelayanan terhadap nasabah bank. Karena hampir semua produk yang ditawarkan kepada nasabah itu tidak jauh berbeda, sehingga persaingan yang terjadi dalam dunia perbankan adalah bagaimana memberikan produk yang serba mudah dan cepat. Kegiatan perbankan dengan *electronic transaction* (*e-banking*) melalui mesin ATM, telepon seluler (*phone banking*) dan jaringan internet (*Internet banking)*, merupakan beberapa contoh pelayanan transaksi perbankan dengan teknologi informasi. Dari sisi keamanan, penggunaan teknologi dapat memberi perlindungan keamanan data dan transaksi.[2]

Namun tampaknya, di balik perkembangan ini terdapat berbagai permasalahan hukum yang berkaitan dengan kejahatan informasi dan transaksi elektronik di bidang perbankan, jika tidak diantisipasi dengan baik, tentu akan merugikan bank, masyarakat dan nasabah.Dalam tatanan implementasi, teknologi informasi dan komunikasi layaknya pisau bermata dua. Satu sisi Teknologi Informasi memberikan manfaat yang tidak sedikit terhadap peningkatan kesejahteraan dan peradaban manusia serta peningkatan sektor pelayanan baik pelayanan publik maupun pelayanan internal. Disisi lain Teknologi Informasi digunakan oleh orang-orang yang tidak bertanggungjawab dengan melakukan perbuatan yang sifatnya melawan hukum, yang menyerang berbagai kepentingan

[2]Tim Perundang-Undangan dan Pengkajian Hukum Direktorat Hukum BankIndonesia, "*Urgensi Cyberlaw diIndonesia Dalam Rangka Penanganan Cybercrime di Sektor Perbankan*", dalam Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 No. 2, Bank Indonesia, Jakarta, 2006.

hukum orang banyak, masyarakat, dan negara.[3]

Fokusnya kajian ilmiah ini akan penulis batasi terhadap dua rumusan masalah yaitu, **pertama** bagaimanakah kejahatan pembobolan uang nasabah denga menggunakan metode skiming dilihat dari persfektif informasi dan transaksi elektronik dan **kedua** bagaimana perlindungan hukum terhadap nasabah korban kejahatan dengan metode skimming ditinjau dari persfektif perbankan.

METODE PENELITIAN

Kejahatan perbankan yang memanfaat-kan teknologi informasi sangat beragam, tetapi dalam kajian ini penulis hanya fokus mengkaji kejahatan pembobolan uang nasabah oleh orang yang tidak bertanggung jawab dengan menggunakan metode Skimming serta mengkaji bagaimana perlindungan hukum terhadap nasabah yang menjadi korban kejahatan dengan metode skimming tersebut.

Untuk itu, penelitian ini menggunakan metode penelitian yuridis normatif yang termasuk kepada jenis penelitian normatif yang menggunakan data sekunder. Data yang didapat kemudian diolah dan dianalisa untuk menjawab persoalan yang ada.

PEMBAHASAN

Kejahatan Skimming Menurut Persfektif Informasi dan Transaksi Elektronik dan Perbankan

Untuk menggambarkan apa yang dimaksud dengan tindak pidana perbankan ini, secara teoritis terdapat banyak istilah yang digunakan. Istilah-istilah tersebut di antaranya adalah kejahatan perbankan, kejahatan dibidang perbankan, kejahatan terhadap perbankan, tindak pidana perbankan, tindak pidana di bidang perbankan, tindak pidana terhadap perbankan, dan berbagai istilah-istilah lainnya.

Menurut Kristian istilah-istilah tersebut dikelompokan menjadi dua bagian, kelompok pertama adalah kelompok tindak pidana di bidang perbankan yang pengertiannya sama juga dengan pengertian dari istilah kejahatan di bidang perbankan, tindak pidana terhadap perbankan atau kejahatan terhadap perbankan. Kelompok keduaadalah tindak pidana perbankan yang pengertiannya mencakup pengertian dari istilah kejahatan perbankan.

Sebagaimana telah dikemukakan diatas, istilah tindak pidana perbankan harus dibedakan dengan istilah tindak pidana di bidang perbankan. Tindak pidana perbankan ialah pelanggaran terhadap ketentuan perbankan yang diatur dan diancam dengan pidana berdasarkan Undang-Undang Perbankan (Undang-Undang Nomor 7 Tahun

[3]H Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik*, Media Nusa Creative, Malang, 2015, hlm.2

1992 sebagaimana telah diubah oleh Undang-Undang No. 10 Tahun 1998 tentang Perbankan).[4]

Adapun yang dimaksud dengan tindak pidana di bidang perbankan adalah perbuatan-perbuatan yang berhubungan dengan kegiatan dalam menjalankan usaha pokok bank, perbuatan mana dapat dipidana berdasarkan ketentuan pidana di luar Undang-Undang Perbankan atau undang-undang yang berkaitan dengan perbankan.[5]

Sebagaimana telah dikemukakan di atas, tindak pidana perbankan merupakan salah satu bentuk dari tindak pidana ekonomi, yaitu suatu tindak pidana yang mempunyai motif ekonomi dan lazimnya dilakukan oleh orang-orang yang mempunyai kemampuan intelektual dan mempunyai posisi penting di dalam masyarakat dan pekerjaannya.[6]

Menurut Sutherland menegaskan bahwa kejahatan kerah putih bisa didefinisikan secara garis besar sebagai suatu tindak kejahatan yang dilakukan oleh orang yang memiliki status terhormat dan status sosial yang tinggi dalam pekerjaannya.[7] Sedangkan tindak pidana di bidang perbankan merupakan salah satu bentuk dari tindak pidana di bidang ekonomi, yaitu tindak pidana konvensional yang mencari keuntungan dengan motif-motif ekonomi seperti: pencurian, penggelapan, perampokan penipuan, dan lain sebagainya yang dalam hal ini ditunjukkan terhadap bank.

Kejahatan pembobolan uang nasabah denga metode skimming merupakan salah satu kejahatan siber (*Cyber Crime*). Kejahatan Siber (*Cyber Crime*) adalah kejahatan yang terjadi di dunia maya (*Cyber Space*) yang menggunakan tekonologi informasi dan komunikasi sebagai alat untuk melakukan kejahatan.

Jika dulu diperkenalkan istilah *Hacker* dan *Cracker* yang menunjuk pada individu dengan kemampuan dan aktivitas khusus memasuki sistem komputer lain untuk beraneka ragam tujuan, maka saat ini sudah banyak diciptakan mesin atau sistem yang dapat bekerja sendiri Secara intelijen untuk melakukan teknik-teknik penyusupan dan perusakan sistem. Intinya adalah bahwa serangan terhadap sistem keamanan teknologi informasi organisasi telah masuk pada kategori kriminal, baik yang bersifat pidana maupun perdata. Walaupun kebanyakan jenis tindakan kriminal tersebut berkaitan erat dengan urusan finansial, tidak jarang akibat serangan tersebut, sejumlah nyawa manusia melayang, karena menimpa

---

[4]Kristian dan Yopi Gunawan, *Tindak Pidana Perbankan*, Nuansa Aulia, Bandung, 2013, hlm.14.

[5]Sudarto, *Kapita Selekta Hukum Pidana*, Alumni, Bandung,1986,hlm.59.

[6]Hermansyah, *Hukum Perbankan Nasional Indonesia*, Kencana, Jakarta, 2009, hlm. 160.

[7]J.Robert Lilly, *et.al., Teori Kriminologi Konteks dan Konsekuensi,* Kencana, Jakarta, 2015, hlm. 319.

sistem yang sangat vital bagi kehidupan manusia.[8]

Secara prinsip ada 4 (empat) jenis aktivitas yang dapat dikatagorikan sebagai kejahatan dalam dunia teknologi informasi. **Pertama** adalah penyadapan (*Interception*) yaitu tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain. Menurut hukum di Indonesia, penyadapan hanya boleh dilakukan oleh Lembaga-lembaga negara tertentu atau pihak lain yang diperbolehkan menurut Undang-undang seperti Institusi POLRI, Badan Intelejen Negara, dan Komisi Pemberantasan Korupsi. **Kedua** adalah Interupsi (*interuption*) yaitu tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua pihak yang seharusnya berinteraksi. Fenomena *Denial of Services* (DoS) atau *Distributed Denial of Services* (DDoS) merupakan salah satu serangan yang dapat mengakibatkan terjadinya kondisi interupsi pada sistem komputer. **Ketiga** adalah Modifikasi (*modification*) yaitu tindakan yang mengakibatkan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan/menerimanya. *Web Defacement* merupakan salah satu jenis serangan yang bisa dikatagorikan dalam kejahatan ini. **Keempat** adalah Fabrikasi (*fabrication*) yaitutindakan mengelabui seolah-olah terjadi suatu permintaan interaksi dari seseorang seperti yang dewasa ini dikenal dengan istilah *Pishing*.[9]

Jika dilihat dari prosesnya skimming adalah aktivitas menggandakan informasi yang terdapat dalam pita magnetik (*magnetic stripe*) yang terdapat pada kartu kredit maupun ATM/debit secara ilegal. Ini artinya, dapat disimpulkan bahwa skimming adalah aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu ATM/debit secara ilegal untuk memiliki kendali atas rekening korban.

Perbuatan skimming diatas termasuk perbuatan mengakses komputer dan atau sistem informasi milik orang lain dengan cara ilegal dengan maksud mengambil secara ilegal data-data pribadi yang terdapat dalam komputer dan atau sistem informasi tersebut. Perbuatan tersebut termasuk dalam tindak pisana informasi dan transaksi elektornik yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan atau dokumen elektronik sebagaimana diatur dalam pasal 30 ayat 2 Undang-undang Nomor 19 tahun 2016 tentang perubahan atas

[8]Eko Richardus Indrajit, *Kemanan Teknologi Informasidan Internet*, Seri Bunga Rampai Pemikiran EKOJI, Preinexus, Jakarta, hlm.13

[9]*Ibid*, hlm. 14

Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik atau dikenal dengan Undang-undang ITE.[10]

Lebih lengkap pasal 30 ayat 2 Undang-undang ITE berbunyi " 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".

Setiap perbuatan dapat dipidana jika memenuhi unsur pidana yang terdapat dalam pasal yang disangkakan, dalam pasal 30 ayat 2 Undang-undang ITE diatas dapat diketahui bahwa yang termasuk unsur-unsur pidananya yaitu : [11]

1. Unsur Kesalahan yaitu *Dengan Sengaja*
2. Unsur Melawan Hukum yaitu *Tanpa Hak atau Melawan Hukum*
3. Unsur Perbuatan yaitu *Mengakses dengan Cara Apapun*
4. Unsur Obyek yaitu *Komputer dan atau Sistem elektronik*
5. Tujuan yaitu *Dengan Tujuan Untuk Memperoleh Informasi Elektronik dan atau Dokumen Elektronik.*

Kata yang dicetak miring merupakan unsur formal yang membentuk pasal 30 ayat 2 Undang-undang ITE.

Metode skimminng adalah metode yang dilakukan pelaku kejahatan dibidang perbankan untuk mencuri data-data nasabah yang terdapat dalam kartu ATM nasabah. Modusnya dengan cara menempelkan alat skimmer pada slot untuk memasukan kartu ATM pada mesin ATM. Sedangkan ATM merupakan salah satu alat elektronik atau sistem elektronik yang digunakan dalam kegiatan perbankan.

Skimmer bukan satu-satunya alat yang digunakan oleh para pelaku skimming. Para pelaku biasanya juga memanfaatkan kamera pengintai (spy cam) untuk mengetahui gerakan jari nasabah saat memasukkan PIN kartu ATM. Namun kamera pengintai sudah jarang digunakan seiring dengan semakin canggihnya alat skimmer yang digunakan para pelaku. Laman How Stuff Works melaporkan jika kini telah beredar pula jenis skimmer yang dilengkapi dengan kemampuan membaca kode PIN kartu ATM. Dan hebatnya lagi, skimmer jenis ini juga bisa langsung mengirimkan data-data yang didapat via SMS pada pelaku. Berikut sistematis cara kerja pelaku skimming :[12]

1. Pelaku mencari target mesin ATM yang ingin dipasangai skimmer. Kriteria yang dicari adalah mesin ATM yang tidak ada penjagaan kemanan, sepi dan tidak ada pengawasan kamera CCTV.

[10]H Adami Chazawi dan Ardi Ferdian, *Op Cit*, hlm. 5

[11]*Ibid*, hlm. 142

[12]http://tekno.liputan6.com/read/2049670/*begini-cara-kerja-iskimmingi-kartu-atm*, diunduh pada selasa, 11 juni 2018 jam 11.51

2. Pelaku memulai aksi pencurian data nasabah dengan memasang alat skimmer pada mulut mesin ATM
3. Melalui alat skimmer para pelaku menduplikasi data magnetic stripe pada kartu ATM lalu mengkloningnya ke dalam kartu ATM kosong. Proses ini bisa dilakukan dengan cara manual, di mana pelaku kembali ke ATM dan mengambil chip data yang sudah disiapkan sebelumnya. Atau bila pelaku sudah menggunakan alat skimmer yang lebih canggih, data-data yang telah dikumpulkan dapat diakses dari mana pun. Umumnya data dikirimkan via SMS.

Kejahatan pembobolan uang nasabah melalui metode skimming termasuk juga kejahatan dibidang perbankan. Menurut perbuatannya skimming dapat diartikan sebagai penggandaan kartuATM. Sebagaimana telah dijelaskan sebelumnya bahwa penggandaan kartu ATM inidilakukan dengan cara memasang*skimmer* pada lubang untukmemasukkan kartu ATM dan kameratersembunyi di atas tombol kunci.Pemasangan *skimmer* bertujuan untukmerekam data elektronik kartu ATMnasabah pada pita magnetic yangterdapat di kartu ATM. Sedangkankamera tersembunyi bertujuan untukmengetahui nomor PIN masing-masingnasabah. Setelah data tersebut diketahuikemudian dibuatkan kartu yang baruhasil duplikasi dari data-data tersebutdan pelaku dapat langsung menggunakankartu ATM palsu tersebut tanpasepengetahuan nasabah.[13]

Sebelum menempatkan alat *skimming*, pelaku kejahatan mempelajari kebiasaan di tempat dan sekitar ATM. Pelaku mengharapkan bahwa alat *skimming* yang dipasang mampu merekam banyak data nasabah, maka ATM yang dipilih adalah yang banyak terjadi transaksi namun minim pengawasan atau orang disekitar cenderung sibuk sendiri dan tidak peduli. ATM yang berada di lokasi wisata sering menjadi sasaran pelaku *skimming*karena kesibukan dan ketidak pedulian orang sekitar. Di pusat-pusat pertokoan juga menjadi sasaran yang sangat menarik pelaku untuk memasang alat *skimming* karena frekuensi transaksi sering terjadi. Bahkan mesin ATM yang jadi sasaran pelaku*skimming* pun bisa berada di lokasi yang sepi.

Serangan skimming terjadi dalam waktu yang pendek, umumnya sekitar satu atau dua jam. Meskipun waktunya pendek, namun kerugian yang dapat dialami nasabah bisa ratusan juta atau bahkan milyaran rupiah bila di ATM yang dipasang alat tersebut banyak terjadi transaksi. Bagi bank yang memiliki kemampuan teknologi canggih dan

[13]Komang Judiawan, *Perlindungan Hukum Terhadap Nasabah Korban Kejahatan Penggandaan Kartu ATM Pada Bank Swasta Nasional di Denpasar*, Jurnal Magister Hukum Udayana, Tahun 2013, hlm. 4. http://ojs.unud.ac.id/index.php/jmhu/article/view/5938, diakses tanggal 11 Juni 2018 jam 10.27

pengawasan teratur pada mesin ATM, kejadian *skimming* dapat segera diidentifikasi. Bank dalam kategori ini dapat mendeteksi kejahatan skimming dalam waktu tiga hingga empat jam. Meskipun cepat terdeteksi namun kerugian bisa sangat besar.[14]

Kejahatan dengan metode skimming ini sebenarnya sudah sejak lama dilakukan oleh pelaku kejahatan dibidang perbankan, teknik pembobolan kartu ATM nasabah melalui teknik skimming pertama kali teridentifikasi pada 2009 lalu di ATM Citibank, Woodland Hills, California. Saat itu diketahui jika teknik skimming dilakukan dengan cara menggunakan alat yang ditempelkan pada slot mesin ATM (tempat memasukkan kartu ATM) dengan alat yang dikenal dengan nama skimmer. Modus operasinya adalah mengkloning data dari magnetic stripe yang terdapat pada kartu ATM milik nasabahakan tetapi seiring perkembangan teknologi informasi yang semakin canggih, metode skimmingpun semakin canggih pula, yaitu dengan memanfaatkan teknologi GSM atau WIFI sehingga pelaku dapat beroperasi dan atau mengambil data nasabah dari wilayah yang jauh dari ATM tersebut bahkan dapat dilakukan dari negara lain.

Kejahatan dibidang perbankan dengan metode skimming telah banyak merugikan sektor perbankan, yang menjadi korban bukan hanya nasabah yang kehilangan uang dalam tabungannya karena dikuras habis oleh pelaku kejahatan skimming, tetapi juga termasuk bank sendiri menjadi korban. Akibat kejahatan skimming telah membuat kepercayaan (*Trust*) nasabah terhadap bank berkurang. Hal ini tentu tidak boleh dibiarkan, harus ada solusi menyeluruh dari semua *stake holder* untuk mengatasi kejahatan ciber di dunia perbankan.

Oleh karena kejahatan skimming termasuk dalam wilayah kejahatan siber (*Cyber Crime*) dimana karakteristik kejahatan ini multi dimensi, tidak terbatas ruang dan waktu maka penanggulangannya harus dilakukan secara konprehensif dan berkelanjutan seiring dengan terus berkembangnya teknologi informasi dan komunikasi.

Untuk menanggulangi kejahatan internet dibidang perbankan yang semakin meluas maka diperlukan suatu kesadaran dari semua pemangku kepentingan (*Stake Holder*) di masing-masing negara akan bahaya penyalahgunaan internet dalam dunia perbankan. maka berikut adalah langkah ataupun cara penanggulangan secara global:[15]

[14] http://www.perbanas.ac.id/id/component/k2/item/677-*skimming*-kejahatan-lama-di-perbankan-yang-belum-terselesaikan, diakses pada hari minggu tanggal 10 juni 2018 jam 15.14

[15] Jurnalis J. Hius ST, (2014), *Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku*, Banda Aceh : Prosiding SNIKOM.

1. Modernisasi hukum pidana nasional berserta hukum acaranya diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
2. Peningkatan standar pengamanan sistem jaringan komputer nasional sesuai dengan standar internasional.
3. Meningkatkan pemahaman serta keahlian aparat hukum mengenai upaya pencegahan, inventigasi, dan penuntutan perkara-perkara yang berhubungan dengan cybercrime.
4. Meningkatkan kesadaran warga negara mengenai bahaya cybercrime dan pentingnya pencegahan kejahatan tersebut.
5. Meningkatkan kerja sama antar negara dibidang teknologi mengenai hukum pelanggaran cybercrime.

Perlindungan Hukum Terhadap Nasabah yang Dirugikan Akibat Kejahatan Skimming

Data nasabah termasuk data-data pribadi nasabah merupakan suatu dokumen dan atau informasi yang wajib dirahasiakan oleh Bank. Bank tidak boleh memberikan data-data nasabah kepada pihak ketiga kecuali hal tersebut diperjanjikan sebelumnya. Data-data perbankan nasabah seperti PIN (*Personal Indentification Number*), nomor kartu kredit dan sejenisnya harus dijaga kerahasiaan oleh bank.

Pelanggaran terhadap kerahasiaan nasabah oleh pihak bank dapat dituntut secara pidana. ATM (Anjungan Tunai Mandiri atau *Automatic Teller Machine*) merupakan salah satu teknologisistem informasi yang digunakan oleh bank. Bank Indonesia sendiri lebih seringmenggunakan istilah Teknologi Sistem Informasi (TSI) Perbankan untuk semua terapanteknologi informasi dan komunikasi dalam layanan perbankan.

ATM (Anjungan Tunai Mandiri atau *Automatic Teller Machine*) merupakan salah satu teknologi yangmenerapkan konsep Proses Data berbasis Digital. *Device* ini mempunyai dua bagian penting yaitu Hardware yang terdiri dari Unit Pemroses dalam hal ini PC, serta sistem device interface yangmenghubungkan pemakai/User melalui suatu kartumagnetik, dan Software yang berfungsi sebagai interface yang menghubungkan User dengan Sistem dalam kaitan Data (Informasi).

Dalam setiap perangkat yang menggunakan Teknologi Informasi harus menyertakan sistem keamanan agar tidak disalahgunakan oleh pihak yang bertanggung jawab. ATM sebagai salah satu peralatan (*device*) perbankan yang menggunakan teknologi informasi juga harus disertai sistem keamanan yang cukup dari tindakan melanggar hukum oleh pihak lain. Kasus penggandaan kartu ATM adalah salah satu kebocoran data yang diakibatkan oleh

lemahnya sistem keamanan ATM sebuah Bank.

Dalam hal terjadi kejahatan penggandaan kartu ATM nasabah tentu mengakibatkan timbulnya kerugian pada nasabah. Kejahatan tersebut akan berdampak pada hilangnya uang nasabah yang ada di bank tentu harus ada perlindungan hukum terhadap nasabah yang menjadi korban kejahatan skimming tersebut. Perlindungan hukum terhadap nasabah yang menjadi korban kejahatan skimming dapat dilakukan dalam konteks hukum pidana dan perdata.

Perlindungan Hukum dalam konteks Hukum Pidana

Sebagaimana telah dijelaskan diawal bahwa kejahatan skimming termasuk dalam pelanggaran terhadap pasal 30 ayat 2 Undang-undang Informasi dan Transaksi Elektronik yaitu tindak pidana dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputerdan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Sanksi terhadap pasal 30 ayat 2 Undang-undang Informasi dan Transaksi Elektronik (ITE) terdapat pada pasal 46 ayat 2 Undang-undang yang sama yang berbunyi "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidanadengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyakRp700.000.000,00 (tujuh ratus juta rupiah)".

Perbuatan Pidana (*Actus reus*) dari tindak pidana tersebut diatas adalah "mengakses". Sedangkan Niat (*Mens rea)* dari tindak pidana tersebut diatas adalah "dengan sengaja". Sedangkan Objek dari tindak pidana tersebut adalah "Komputer dan/atau Sistem Elektronik". Sedangkan Tujuan tindak pidana tersebut adalah "untuk memperoleh InformasiElektronik dan/atau Dokumen Elektronik". Artinya seseorang hanya dapat dipidana berdasarkan ketentuan Pasal 30 ayat (2) *jo* Pasal 46 ayat (2) UU ITE apabila yang diakses oleh pelaku adalah Komputer dan/atau Sistem Elektronik. Yang menjadi korban tindak pidana tersebut adalah pemilik komputer dan/atau sistem elektronik dan atau pemilik data.

Agar pelaku dapat dipidana sesuai dengan ketentuan pasal 46 ayat 2 tersebut, maka pihak nasabah sebagai korban harus melaporkan tindak pidana tersebut kepada pihak Bank kemudian melaporkannya kepada pihak kepolisian.

Penyidik berdasarkan laporan yang ada harus melakukan penyelidikan dan penyidikan terhadap kasus skimming yang terjadi dengan berbagai cara dan upaya agar pelaku segera tertangkap dan membuktikan unsur-unsur pidana sebagaimana terdapat dalam pasal 30 ayat 2 Undang-undang ITE.

Perlindungan Hukum dalam Konteks Hukum Perdata.

Pasal 1365 Kitab Undang-undang Hukum Perdata menjelaskan bahwa "Tiap perbuatan melanggar hukum, yang membawa kerugian kepada orang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut".

Dalam regulasi sektor jasa keuangan, pihak perbankan harus bertanggung jawab terhadap kerugian yang menimpa para nasabah. Hal ini dapat dilihat dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Dalam Pasal 19 ayat (1) Undang-Undang Perlindungan Konsumen menyebutkan pelaku usaha dalam hal ini perbankan bertanggung jawab memberikan ganti rugi atas kerugian konsumen akibat mengkonsumsi jasa yang dihasilkan.[16] Aturan mengenai kewajiban perbankan harus bertanggung jawab atas dana nasabah juga tercantum dalam Peraturan Bank Indonesia (PBI) Nomor 16/1/2014 tentang Perlindungan Konsumen. Dalam Pasal 10 , aturan tersebut menyebutkan "Penyelenggara wajib bertanggung jawab kepada konsumen atas kerugian yang timbul akibat kesalahan pengurus dan pegawai Penyelenggara."[17]

Peraturan Otoritas Jasa Keuangan (PJOK) juga mewajibkan perbankan mengganti kerugian yang dialami nasabah. Dalam Pasal 29 PJOK Nomor 1/PJOK.07/2013 menyebutkan "Pelaku Usaha Jasa Keuangan wajib bertanggung jawab atas kerugian Konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai Pelaku Usaha Jasa Keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan Pelaku Usaha Jasa Keuangan."[18]

Penggantian kerugian nasabah yang menjadi korban kejahatan skimming tentu harus dilakukan dengan membuktikan terlebih dahulu apakah hilangnya dana nasabah tersebut benar-benar dikarenakan kejahatan skimming atau justru karena kelalaian nasabah sendiri. Oleh karena itu pihak bank yang mendapatkan laporan hilangnya dana nasabah akan menyelidiki terlebih dahulu detail transaksi terhadap uang nasabah yang hilang tersebut.

Proses klarifikasi diawali denganmelakukan pengecekan data transaksiyang dilakukan oleh para nasabah. Daridata transaksi tersebut menunjukkan apasaja yang dilakukan oleh nasabahterhadap rekeningnya seperti penyetoran,penarikan melalui teller, penarikanmelalui ATM, transfer dana via ATMserta transaksi lainnya yangmenyebabkan berkurang atau bertambahnya saldo rekening nasabah

[16]Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

[17]Peraturan Bank Indonesia (PBI) Nomor 16/1/2014 tentang Perlindungan Konsumen.

[18]Peraturan Otoritas Jasa Keuangan (PJOK) Nomor 1/PJOK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.

tersebut. Khusus terhadap nasabah yang mengadukan saldo rekeningnya berkurang tanpa melakukan transaksi,akan diperiksa transaksi penarikan atautransfer yang pernah dilakukan olehnasabah. Rekaman transaksi tersebutakan diklarifikasi kepada nasabah yangbersangkutan untuk mengetahuitransaksi yang mana saja yang dianggaptidak pernah dilakukan oleh nasabah danyang mana saja yang diakui olehnasabah.Dari beberapa transaksi yang tidakdiakui oleh nasabah tersebut kemudiandilakukan pengecekan detail transaksi.Apabila transaksi dilakukan melaluiATM, akan dilakukan pengecekan padarekaman CCTV pada mesin ATMtersebut. Dari rekaman tersebut dapat diketahui siapa yang melakukantransaksi di mesin ATM menggunakankartu ATM nasabah.

Jika berdasarkan proses klarifikasi transaksi dinyatakan bahwa hilangnya uang nasabah diakibatkan karena kejahatan skimming maka pihak bank akan mengganti uang nasabah sejumlah uang yang dinyatakan hilang dari rekening. Sebaliknya jika berdasarkan hasil klarifikasi transaksi, hilangnya uang nasabah diakibatkan karen kelalaian nasabah, maka pihak bank tidak akan mengganti uang nasabah tersebut.

Selain bertanggung jawab terhadap kerugian yang menimpa nasabah, upaya yang paling tepat saat ini adalah meningkatkan manajemen risiko operasional perbankan untuk mencegah tindak kejahatan skimming. Hal tersebut dilakukan agar dampak dari pencurian dana tersebut tidak semakin membesar.[19] Pihak perbankan juga harus melakukan pengawasan secara rutin di setiap mesin-mesin ATM (anjungan tunai mandiri). Dalam hal ini OJK (Otoritas Jasa Keuangan) yang bertugas mengawasi bank-bank secara rutin juga berkoordinasi bersama dengan Bank Indonesia (BI) untuk mengantisipasi permasalahan *skimming* ini.

Selain itu bank juga harus meningkatkan pengamanan di masing-masingmesin ATM yang menjaditanggung jawab bank, antara lainpemasangan tutup pelindung *keypad* atautombol angka pada mesin ATM agartidak terlihat kode angka yang ditekannasabah pada saat memasukkan kodePIN, pemasangan alat anti *skimmer* padalubang pembaca kartu ATM, mengoptimalkan operasional CCTV diseluruh mesin ATM, memasang /menempel himbauan kepada nasabahuntuk berhati-hati dalam kegiatantransaksi di mesin ATM, melaksanakanpengecekan secara berkala terhadapkondisi mesin dan ruang ATM danImplementasi teknologi *chip* sebagai pengganti pita magnetik (*magneticstripe*) pada kartu ATM beserta saranapemrosesnya.

[19] http://m.hukumonline.com/berita/baca/lt5ab0dcf7a8cc6/*cegah-kasus-skimming--ojk-minta-perbankan-tingkatkan-manajemen-resiko-*, diakses pada hari senin tanggal 11 Juni 2018 jam 05.05

PENUTUP

Kejahatan pembobolan uang nasabah dengan metode skimming merupakan salah satu kejahatan siber (*Cyber Crime*). Kejahatan Siber (*Cyber Crime*) adalah kejahatan yang terjadi di dunia maya (*Cyber Space*) yang menggunakan tekonologi informasi dan komunikasi sebagai alat untuk melakukan kejahatan. Perbuatan tersebut termasuk dalam tindak pidana informasi dan transaksi elektronik yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan atau dokumen elektronik sebagaimana diatur dalam pasal 30 ayat 2 Undang-undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik atau dikenal dengan Undang-undang ITE.

Perlindungan terhadap nasabah korban kejahatan skimming dapat dilakukan dalam konteks penegakan hukum pidana dan penegakan hukum perdata.

DAFTAR PUSTAKA

Buku-buku

Abdulkadir Muhammad, (2004), *Lembaga Keuangan dan Pembiayaan*, Bandung : Citra Aditya Bhakti.

Eko Richardus Indrajit, *Kemanan Teknologi Informasidan Internet*, Seri Bunga Rampai Pemikiran EKOJI, Jakarta : Preinexus.

H Adami Chazawi dan Ardi Ferdian, (2015), *Tindak Pidana Informasi & Transaksi Elektronik,* Malang : Media Nusa Creative.

Hermansyah, (2009), *Hukum Perbankan Nasional Indonesia*, Jakarta :Kencana

J.Robert Lilly, *et.al.*,(2015), *Teori Kriminologi Konteks dan Konsekuensi,* Jakarta : Kencana.

Jurnalis J. Hius ST, (2014), *Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku,* Banda Aceh : Prosiding SNIKOM.

Kristian dan Yopi Gunawan, (2013), *Tindak Pidana Perbankan*, Bandung :Nuansa Aulia.

Komang Judiawan, (2013), *Perlindungan Hukum Terhadap Nasabah Korban Kejahatan Penggandaan Kartu ATM Pada Bank Swasta Nasional di Denpasar*, Jurnal Magister Hukum Udayana.

Mahesa Jati Kusuma, (2012), *Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE di BidangPerbankan,* Bandung : Nusa Media.

Rachmadi Usman, (2001), *Aspek-aspek Hukum Perbankan di Indonesia*, Jakarta : PT Gramedia Pustaka Utama.

Sudarto, (1986), *Kapita Selekta Hukum Pidana*, Bandung :Alumni.

Tim Perundang-Undangan dan Pengkajian Hukum Direktorat Hukum Bank Indonesia, (2006), "*Urgensi Cyberlaw di Indonesia Dalam Rangka Penanganan Cybercrime di Sektor Perbankan*", dalam Buletin Hukum

Perbankan dan Kebanksentralan, Volume 4 No. 2, Jakarta : Bank Indonesia.

Perundang-undangan

Kitab Undang-undang Hukum Perdata (KUHPerdata) Pasal 1365

Undang-Undang Nomor 10 Tahun 1998Tentang Perubahan atas Undang-undang Nomor 7 Tahun 1992 tentang Perbankan

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Peraturan Otoritas Jasa Keuangan (PJOK) Nomor 1/PJOK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Peraturan Bank Indonesia (PBI) Nomor 16/1/2014 tentang Perlindungan Konsumen.

Artikel & Website

http://m.hukumonline.com/berita/baca/lt5ab0dcf7a8cc6/*cegah-kasus-skimming--ojk-minta-perbankan-tingkatkan-manajemen-resiko-*, diakses pada hari senin tanggal 11 Juni 2018 jam 05.05.

http://ojs.unud.ac.id/index.php/jmhu/article/view/5938, diakses tanggal 11 Juni 2018 jam 10.27.

http://www.perbanas.ac.id/id/component/k2/item/677-*skimming-kejahatan-lama-di-perbankan-yang-belum-terselesaikan*, diakses pada hari minggu tanggal 10 juni 2018 jam 15.14.

http://tekno.liputan6.com/read/204967/*begini-cara-kerja-iskimmingi-kartu-atm*, diunduh pada selasa, 11 juni 2018 jam 11.51.