FAKULTAS HUKUM
UNIVERSITAS BUNG HATTA

PERSETUJUAN ARTIKEL
No. Reg. :17/Pid-02/VIII-2021

Nama	:**Salma Larasanti**
NPM	: **1710012111085**
Program Kekhususan	: **Hukum Pidana**
JudulSkripsi	: **Penegakan Hukum Terhadap Tindak Pidana Pemboboblan Rekening Dengan Modus Operandi Skimming Oleh Polresta Padang**

Telah**dikonsultasikan**dan**disetujui**oleh**pembimbing**untuk di upload di website.

Dr. UningPratimaratri, S.H., M.Hum. (Pembimbing)

Mengetahui

DekanFakultasHukum
Universitas Bung Hatta

Dr. UningPratimaratri, S.H., M.Hum.

KetuaBagian
HukumPidana

YetismaSaini, S.H., M.H.

PENEGAKAN HUKUM TERHADAP TINDAK PIDANA PEMBOBOLAN REKENING DENGAN MODUS OPERANDI SKIMMING OLEH POLRESTA PADANG

Salma Larasanti[1)], Uning Pratiramaratri[1)]
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Bung Hatta
Email: **salmalarasanti259@gmail.com**

ABSTRACT

The crime of skimming is also known as a bank account break-in. This act is regulated in Article 11 of Law Number 30 of 2011 concerning Information and Electronic Transactions. One of the cases that occurred in the Padang Polresta area was the theft of debit or credit card information by copying the information contained on the card's magnetic strip or known as skimming. This study uses a sociological juridical approach. The data sources used are primary data in the form of interviews with investigators at the Padang Police, and secondary data in the form of criminal statistics and BAP. The data were obtained by semi-structured interviews and document studies, the data were analyzed qualitatively. From the results of the study it was concluded that: (1) The skimming crime mode was carried out by several people or groups looking for an ATM machine as a target, then using various tools to commit the crime of skimming, then the perpetrator copied the data into the card and then the perpetrator copied the data. into a new ATM card. (2) Obstacles to law enforcement, the Padang Police in tackling the crime of skimming carried out through Automated Teller Machines, are with all the limitations of human resources and other supporting media.

Keywords: Crime, Modus Operandi, Skimming, Burglary

PENDAHULUAN

Salah satu bentuk kejahatan berbasis teknologi *cyber crime* adalah *Skimming*. *Skimming* adalah tindakan pencurian informasi kartu baik debit maupun kredit dengan cara menyalin informasi yang ada pada strip magnetik kartu. *Skimming* diatur dalam Pasal 30 UU NOMOR 11 Tahun 2008 tentang ITE. Yang telah diubah dengan UU No. 19 Tahun Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Skimming di samping merugikan nasabah bank, juga merugikan pihak bank. Penanganan kejahatan ini tidak mudah, kecuali jika tertangkap tangan. Bank adalah bisnis yang sangat tergantung kepercayaan, jika kepercayaan nasabah atau masyarakat turun akan berimbas pada operasional bank. Skimming merupakan kejahatan dengan menggunakan teknologi tinggi atau hi-tech technology, kejahatan ini dilakukan oleh orang-orang yang memiliki kemampuan teknologi informasi.

Pengungkapan kasus skimming di ATM BNI Lubuk Begalung pada tahun 2020 karena tertangkap tangan. Kasus tersebut melibatkan lima orang pelaku, yang kesemuanya merupakan *dader*. Di samping itu ada intellectual dader, intelektual dader kasus tersebut adalah seseorang yang diidentifikasi ada di Malaysia. Modus skimming adalah dengan memasang kamera chip di atas keyboard ATM. Kamera tersebut digunakan untuk mengintai PIN nasabah yang sedang melakukan transaksi.

Kasus skimming yang terjadi di ATM Lubuk Begalung berhasil diungkap oleh Polresta Padang karena adanya laporan dari warga masyarakat yang curiga gerak-gerik beberapa orang di ATM BNI. Warga yang curiga melaporkan mereka kepada aparat Polisi di Polsek Lubuk Begalung.

Berdasarkan kasus di atas, maka penulis memiliki ketertarikan dalam pengkajian lebih lanjut dengan judul

"PENEGAKAN HUKUM TERHADAP TINDAK PIDANA PEMBOBOLAN REKENING DENGAN MODUS OPERANDI *SKIMMING* OLEH POLRESTA PADANG".

RUMUSAN MASALAH

1. Bagaimana upaya kepolisian Polresta Padang dalam penanggulangan tindak pidana *skimming* yang dilakukan melalui mesin Anjungan Tunai Mandiri (ATM)?

2. Apa kendala-kendala Polresta Padang dalam menanggulangi tindak pidana *skimming* yang dilakukan melalui mesin Anjungan Tunai Mandiri (ATM)?

METODE

a. Jenis Penelitian

Jenis penelitian yang digunakan adalah yuridis sosiologis yaitu menekankan pada aspek hukum yang berlaku dikaitkan dengan kenyataan hukum dalam prakteknya di lapangan.

b. Sumber Data

1) Data Primer

Dalam penelitian ini diperoleh dengan wawancara dengan Aipda Adeka Putra (penyidik di Polresta Padang) yang melakukan penyidikan kasus *skimming* yang dilakukan melalui mesin Anjungan Tunai Mandiri (ATM). Dalam kasus ini, penulis memilih mewawancarai salah seorang penyidik atau petugas Kepolisian Resor Kota Padang yang memiliki andil besar yaitu pemimpin dari penyelesaian kasus ini di ruangan Bareskrim Unit II Tipidter Sat Reskrim Polresta Padang. Selain itu, data primer penelitian ini adalah hasil observasi di beberapa mesin ATM yang ada di Kota Padang. Observasi dilakukan untukmengetahui upaya non penal yang dilakukan oleh pihak bank.

2) Data Sekunder

Dalam penelitian ini, bahan hukum sekunder yang digunakan berupa statistik kriminal dan BAP kasus *cyber crime skimming* Tahun 2020 dari Polresta Padang. Selain itu, penulis juga melakukan penelusuran upaya non penal yang dilakukan oleh Polresta Padang dan bank di media sosial.

c. Teknik Pengumpulan Data

Dalam mengumpulan data, penulis melakukan wawancara, observasi, dan studi dokumen.

d. Teknik Analisis Data

Guna menganalisis data, penulis menggunakan metode kualitatif, metode ini digunakan karena data yang ada adalah data yang bersifat kualitatif.

HASIL DAN PEMBAHASAN

Upaya Kepolisian Polresta Padang dan Kendala-Kendala Polresta Padang Dalam Penanggulangan Tindak Pidana *Skimming* Yang Dilakukan Melalui Mesin Anjungan Tunai Mandiri (ATM)

1. Tindakan Represif (Upaya Penal) oleh Polresta Padang

Upaya penal merupakan tindak represif dari penegak hukum, dalam hal ini adalah tindakan penegakan hukum pidana oleh aparat kepolisian Resort Kota Padang. Berdasarkan statistik kriminal tahun 2020 sampai 2021 tindak pidana *skimming* di Indonesia ada tiga kasus. Khusus di Padang, terjadi satu kasus di wilayah Polsek Lubuk Begalung, selanjutnya kasus ini ditangani oleh Polresta Padang.

Dalam rangka upaya represif, Polresta Padang telah melakukan penyidikan dan melimpahkan perkara tindak pidana skimming ke Kejaksaan Negeri Padang.

2. Upaya Non Penal oleh Polresta Padang

Upaya non penal yang dilakukan oleh Polresta Padang dalam memberantas tindak pidana *skimming* yaitu dengan melakukan sosialisasi melalui media sosial, melakukan dialog-dialog masyarakat tentang pencurian atau pembobolan data (akses ilegal) yang menyangkut data nasabah atau masyarakat yang ada perbankan, permasalahan ini meminta turut serta dan peran masyarakat dan pihak-pihak bank.

3. Penanggulangan oleh pihak perbankan

   Upaya penangggulangan yang dilakukan oleh pihak perbankan terhadap kejahatan *skimming* ini ialah dengan menyelesaikan pengaduan dari nasabah yang menjadi korban kejahatan tindak pidana *skimming*. Di samping itu, pihak bank melakukan edukasi kepada nasabah supaya berhati-hati pada saat melaksanakan transaksi di ATM ataupun transaksi elektronik apa pun. Edukasi dan peringatan dilakukan dengan pemasangan flyer di mesin ATM dan melalui media sosial. Seruan dan edukasi yang dibutuhkan kepada nasabah untuk tidak sembarangan membuang struk transaksi kartu kredit atau debit yang sudah digunakan, karena dari struk transaksi kartu kredit atau debit tersebut ada data yang bisa dilacak buat digunakan dalam tindak pidana pencurian data dan pengembangan pengetahuan buat para warga universal terkait dengan jenis-jenis kejahatan perbankan serta modus operandi pelaku tindak pidana skimming tersebut.

4. Upaya penanggulangan oleh pihak nasabah

   Nasabah harus berhati-hati, dan jika ada yang mencurigakan segera lapor kepada yang berwajib. Terungkapnya kasus skimming di ATM BNI Lubuk Begalung karena adanya laporan dari masyarakat.

Adapun kendala yang dihadapi oleh Polresta Padang yaitu :

1) Faktor Internal
   a. Kurangnya sumber daya manusia
   b. Sarana dan prasarana
2) Faktor Eksternal
   a. Kurangnya pemahaman masyarakat tentang bahaya *skimming*
   b. Faktor pelaku
   c. Faktor perbankan dan pemerintah

KESIMPULAN DAN SARAN

Tindak kejahatan *skimming* pada kasus ini ialah modus kejahatan yang meletakan alat scan (*skimmer*) pada mulut tempat keluar masuknya ATM ditambah dengan mengganti salah satu komponen "*insert card*" dengan bahan fiber dan memasang kamera kecil dibagian atas pelindung yang ada pada bagian *keyword* pin ATM. *Skimmer* ini digunakan untuk mengambil data nasabah seperti data yang terdapat pada bagian hitam di kartu ATM dan merekam pin nasabah yang selanjutnya disalin pada kartu ATM kosong atau palsu. Jika upaya merekam tidak berhasil, maka pelaku akan mencoba menghubungi korban agar mendapatkan pasword dari data nasabah yang diambil dengan berbagai modus penipuan seperti berperan sebagai pihak bank atau pihak berwajib lain sehingga nasabah percaya dan memberi data nya ke mereka.Adapun pertimbangan hakim dalam menjatuhkan sanski pidana dengan aspek yuridis meliputi : Dakwaan Jaksa Penuntut Umum, Tuntutan Jaksa Penuntut Umum, Keterangan Saksi, Keterangan Terdakwa, dan aspek non yuridis memperhatikan hal-hal yang memberatkan dan meringankan terhadap terdakwa.

Pihak berwajib juga harus lebih memperhatikan bakat-bakat yang dimiliki masyarakat khususnya di bidang IT dan membuka lowongan pekerjaan untuk itu seperti menjadi polisi di bagian IT, bekerja di bank sebagai pengamanan data atau bekerja disuatu perusahaan yang menangani seputar IT sehingga pihak berwajib bisa bekerja sama untuk penanganan kasus seperti ini. Pengamanan tambahan untuk ATM juga diperlukan, seperti adanya satpam di setiap ATM walaupun hanya ATM yang berada di SPBU atau satu ATM karena kejahatan bisa terjadi kapan saja jika ada kesempatan dan kurangnya pengamanan. Pihak bank juga perlu menambahkan media pendukung keamanan seperti alarm atau jenis alat peringatan atau bahkan sensor jika ada pelaku yang mencoba merusak dan merugikan pihak bank. Contohnya jika pelaku tindak pidana *skimming* tengah melakukan aksinya, sensor alarm langsung berbunyi sehingga satpam bisa mengamankan pelaku dan sensor juga langsung

terhubung ke pihak bank dengan demikian penangkapan pelaku akan lebih cepat dan efektif. Sehingga pihak bank atau kepolisian bisa dengan sigap menangani kasus dengan tidak membuang waktu lama untuk mencari tahu siapa pelaku, dimana pelaku atau info mengenai pelaku.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada seluruh pihak yang turut membantu penulis dalam melaksanakan penelitian ini sehingga penelitian ini dapat terlaksana dengan baik.

DAFTAR PUSTAKA

Buku-buku

MH Dian Ekawati, 2018, Rusli Muhammad, 2006, *Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Persepektif Teknologi Informasi dan Perbankan,* Persada, Jakarta.

Peraturan Perundang-undangan

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.