INDONESIAN JOURNAL of INTELLECTUAL PUBLICATION
IJI Publication
p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

ANALISIS TINDAK PIDANA *SKIMMING* OLEH KEPOLISIAN DAERAH SULAWESI SELATAN

ANALYSIS OF CRIMINAL SKIMMING BY THE POLICE SOUTH SULAWESI AREA

Andi Tanwir Mappanyukki
Universitas Indonesia Timur, Indonesia[1]
email: anditanwirmappanyukki@gmail.com

IJI Publication
p-ISSN: 2774-1907
e-ISSN: 2774-1915
Vol.3, No.1, pp. 72-83
Nopember 2022

Unit Publikasi Ilmiah Intelektual Madani Indonesia

Abstrak: Tujuan penelitian ini untuk mengetahui cara tindak pidana *skimming* Polda Sulawesi Selatan. Disamping untuk mengetahui upaya penyelamatan dan pencegahan kejahatan *skimming* yang dapat dituntutaskan melalui kepolisian. Manfaat dari penelitian ini diharapkan dapat menjadi referensi bagi penelitian selanjutnya, khususnya dalam upaya penanggulang dan pencegahan kejahatan *skimming* oleh kepolisian. Dan dapat dijadikan sebagai bahan menyelesaikan masalah-masalah kejahatan yang terjadi di masyarakat secara khusus penanggulang dan pecegahan kejahatan *skimming*. Teknik Pengumpulan data dalam penelitian ini menggunakan metode wawancara yang dilakukan dengan cara mengadakan tanya jawab secara langsung kepada pihak yang terkait dan dengan metode kepustakaan yaitu teknik pengumpulan data dengan cara menganalisis dan mengkaji berbagai literatur yang berlaku dan sekaligus dikatkan dengan objek kajian, kemudian data yang telah dikumpulkan, baik data primer maupun data sekunder akan disusun dengan menggunakan analisis kualitatif dan kuantitatif, kemudian disajikan dalam bentuk deskriptif. Dari hasil penelitian ini penulis menemukan bentuk kejahatan *skimming* sesuai dengan data yang diperoleh dari 3 (tiga) Instansi penegak hukum yaitu Kepolisian Resort Sinjai Sulawesi Selatan, Kejaksaan Negeri Sinjai, dan Pengadilan Negeri Sinjai, sehingga penulis dapat menyimpulkan bahwa kejahatan *skimming* yang terjadi di Kabupaten Sinjai dari tahun 2018 sampai tahun 2020 mengalami peningkatan.
Kata Kunci: Kriminologis, *Skimming*.

Abstract: *The purpose of this study was to find out how the crime of skimming at the South Sulawesi Regional Government was carried out. Besides knowing the efforts to save and prevent skimming crimes that can be prosecuted through the police. The benefits of this research are expected to be a reference for further research, especially in efforts to counter and prevent skimming crimes by the police. And can be used as material to solve the problems of crime that occur in society, specifically the countermeasures and prevention of skimming crimes.The data collection technique in this study used the interview method which was carried out by holding questions and answers directly to the parties concerned and with the library method, namely data collection techniques by analyzing and reviewing various applicable literature and at the same time tied to the object of study, then the data that has been collected collected, both primary data and secondary data will be compiled using qualitative and quantitative analysis, then presented in descriptive form.From the results of this study the authors found the form of skimming crime in accordance with the data obtained from 3 (three) law enforcement agencies, namely the Sinjai Resort Police of South Sulawesi, the Sinjai District Attorney, and the Sinjai District Court, so the author can conclude that skimming crimes that occurred in Sinjai Regency from 2018 to 2020 has increased*
Keywords: Criminology, Skimming.

PENDAHULUAN

Makassar adalah kota metropolitan terbesar di Indonesia Timur, sehingga hal ini mengakibatkan pertumbuhan perekonomian di Kota Makassar menjadi lebih tinggi. guna menunjang kebutuhan masyarakat, maka bank-bank menempatkan Anjungan Tunai Mandiri (ATM) di setiap sudut kota metropolitan untuk memudahkan manusia dalam bertransaksi. Peningkatan transaksi digital merupakan konsekuensi dari peningkatan ilmu pengetahuan dan generasi. Peningkatan pengetahuan teknologi dan teknologi pencatatan juga disertai dengan bantuan dari unsur-unsur mengerikan melekat padanya, membuktikan munculnya kejahatan paling belakang yang benar-benar kompleks diikuti dengan modus operandi yang berbeda benar-benar baru. Sejatinya hukum berfungsi sebagai ala tuntuk melindungi kepentingan dalam bermasyarakat. Maksud dari melindungi kepentingan tersebut ialah sebagai perlindungan yang diberikan oleh hukum guna melindungi segala bentuk kepentingan masyarakat yang bertujuan menciptakan

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

kehidupan manusia yang normal, tentram dan damai.

Tidak hanya kejahatan konvensional yang belum diberantas karena dilatarbelakangi oleh gaya modernitas yang tidak mengedepankan prinsip kemanusiaan, namun juga munculnya *cybercrime* yang muncul sebagai kebenaran sektoral. jaringan. Kejahatan dunia maya hanyalah bentuk negatif dari peningkatan pengetahuan teknologi dan era dan statistik. Jangka waktu "kejahatan dunia maya" di dalam kertas warisan untuk lokakarya pada kongres PBBX/2000 mengatakan bahwa kejahatan dunia maya memiliki dua jenis arti, kejahatan dunia maya dalam pengalaman ramping "dalam arti panah" didefinisikan sebagai "kejahatan komputer" dan kejahatan dunia maya di perasaan yang lebih luas "dalam pengalaman yang lebih luas". Sebagai "kejahatan terkait laptop". *Cybercrime* dilakukan melalui *cyber crime* dengan memanfaatkan jaringan laptop sebagai media alat jaringan. Kegiatan kejahatan dunia maya dapat dilakukan dengan berbagai metode dan tujuan dengan memanfaatkan pelaku peristiwa yang menguasai bidang teknologi dan statistik dewasa ini dan menggunakannya dalam jalur negatif.

Kejahatan ini melawan hukum melalui suatu komunitas sistem komputer dan struktur percakapan masing-masing secara regional dan global (internet) dengan menggunakan pemanfaatan perangkat komputer pembangkit data total yang merupakan perangkat elektronik yang dapat dilihat hanya dengan menggunakan klien internet sebagai korban. Kejahatan tersebut meliputi manipulasi data (*Trojan steed*), mata-mata, *hacking*, penipuan kartu kredit online (*carding*), merusak widget (*cracking*), menyalin catatan dari kartu ATM *(Skimming ATM)* dan lain-lain. Penjahat dunia maya ini memiliki warisan kapasitas tinggi dalam disiplin mereka sehingga sulit untuk melacak dan menyingkirkan mereka sepenuhnya.

Terkait dengan kejahatan siber yang terus berkembang, pihak berwenang telah mengeluarkan liputan melalui UU 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah menjadi UU No. 19 Tahun 2016. UU ITE merupakan gagasan untuk penegakan hukum di Internet, substansi/struktur yang diatur dalam UU ITE tentang pemerintahan, keamanan hak-hak tertentu, standar pertukaran, prinsip persaingan usaha tidak sehat dan keamanan pelanggan, standar barang kelas atas (HaKI) dan Hukum Internasional dan Kejahatan Dunia Maya.

UU ITE mengatur tentang kejahatan dunia maya atau cybercase, yaitu segala kegiatan yang dilakukan dalam kejahatan dunia maya yang meliputi permainan, pornografi, ancaman, Pemotongan dan fitnah melalui media internet selain komputer yang membawa hak masuk yang tidak sah melalui peristiwa lain *(cracking)* dan membuatnya muncul seakan dokume notentik*(phising*). Sehingga dengan adanya UU ITE merupakan sebagai paying hukum dalam pemanfaatan teknologi untuk mencegah penyalahgunaannya sehingga penggunaan teknologi informasi dan elektronik dapat dilakukan dengan aman.

Cybercrime terjadi di Indonesia yaitu kejahatan dengan modus terbaru yang dilakukan melalui mesin ATM, oleh apa yang dikenal dengan istilah kejahatan "*skimming"*. ATM Merupakan terminal/perangkat pc yang berhubungan dengan jaringan komunikasi bank, yang membolehkan nasabah buat melaksanakan transaksi moneter secara mandiri tanpa dorongan teller ataupun pejabat bank yang lain. Lewat ATM, nasabah lembaga keuangan bisa masuk ke utangnya buat melaksanakan bermacam transaksi moneter, ialah penarikan tunai serta transaksi non tunai, semacam cek saldo, pembayaran tagihan kartu kredit, pembayaran tagihan listrik, belanja pulsa, serta sebagainya.

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

Kejahatan *skimming* merupakan aksi mencuri data kartu kredit/debit dengan metode menyalin secara tidak legal seluruh statistik yang ada pada magnetic strip kartu serta setelah itu informasi ataupun informasi nasabah tersebut disalin ke dalam kartu kosong. Motif kejahatan ini merupakan pembobolan anggaran terhadap nasabah bank. Tipe kejahatan *skimming* yang kerap terjalin bukan cuma *skimming* yang sangat simpel lewat ATM, namun pula tipe kejahatan *skimming* yang lain, tercantum pemakaian Hand- Held POS *skimming*, ialah perlengkapan yang umumnya langsung disalin. Ataupun menggandakan kartu debit dan/atau kredit tanpa penundaan. Modus operandi ini umumnya dilakukan dengan cara menempatkan skimmer di mulut entri kartu debit klien di Anjungan Tunai Mandiri (ATM) atau di Electronic Data Capture (EDC). Tipe ke-2 adalah Dummy ATM, yaitu perangkat ATM yang paling baik digunakan untuk transaksi online.

Modus yang digunakan dalam memberantas kejahatan ini merupakan dengan memakai pocket WiFi router dengan kamera yang diganti menyamai penutup Personal Identification Number (PIN) pada mesin ATM buat mencuri PIN konsumen Bank. Lewat perlengkapan ini, pelakon menggandakan kenyataan strip magnetik pada kartu ATM setelah itu mengkloningnya ataupun mereproduksi data tersebut ke kartu ATM kosong. Wujud perlengkapan *skimming* pula bermacam- macam cocok dengan wujud, warna, serta dimensi sistem ATM, artinya supaya kejahatan tidak senantiasa gampang ditemukan begitu mereka melaksanakan aksi, sebab pengidap tidak hendak menyadarinya. mesin ATM sudah dilengkapi dengan sistem *skimming*. Metode kerja ATM *skimming* diawali kala kartu ATM pengidap dimasukkan ke dalam card reader ATM, sistem *skimming* diawali dengan menyalin fakta- fakta yang sudah diperoleh dari mesin skimmer ke dalam kartu ATM kosong.

Mesin ATM yang disediakan oleh berbagai Bank yang tersebar diberbagai tempat guna memudahkan para nasabah dalam transansi, hari ini tidak lagi seaman sebagaimana dalam penggunaannya, sebab kejahatan *skimming* tidak dibatasi oleh apapun tercantum Negeri, serta bisa diakses kapanpun serta dimanapun selagi ada layanan internet. Sangat membolehkan dalam pertumbuhan yang pesat ini orang juga bisa hadapi kerugian ataupun akibat negative terhadapat transaksi di mesin ATM.

Sebagai contoh kasus kejahatan *skimming* yang pernah yang menimpa Indonesia adalah enam warga Malaysia yang dirawat dengan menggunakan Mabes Polri berkolaborasi dengan Departemen Hukum serta Hak Asasi Manusia. Keenam masyarakat Malaysia ini ialah sindikat pencuri ATM dengan modus *skimming* kartu. Mereka sukses menghabiskan 112 tagihan konsumer Bank Central Asia di Jakarta serta Bandung. Total kerugian patron menggapai lebih dari 1, 25 miliyar. Modus yang digunakan komplotan ini merupakan memasang skimmer serta kamera pengintai di mesin ATM. Skimmer digunakan buat *scouse* meminjam data berarti di kartu ATM korban, sebaliknya kamera pengintai digunakan buat *scouse* meminjam nomor pin korban.

Kejahatan *skimming* tidak berkurang dari hari ke hari, tetapi korbannya semakin hari semakin bertambah dan alat kerja kejahatan *skimming* semakin canggih. Kasus yang Terjadi di Indonesia terkait tindak pidana *skimming* menjadi kasus yang terjadi di Jakarta pada Maret 2019, tindak pidana ini dilakukan melalui orang asing yang membuang nasabah Bank Mandiri. Namun kejahatan *skimming* ini terjerat oleh petugas pengamanan bank yang melihat pelaku (YMH) masuk ke ruang ATM Bank Mandiri, namun di dalam ruang ATM tersebut pelaku menunjukkan gerakan mencurigakan, saat didekati dengan baik, pelaku ingin kabur, maka pelakunya ternyata ditangkap. Dengan cara keamanan setelah itu

diserahkan ke polisi. Dari situasi ini, tersangka berinisial YMH (33) ditangkap, yang merupakan warga negara asing, terutama Taiwan. Kasus lainya yang terjadi di Makassar, Sulawesi Selatan tepatnya di bulan September 2019. Pelaku yang merupakan warga negara Rumania yang memasang *hiddencamera* untuk merekam password kartu ATM nasabah serta memasang alat *skimming* untuk merekam data rekening nasabah. Mereka juga sudah siapkan kartu ATM kosong yang di beli online di luar negeri. Kemudian ketika mengetahui pin nasabah, mereka sudah bisa menguras habis seluruh tabungan nasabah.

Kasus serupa juga pernah terjadi di Kab. Sinjai, Sulawesi Selatan tepatnya di bulan September 2020, yang dialami seorang nasabah BRI, yang awalnya korban menerima telpon yang mengaku sebagai pegawai bank BRI yang menyuruh korban untuk membuka pesan singkat yang masuk di hp korban kemudian menyuruh korban untuk menyebut nomor server id dan kode otp yang tertera dalam pesan singkat dari bank BRI, tidak lama setelah korban menyebut nomor server id dan kode otp tersebut tiba-tiba uang direkening korban raib secara misterius. Ia mengaku uang sebesar Rp. 39.000.000 raib tidak diketahui kemana hilangnya.

Terungkapnya kejahatan di maksimal *cybercrime* di Indonesia, terutama di Kota Makassar seperti yang tergambar dalam kebanyakan kasus saat ini, dapat berdampak lebih buruk pada masyarakat, khususnya masyarakat yang menggunakan media digital, atau kecanggihan yang ada saat ini. Ini juga meresahkan jaringan dan juga memungkinkan penjahat di dunia online kita untuk lebih fleksibel untuk memulai penjahat baru untuk mendedikasikan kejahatan atau kejahatan *cybercrime.*

Bahkan Kecanggihan strategi *skimming* modern adalah tanpa penundaan mencerminkan statistik yang diterima dari skimmer online, menggunakan remote, era GSM, atau Bluetooth. Jadi metode ini memungkinkan pelakunya untuk mengirimkan data yang diperoleh dari skimmer ke komputer atau ponsel yang dipasang di wilayah berkualitas tinggi, sehingga pelakunya dapat melakukan *skimming*. bisa masuk ke catatan di mana saja.

Tindak pidana *skimming* ATM harus dilakukan dengan Kebijakan Formulasi Hukum dan integrasi sistem peradilan pidana yang terpadu agar dapat diharapakan menekan atau menanggulangi kejahatan ini. Indonesia sendiri belum mengatur secara khusus perundang-undangan tentang kejahatan *skimming* ATM, untuk itulah perlu dilakukan upaya pencegahan dan penanggulangan Menuju *skimming* ATM sebagai kejahatan agar tidak semakin meluas dan membahayakan masyarakat. Beranjak dari segala permasalahan, maka tujuan penelitian ini adalah untuk mengetahui dan menganalisis tindak pidana *skimming* oleh Kepolisian Daerah Sulawesi Selatan."

METODE

Teknik Pengumpulan data dalam penelitian ini menggunakan metode wawancara yang dilakukan dengan cara mengadakan tanya jawab secara langsung kepada pihak yang terkait dan dengan metode kepustakaan yaitu teknik pengumpulan data dengan cara menganalisis dan mengkaji berbagai literatur yang berlaku dan sekaligus dikaitkan dengan objek kajian, kemudian data yang telah dikumpulkan, baik data primer maupun data sekunder akan disusun dengan menggunakan analisis kualitatif dan kuantitatif, kemudian disajikan dalam bentuk deskriptif.

HASIL DAN DISKUSI

Proses Penyidikan Tindak Pidana *Skimming* di Polda Sulawesi Selatan

Jika dilihat dari tekniknya, *skimming* adalah kepentingan untuk menggandakan fakta secara ilegal yang terdapat dalam pita

magnetik pada kartu kredit atau kartu remi debit. Dari metode ini dapat disimpulkan bahwa *skimming* adalah kegiatan yang terkait dengan upaya pelaku secara ilegal mencuri informasi dari pita magnetik kartu debit ATM untuk menguasai rekening korban.

Teknik penelitian yang dilakukan penyidik dalam penanganan kasus *SKIMMING* adalah begitu mendapat laporan tentang maraknya tindak pidana, Polda Sulsel langsung melakukan penyidikan. Hal ini sebagaimana dikatakan dalam Pasal 102 ayat (1) KUHAP, yaitu Penyidik yang mengetahui, menerima peninjauan kembali, atau tuntutan hukum tentang terjadinya suatu peristiwa yang dalam segala kewajarannya diduga merupakan perbuatan bajingan wajib untuk saat ini juga melaksanakan penyidikan. langkah investigasi penting.

Penyelidikan tersebut dilakukan dengan tujuan untuk mengumpulkan bukti permulaan Sehingga penyelidikan serupa dapat dicapai. Bukti awal sudah cukup, setidaknya dua bagian bukti terpenuhi. Alat bukti yang dimaksud dalam Pasal 184 KUHAP dapat berupa keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan dari terdakwa. Jadi berdasarkan sepenuhnya pada kasus *skimming* yang terjadi di wilayah hukum Polda Sulsel telah terpenuhi bukti permulaan yang cukup yaitu dengan adanya laporan dari pihak Bank BNI dan ditemukannya bukti berupa alat bantu *skimming* yang digunakan oleh pelaku untuk melakukan kejahatan.

Sehingga dengan terpenuhinya bukti permulaan yang cukup tersebut, maka akan dinaikkan ketahap penyidikan untuk ditindak lanjuti. Dimana Penyidik Polda Sulsel dalam hal ini telah mendengarkan keterangan dari tersangka sehingga Penyidik dapat mengetahui kronologi terjadinya suatu tindak pidana *skimming* tersebut. Serta diperkuat dengan bukti-bukti yang ditemukan dalam tempat kejadian perkara sehingga semakin membuat tindak pidana itu menjadi jelas untuk kemudian diserahkan kepada Jaksa Penuntut Umum. Sebagaimana ditentukan dalam Pasal seratus sepuluh KUHAP, bahwa dalam hal penyidik selesai melakukan penelitian, penyidik wajib segera menyerahkan berita acara kepada penuntut umum.

Tindakan *skimming* terdiri dari tindakan secara tidak sah memiliki akses ke laptop dan atau mesin statistik milik orang lain dengan maksud mengambil tanpa izin dan hak dari catatan non-publik korban di dalam laptop atau gadget statistik. Tindakan *skimming* termasuk dalam kejahatan statistik dan transaksi digital yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum memperoleh akses ke komputer dan atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi digital dan atau file digital sebagaimana diatur dalam Pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor sebelas Tahun 2008 tentang Informasi dan Transaksi Elektronik atau selanjutnya disebut UU ITE.

Kasus kejahatan *skimming* pada wilayah hukum Kepolisan Daerah Sulawesi Selatan resor sinjai, telah pernah ditangani oleh Penyidik yaitu dimana korbanya merupakan warga kec. Bulupoddo kab. Sinjai. Adapun rincian mengenai kasus kejahatan *skimming* yang ditangani oleh Kepolisian Daerah Sulawesi Selatan resor sinjai rentang waktu selama tahun 2020 adalah sebagai berikut :

Kesatuan yang menangani	Tersangka	Pelapor	Uraian Perkara
Reskrim Polres Sinjai	Dalam Lidik	AKHMAD L	Melanggar Pasal 30 Ayat (1) dan/atau Ayat (2) jo. Pasal 46 Ayat (1) dan/atau Ayat (2) dan/atau Pasal 31 Ayat 1 jo. Pasal 47 Ayat Undang-Undang RI Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi da Transaksi Elektronik (ITE) jo. Pasal 55 Ayat (1) ke-1 KUHP.

Sumber: Reskrim Polres Sinjai

Berdasarkan data diatas bahwa memang kejahatan *skimming* ini ter masuk dalam

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

modus operandi jenis baru Dalam tindakan penipuan fakta dan transaksi elektronik. Hal itu dibuktikan dengan hanya ada 1 (satu) kasus *skimming* yang terjadi di wilayah hukum Kepolisian Daerah Sulawesi Selatan, namun hal itu tidak bias dikesampingkan karena apabila kejahatan ini tidak dicegah sedini mungkin maka akan semakin pesat perkembangannya seiring dengan perkembangan teknologi.

Penerapan pasal pada pelaku tindak pidana kejahatan *skimming* yaitu dapat dikenakan dalam Pasal 30 ayat (2) UU ITE menyatakan bahwa, "Setiap orang dengan sengaja dan tanpa hak atau tindak pidana mengakses komputer dan/atau struktur digital dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Cara ini yang setiap perbuatan dapat dipidana jika telah memenuhi unsur pidana yang terkandung dalam pasal yang dituduhkan, yaitu:

1. Detail kesalahan disengaja.
2. Unsur melanggar hukum, khususnya tanpa hak atau melawan hukum.
3. Elemen tindakan mengakses dengan cara apa pun.
4. Unsur benda, yaitu komputer dan atau sistem elektronik.
5. Motifnya dengan tujuan untuk memperoleh informasi elektronik dan atau dokumen elektronik

Unsur-unsur diatas haruslah dapat diungkapkan oleh kepolisian dalam proses penyidikan untuk Bersihkan tentang kejahatan yang terjadi. Sebagaimana didefinisikan dalam Pasal 1 faktor 2 UU No. Delapan Tahun 1981 tentang Hukum Acara Pidana bahwa penelitian adalah serangkaian tindakan yang dilakukan oleh penyidik menurut dan menurut cara yang diatur dalam peraturan ini untuk mencari dan memperoleh bukti yang dengan alat bukti itu meringankan perbuatan pidana tersebut. yang terjadi dan dalam perjalanan untuk menemukan tersangka.

Berdasarkan wawancara dengan penyidik AIPDA IRMAN, S.H., bahwa satuan reserse criminal Polres Sinjai pernah menerima laporan Tindak pidana penipuan dengan modus operandi *scimming* dari seorang warga yang berdomisil di Kec. Bulupoddo kab. Sinjai hal tesebut terungkap sebagai kejahatan *scimming* karena berdasarkan keterangan pelapor bahwa mulanya ia menerima telpon dari seseorang yang mengaku dari pihak bank BRI dan mengatakan bahwa nomor rekening BRI milik pelapor terpilih menjadi pemenang undian yang akan diterima langsung pada bank BRI cabang sinjai dan saat itu seseorang yang mengaku dari pihak bank BRI tersebut sambil menyebut nomor rekening pelapor sehingga pelapor menjadi yakin bahwa yang menelponnya adalah benar dari pihak BRI dan setelah itu seseorang yang mengaku dari pihak bank BRI tersebut kemudian meminta nomor kode OTP yang masuk pada nomor handphone pelapor yang dikirim langsung oleh bank BRI dan karena saat itu pelapor tidak paham dengan kode OTP tersebut, ia kemudian langsung saja memberikan nomor kode OTP miliknya dan setelah itu tidak lama kemudian uang dalam rekening pelapor langsung hilang sebesar Rp. 39.000.000,- atau telah terkirim secara otomatis ke rekening seseorang yang bernama YAYAN ABDUL, dari keterangan pelapor tersebut diatas maka penyidik satuan reserse criminal polres sinjai menduga kuat pelaku yang mengambil uang pelapor sebelumnya menggunakan alat *scimming* pada salah satu mesin atm yang pernah pelapor gunakan melakukan transaksi keuangan karena pelaku mengetahui data perbankan milik pelapor.

Sehingga berdasarkan uraian kronologi tersebut setelah mendapatkan Jika ada laporan tentang terjadinya tindak pidana korupsi, penyidik Satuan Reserse Kriminal Polres Sinjai segera melakukan penelitian. Hal ini sebagaimana dikatakan dalam Pasal 102 ayat (1) KUHAP, khususnya penyidik yang

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

memahami, menerima pemeriksaan atau pengaduan tentang terjadinya suatu peristiwa yang patut diduga sebagai tindak pidana wajib segera melakukan penyidikan yang vital. bergerak.

Penyelidikan dilakukan dengan tujuan untuk mengumpulkan bukti awal agar dapat dilakukan gerakan lanjutan pada tahap penelitian. Bukti awal sudah cukup, karena bukti minimum terpenuhi. Alat bukti yang dimaksud dalam Pasal 184 KUHAP dapat berupa keterangan saksi, keterangan ahli, surat, perintah, dan keterangan dari terdakwa. Namun, kasus *skimming* yang terjadi di wilayah hukum Polres sinjai tersebut, sampai saat ini belum dapat ditingkatkan ke tahap penyidikan dengan berbagai macam kendala yang menyulitkan penyidik untuk mengungkap pelaku dalam kasus sciming tersebut, namun hingga saat ini penyidik masih terus berusaha mengumpulkan bukti-bukti untuk dapat mengungkap kasus skiming tersebut.

Dapat diduga bahwa kejahatan *skimming* yang terjadi di wiliayah hukum polres sinjai ini merupakan kejahatan yang terorganisir, namun dalam proses penyelidikan pihak kepolisian belum dapat mengungkap pelaku yang telah mengambil uang pelapor saat itu.

Kemudian berdasarkan wawancara yang dilakukan terhadap Penyidik Polda Sulsel resor sinjai, bahwa faktor penyebab terjadinya kejahatan *skimming* adalah terdiri dari faktor ekonomi, factor lingkungan, dan factor intelektual. Dalam faktor ekonomi, bahwa Salah satu unsur yang mendorong terjadinya kejahatan *skimming* adalah kurang sejahteranya kehidupan dari pelaku. Untuk mendapatkan jalan pintas dalam mencukupi kebutuhan hidupnya inilah pelaku kemudian belajar ataupun mendapat pengarahan tertentu dari pemimpin sindikat kejahatan *skimming* secara langsung maupun melalui *skimmer* yang telah lebih dulu berkecimpung di dalam sindikat kejahatan *skimming* ini.

Krisis ekonomi juga menjadi keadaan yang mendorong pelaku untuk melakukan kejahatan *skimming* ini. Hal ini dapat dikatakan sangatlah miris, karena pada dasarnya seluruh komponen bangsa atau negara harusnya berpartisipasi dalam mendukung pemulihan ekonomi sehingga bangsa dan negara dapat segera bangkit dari krisis ekonomi.

Menurut analisa penulis, dimana faktor ekonomi yang didorong oleh krisis ekonomi dan tidak memadainya lapangan kerja untuk skimmer pada awalnya, hingga sampai kepada jalan pintas untuk mendapatkan penghasilan lebih oleh pelaku dalam bentuk kejahatan yang notabene juga merugikan berbagai pihak. tidak hanya sampai pada itu saja, karena pada dasarnya bank dan nasabah punya hak untuk diberikan perlindungan hukum dari segala bentuk kejahatan termasuk kejahatan *skimming* ini.

Kemudian faktor lingkungan, bahwa lingkungan sangat berpengaruh memutuskan pembentukan mental dan pria atau wanita dari seseorang yang mulai tersinggung tidak lagi sebagai pelaku kejahatan kemudian menjadi penjahat pada akhirnya. Semua ini disebabkan dari proses pembelajaran yang di terima oleh pelaku dalam lingkungan sekitarnya. Pernyataan Hal ini memperkuat prinsip *differential affiliation* yang dikemukakan oleh Sutherland yang menyatakan bahwa seseorang melakukan tindak pidana karena dari lingkungan sekitarnya ia mengetahui bahwa perbuatan jahat atau pelanggaran hukum lebih berharga daripada perilaku non kriminal atau ketaatan pada hukum.

Lalu faktor intelektual, bahwa faktor intelektual sangat memegang peranan penting dalam kejahatan *skimming* ini. Faktor intelektual ini dilatar belakangi oleh kemampuan yang di miliki oleh pelaku kejahatan *skimming* sebelumnya atau orang yang memiliki pengetahuan terkait perbuatan kejahatan *skimming* yang di berikan kepada orang lain yang kemudian menjadi bagian dari

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

sindikat kejahatan *skimming*. Kemudian kejahatan *skimming* ini bisa terlaksana dengan pengetahuan yang lebih pada bidang teknologi, ini sangat berbeda dengan melakukan kejahatan-kejahatan konvensional.

Hambatan Kepolisian Daerah Sulawesi Selatan dalam Menangani Kejahatan *Skimming*

Berdasarkan Pasal 1 Angka 1 KUHAP, Penyidik adalah polisi negara Republik Indonesia atau Pegawai Negeri Sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan. Dalam hal penyidikan yang dilakukan oleh penyidik terhadap pelaku tindak pidana *skimming* mengalami keterbatasan, baik hambatan dari dalam maupun dari luar. Berdasarkan wawancara yang dilakukan, batas-batas penyelidikan dijelaskan sebagai berikut:

a. Faktor Internal, meliputi
    1. Sumber Daya Manusia, Dalam menjalankan tugas mengungkap kasus-kasus kejahatan *skimming* yang dilakukan Polda Sulsel, Polda Sulsel memiliki berbagai keterbatasan sumber daya manusia. Sebenarnya, penyidik Polda Sulsel telah melakukan berbagai langkah untuk mengungkap kasus-kasus tindak pidana *skimming*. Diperlukan standar khusus bagi penyidik yang juga mengetahui rahasia perbankan dan urusan perbankan serta memahami tentang kejahatan *skimming*. Sehingga menghambat teknik penyidikan dalam kasus-kasus kejahatan *skimming*. Hambatan-hambatan yang dimaksud mengenai kemampuan dan kreativitas dianggap masih belum memadai dalam menangani tindak pidana *skimming*. Ini karena perkembangan zaman sehingga semuanya tepat. Pendidikan dalam kualitas tinggi keahlian pemberdayaan tumbuh dan berkembang dalam tingkat kejahatan atau tindakan ilegal menjadi lebih kreatif dan rapi.
    2. Sarana dan prasarana, beberapa fasilitas canggih justru membantu penyidik dalam mengungkap kasus kejahatan kartu kredit atau *skimming* crime. Karena dalam beberapa kasus yang tidak biasa, penyidik mengatasinya karena tidak ada peralatan dan pusat mutakhir yang memenuhi sistem penyidikan.

a. Faktor External, meliputi:
    1. Kurangnya pengetahuan masyarakat tentang bahaya kejahatan *skimming*, ketidaktahuan masyarakat bahwa kejahatan pencurian melalui kartu kredit atau *skimming* semkain berkembang pesat, sehingga membuat masyarkat itu sendiri menjadi korban kejahatan *skimming* tersebut.
    2. Faktor pelaku, Hal ini juga menjadi kendala yang dilakukan oleh penyidik. Hal ini dikarenakan para pelaku semakin ingin mendapatkan banyak akibat dari kejahatan *skimming* tersebut, khususnya dengan bantuan intelijen dan intelijen. keintelektualannya. Pelaku sangat paham pula dengan perkembangan teknologi sehingga sangat menghambat penyidik dalam mengungkap kasus kejahatan *skimming* ini. Serta berbagai celah atau peluang yang dimiliki para pelakunya karena kini manusia telah berpindah dari membayar koin dan menggunakan kartu kredit.

Dalam menanggulangi terjadinya kejahatan skimming, pihak kepolisian telah melakukan berbagai upaya. Bahkan bukan hanya dalam rangka menanggulangi tetapi juga melakukan upaya pencegahan terhadap kejahatan *skimming* ini. Berdasarkan wawancara penulis lakukan dengan penyidik AIPDA Adi Dermawan N, S.H pada hari senin 25 Juli 2020, Upaya-upaya yang dilakukan kepolisian yaitu menanggulangi

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

dan menghentikan kejahatan skimming yang meliputi 3 upaya yaitu pre-emptif, preventif, dan represif.

1. Upaya Pre-emtif

Melakukan pre-emtif ini, pihak kepolisian melakukan penanaman nilai dan norma terhadap seluruh masyarakat dengan melakukan sosialisasi akan pentingnya penggunaan teknologi dengan bijak sehingga hal tersebut dapat terinternalisasi dalam diri setiap orang. Hal ini bertujuan untuk menghilangkan niatan seseorang untuk melakukan perbuatan menyimpang dari teknologi yang berkembang pesat.

Menurut analisa penulis dengan upaya pre-emtif ini sangatlah penting untuk tetap dipertahankan atau bahkan lebih dikembangkan dengan Ikuti perkembangan teknologi dan generasi sehingga upaya yang dilakukan oleh polisi tidak lagi terkesan hanya formalitas dalam menjalankan tanggung jawab mereka untuk mencegah timbulnya berbagai jenis kejahatan dalam perjalanan untuk muncul di jaringan. Ini bisa menjadi sangat vital karena upaya awal yang dilakukan oleh polisi untuk mencegah kejahatan, terutama dalam situasi ini kejahatan *skimming.* Jika upaya yang dilakukan pihak kepolisian ini di laksanakan secara efektif maka kejahatan *skimming* bisa lebih di minimalisir potensi teradinya. Adapun masukan penulis sebagai salah satu upaya pre-emtif yaitu kepolisian harus membuat konten-konten positif yang berkaitan dengan penanaman nilai dan norma yang baik kemudian disebarluaskan di media-media sosial sehingga dengan mudah menjangkau seluruh elemen masyarakat.

2. Upaya Preventif

Upaya ini merupakan kelanjutan dari upaya pencegahan yang merupakan upaya untuk pencegahan yang di lakukan pihak kepolisian terhadap kejahatan *skimming.* Upaya preventif pihak kepolisian melakukan pengaturan, penjagaan, serta pengawasan khusus di lokasi-lokasi yang memiliki potensi besar terjadinya kejahatan *skimming.* Kemudian pihak kepolisian juga melakukan koordinasi terhadap pihak terkait dengan memberikan edukasi akan pentingnya peran pihak terkait untuk lebih meningkatkan keamanan serta kewaspadaan terhadap segala bentuk kejahatan, khususnya kejahatan skimming.

Menurut analisa penulis, upaya preventif dari kepolisian perlu lebih memasifkan di berbagai tempat mesin ATM yang memiliki potensi besar terjadinya kejahatan skimming ini. Hal ini sebabkan dengan modus operandi dari kejahatan skimming tidaklah sama cara kejahatan-kejahatan konvensional lainnya yang dengan mudahnya di awasi. Pelaksaan kejahatan skimming ini lebih profesional dan lebih mengikuti perkembangan ilmu pengetahuan dan teknologi sehingga pihak kepolisian pun harus lebih mewaspadai kondisi seperti ini ke depannya.

3. Upaya Represif

Upaya ini merupakan upaya untuk mengatasi dilakukan oleh pihak kepolisian ketika terjadinya kejahatan skimming. Adapun upaya kepolisian terhadap kejahatan skimming dengan melakukan upaya penyelidikan dan penyidikan. Upaya ini bertujuan untuk menindak lanjuti laporan dari pihak yang di rugikan oleh kejahatan skimming ini.

Berdasarkan dari Menurut penulis, upaya represif yang dilakukan dengan bantuan polisi ingin selain tindakan yang dilakukan melalui polisi. Adapun upaya represif yang dapat diselesaikan dengan menggunakan polisi untuk mengatasi kejahatan *skimming* yaitu dengan terjadi kejahatan tersebut maka pihak kepolisian perlu memberikan tekanan kepada pihak-pihak yang bersangkutan untuk lebih meningkatkan keamanan di setiap lokasi mesin ATM kemudian mengusut hingga ke akar dari kejahatan *skimming* ini. Bukan hanya selesai pada upaya penyelidikan dan penyidikan untuk menindak pelaku saja, namun membongkar seluruh jaringan-jaringan dari kejahatan skimming terkait,

p-ISSN: 2774-1907; e-ISSN: 2774-1915; Vol.3, No.1 Nopember 2022

sebagai tindak lanjut dari penyidikan, demi mencegah terjadinya jumlah kejahatan skimming yang lebih luas ke depannya. Hasil dari tindak lanjut inilah yang akan menyempurnakan upaya preventif kepolisian terkait kejahatan skimming ini.

Kemudian dalam perspektif perbankan, juga penulis telah mekakukan wawancara terkait pencegahan yang dapat dilakukan untuk melindungi korban kejahatan skimming tersebut. Berdasarkan hasil wawancara dengan Latifah Nur Cahyanibahwa modus pemboblan ATM dengan skimming kartu biasanya menggunakan kamera kecil. Bahkan diharapkan nasabah tidak perlu khawatir lagi karena Bank BRI telah menerapkan IT Security yang kuat dan anti skimming. Lebih lanjut dikatakan, dengan adanya anti-*skimming*, ATM Bank BRI kini tidak memiliki celah untuk ditembus oleh kamera mikro. Bahkan jika tampaknya dana Sabah telah mengetahui adanya dugaan pembobolan stabilitas melalui gadget ATM, mereka dapat segera mencatatnya ke Call Center atau datang langsung ke Kantor Cabang Terdekat. Kemudian pihak lembaga keuangan akan melakukan konfirmasi, jika memang nasabah tidak melakukan transaksi namun saldonya berkurang, dan dipastikan tidak selalu konsumen yang bersangkutan yang melakukan transaksi, terbukti dari foto CCTV, stabilitas yang hilang akan diganti. Dengan cara ini, nasabah hanya perlu membawa kartu ATM dan ebook tabungan.

Hal ini sesuai dengan ketentuan yang diatur dalam Pasal 29 (4) UU No. 10 Tahun 1998 tentang Perbankan yang menyatakan bahwa untuk kepentingan nasabah, bank wajib menyediakan data mengenai peluang risiko kerugian yang mengacu pada transaksi pembeli yang dilakukan melalui lembaga keuangan. Artinya bank harus menyediakan informasi terkait antisipasi apabila terjadikerugian yang dialami nasabah serta penggantian kerugian oleh bank itusendirikepadanasabah yang mengalami kerugian akibat kejahatan *skimming*.

Lebih lanjut dalam Pasal 15 UU ITE telah menetapkan tanggung jawab yang harus dipenuhi oleh bank sebagai vendor struktur elektronik, yaitu:

a. Setiap operator perangkat digital harus memfungsikan sistem digital dengan andal dan benar serta bertanggung jawab atas pengoperasian sistem digital yang benar.
b. Operator gadget elektronik bertanggung jawab atas pengoperasian perangkat digital
c. Ketentuan sebagaimana dimaksud pada ayat (2) tidak mengikuti dalam hal dapat dipastikan bahwa terjadinya peristiwa pemaksaan, kesalahan, dan/atau kelalaian di pihak Pengguna sistemel ektronik.

Adapun untuk Otoritas Jasa Keuangan pun juga memiliki peran penting dalam pencegahan dan perlindungan bagi korban kejahatan skimming ini. Berdasarkan hasil wawancar adengan Kepala Otoritas Jasa Keuangan Regional 6 Sulampua, Moh. Nurdin Subandi, menyatakan bahwa Otoritas Jasa Keuangan dalam memberikan keamanan nasabah kepada nasabah yang mengalami kerugian atau dalam hal ini para pelaku kejahatan skimming tetap berpedoman sepenuhnya pada Undang-Undang di Otoritas Jasa Keuangan.

Pasal 28 UU OJK menyebutkan bahwa tindakan pencegahan sebagai akibat kerugian konsumen dan masyarakat meliputi:

1. Memberikan catatan dan pendidikan kepada publik tentang ciri-ciri zona penawaran ekonomi, produk dan layanan.
2. Meminta lembaga pemberi dana untuk menghentikan olahraga mereka jika kegiatan tersebut memiliki kemampuan untuk merusak kegiatan masyarakat.
3. Gerakan lain yang dianggap vital sesuai dengan ketentuan peraturan perundang-undangan.

Lebih lanjut dalam wawancara, dalam hal kewenangan OJK memiliki ada dua perlindungan pemerintah dalam penjara bagi

pembeli, yaitu dapat memerintahkan atau melakukan tindakan positif kepada pelaku usaha di kawasan jasa keuangan untuk menyelesaikan pengaduan konsumen yang dirugikan oleh pelaku usaha komersial di sektor jasa keuangan dan dapat melaporkan ke pengadilan. kasus. Ketentuan tersebut diatur dalam Pasal 30 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.

Berdasarkan urain-uraian tersebut maka dalam pencegahan kejahatan *skimming*, Kepolisian Daerah Sulawesi Selatan harus semakin meningkatkan kordinasi dengan pihak bank dan OJK. Hal itu dikarenakan melalui kordinasi yang baik antar ketiga lembaga tersebut dapat saling berintegrasi dan meminimalisir hambatan yang dialami Polda Sulsel untuk mencegah semakin maraknya tindak pidana skimming yang terjadi.

KESIMPULAN

Berdasarkan pembahasan yang telah penulis uraikan, maka penulis menyimpulkan sebagai berikut:

1. Adapun proses penyidikan dilakukan dalam rangka penanganan kasus *skimming* adalah begitu mendapat laporan adanya kejadian melawan hukum, Polda Sulsel langsung melakukan penyidikan. Penelitian ini diselesaikan dengan tujuan untuk mengumpulkan bukti awal sehingga dapat dilakukan gerakan tindak lanjut pada tahap penyelidikan. Bukti awal sudah cukup, karena minimal dua alat bukti terpenuhi. Sehingga dengan keberhasilan bukti awal yang cukup maka akan diangkat ke tahap penelitian untuk observasi. Berdasarkan statistik dan bukti yang diperoleh, penyidik menerapkan Pasal 30 ayat (1) dan/atau ayat (2) jo. Pasal 46 Ayat (1) dan/atau Ayat (2) dan/atau Pasal 31 Ayat 1 jo. Pasal empat puluh tujuh Ayat Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor sebelas Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) jo. Pasal 55 Ayat (1) KUHP Pertama.
2. Dalam hal penelitian yang dilakukan oleh penyidik terhadap pelaku tindak pidana *skimming* menemui hambatan, baik keterbatasan dalam maupun keterbatasan eksternal. Elemen internal terdiri dari, sumber daya manusia dan pusat dan infrastruktur. Sementara elemen luar mencakup, kurangnya pemahaman masyarakat dan factor intelektual pelaku.

REFERENSI

Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime*, PT. Refika Aditama, Jakarta.

Adamichazawi, 2011, *Pelajaran Hukum Pidana I*, Rajawali Pers, Jakarta.

Andi Sofyan dan Nur Azisa, 2016, *Hukum Pidana*, Pustaka Pena Press, Makassar.

A.S. Alam, 2010, *PengantarKriminologi*, Pustaka Refleksi, Makassar.

Barda Nawawi Arief, 2001, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*, Citra Aditya Bakti, Bandung. 1996 *Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung. 2007, *MasalahPenegakan Hukum dan Kebijakan Hukum Pidanadalam Penanggulangan Kejahatan*, Kencana Predana Media Group, Jakarta.

C.S.T. Kansil dan Christine S.T. Kansil, 2004, *Pokok-pokok Hukum Pidana*, Pradnya Paramita, Jakarta.

Depdikbud Kamus Besar Bahasa Indonesia, 1989, cet. ke-2, Balai Pustaka, Jakarta.

Esmil Anwar, 2009, Saat Menuai Kejahatan Sebuah Pendekatan Sosio cultural Kriminologi, Hukum, dan Ham, Refika Aditama, Bandung.

I S. Susanto, 1991, Diktat Kriminologi, Fakultas Hukum Universitas Diponegoro Semarang, Semarang.

Maskun, 2013, Kejahatan Siber, Kencana, Jakarta.

Munir Fuady, 2013, Teori-Teori Besar (grand Theory) Dalam Hukum, cetakan ke-3, Kencana Pranamedia Group, Jakarta.

Muladi dan DwidjaPriyatno, 2013, Pertanggung jawaban Pidana Korporasi, EdisiRevisi, Cetakan Ke-4, Kencana Pernamedia Group, Jakarta.

Nandang Sambas, 2010, Pembaruan Sistem Pemidanaan Anak di Indonesia, Grahailmu, Yogyakarta.

Nur Fadhilah Mappaselleng dan Zul Khaidir Kadir, 2018, Rethingking cyber crime, Arti BumiIntaran. Yogyakarta.

Ramli Atmasasmita. 1992.Teori Dan Kapita Selekta Kriminologi. Tarsito. Bandung

Satochid Kartanegara, 1955, Hukum Pidana Bagian Pertama, Balai Lektur Mahasiswa, Jakarta.

Sudarto, 1990, Hukum Pidana I, Yayasan Sudarto, Semarang.

S.R. Sianturi, 2002, Asas-asas Hukum Pidana di Indonesia dan Penerapan, Cet. 3, Jakarta Storia Grafika, Jakarta.

Sudikno Mertokusumo dan A. Pitlo, 1993, Bab-bab Tentang Penemuan Hukum, Cet. I, PT. Citra Aditya Bakti, Bandung.

Teguh Prasetyo, 2010, Hukum Pidana, Rajawali Pers, Jakarta.

Topo Santoso, 2001, Kriminologi, raja grafindopersada, Jakarta.

Widodo, 2011, Aspek Hukum KejahatanMayantara, Aswindo, Yogyakarta.

Widyopramono Hadi Widjojo, 2005, Cybercrimes dan Pencegahannya, Jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia.

Michael Enrick, Pembobolan ATM Menggunakan Teknik *Skimming* Kaitannya Dengan Pengajuan Restitusi, Universitas Airlangga, Juris-Diction Vol.2 No. 2, Maret 2019

https://regional.kompas.com/read/2019/10/09/14193581/jadi-pelaku-*skimming*-nasabah-bank-bni-2-wn-rumania-ditangkap.

https://tekno.tempo.co/read/1070680/teknologi-kejahatan-*skimming*-perbankan-berevolusi-sejak-2002/full&view=ok