Bhirawa Law Journal
Volume 2, Issue 2, November 2021
ISSN ONLINE; 2775-2070, ISSN CETAK; 2775-4464
Journal homepage: http://jurnal.unmer.ac.id/index.php/blj/

Tindak Pidana Turut Serta Mengakses Komputer dan/atau Sistem Elektronik dengan Modus Skimming

Hatarto Pakpahan, Ahmad Aryo

Fakultas Hukum Universitas Merdeka Malang
Jl. Terusan Raya Dieng Nomor 62-64; Malang; 65146; JawaTimur; Indonesia.

Abstrak

Penulisan Artikel ini bertujuan untuk mengetahui dan menganlisis tentang bagaimana modus operandi dari skimming dan juga untuk mengetahui pertimbangan dan ketentuan peraturan perundang-undangan yang diterapkan kepada pelaku kejahatan. Skimming disertai dengan analisis yuridisnya dalam perkara Nomor 334/Pid.Sus/2020/PN.Mlg. Dalam artikel jurnal ini menggunakan penelitian hukum normatif dengan pendekatan *caseapproach* dan *statue approach*. Hasil penelitian ini memberikan pengetahuan mengenai modus operandi skimming yang dalam pelaksanaannya menggunakan router dan/atau alat skimmer yang dapat menyalin data kartu ATM atau sekaligus PIN ATM serta menggunakan hidden kamera untuk mendapatkan PIN ATM. Setelah mendapat data dan PIN ATM, kemudian disalin menggunakan MSR900SEN untuk mengkloning ATM tersebut guna melakukan penarikan uang tunai. Sedangkan pertimbangan hakim pada putusan No.334/Pid. Sus/2020/PN.Mlg dakwaan Pasal 30 ayat 3 UU ITE terdapat upaya atau cara yang sesuai dengan skimming yaitu melanggar, menerobos, melampaui, atau memasuki sistem pengamanan dengan cara ilegal dan dalam dakwaan pasal 30 ayat 1 UU ITE tidak merinci mengenai upaya atau cara dalam melakukan perbuatan kejahatan skimming serta untuk mengetahui perbuatan para pelaku termasuk tindak pidana turut serta uitlokker yang mana terdapat pembuat penganjur yang menganjurkan orang yang dianjurkan agar niat dari orang tersebut terbentuk untuk melakukan perbuatan tindak pidana dimana pembuat penganjur tidak berperan aktif dalam perbuatan tindak pidana.

Kata kunci:

Tindak Pidana, Turut Serta, Skimming

Abstract

The writing of this article aims to find out and analyze how the modus operandi of skimming is and also to find out the considerations and provisions of the laws and regulations applied to criminals. Skimming is accompanied by a juridical analysis in case Number 334/Pid.Sus/2020/PN.Mlg. In this journal article, normative legal research uses a case-approach and statue approach. The results of this study provide knowledge about the modus operandi of skimming which in its implementation uses a router and/or skimmer that can copy ATM card data or ATM PIN at the same time and use a hidden camera to get an ATM PIN. After getting the data and ATM PIN, then copy it using MSR900SEN to clone the ATM to make cash withdrawals. While the judge's consideration of the decision No. 334/Pid.Sus/2020/PN.Mlg

Keywords:

Crime, Participation, Skimming

indictment of Article 30 paragraph 3 of the ITE Law there are efforts or methods that are in accordance with skimming, namely violating, breaking through, exceeding, or entering the security system by illegal means and in the indictment. Article 30 paragraph 1 of the ITE Law does not specify the efforts or methods of committing the crime of skimming and to find out the actions of the perpetrators including the crime of participating in uitlokker where there are advocates who recommend people who are recommended so that the intention of that person is formed to commit criminal acts. where the proponent does not play an active role in the criminal act.

Koresponden Penulis;
Hatarto Pakpahan
Email; hatarato.pakpahan@unmer.ac.id

1. Latar Belakang

Seiring meningkatnya persaingan di industri perbankan kebutuhan transaksi masyarakat semakin meningkat, dalam hal itu perbankan mengeluarkan berbagai produk untuk menunjang kenyamanan, keamanan dan akses yang cepat saat nasabah bertransaksi. Diawali dengan munculnya ATM (Anjungan Transaksi Mandiri) yang memudahkan masyarakat saat bertransaksi tanpa melalui kantor bank tertentu sehingga masyarakat tidak perlu menunggu lama saat melakukan proses transaksi. Kemudian dengan adanya teknologi informasi (Internet) industri perbankan melakukan inovasi dengan mengeluarkan produk baru untuk memudahkan mayarakat dalam bertransaksi. Produk tersebut yaitu *E-banking (electronic banking)*, produk perbankan tersebut menggunakan basis teknologi informasi (*Internet*) untuk mempermudah melakukan transaksi. Perkembangan teknologi ini memberikan pengaruh peningkatan di berbagai aspek antara lain aspek sosial, ekonomi, budaya serta aspek politik. Seiring majunya perkembangan teknologi ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai tindak pidana (Dian Alan Setiawan, 2018).

Salah satu perbuatan tindak pidana yang sering dilakukan untuk memperlancar aksinya dalam melakukan tindak pidana adalah tindak pidana penyertaan (Agusman, 2018). Tindak pidana penyertaan atau turut serta adalah tindak pidana yang dilakukan lebih dari satu orang yang melakukan kerja sama untuk memperlancar aksinya dalam melakukan perbuatan tindak pidana. Tindak pidana penyertaan diatur di dalam pasal 55 KUHP (Kitab Undang-Undang Kitab Hukum Pidana) yang mengklasifikasikan menjadi 4 bagian yaitu *pleger, doenpleger, medepleger* dan *uitlokker* serta pembantuan yang diatur di dalam pasal 56 KUHP. Dalam tindak pidana ini keterlibatan orang lain harus dicari pertanggungjawaban masing-masing sebab tiap orang yang terlibat di dalam tindak pidana turut serta memiliki peranannya masing-masing (Fahrurrozi, 2018).

Dengan perkembangan teknologi yang semakin cepat, kejahatan *cyber crime* di indonesia memberikan pengaruh terhadap hukum yang mengatur mengenai hal tersebut, contohnya modus operandi skimming yang dilihat dari tindak kejahatannya. Dalam pelaksanaan kejahatan dengan modus operandi skimming, hal tersebut tidaklah mudah dan memerlukan keahlian khusus dibidang tersebut sehingga tidak dapat dilakukan oleh sembarang orang. Skimming adalah tindakan pencurian dengan menyalin data dari kartu debit atau kredit dengan cara mengambil informasi di bagian strip hitam dibelakang kartu ATM *(magneticstripe)* secara illegal (Destya Fidela Pratiwi, 2019).

Kasus kejahatan skimming di Indonesia semakin banyak terjadi, salah satu sebagaimana yang terjadi di Kota Malang dengan berdasarkan Putusan Pengadilan Negeri Malang No :334/ Pid.sus/2020/PN Mlg, dimana Bank Negara Indonesia (BNI) mengalami kerugian sekitar Rp. 588.432.026,- (Lima Ratus Delapan Puluh Delapan Juta empat ratus Tiga Puluh Dua Ribu Dua Puluh Enam Rupiah) akibat tindak kejahatan skimming yang dilakukan oleh para pelakunya : Rizal Yanuar, Dani Mahendra, Predi Suryadi dan Krishna. Oleh karena perbuatan tersebut, para pelaku terbukti memenuhi unsur pasal 46 ayat 3 jo. pasal 30 ayat 3 Undang-undang No.19 tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik jo. Pasal 55 ayat ke-1 KUHP jo. Pasal 64 ayat 1 KUHP.

Dalam artikel ini akan mencoba menjelaskan terkait Modus operandi tindak pidana turut serta mengakses komputer dan/atau sistem komputer dengan modus skimming dan juga Analisis yuridis tindak pidana turut serta mengakses komputer dan/atau sistem komputer dengan modus skimming dalam perkara Nomor 334/Pid. Sus/2020/PN.Mlg.

2. Metode

Metode penulisan di dalam penelitian ini bersifat normatif. penelitian hukum normatif yang dimaksud adalah adalah penelitian hukum yang menganalisis norma-norma hukum serta kaidah-kaidah hukum positif yang berlaku. Metode ini digunakan untuk memecahkan permasalahan hukum secara teoritis dengan menganalisa dan mengkaji peraturan perundang undangan dalam hal ini UU Informasi dan Transaksi Elektronik (ITE) dalam hal penerapan hukumnya dalam sebuah kasus kongkrit yaitu dalam Putusan Perkara Nomor 334/PID.SUS/2020/PN. Mlg. Lebih lanjut dalam penulisan ini menggunakan pendekatan *caseapproach* dan *statue approach* (Peter, 2016).

3. Pembahasan

3.1 Modus Operandi Tindak Pidana Turut Serta Mengakses Komputer Dan/ Atau Sistem Elekronik Dengan Modus *Skimming*

Dalam pelaksanaan Tindak pidana skimming ini dilakukan dengan berbagai macam cara. Ada yang menggunakan alat khusus yang berupa perangkat kecil (skimmer) yang dipasang di mulut mesin ATM. Skimmer memiliki fungsi untuk meyimpan data dan dapat disalin serta dipindahkan ke tempat peyimpanan data yang lain. untuk alat skimmer yang canggih juga dapat menyalin data dari kartu ATM dan nomor PIN ATM korban sekaligus yang dapat menyalin data dan/atau PIN kartu debit atau kredit sekaligus.

Adapun cara lain untuk melakukan skimming yaitu dengan cara memasang router ke mesin ATM dengan kabel sehingga dapat tersambung dengan sistem jaringan ATM yang bertujuan untuk mendapatkan data dari nasabah-nasabah bank, kemudian memasang kamera tersembunyi di cover pinpad yang bertujuan untuk menggambil gambar dari PIN yang diketik oleh nasabah. Setelah mendapat data dan PIN ATM, kemudian data dan PIN ATM tersebut dikloning atau disalin kedalam kartu kosong *(blank card)* yang bertujuan agar dapat melakukan tarik uang tunai yang telah didapatkan dimanapun dan kapanpun. Cara ini sering dilakukan oleh pelaku kejahatan skimming yang melakukan kejahatannya di Indonesia.

Dalam perkara Nomor : 334/Pid.Sus/2020/ PN.Mlg. Kejahatan skimming ini dilakukan oleh 4 pelaku yaitu : Rizal Yanuar, Dani Mahendra dan Predi Suryadi dengan status Terpidana sedangkan Krishna dengan status DPO. Pada awalnya Predi Suryadi diminta oleh Krishna (DPO) untuk mencari orang yang bisa mengkloning kartu ATM, kemudian Predi Suryadi ingat temannya yang bisa mengkloning kartu ATM yaitu Rizal Yanuar. Pada pertengahan tahun 2019 Rizal Yanuar diperkenalkan oleh Predi Suryadi kepada Krishna.

setelah berkenalan dengan Krishna melalui media sosial *facebook* kemudian Rizal Yanuar menerima data berupa *soft file* data, nomor kartu kredit dan atau debit beserta PIN serta kartu kredit dan/atau debit dalam bentuk fisik dari berbagai jenis bank untuk dilakukan kloning yang dikirim melalui paket dari Sdr. Krishna sebanyak lebih dari 50 (lima puluh) kartu yaitu antara lain Rekening Bank BNI Taplus Nomor :00067254482 atas nama Ristiono**.** Dari data kartu ATM dan PIN tersebut terdapat indikasi bahwa data kartu ATM dan PIN tersebut didapat dari pemasangan alat *skimmer* dan *hidden camera* pada tanggal 28-29 Februari 2020 di ATM BNI yang terletak di Jl. Raya Taman Pinang Indah No. 1 Sidoarjo (Top Swalayan) berdasarkan rekaman *CCTV* dan keterangan dari saksi Darwoto yang meminta *EJ* (*Elektronik Jurnal*) kepada ATR (ATM Regional wilayah Surabaya).

Kemudian Rizal Yanuar di Dei Kost Jl. Ahmad Yani Nomor 10 Polowijen Kecamatan Blimbing Kota Malang, menyiapkan perangkat laptop aplikasi *MSR900S EN* serta alat *skimmer type seri model SLA3-00008* bewarna hitam yang dibeli oleh Dani Mahendra dihubungkan ke perangkat laptop merk *HP* warna abu-abu hitam yang sudah terpasang aplikasi *MSR900S EN*. Setelah alat skimmer tersebut terpasang, terhubung dan membuka aplikasi *MSR900S EN*, kemudian Terdakwa I menginput nomor kartu debit ke dalam kolom "*Track2 75 BPI 5 BPC Odd Parity*" lalu tekan *write,* selanjutnya terdakwa menggesekan kartu debit tersebut ke dalam mesin *MSR* sesuai arah tanda yang terdapat di mesin tersebut. Setelah fisik kartu tersebut digesek, lalu Rizal Yanuar menuju ATM untuk melakukan transaksi cek saldo Rekening Bank BNI Taplus Nomor : 00067254482 atas nama Ristiono dengan saldo sejumlah Rp. 588.432.026,- (lima ratus delapan puluh delapan juta empat ratus tiga puluh dua ribu dua puluh enam rupiah) ;

Setelah mengetahui isi saldo Rekening Bank BNI Taplus Nomor : 00067254482 atas nama Ristionolalu terdakwa I Rizal Yanuar melakukan transaksi sebanyak 39 (tiga puluh Sembilan) kali yaitu 28 kali tarik tunai, 7 kali transfer dan 4 kali transaksi belanja. Selanjutnya uang tunai yang Rizal Yanuar tarik tunai tersebut, Rizal Yanuar kumpulkan dan diserahkan kepada Dani Mahendra kemudian di transfer ke Krishna dan Dani Mahendra mentransfer ke Rekening milik Predi Suryadi Nomor : 1560015872098 atas nama Predi Suryadi sesuai permintaan Krishna selanjutnya Predi Suryadi metransfer uang tersebut ke Indodax.com dengan user saitamakun dan password samuraix10@yahoo untuk pembelian *Bitcoin*. Bahwa dari perbuatan membobol sistem keamanan kartu ATM maka Rizal Yanuar mendapatkan keuntungan sebesar Rp. 7.000.000,- s/d Rp. 10.000.000,-, untuk terdakwa II Dani Mahendra mendapatkan keuntungan Rp. 1.000.000,- dan terdakwa III Predi Suryadi mendapat keuntungan Rp. 1.700.000,-

3.2 Analisis Yuridis Tindak Pidana Turut Serta Mengakses Komputer dan/ atau Sistem Elektronik dengan Modus Skimming (Putusan No. 334/Pid.Sus/2020/Pn.Mlg)

Skimming merupakan pencurian data bank dengan cara menyalin data pada *magnetic stripe* pada bagian belakang kartu ATM yang merugikan pemilik data bank dan / atau bank. Jerat pidana bagi pelaku Skimming sendiri diatur di dalam pasal 30 UU ITE. Dalam perkara aquo telah diajukan dakwaan pertama oleh JPU Pasal 46 ayat (3) jo. Pasal 30 ayat (3) UU No. 19 Tahun tentang Perubahan atas UU No. 11 Tahun 2008 ITE jo. Pasal 55 ayat (1) ke-1 KUHP jo. Pasal 64 ayat (1) KUHP dan dakwaan kedua Pasal 46 ayat (1) jo. Pasal 30 ayat (1) UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang ITE jo. Pasal 55 ayat (1) ke-1 KUHP jo. Pasal 64 ayat (1) KUHP.

Frasa "setiap orang" berarti seseorang atau sekumpulan orang yang bertindak atas dirinya dan seseorang atau sekumpulan orang yang bertindak

atas nama badan hukum. Maksud dengan sengaja ini berarti mengetahui dan menghendaki suatu perbuatan yang dilarang dan akibat yang timbul dari perbuatan yang dilarang. Apabila dilihat dari pembahasan ini, dengan sengaja ini bermakna mengetahui dan menghendaki perbuatan mengakses komputer dan/atau sistem elektronik. Setiap orang memiliki hak untuk mengakses komputer dan/atau sistem elektronik. Definisi hak adalah segala sesuatu yang harus didapatkan oleh setiap individu yang telah ada sejak masih dalam kandungan (Serafica Gischa, 2021). hak sendiri pada dasarnya merupakan kewenangan dan kekuasaan seseorang yang diterima dan dinikmati sehingga setiap orang berhak menerima hak-hak yang dimilikinya serta tidak boleh melanggar hak-hak yang dimiliki oleh orang lain. dari hal tersebut yang dapat diartikan bahwa setiap orang memiliki hak atau kewenangan dalam mengakses komputer dan/atau sistem elektronik untuk mengontrol, meyimpan, mengeluarkan, mengolah, menganalisis, mengirim, mengumumkan data elektronik yang dimilikinya. Adapun yang dapat mengakses komputer dan/sistem elektronik milik orang lain apabila orang tersebut telah mendapatkan persetujuan atau izin dari orang yang memiliki data elektronik tersebut.

Dalam hak atau kewenangan setiap orang untuk mengakses komputer dan/atau sistem elektronik, ada pula perbuatan dengan sengaja tanpa hak mengakses komputer dan/atau sistem elektronik dengan cara apapun, berarti perbuatan tanpa hak tersebut perbuatannya tidak memiliki kewenangan dalam melaksanakan perbuatannya yang bertentangan dengan hak orang lain dan melanggar peraturan perundang-undangan. Perbuatan dengan sengaja tanpa hak mengakses komputer dan/atau sistem elektronik dengan cara apapun merupakan perbuatan melawan hukum sebab perbuatan tersebut secara jelas dilarang sebagaimana diatur dalam peraturan perundang-undangan, kemudian perbuatan itu juga dilakukan tanpa kewenangan dan kekuasaan serta perbuatan yang melanggar norma-norma yang ada di dalam masyarakat (Hukum tidak tertulis).

Mengakses berasal dari kata akses yang berarti interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan. Apabila ditinjau dari frasa "mengakses komputer dan/ atau sistem elektronik" maka tindakan yang menggunakan komputer ke sistem elektronik untuk mengola data elektronik.

Kejahatan *Skimming* merupakan perbuatan dengan sengaja tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun. Dalam putusan No.334/ Pid.Sus/2020/PN.Mlg, dakwaan kesatu terdapat frasa "milik orang lain" dalam hal ini berarti suatu kepunyaan seseorang atau sekumpulan orang yang bertindak atas dirinya dan seseorang atau sekumpulan orang yang bertindak atas nama badan hukum. Di dalam dakwaan kesatu pasal 30 ayat (3) UU ITE terdapat frasa "dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan." Melanggar ini berarti melanggar hak-hak privasi yang dimiliki orang lain dalam mengakses komputer dan/atau sistem elektronik. Menerobos ini berarti menembus kedalam hak akses orang lain atau memaksa masuk hak-hak akses milik orang lain seperti menggunakan berbagai teknologi khusus dalam pelaksanaan perbuatannya. Melampaui ini berarti melewati batas-batas kekuasaan/kewenangan dalam menggunakan hak akses dalam menggunakan komputer dan/atau sistem elektronik. Kemudian menjebol sistem keamanan berarti merusak secara paksa sekumpulan elemen atau unsur yang memiliki fungsi untuk melindungi suatu data elektronik.

Perbedaan pasal 30 ayat 1 dan 30 ayat 3 ini yaitu bahwa didalam pasal 30 ayat 1 tidak dijelaskan lebih lanjut mengenai upaya-upaya atau cara dalam melakukan perbuatan tindak pidana sedangkan dalam pasal 30 ayat 3 dijelaskan mengenai upaya-upaya atau cara

dalam melaksanakan perbuatan tindak pidana (Andi, 2010). Dalam melakukan kejahatan untuk memperlancar pelaksanaannya, pelaku tindak pidana melibatkan orang lain atau lebih dari satu orang dalam melakukan perbuatan tindak pidananya. perbuatan tersebut disebut turut serta sebagaimana diatur didalam pasal 55 KUHP (Kitab Undang-udang Hukum Pidana) (Teguh, 2016).

Dalam kasus *skimming* pada Putusan No.334/ Pid.Sus/2020/PN.Mlg, Predi Suryadi diminta oleh Krishna (DPO) untuk mencari orang yang bisa menkloning ATM kemudian Predi Suryadi memperkenalkan Rizal Yanuar kepada Krishna. Rizal Yanuar berkenalan dengan Krishna melalui media sosial facebook kemudian terdakwa I Rizal Yanuar menerima kiriman data berupa *soft file* data, nomor kartu kredit dan atau debit beserta PIN serta kartu kredit dan/atau debit dalam bentuk fisik dari berbagai jenis bank untuk dilakukan kloning yang dikirim melalui paket dari Krishna sebanyak lebih dari 50 (lima puluh) kartu yaitu antara lain Rekening Bank BNI Taplus Nomor :00067254482 atas nama Ristiono.

Rizal Yanuar di Dei Kost Jl. Ahmad Yani Nomor10 Polowijen Kecamatan Blimbing Kota Malang, menyiapkan perangkat laptop aplikasi *MSR900S EN* serta alat skimmer *type seri model SLA300008* bewarna hitam yang dibeli oleh Dani Mahendra dihubungkan ke perangkat laptop merk *HP* warna abu-abu hitam yang sudah terpasang aplikasi *MSR900SEN*. Setelah alat skimmer tersebut terpasang, terhubung dan membuka aplikasi *MSR900S EN*, kemudian menginput nomor kartu debit ke dalam kolom "*Track2 75 BPI 5 BPC Odd Parity*" lalu tekan *Write*, selanjutnya Rizal Yanuar menggesekan kartu debit tersebut ke dalam mesin *MSR* sesuai arah tanda yang terdapat di mesin tersebut. Setelah fisik kartu tersebut digesek, lalu Rizal Yanuar menuju ATM untuk melakukan transaksi cek saldo Rekening BankBNI Taplus Nomor : 00067254482 atas nama Ristiono dengan saldosejumlah Rp. 588.432.026,- (lima ratus delapan puluh delapan juta empat ratustiga puluh dua ribu dua puluh enam rupiah);

Setelah mengetahui isi saldo atas nama Ristionolalu Rizal Yanuar melakukan transaksi sebanyak 39 (tiga puluh Sembilan) kali yaitu 28 kali tarik tunai, 7 kalitransfer dan 4 kali transaksi belanja yang dilakukan mulai tanggal 5 Maret 2020 sampai 9 Maret 2020. Setelah melakukan penarikan uang tunai, Rizal Yanuar kumpulkan dan diserahkan kepada Dani Mahendra kemudian ditransfer ke Krishna dan Dani Mahendra mentransfer ke rekening milik Predi Suryadi Nomor 1560015872098 atas nama Predi Suryadi sesuai permintaan Krishna selanjutnya Predi Suryadi mentransfer uang tersebut ke indodax. com dengan user saitamakun dan password samuraix10@yahoo untuk pembelian bitcoin.

Berdasarkan keterangan tersebut bahwa tindakan yang dilakukan oleh pelaku termasuk dalam tindak pidana turut serta Orang yang sengaja menganjurkan (*uitlokker).* Krishna bertindak sebagai *auctor intellectualis* atau pembuat penganjur) yaitu orang yang menganjurkan atau membujuk untuk melakukan sesuatu. pembuat penganjur tidak melakukan tindak pidananya secara aktif hanya menganjurkan atau membujuk orang lain untuk mewujudkan tindak pidananya dengan pemberian imbalan berupa uang untuk menentukan kehendak dari para pelaku.

Pelaku lainnya yaitu Rizal Yanuar, Dani Mahendra, Predi Suryadi merupakan Orang yang dianjurkan atau dibujuk disebut juga (*auctor materialis* atau *materiele dader*) kehendak dari para pelaku ini terbentuk dengan upaya yang dilakukan oleh Krishna dengan cara memberikan janji berupa uang apabila telah melakukan apa yang diperintah oleh Krishna. Rizal Yanuar, Dani Mahendra, Predi Suryadi termasuk kedalam tindak pidana turut serta menganjurkan sebab kehendak dari pelaku tersebut terbentuk oleh anjuran dari Krishna serta perbuatannya tersebut mengikuti instruksi dari Krishna yang mana Rizal Yanuar, Dani Mahendra, Predi Suryadi melakukan perbuatan tindak

pidana skimming tersebut dilakukan secara aktif yang bertujuan agar memperlancar terwujudnya perbuatan *skimming* tersebut.

Berdasarkan pertimbangan hakim tersebut menjelaskan bahwa hakim menjatuhkan amar putusan sebagai berikut : Memperhatikan, Pasal46 ayat (3) jo. Pasal 30 ayat (3) UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik jo. Pasal 55 ayat (1) ke-1 KUHP Jo. Pasal 64 ayat (1) KUHP, Surat Dirjen Badilum MARI Nomor : 379/DJU/PS.00/3/2020 tanggal 27 Maret 2020 tentang Persidangan Perkara Pidana Secara *Teleconference* dan Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana serta peraturan perundang-undangan lain yang bersangkutan; Mengadili Menyatakan terdakwa I Rizal Yanuar, terdakwa II Dani Mahendra dan terdakwa III Predi Suryadi, telah terbukti secara sah dan menyakinkan bersalah melakukan tindak pidana "turut serta melakukan perbuatan mengakses komputer dan/atau sistem elektronik dengan cara menjebol sistem pengamanan yang dipandang sebagai satu perbuatan berlanjut" dengan menjatuhkan pidana terhadap terdakwa I Rizal Yanuar, terdakwa II Dani Mahendra dan terdakwa III Predi Suryadi**,** oleh karena itu dengan pidana penjara masing-masing selama 1 (satu) tahun dan denda sebesar Rp5.000.000,00 (lima juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar maka diganti pidana kurungan selama 2 (dua) bulan;

Berdasarkan pertimbangan hakim bahwa perbuatan yang dilakukan oleh para pelaku merupakan perbuatan yang telah memenuhi pasal 30 ayat 3 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan" Sebab didalam pasal Tersebut upaya atau cara dalam melakukan perbuatan kejahatan telah sesuai dengan kejahatan skimming yaitu melanggar, menerobos, melampaui, atau menjebol sistem pengamanan sedangkan dalam pasal 30 ayat 1 tidak merinci mengenai upaya atau cara dalam melakukan perbuatan kejahatan skimming.

Para pelaku tersebut juga telah memenuhi unsur tindak pidana turut serta Uitlokker yang mana terdapat auctor intelectuallis/ pembuat penganjur yang menganjurkan atau membujuk auctor materialis /orang yang dianjurkan agar kehendak atau niat dari orang tersebut terbentuk untuk melakukan perbuatan tindak pidana dimana pembuat penganjur tidak berperan aktif dalam perbuatan tindak pidana (Adami, 2005).

4. Simpulan

Modus operandi atau cara pelaksanaan perbuatan skimming bervariasi ada yang menggunakan alat skimmer yang dapat menyalin data kartu ATM atau sekaligus data dan PIN ATM , ada pula yang menggunakan *router* yang dihubungkan dengan kabel LAN ke laptop untuk menyalin data dan menggunakan *hidden camera* untuk PIN ATM. Pada kasus skimming dalam Putusan No. 334/Pid.Sus/2020/PN.Mlg, setelah para pelaku mendapat data serta PIN ATM kemudian disalin menggunakan aplikasi *MSR900SEN*serta alat *skimmer type seri model SLA3-00008* bewarna hitam untuk mengkloning ATM tersebut guna melakukan penarikan uang tunai.

Analisis terhadap pertimbangan hakim tentang perbuatan yang dilakukan oleh para pelaku merupakan perbuatan yang telah memenuhi pasal 30 ayat 3, sebab didalam pasal tersebut upaya atau cara dalam melakukan perbuatan kejahatan telah sesuai dengan kejahatan skimming yaitu melanggar, menerobos, melampaui, atau memasuki sistem pengamanan secara ilegal sedangkan dalam pasal 30 ayat 1 tidak merinci mengenai upaya atau cara dalam melakukan perbuatan kejahatan skimming. Para

pelaku tersebut juga telah memenuhi unsur tindak pidana turut serta *uitlokker* yang mana terdapat *auctor intelectuallis* atau pembuat penganjur yang menganjurkan atau membujuk *auctor materialis* atau orang yang dianjurkan agar kehendak atau niat dari orang tersebut terbentuk untuk melakukan perbuatan tindak pidana dimana pembuat penganjur tidak berperan aktif dalam perbuatan tindak pidana.

Daftar Pustaka

Dian Alan Setiawan, The Implication of Pancasila Values on the Renewal of Criminal Law in Indonesia, //journal.uniku.ac.id/index.php/unifikasi, Volume 5 No 2 Tahun 2018

Destya Fudela Pratiwi, Pertanggungjawaban Tindak Pidana Skimming, Juris-diction Law Journal, Volume 2 No 4 tahun 2019

Serafica Ghisca, Pola Kominikasi Humas BNNP Riau Dan LSM Dalam Mensosialisasikan Bahaya Narkoba, Jurnal Riset Mahasiswa Dakwah dan Komunikasi, Volume 3 No 1 Tahun 2021

Agusman Heri, "ANALISIS YURIDIS TERHADAP TINDAK PIDANA PENYERTAAN PEMBUNUHAN (Studi Putusan MA Nomor 2462/Pid.B/2017/PN Medan 2018)", Jurnal Abdi Ilmu, Volume 1 No. 2, Desember 2018.

Fahrurrozi, "Sistem Pemidanaan Dalam Penyertaan Tindak Pidana Menurut KUHP", Media Keadilan. Volume 10 Nomor 1, April 2019.

Peter Mahmud Marzuki, *Penelitian Hukum*, Cetakan kedua belas, Kencana Prenadamedia Group, Jakarta, 2016.

Andi Hamzah, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta, 2010.

Teguh Prasetyo, *Hukum Pidana Edisi Revisi*, Rajawali Pers, Jakarta, 2016.

Adami Chazawi, *Pelajaran Hukum Pidana 3 : Percobaan & Penyertaan*, PT RajaGrafindo Persada, Jakarta, 2005.