UPAYA BANK DALAM MEMBERIKAN PERLINDUNGAN HUKUM TERHADAP NASABAH AKIBAT SKIMMING KARTU ANJUNGAN TUNAI MANDIRI

(STUDI BANK RAKYAT INDONESIA UNISMA)

Novitasari Gogani [1], Isdiyana Kusuma Ayu [2], M Faisol [3]

Fakultas Hukum Universitas Islam Malang
Jalan Mayjen Haryono No 193 Malang 65144, Telepon (0341) 551932, Fax (0341) 552249
Email : aryafirm24@gmail.com

ABSTRACT

The development of technology is such that in its development also creates a gap for perpetrators of crime in using more sophisticated methods of crime. The development of information technology has led to evolution leading to digital banking services. This technology development not only provides convenience for customers but also coupled with negative aspects, namely creating a new mode in the case of theft of customer funds using the skimming method. Legal arrangements for crime of skimming, namely: based on the Criminal Code, skimming criminals are charged with Article 363 of the Criminal Code. Based on the ITE Law, skimming criminals are charged with Article 30 paragraph 1, paragraph 2 and paragraph 3 of the ITE Law, article 32 of the ITE Law.

Keywords: Cyber crime, skimming, banking

ABSTRAK

Perkembangan teknologi berjalan sedemikian rupa sehingga dalam perkembangannya juga menimbulkan celah bagi pelaku kejahatan dalam menggunakan metode kejahatan yang lebih canggih juga. Perkembangan teknologi informasi menimbulkan evolusi yang mengarah kepada layanan perbankan digital . Perkembaangan teknologi ini tidak hanya memberikan kemudahan bagi nasabah tapi juga dibarengi dengan aspek negatif yaitu menimbulkan modus baru dalam kasus pencurian dana nasabah dengan metode *skimming*. Pengaturan hukum kejahatan *skimming*, yaitu : berdasarkan KUHP pelaku kejahatan *skimming* dijerat dengan Pasal 363 KUHP. Berdasarkan UU ITE pelaku kejahatan *skimming* dijerat dengan pasal 30 ayat 1, ayat 2 dan ayat 3 UU ITE, pasal 32 UU ITE.

Kata Kunci : **Cyber crime, skimming, perbankan**

DINAMIKA
ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 28 Nomor 10 Bulan Januari Tahun 2022 , 4669 - 4685

PENDAHULUAN

Era digitalisasi seperti sekarang sering terjadi kejahatan di dunia perbankan. Mayoritas kejahatan dilakukan pada kalangan usia lanjut dan orang yang gagap akan teknologi. Kejahatan adalah perbuatan atau tingkah laku yang selain merugikan si korban, juga sangat merugikan masyarakat yaitu berupa hilangnya keseimbangan, ketentraman dan ketertiban. Sedangkan pengertian perbankan adalah industri yang menangani uang tunai, kredit, dan transaksi keuangan lainnya. Bank menyediakan tempat yang aman untuk menyimpan uang tunai dan kredit ekstra, bank yang menawarkan rekening tabungan, sertifikat setoran, serta rekening giro. Jenis kejahatan pada umumnya sangat banyak terjadi di dunia perbankan itu sendiri, seperti, *phising, Spam*, *Fraud* penyalahgunaan transaksi yang sah, *cyberattack* pembocoran data nasabah, ataupun serangan kepada sistem bank dan *skimming* atau *card skimming*.[1]

Semua kejahatan perbankan sudah diatur di undang-undang ITE, Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mulai berlaku pada tanggal 21 April 2008, pada intinya mengatur mengenai keabsahan informasi / dokumen elektronik sebagai alat bukti aktivitas yang menggunakan sistem elektronik. Keberadaan UU ini sebenarnya dapat meningkatkan keamanan dan kenyamanan nasabah[2] saat melakukan kegiatan perbankan melalui sistem elektronik yang disediakan bank. Ada beberapa alasannya, Pertama, UU ITE menegaskan bahwa bank, sebagai pihak yang menyelenggarakan sistem elektronik dalam memfasilitasi pelayanan jasa bank via Internet (*e-banking*), bertanggung jawab secara hukum terhadap kerugian yang dialami nasabah berkaitan dengan pemanfaatan layanan yang disediakannya.

[1] Lex Privatum Tentang PERLINDUNGAN HUKUM TERHADAP NASABAH BANK PENGGUNA INTERNET BANKING DARI ANCAMAN *CYBERCRIME* Vol.III/No. 1/hal 149

[2] Fitria Dewi Navisa, 2013, Analisis Perjanjian Kredit Berdasar Prinsip Kehati-Hatian Yang Berwawasan Lingkungan, Universitas Brawijaya

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 28 Nomor 10 Bulan Januari Tahun 2022 , 4669 - 4685

Namun, jika kerugian disebabkan oleh force majeur atau kesalahan dan kelalaian nasabah, maka bank tidak dapat dimintai pertanggung jawaban. Kedua, UU ITE mengharuskan bank untuk menyelenggarakan sistem elektronik yang andal dan aman, serta bertanggung jawab terhadap operasional sistem elektroniknya. Bank juga wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagaimana diatur dalam UU ITE. Ketiga, dalam UU ITE, ada pengakuan terhadap kontrak elektronik, yaitu perjanjian yang dibuat melalui sistem elektronik.[3]

Kejahatan-kejahatan seperti ini disebut sebagai kejahatan mayantara (*cybercrime*) yang merupakan suatu aspek negatif yang melekat pada perkembangan teknologi. Perkembangan teknologi yang sedemikian pesatnya seperti komputer, telekomunikasi, dan informasi yang didukung oleh jaringan yang sangat luas berupa internet dan juga memiliki kecepatan yang terus berkembang memudahkan manusia dalam melaksanakan kehidupan, yang di mana manusia antar benua bahkan belahan dunia dapat berkomunikasi hanya menggunakan alat telekomunikasi berupa komputer dan juga telepon genggam tanpa bertatap muka secara langsung, serta berbagai macam informasi dapat mudah disajikan dengan kecanggihanya dan sangat mudah diperoleh. Hal ini lah yang memberi isyarat bahwa era *cyber* dalam dunia bisnis dimulai.[4]

Cybercrime atau *cyberspace* sendiri merupakan kejahatan yang dilakukan menggunakan jaringan sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual menggunakan jaringan internet dan menjadikan pengguna internet lainya sebagai korban atau sasarannya. Beberapa bentuk kejahatan *cyber* adalah seperti memanipulasi data, *spionase*, *hacking*, penipuan kartu kredit orang (*carding*), merusak sistem (*cracking*), penyalinan data dari kartu ATM (*skimming* ATM), dan berbagai

[3] Ibid
[4] Budi Suhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime)- Urgensi Pengaturan dan Celah Hukumnya, Rajagrafindo Persada, Depok, 2012, hal 2

macam kejahatan lainya. Kejahatan ini merupakan kejahatan yang sulit dibasmi mengingat para pelaku adalah para ahli di bidangnya.[5]

Terdapat perbedaan antara *cybercrime* dan kejahatan yang berhubungan dengan dunia virtual, ada banyak kejahatan seperti *pedophilia*, *stalking*, dan *pornografi* bisa disebarkan dengan atau tidak menggunakan *cybertecnology*, jadi tindakan-tindakan tersebut tidak dapat disebut sebagai *cybercrime* walau menggunakan komputer.[6]

Skimming sendiri merupakan modus kejahatan yang berupa penggandaa data kartu ATM (Anjungan Tunai Mandiri) nasabah yang menggunkan alat yang ditempatkan pada *card reader*, dengan cara menempatkan alat yang dibentuk sedemikian rupa menyerupai sebuah *card reader*. Kemudian menggunakan modus ini ketika nasabah memasukkan kartu ATM ke mesin secara otomatis alat tersebut dapat menggandakan data dan menyalin pin nasabah, kemudian pelaku menggunakan kartu palsu yang sudah disiapkan untuk mengambil uang nasabah dengan cepat, pada umumnya para nasabah tidak menyadari bahwa mereka telah menjadi korban *skimming*.[7]

PEMBAHASAN

A. Modus Operandi Tindak Pidana Skimming Terhadap Nasabah BRI

Modus Operandi berasal dari bahasa latin yang memiliki arti prosedur atau cara untuk bergerak tau cara untuk melakukan sesuatu. Sesorang dapat disebut sebagai penjahat atau pelaku suatu tindak pidana apabila seseorang telah melakukan sesuatu tindak perbuatan yang di mana perbuatan tersebut dapat dijatuhi hukaman atau telah melanggar atau melakukan sesuatu perbuatan yang telah diatur dalam suatu aturan yang berlaku. Modus Operandi merupakan bentuk suatu operasi dari perorangan maupun

[5] Budi Suhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime):Urgensi Pengaturan dan Celah Hukumnya, hal17

[6] Dista Amalia Arifah, Kasus Cybercrime di Indonesia,Volume 18 No. 2 hal 188

[7] Jovin Ganda Ramdhan dan Sumiyati, Perlindungan Hukum Terhadap Nasabah Korban Skimming Ditinjau Dari Undang Undang Nomor 8 Tahun 1999, Volume 12. No. 1 hal 89

kelompok yang melakukan suatu tindak kejahatan. Pengertian modus operandi sendiri dalam lingkup kejahatan adalah suatu operasi, cara, atau teknik khusus yang dimiliki oleh perorangan atau kelompok dalam melakukan suatu tindak kejahatan.[8]

PT Bank Rakyat Indonesia Tbk (BRI) terus berupaya memerangi kejahatan *skimming* dengan mengembangkan sistem dan berbagai fitur keamanan serta terus berkoordinasi dengan pihak berwajib untuk menangkap sindikat kejahatan perbankan yang merugikan perbankan nasional. Kejahatan *skimming* ini tak hanya merugikan nasabah, tapi juga merugikan pihak bank. BRI juga terus melakukan respon dan investigasi cepat terhadap pengaduan nasabah yang menjadi korban kejahatan perbankan, salah satunya adalah *skimming*.

Corporate Secretary BRI Aestika Oryza Gunarto mengatakan BRI menjamin keamanan simpanan seluruh nasabah. Perusahaan juga akan bertanggung jawab atas seluruh kerugian nasabah yang terbukti menjadi korban kejahatan *skimming*. "Terhadap seluruh aduan yang masuk, BRI melakukan proses investigasi terlebih dahulu sesuai dengan SOP (Standar Operasional Prosedur). Namun demikian, sebagian nasabah yang sudah selesai proses investigasi akan diganti rugi. BRI menjamin simpanan nasabah tetap aman, dan masyarakat tak perlu khawatir dananya hilang. Apabila terbukti merupakan korban tindak kejahatan *skimming*, BRI bertanggung jawab untuk segera menyelesaikan hal tersebut.[9]

Seiring berkembangnya teknologi informasi menimbulkan evolusi yang merubah strategis berbisnis bank mengarah kepada perbankan digital(digital banking). Layanan ini bertujuan untuk meningkatkan efisiensi atas kegiatan operasional perbankan dan mutu untuk lebih mengetahui dan memahami pelayanan bank terhadap

[8] Alfitra, Modus Operandi Pidana Khusus di Luar KUHP, (Jakarta: RAS, 2014), hal 28
[9] Aestika mengutip akan di kembalikan dana BRI keterangan tertulisnya di Jakarta, Rabu (7/4/2021)

nasabah. Yang dimaksud dengan layanan perbankan digital adalah kegiatan perbankan yang dilakukan menggunakan sarana elektronik yang dilakukan secara mandiri. Layanan perbankan yang berbasis teknologi informasi ini dikenal sebagai electronic banking (e-banking).[10]

Nasabah yang menggunakan produk bank, dalam hal ini adalah menggunakan jasa sistem pembayaran untuk transaksi keuangan, dikenal sebagai konsumen sebagaimana tertuang dalam Pasal 1 ayat (3) Peraturan Bank Indonesia Nomor 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran (selanjutnya disebut sebagai PBI No.16/1/PBI/2014) yang menentukan:

"*Konsumen Jasa Sistem Pembayaran yang selanjutnya disebut Konsumen adalah setiap pihak individu yang memanfaatkan jasa Sistem Pembayaran dari Penyelenggara untuk kepentingan diri sendiri dan tidak untuk diperdagangkan*". Dalam hal ini, bank menawarkan produk–produk kepada nasabah sehingga konsumen dapat menghimpun dana melalui jasa sistem pembayaran bank.[11]

Di Indonesia semakin marak kejahatan *skimming* dan menurut laporan Edmiraldo Siregar dalam tulisannya "*Indonesia Jadi Target Kejahatan Skimming"*, selama enam tahun berturut-turut sejak tahun 2011, kasus *skimming* di Indonesia terus meningkat dan pada tahun 2015, terjadi 1.549 kasus *skimming* atau dengan kata lain, ⅓ kasus *skimming* di dunia terjadi di Indonesia. Posisi ini menempatkan Indonesia sebagai negara yang dominan menyumbang kasus *skimming*. Dari segi hukum perbankan Indonesia, kejahatan *skimming* merupakan salah satu tindak pidana yang ada hubungannya dengan kegiatan perbankan. Berdasarkan ketentuan pasal-pasal UU Perbankan di atas dikaitkan dengan kasus pembobolan ATM melalui modus operandi

[10] Jurnal magister hukum , tanggung jawab kejahatan perbankan melalui modus operandi skimming Volume7|Nomor 1| Maret 2020 hal 36
[11] Ibid

skimming, menarik bagi saya untuk membahas "Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi *Skimming"*[12]

Tindak pidana perbankan melibatkan dana simpanan nasabah di bank sehingga perbuatan tersebut merugikan kepentingan berbagai pihak, diantaranya adalah bank selaku badan usaha, nasabah, sistem perbankan, otoritas perbankan, pemerintah serta masyarakat luas.Kejahatan di dunia ATM semakin marak dari waktu ke waktu, sehingga tidak ada lagi rasa aman atau jaminan untuk nasabah sebagai penghimpun dana di bank. ATM begitu mudah di bobol dan kartu ATM dengan mudah dipalsukan dengan berbagai macam cara, diantaranya adalah dengan modus operandi *skimming*. UU Perbankan sendiri mengatur tentang ketentuan pidana dan sanksi administratif yang diatur dalam Pasal 46 sampai dengan Pasal 50A UU Perbankan, namun tindak pidana tersebut umumnya menyangkut pihak internal bank sendiri. Terkurasnya dana simpanan nasabah akibat kejahatan *skimming* menunjukan bahwa nasabah bank tidak mendapatkan perlindungan hukum secara penuh. Bank menggunakan uang nasabah, yang dalam hal ini menghimpun dana sebanyak-banyaknya dalam bentuk simpanan lalu mengelola dana tersebut untuk disalurkan kembali ke kreditur atau nasabah lainnya dalam bentuk pinjaman atau kredit. Nasabah dalam konteks UU Perbankan dapat dibagi menjadi dua, yakni nasabah penyimpan dan nasabah debitur. Berdasarkan Pasal 1 ayat 17 UU Perbankan, "Nasabah penyimpan adalah nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan". Sementara menurut Pasal 1 ayat (18) UU Perbankan, "Nasabah debitur adalah nasabah yang memperoleh fasilitas kredit atau pembiayaan berdasarkan prinsip syariah atau yang dipersamakan dengan itu berdasarkan perjanjian bank dengan nasabah yang bersangkutan".[13]

ATM adalah sarana transaksi perbankan yang ada di bawah pengawasan bank

[12] Jurnal Arnazio Aulia Lesmana Magister Hukum Argumentum Volum 7 Nomor 1 , Maret 2020

[13] Jurnal Dian Eka Safitri Magister Hukum Argumentum Volum 7 Nomor 1 , Maret 2020 hal 41

sehingga bank bertanggung jawab atas segala akibat yang disebabkan oleh ATM sesuai ketentuan Pasal 1367 BW. *Skimming* adalah perbuatan pencurian data kartu ATM nasabah dengan cara menyalin informasi pada *strip magnetic* secara ilegal. Akibat perbuatan *skimming* adalah uang nasabah yang dipercayakan dalam bank dapat diambil secara melawan hukum. Dikatakan melawan hukum karena tanpa sepengetahuan dan persetujuan dari nasabah atau pemilik uang yang dipercayakan dalam bank. *Skimming* yang berakibat hilangnya atau berkurangnya uang nasabah di bank jelas merupakan tanggung jawab bank karena alat yang digunakan, yang dalam hal ini adalah mesin ATM, adalah sarana di bawah pengawasan dan kepemilikan bank. Pertanggungjawaban bank terhadap hilangnya dana simpanan nasabah ditinjau dari regulasi yang diterapkan oleh regulator jasa keuangan, yaitu pihak bank harus bertanggung jawab atas hilangnya dana simpanan nasabah dan kerugian yang menimpa nasabah. Hal ini tertuang dalam Pasal 19 ayat (1) UU Perlindungan Konsumen, yakni "Pelaku usaha bertanggung jawab memberikan ganti rugi atas kerusakan, pencemaran, dan/atau kerugian konsumen akibat mengkonsumsi barang dan/atau jasa yang dihasilkan atau diperdagangkan".

Tanggung jawab bank atas hilangnya dana simpanan nasabah juga tertuang dalam Pasal 10 PBI No. 16/1/PBI/2014 yakni *"*Penyelenggara wajib bertanggung jawab kepada Konsumen atas kerugian yang timbul akibat kesalahan pengurus dan pegawai Penyelenggara."Dipertegas dalam Pasal 29 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan (selanjutnya disebut sebagai POJK No.1/POJK.07/2013), bahwa *"*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". Kecuali pelaku *skimming* ditemukan, yang dalam hal ini nasabah tetap meminta pertanggungjawaban atau pengembalian kerugian di bank karena berawalan dari

perikatan nasabah dan bank yang mempercayakan uangnya untuk dikelola bank, baru pihak bank akan menindaklanjuti dengan pelaku *skimming* yang tertangkap.[14]

B. Upaya Perlindungan Hukum Bank BRI Terhadap Nasabah

Unsur dengan sengaja tampak dari sikap batin pelaku yang berniat untuk mencuri dana nasabah secara ilegal. Unsur tanpa hak atau melawan hukum tampak dari perbuatan sengaja pelaku *skimming* yang melanggar peraturan perundang-undangan atau tidak berdasarkan hukum. Unsur komputer atau sistem elektronik berkaitan dengan perangkat teknologi informasi dan komunikasi yang dipergunakan dalam kejahatan skimming, yaitu mengakses komputer atau sistem elektronik secara melawan hukum untuk mendapatkan data-data nasabah. Uraian dan analisa dalam isu hukum ini menunjukkan bahwa bank sebagai penyedia fasilitas ATM bertanggung jawab atas kerugian yang disebabkan oleh mesin ATM, yang dalam hal ini adalah hilangnya dana simpanan nasabah akibat *skimming,* yang berupa pengembalian uang ke nasabah. Di samping itu, kejahatan *skimming* merupakan tindak pidana di bidang perbankan yang disamping melanggar ketentuan UU Perbankan,[15] merupakan pelanggaran terhadap KUHP dan UU ITE. Apabila pelaku *skimming* tertangkap, pelaku dijerat pasal berlapis yakni Pasal 362 jo. Pasal 263 KUHP dan/ atau Pasal 30 ayat (3) jo, Pasal 46 ayat (3) UU ITE.[16]

Sifat melawan hukum yang tertuju kepada sikap batin terdakwa merupakan unsur melawan hukum yang subyektif. Niat pelaku *skimming* untuk memperoleh dan menguasai dana simpanan nasabah secara melawan hukum telah memenuhi unsur subyektif yang mensyaratkan adanya unsur "*mens rea"* untuk dapat dipidananya suatu perbuatan. Sementara perbuatan pelaku *skimming* yang mencuri dana simpanan

[14] Pasal 29 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan

[15] Fitria Dewi Navisa, Penerapan Actio Paulina Sebagai Perlindungan Hukum Kreditur Dalam Kepailitan, ADIL Indonesia Journal (Vol 2, No 1 (2020))

[16] Ibid

nasabah bank yang seharusnya bukan miliknya telah memenuhi unsur objektif, yang dalam hal ini adalah perbuatan pidana atau *actus rea.*[17]

Skimming merupakan kegiatan menggandakan informasi yang terdapat dalam pita magnetik (*magnetic stripe*) yang terdapat pada kartu kredit maupun ATM/debit secara illegal. Artinya dapat disimpukan bahwa *skimmin*g merupakan suatu kejahatan yang dilakukan untuk menggandakan data yang terdapat pada pita magnetik yang ada pada kartu kredit maupun ATM/debit untuk memiliki kendali atas kartu tersebut atau rekening tersebut. [18] Di Indonesia sendiri kasus kejahatan *skimming* mengalami peningkatan yang sangat signifikan, seperti yang terjadi di Kediri dimana PT Bank Rakyat Indonesia (BRI) Tbk mengalami kerugian sebanyak Rp.145.000.000,00 akibat dari kejahatan skimming.[19]

Corporate Secretary BRI Aestika Oryza Gunarto mengatakan BRI menjamin keamanan simpanan seluruh nasabah. Perusahaan juga akan bertanggung jawab atas seluruh kerugian nasabah yang terbukti menjadi korban kejahatan *skimming*. "Terhadap seluruh aduan yang masuk, BRI melakukan proses investigasi terlebih dahulu sesuai dengan SOP (Standar Operasional Prosedur). Namun demikian, sebagian nasabah yang sudah selesai proses investigasi akan diganti rugi. BRI menjamin simpanan nasabah tetap aman, dan masyarakat tak perlu khawatir dananya hilang. Apabila terbukti merupakan korban tindak kejahatan *skimming*, BRI bertanggung jawab untuk segera menyelesaikan hal tersebut.[20]

---

[17] Ibid

[18] Dian Alan Setiawan, Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybrcrime), Volume 16. No. 2 (Jakarta: 2018, Edisi Oktober), h. 181

[19] Kontan.co.id, "Kerugian Bank BRI Akibat Skimming Sekitar Rp 145 juta", Diakses dari https://keuangan.kontan.co.id/news/kerugian-bri-akibat-skimming-sekitar-rp-1-miliar, Pada Tanggal 31 Mei 2022 Pukul 11.45

[20] Aestika mengutip akan di kembalikan dana BRI keterangan tertulisnya di Jakarta, Rabu (7/4/2021)

Nasabah yang menggunakan produk bank, dalam hal ini adalah menggunakan jasa sistem pembayaran untuk transaksi keuangan, dikenal sebagai konsumen sebagaimana tertuang dalam Pasal 1 ayat (3) Peraturan Bank Indonesia Nomor 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran (selanjutnya disebut sebagai PBI No.16/1/PBI/2014) yang menentukan:[21]

"*Konsumen Jasa Sistem Pembayaran yang selanjutnya disebut Konsumen adalah setiap pihak individu yang memanfaatkan jasa Sistem Pembayaran dari Penyelenggara untuk kepentingan diri sendiri dan tidak untuk diperdagangkan*". Dalam hal ini, bank menawarkan produk – produk kepada nasabah sehingga konsumen dapat menghimpun dana melalui jasa sistem pembayaran bank.[22]

Adapun salah satu layanan perbankan melalui e -banking adalah penggunaan fasilitas ATM (*Automatic Teller Machine*) atau Anjungan Tunai Mandiri. Definisi ATM menurut OJK merupakan "suatu terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah melakukan transaksi keuangan secara mandiri tanpa bantuan dari teller ataupun petugas bank lainnya" Sementara menurut Suheimi, kartu ATM adalah " kartu plastik yang dapat digunakan oleh pemegangnya untuk membeli barang – barang dan jasa secara tunai maupun kredit dan bisa berguna sebagai penarikan uang secara tunai. Sedangkan ATM (*Automated Teller Machine*) adalah mesin/komputer yang digunakan oleh bank untuk melayani transaksi keuangan seperti penyetoran uang, pengambilan uang tunai, pengecekan saldo, transfer uang dari satu rekening kerekening lainnya, serta transaksi keuangan sejenis lainya secara elektronik". Jenis – jenis ATM dapat dibagi menjadi tiga,yaitu:

1. Mesin ATM yang hanya melayani transaksi non tunai.
2. Mesin ATM yang melayani transaksi penyetoran uang tunai *Cash Deposit Machine* atau CDM.

[21] Fitria Dewi Navisa, 2020, Prinsip Kehati-Hatian Notaris Membuat Akta Dan Akibat Notaris Terindikasi Tindak Pidana Dalam Okta Otentik, Proceeding dalam Konferensi Nasional Hukum Birokrasi Untuk Indonesia Tangguh,Hlm 191-206

[22] Jurnal magister hukum , tanggung jawab kejahatan perbankan melalui modus operandi skimming Volume7|Nomor 1| Maret 2020 hal 36

3. Mesin ATM yang dapat melayani semua transaksi yang telah disebutkan diatas.[23]

Berdasarkan Pasal 1 angka (1) UU ITE yang termasuk ke dalam informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sementara itu menurut Pasal 1 angka (4) disebutkan yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Di dalam Pasal 5 juga dikuatkan eksistensi dari alat bukti elektronik ini sebagai alat bukti yang sah, yakni sebagai berikut :

1. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di indonesia.
3. Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

Pengakuan alat bukti elektronik selain diatur dalam UU ITE juga telah datang sebelumnya melalui UU No. 8 Tahun 1997 tentang Dokumen Perusahaan, di dalam

[23] Jurnal magister hukum , tanggung jawab kejahatan perbankan melalui modus operandi skimming Volume7|Nomor 1| Maret 2020 Hal 37

Pasal 15 ayat (1) menyebutkan bahwa dokumen perusahaan yang telah dimuat dalam mikrofilm2 atau media lainnya sebagaimana dimaksud dalam Pasal 12 ayat (1) dan atau hasil cetaknya merupakan alat bukti yang sah.[24]

Ekstensifikasi alat bukti konvensional sebagaimana yang terdapat dalam Pasal 184 ayat (1) KUHAP mengintroduksi alat bukti baru yang bersifat progresif dan responsif terhadap perkembangan jaman, akan tetapi di dalam penerapannya sebagai alat bukti, data elektronik atau alat bukti elektronik ini memiliki beberapa permasalahan, yaitu seperti :

1) Permasalahan mengenai locus delicti (tempat kejadian tindak pidana), dalam tindak pidana siber penyidik dapat menemukan kesulitan dalam menentukan lokasi atau tempat yang akurat terjadinya tindak pidana. Karena pelaku dapat merubah atau menghapus "jejak digital" perangkat yang dipergunakannya untuk melakukan tidak pidana siber maupun mensetting lokasi yang berbeda dengan lokasi yang sebenarnya.

2) Permasalahan mengenai tempus delicti (waktu kejadian tindak pidana), penyidik tidak bisa menentukan kapan terjadinya tindak pidana secara tepat, karena para pelaku tindak pidana siber biasanya juga memiliki kemampuan untuk dapat mengacaukan waktu dan tanggal perbuatannya dilakukan.

3) Permasalahan barang bukti juga menjadi promblematik tersendiri bagi aparat penegak hukum. Barang bukti yang dicari adalah terkait dengan segala sesuatu yang dipergunakan untuk mempersiapkan, melakukan dan hasil tindak pidana siber sangat sulit untuk melacaknya karena karena dibalik kecangihan sistem jaringannya internet juga memiliki celah bagi orang-orang yang memiliki keahlian untuk menghapus atau memalsukan identitasnya di dunia maya. Di sisi lain, teknologi informasi adalah teknologi dengan sistem yang terbuka yang tidak

[24] Journal of Moral and Civic Education, 1 (1) 2017 ISSN: 2549-8851 (online)| 59

mustahil untuk dapat dibajak atau dikloning secara ilegal, dimana setiap orang yang memiliki keahlian di bidang tersebut dapat memanipulasi data, mengubah data, seperti menjadikan data palsu (fake data) menjadi data yang asli. Sementara itu Asril Sitompul menyampaikan siapa dan bagaimana bentuk kesaksian yang dapat diajukan untuk peristiwa hukum yang terjadi di media internet. Dapatkah pegawai internet atau karyawannya (web-designer, programmer, data entier dan pegawai lainnya) diajukan sebagai saksi bahwa di media yang dikelolanya telah terjadi pelanggaran hukum, misalnya tentang pencemaran nama baik, penghinaan, atau tindak pidana penipuan, pornografi atau yang lainnya.

4) Tindak pidana siber ini memiliki karakteristik dilakukan oleh satu orang dalam ruangan tertutup, sehingga untuk beberapa bentuk tindak pidana siber biasa penyidik sulit untuk mendapatkan saksi yang menyaksikan langsung pelaku saat sedang melakukan tindak pidana siber, sehingga saksi yang dimiliki terbatas pada saksi korban. Dalam hal tindak pidana siber terkait dengan perbankan, bisa saja pihak perbankan cenderung menutupi telah terjadinya serangan tindak pidana siber terhadap mereka, karena hal ini menjadi aib yang dapat menghilangkan kepercayaan masyarakat secara umum dan nasabah penyimpan dana di bank tersebut.

5) Yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara komunikasi multimedia bersifat internasional, multi yurisdiksi, dan tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia sebagai salah satu pemanfaatan teknologi informasi. Dengan demikian terkait kewenangan hukum (*yurisdiksi*) dalam penindakannya juga dapat menumbulkan permasalahan yang serius, hal ini disebabkan karena internet tidak mengenal batas wilayah. Sehingga mungkin saja terjadi tarik menarik kewenangan oleh beberapa negara yang merasa dirugikan oleh tindak pidana *cyber* dalam penegakan hukumnya.

6) Terbatasnya kemampuan penegak hukum dalam hal ini penyidik Polri dalam menangani tindak pidana siber ini, keterbatasnya baik dalam hal sumber daya manusianya maupun dalam hal peralatan-peralatannya. Unit kejahatan siber di kepolisian pun baru terbentuk secara khusus di Reskrim Polri di bawah Direktorat Tindak Pidana Siber pada tanggal 3 Februari 2017 (www.kompas.com, 3 Februari 2017). Sebelumnya tindak pidana siber ini penanganan berada di Direktorat Tindak Pidana Ekonomi Khusus (DIT TIPPID EKSUS) di Subdirektorat V yang menangani tindak pidana antara lain tindak pidana yang terkait dengan *cyber crime*, tindak pidana informasi dan transaksi elektronik.[25]

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, baik penelitian kepustakaan maupun lapangan diperoleh kesimpulan sebagai berikut :

1. Maraknya kasus skimming di era digitalisasi ini sangat membuat masyarakat resah khususnya nasabah yang sudah sangat banyak menjadi korban terutama nasabah bank BRI Unisma yang juga sangat banyak pengaduan di customer service BRI untuk permasalahan skimming tersebut. Hal ini terlihat bahwa masyarakat tidak banyak mengerti akan kewaspadaan penggunaan di mesin ATM (Anjungan Tunai Mandiri). Prosedural untuk pengaduan nasabah saat ada penipuan skimming ada 2 yaitu:
   a) Nasabah datang langsung ke petugas bank BRI untuk menjelaskan permasalahan yang dialami oleh nasabah tersebut.
   b) Nasabah akan diberikan nomor pelaporan untuk ditindak lanjuti di kantor pusat BRI
2. Faktor penghambat dan pendukung

[25] Jurnal Muhammad Prima Ersya Permasalahan Hukum dalam menanggulangi tindak pidana cyber hal 58

a. Faktor Penghambat
   1) Kurangnya pengetauan masyarakat tentang teknologi
   2) Terlalu acuh terhadap keamanan-keamanan yang sudah dihimbau kepada masyarakat.
   3) Terlalu kondisi sekitar saat akan melakukan transaksi.

b. Faktor Pendukung

   Masyarakat tetap mengikuti perkembangan teknologi yang sedang berkembang.

3. Upaya-upaya dari pemerintah dan pihak bank untuk meningkatkan keamanan bagi nasabah pengguna kartu ATM (Anjungan Tunai Mandiri) antara lain :
   a. Selalu mengedukasi nasabah untuk tetap waspada dalam bertransaksi melalui mesin ATM.
   b. Menghilangkan kebiasaan masyarakat yang selalu tidak ingin tau tentang perkembangan teknologi yang sudah berkembang pesat saat ini.
   c. Selalu tanggap dan bertindak tegas terhadap pelaku kasus kejahatan yang berkedok digital.

DAFTAR PUSTAKA

BUKU

Dian Alan Setiawan, *Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybrcrime), Volume 16. No. 2 (Jakarta: 2018, Edisi Oktober), hal181*

Jurnal Dian Eka Safitri *Magister Hukum Argumentum Volum 7 Nomor 1 , Maret 2020 hal 41*

Jurnal Arnazio Aulia Lesmana *Magister Hukum Argumentum Volum 7 Nomor 1 , Maret 2020 hal 21*

Jurnal Arnazio Aulia Lesmana *magister hukum , tanggung jawab kejahatan perbankan melalui modus operandi skimming Volume7|Nomor 1| Maret 2020 hal 36*

Alfitra, *Modus Operandi Pidana Khusus di Luar KUHP, (Jakarta: RAS, 2014), hal 28*

Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime):Urgensi Pengaturan dan Celah Hukumnya, hal17*

Dista Amalia Arifah, *Kasus Cybercrime di Indonesia,Volume 18 No. 2 hal 188*

Fitria Dewi Navisa, Penerapan Actio Paulina Sebagai Perlindungan Hukum Kreditur Dalam Kepailitan, ADIL Indonesia Journal (Vol 2, No 1 (2020))

----------, 2013, Analisis Perjanjian Kredit Berdasar Prinsip Kehati-Hatian Yang Berwawasan Lingkungan, Universitas Brawijaya

----------, 2020, Prinsip Kehati-Hatian Notaris Membuat Akta Dan Akibat Notaris Terindikasi Tindak Pidana Dalam Okta Otentik, Proceeding dalam Konferensi Nasional Hukum Birokrasi Untuk Indonesia Tangguh, Hlm 191-206

Jovin Ganda Ramdhan dan Sumiyati, *Perlindungan Hukum Terhadap Nasabah Korban Skimming Ditinjau Dari Undang Undang Nomor 8 Tahun 1999, Volume 12. No. 1 hal 89*

Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)- Urgensi Pengaturan dan Celah Hukumnya, Rajagrafindo Persada, Depok, 2012, hal 2*

Lex Privatum *Tentang PERLINDUNGAN HUKUM TERHADAP NASABAH BANK PENGGUNA INTERNET BANKING DARI ANCAMAN CYBERCRIME Vol.III/No. 1/hal 149*

PERATURAN PERUNDANG-UNDANGAN

Pasal 29 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan

INTERNET

Kontan.co.id, "Kerugian Bank BRI Akibat Skimming Sekitar Rp 145 juta", Diakses dari https://keuangan.kontan.co.id/news/kerugian-bri-akibat-skimming-sekitar-rp-1-miliar, Pada Tanggal 31 Mei 2022 Pukul 1