# Tindak Pidana Terkait Akses Akun *Mobile Banking* dengan Mengaktifkan Kembali *Simcard* yang Sudah Tidak Aktif

Rengga Aditya Mulawardhana (a), Go Lisanawati (b)

(a) Fakultas Hukum Universitas Surabaya, renggaaditya124@gmail.com
(b) Fakultas Hukum Universitas Surabaya, go_lisanawati@staff.ubaya.ac.id

***Abstract***

*Criminal activities related to the use of the internet (cybercrime) are growing rapidly in Indonesia with various modes. This article aims to analyze one of the cases that has occurred regarding illegal access to fund transfers based on normative juridical methods. The action being studied was access to a mobile bank account using an inactive card to transfer funds. Based on this mode, two violations occurred in 2 (two) laws as well as Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 3 of 2011 concerning Fund Transfers. The result of this research is that perpetrators with mobile banking account access mode by using an inactive card and transferring funds can fulfill the criminal elements according to the provisions of Article 30 paragraph (3) of Law Number 11 of 2008 concerning Electronic Information and Transactions, and can subject to criminal penalties according to Article 46 paragraph (3) of Law Number 11 of 2008 concerning Electronic Information and Transactions, and also fulfills criminal elements according to the criminal provisions of Article 81 of Law Number 3 of 2011 concerning Fund Transfers.*

***Keywords:*** *cybercrime; illegal access; fund transfer.*

**Abstrak**

Kegiatan kriminal terkait penggunaan internet (kejahatan siber) berkembang pesat di Indonesia dengan beragam modus. Artikel ini bertujuan menganalisis salah satu kasus yang telah terjadi terkait perbuatan akses ilegal untuk tranfer dana berdasarkan metode yuridis normatif. Perbuatan yang dikaji yakni akses ke rekening bank seluler menggunakan kartu yang tidak aktif untuk melakukan transfer dana. Berdasarkan modus ini, maka terjadi dua pelanggaran pada 2 (dua) peraturan perundang-undangan sekaligus Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana. Hasil penelitian ini adalah pelaku dengan modus akses rekening mobile banking dengan menggunakan kartu yang tidak aktif dan melakukan transfer dana dapat memenuhi unsur-unsur pidana menurut ketentuan Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta dapat dikenakan pidana menurut Pasal 46 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan juga memenuhi unsur-unsur pidana menurut ketentuan pidana Pasal 81 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana.

**Kata kunci:** kejahatan siber; akses ilegal; transfer dana.

**Jurnal**
**YUSTIKA**
**Media Hukum dan Keadilan**
Fakultas Hukum Universitas Surabaya
Vol. 23 No. 02, Desember 2020
P-ISSN: 1410-7724
E-ISSN: 2655-7479

## 1. Pendahuluan

Penggunaan hukum pidana untuk penanggulangan kejahatan perlu memperhatikan fungsi hukum pidana yang subsider, yaitu hukum pidana baru digunakan apabila upaya-upaya

lainnya diperkirakan kurang memberi hasil yang memuaskan atau kurang sesuai. Akan tetapi kalau hukum pidana akan tetap dilibatkan, maka hendaknya dilihat dalam hubungan keseluruhan politik kriminal atau istilah yang lazim digunakan dalam kongres PBB IV 1970 adalah *planning for social defence* yang harus merupakan bagian yang integral dari rencana pembangunan nasional (Supanto, 2016). Perkembangan teknologi komunikasi dan informasi juga mengubah cara berpikir, cara bertindak, dan cara bersikap masyarakat. Perkembangan-perkembangan tersebut telah terbukti membawa dampak positif bagi kehidupan manusia, tetapi tidak terlepas juga dari dampak negatif akibat suatu perkembangan tersebut. Karena hal demikian pada kenyataannya membuat kreativitas masyarakat untuk melakukan kejahatan juga semakin berkembang seiring dengan perkembangan zaman termasuk di dalamnya perkembangan teknologi komunikasi dan informasi. Perkembangan teknologi informasi dan komunikasi membawa pengaruh positif dan negatif, ibarat pedang bermata dua. Pemanfaatan teknologi informasi dan komunikasi di satu pihak memberikan kontribusi bagi peningkatan kesejahteraan dan peradaban manusia.

Di lain pihak kemajuan teknologi Informasi dan Transaksi Elektronik selanjutnya disebut ITE tersebut dapat dimanfaatkan untuk melakukan perbuatan-perbuatan yang bersifat melawan hukum, yang menyerang berbagai kepentingan hukum orang, masyarakat, dan negara (Adami dan Ardi, 2015). Meskipun perkembangan teknologi informasi sangat pesat, namun perkembangan yang ada tidak selamanya digunakan untuk kepentingan yang positif, namun juga sering disalahgunakan untuk hal-hal yang negatif. Sejatinya, perkembangan teknologi informasi berbasis komputer yang terhubung melalui jaringan internet sering dijadikan sebagai sarana serta media untuk melakukan kejahatan (Samudra and Julius, 2017). Misalnya melakukan pencemaran nama baik terhadap seseorang atau mungkin juga transaksi bisnis prostitusi online yang sekarang marak diberitakan (Nani Widya Sari, 2018). Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya disebut UUD NRI 1945) menentukan bahwa "Negara Indonesia adalah negara hukum". Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP), menyatakan bahwa "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada, sebelum perbuatan dilakukan". Pasal 1 ayat (1) KUHP tersebut juga dikenal dengan asas legalitas. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik bersamaan dengan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, selanjutnya disebut UU ITE, merupakan peraturan perundang-undangan mengenai pengelolaan informasi dan transaksi elektronik yang berlaku saat ini di Indonesia.

Modus dan motif *cybercrime* semakin kompleks maka dari itu tidak ada jaminan keamanan dalam *cyberspace*, dan tidak ada sistem keamanan komputer yang mana para *hacker* akan terus mencoba untuk menaklukkan sistem keamanan yang paling canggih, dan merupakan kepuasan tersendiri bagi *hacker* jika dapat membobol sistem keamanan komputer orang lain (Ervina Chintia, 2018). Muhammad Khairul Faridi (2018) dalam kejahatan siber terdapat dua tipe kejahatan. Tipe yang pertama adalah kejahatan di mana komputer menjadi target aktivitas kriminal, sedangkan Tipe yang kedua adalah kejahatan yang menggunakan komputer sebagai alatnya. Dari kedua jenis tindak kejahatan di atas, tindak kejahatan yang paling sering terjadi pada perbankan antaranya *skimming, hacking dan malware*. Target utama tindak kejahatan ini adalah nasabah yang menggunakan akses internet dalam melakukan transaksi. Berikut ini adalah survei yang dilakukan oleh APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mengenai

Jurnal Yustika
Vol. 23 No. 02, Des 2020



Rengga Aditya M.
Go Lisanawati

perilaku pengguna internet dalam bertransaksi secara online. Teknologi informasi menjadi sarana efektif perbuatan melawan hukum, salah satu contohnya adalah akses ilegal. Aris Hardinanto (2019) menjelaskan bahwa akses ilegal merupakan salah satu tindak pidana yang sering menduduki peringkat pertama dalam pembahasan atau kongres internasional, salah satu contohnya adalah Kongres Perserikatan Bangsa-Bangsa ke X di Wina yang menempatkan akses ilegal menjadi sorotan utama dalam pembahasan. Di Indonesia akses ilegal sudah diatur sebagai perbuatan yang dilarang dalam Pasal 30 UU ITE. Berdasarkan Pasal 30 UU ITE terdapat tiga jenis kategori perbuatan yang dilarang dengan cara akses ilegal. Aris Hardinanto (2019, hal. 67) menjelaskan mengenai setiap ayat pada Pasal 30 UU ITE bahwa "Pertama adalah akses ilegal secara umum, kedua adalah akses ilegal dengan maksud mendapatkan informasi dan/atau dokumen elektronik, dan yang ketiga adalah akses ilegal dengan cara melumpuhkan sistem pengaman". Mengenai ancaman hukuman pidana bagi para pelaku akses ilegal terdapat pada Pasal 46 UU ITE. Dengan adanya UU ITE, akses ilegal dapat dikenakan sanksi pidana.

Di era modern seperti ini transaksi perbankan bisa dilakukan secara online, salah satunya menggunakan fitur *e-banking*. Salah satunya adalah dengan menggunakan aplikasi *mobile banking*.Pelanggaran terhadap *mobile banking* salah satunya adalah adanya akses ilegal terhadap aplikasi *mobile banking* orang lain dengan modus yang semakin berkembang seperti menggunakan *simcard* yang sudah tidak aktif. Data pribadi yang melekat pada simcard ini diambil pelaku untuk mengendalikan akun mobile banking, mirip seperti skimming, namun berbeda metoda (Samudra and Qisthi, 2018).

Seperti yang sudah diketahui bahwa akses ilegal sudah diatur dalam UU ITE. Ketentuan Pasal 30 ayat (3) UU ITE menenentukan bahwa "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan". Akses ilegal terhadap akun *mobile banking* tentu tidak berhenti hanya terbatas sampai akses ke akun *mobile banking* saja, melainkan juga akan menguasai rekening yang berisikan sejumlah dana di akun *mobile banking* tersebut.Dengan demikian dapat dipastikan, pelaku akan mentransfer dana yang ada dalam akun *mobile banking* yang dikuasainya tersebut.dapat dipahami bahwa pelaku mentransfer dana yang ada dalam akun *mobile banking* tersebut termasuk dalam melalui perintah transfer dana untuk mentransferkan sejumlah dana terhadap rekening pelaku sendiri. Perbuatan semacam ini juga sudah diatur dalam UU Transfer Dana. Ketentuan Pasal 81 UU Transfer Dana menentukan bahwa "Setiap orang yang secara melawan hukum mengambil atau memindahkan sebagian atau seluruh Dana milik orang lain melalui Perintah Transfer Dana palsu dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)".

Salah satu kasus mengenai akses akun *mobile banking* menggunakan *simcard* yang sudah tidak aktif untuk mentransfer danaseperti yang dilansir pada Jawa Pos pada tanggal 9 Agustus 2019 yaitu Kepolisian Daerah Metro Jaya berhasil mengungkap kejahatan dengan modus akses akun *mobile banking* menggunakan *simcard* yang sudah tidak aktif namun masih terhubung dengan aplikasi *mobile banking*. Dua orang diamankan dalam perkara ini yaitu RI dan DV. RI dan DV memiliki peran berbeda-beda. RI berperan sebagai pencari data nasabah yang menjadi target kejahatannya. Setelah itu, RI mencari data nasabah yang mengaktifkan layanan *mobile banking* yang terhubung dengan *simcard*. Lalu RI mengerucutkan pencariannya pada nasabah yang masa berlaku *simcard* nya sudah tidak aktif tetapi masih terhubung dengan layanan *mobile banking*. Setelah itu pelaku akan berusaha mengaktifkan kembali kartu tersebut di gerai provider.

Akhirnya *mobile banking* dalam kartu yang sudah tidak aktif tersebut dapat aktif kembali tetapi masih atas nama korban. Sedangkan DV berperan membuat rekening baru untuk menampung hasil kejahatan terhadap rekening tersebut serta juga mencairkan uang milik korban melalui aplikasi digital *wallet* seperti Sakuku. Kepala Bidang Humas Polda Metro Jaya Kombes. Pol. Argo Yuwono mengatakan bahwa kasus ini terungkap berawal dari adanya korban yang merasa uang di rekeningnya berkurang drastis. Kemudian korban membuat laporan polisi dan menyatakan mengalami kerugian mencapai Rp 1.100.000.000,00,-

RI dan DV mengakses rekening korbannya dengan cara mengaktifkan kembali *simcard* milik korban yang pernah terhubung dengan *mobile banking* namun saat ini sudah tidak aktif. Setelah *simcard* tersebut diaktifkan, RI dan DV kemudian berusaha menerobos masuk ke sistem *mobile banking* korban. Tidak berhenti hanya sampai mengakses rekening *mobile banking* saja, tetapi setelah berhasil masuk ke *mobile banking* korban RI dan DV langsung menguras uang di dalamnya dan kemudian dipindahkan ke rekening yang sudah disiapkan serta mencairkannya melalui aplikasi Sakuku. Dalam upaya mengakses*mobile banking* korbannya, pelaku mencoba menggunakan tanggal lahir korban, dan ternyata berhasil. Oleh karena itu, polisi menghimbau kepada masyarakat supaya tidak menggunakan tanggal lahir sebagai kata sandi dalam perbankan. Lebih lanjut, Argo menyampaikan, kedua pelaku ini ditangkap di daerah Palembang, Sumatera Selatan pada 7 Agustus kemarin. Saat hendak diciduk, RI dan DV bahkan melakukan perlawanan menggunakan senjata api rakitan. (JawaPos.com, 2019).

Modus operandi akses ilegal dengan cara seperti ini terjadi secara *real*, oleh karena itu perlu diadakan penelitian untuk menanggulangi tindak pidana dengan modus operandi semacam itu. Maka dari itu, isu yang dibahas dalam artikel ini adalah: apakah akses akses akun *mobile banking*dengan mengaktifkan kembali *simcard* yang sudah tidak aktif untuk melakukan transfer dana palsu dapat memenuhi ketentuan Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Pasal 81 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana?

## 2. Metode Penelitian

Jenis metode penelitian yang digunakan adalah yuridis-normatif dengan melakukan studi kepustakaan terhadap bahan-bahan hukum baik bahan hukum primer yaitu peraturan perundang-undangan dan bahan hukum sekunder yaitu literatur yang berkaitan dengan topik permasalahan. Metode penelitian yang digunakan terdiri dari berbagai cara dan kegiatan yang dilakukan dalam rangka mengumpulkan data-data dari bahan-bahan hukum yang diperlukan. Pendekatan masalah yang digunakan adalah *statute approach* yakni melakukan pendekatan melalui telaah terhadap undang-undang serta regulasi yang terkait dengan isu hukum yang dibahas serta *conceptual approach* yaitu pendekatan dengan berpedoman pada pandangan serta doktrin para ahli yang berkembang dalam ilmu hukum sedangkan bahan hukum yang digunakan meliputi bahan hukum primer yaitu peraturan perundang-undangan terkait antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, serta bahan hukum sekunder, adalah bahan hukum yang bersumber dari pendapat ilmiah para sarjana dan buku-buku literatur yang berkaitan dengan akses ilegal dan transfer dana.

.

## 3. Hasil Penelitian dan Pembahasan

Indonesia telah menjadi bagian masyarakat dunia globalisasi informasi yang pada akhirnya menerbitkan suatu aturan mengenai hal-hal yang berkaitan dengan teknologi informasi. Aturan tersebut dituangkan dalam bentuk Undang-Undang yaitu dengan disahkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam perkembangannya Undang-Undang tersebut diperbarui dengan dikeluarkannya Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Dengan demikian, UU ITE merupakan peraturan perundang-undangan mengenai pengelolaan informasi dan transaksi elektronik yang berlaku saat ini di Indonesia. Penjelasan mengenai apa yang dimaksud Informasi Elektronik sudah dijelaskan dalam Pasal 1 angka 1 UU ITE bahwa "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."

Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan." Serta sanksi apabila melanggar perbuatan dalam Pasal 30 ayat (3) UU ITE terdapat pada Pasal 46 ayat (3) UU ITE yang menyatakan bahwa: "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah)." Menurut Adami Chazawi dan Ardi Ferdian (2011) Unsur-Unsur Pasal 30 ayat (3) dapat diuraikan sebagai berikut:

1. Setiap orang;
2. Kesalahan: dengan sengaja;
3. Melawan hukum: tanpa hak atau melawan hukum;
4. Perbuatan: mengakses
5. Obyek: Komputer dan/atau Sistem Elektronik;
6. Caranya: Dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Masing-masing unsur tersebut dapat dijelaskan sebagai berikut:

Unsur setiap orang yang dimaksud yaitu orang perorangan, baik Warga Negara Indonesia, Warga Negara Asing, maupun badan hukum tercantum pada Pasal 1 angka 21 UU ITE. Apabila melihat dari modus yang terjadi, unsur ini telah dipenuhi oleh RI dan DV karena RI dan DV adalah orang perorangan serta RI dan DV adalah Warga Negara Indonesia, dan ditangkap oleh pihak kepolisian di tempat tinggalnya yang beralamatkan di daerah Palembang, Sumatera Selatan.

Unsur yang selanjutnya adalah dengan sengaja. Perbuatan RI dan DV termasuk dalam kesengajaan sebagai maksud, dikarenakan RI dan DV telah menghendaki akibat dari perbuatan yang dilakukan dimana akibat dari perbuatannya tersebut dapat dikenakan ancaman pidana.

Unsur yang selanjutnya adalah tanpa hak atau melawan hukum. Menurut Adami Chazawi(2005, hal. 87) bahwa:

Setiap perbuatan yang ditetapkan sebagai dilarang dengan mencantumkannya dalam peraturan perundang-undangan (menjadi tindak pidana), tanpa melihat apakah unsur melawan hukum itu dicantumkan ataukah tidak dalam rumusan, maka pidana itu sudah mempunyai sifat melawan hukum, dalam kata lain melawan hukum adalah unsur mutlak dari tindak pidana.

Menurut Teguh Prasetyo dan Abdul Halim Barkatullah (2005) terdapat dua ajaran sifat melawan hukum yaitu ajaran sifat melawan hukum formal dan ajaran sifat melawan hukum material:

1. Ajaran sifat melawan hukum formal apabila suatu perbuatan telah memenuhi semua unsur yang termuat dalam rumusan tindak pidana, perbuatan tersebut adalah tindak pidana. Ajaran ini berpegang pada asas legalitas bahwa perbuatan yang diancam pidana di dalam undang-undang yang tertulis.
2. Ajaran sifat melawan hukum materiil menyatakan bahwa sifat melawan hukum tidak hanya terdapat di dalam undang-undang (yang tertulis), tetapi harus dilihat berlakunya asas-asas hukum yang tidak tertulis juga. Sifat melawan hukum dapat dihapuskan berdasarkan ketentuan undang-undang atau aturan yang tidak tertulis.

Perbuatan yang dilakukan RI dan DV memenuhi unsur melawan hukum seperti yang dijelaskan oleh Adami Chazawi dan Ardi Ferdian, serta Teguh Prasetyo bahwa perbuatan bertentangan dengan peraturan perundang-undangan karena perbuatan tersebut telah melanggar ketentuan hukum yang berlaku yang ada di dalam UU ITE. Hal tersebut termasuk dalam ajaran sifat melawan hukum formal. Ditunjukkan pada RI dan DV cara mengakses akun *mobile banking* tersebut dengan menerobos sistem pengaman.

Unsur yang selanjutnya adalah mengakses. Menurut Adami Chazawi dan Ardi Ferdian (2011, hal. 141) menjelaskan bahwa:

Mengakses adalah istilah yang sangat populer digunakan dalam bidang informasi dan transaksi elektronik. Kata dasar dari mengakses adalah akses. UU ITE memberi tafsir otentik tentang akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau jaringan. Sebagai suatu kegiatan, maka akan terdapat banyak cara yang digunakan dalam mengakses.

Perbuatan RI dan DV dalam mengakses pada modus ini yaitu RI dan DV memasuki atau mengakses akun *mobile banking* korban dengan mengaktifkan *simcard* yang sudah tidak aktif. Akses tersebut berupa interaksi dengan akun *mobile banking* korban yaitu mentransferkan dana yang ada dalam rekening akun *mobile banking* korban.

Unsur yang selanjutnya adalah Komputer dan/atau Sistem Elektronik. Komputer sendiri seperti yang dijelaskan dalam Pasal 1 angka 14 UU ITE adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan. Sistem Elektronik sendiri seperti yang dijelaskan dalam Pasal 1 angka 5 adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. Pada modus ini, yang diakses adalah Sistem Elektronik yaitu berupa aplikasi *mobile banking*.

Unsur yang selanjutnya adalah dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Menurut Kamus Besar Bahasa Indonesia, unsur melanggar sendiri berarti menyalahi; melawan. Unsur menerobos sendiri berarti menembus; mendobrak; memintas. Unsur melampaui sendiri berarti melebihi (batas, ketentuan, dan

Jurnal Yustika
Vol. 23 No. 02, Des 2020



sebagainya). Unsur menjebol sendiri berarti merusak hingga tembus (KBBI Daring, 2016). Menurut Adami Chazawi dan Ardi Ferdian (2011) menjelaskan bahwa letak sifat melawan hukumnya perbuatan mengakses kiranya terdapat pada caranya mengakses dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Penjelasan ayat (3) menjelaskan tentang arti sistem pengamanan, adalah sistem yang membatasi akses komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klarifikasi pengguna beserta tingkatan kewenangan yang ditentukan. Misalnya sistem pengamanan yang dibuat pemilik suatu *website* atau penyelenggara sistem elektronik, ialah untuk dapat memasuki *website* atau sistem elektronik tersebut harus menggunakan kombinasi *username* dan *password*. Apabila seorang *cracker* melanggar, menerobos, atau menjebol sistem pengamanan tersebut maka terjadilah tindak pidana menurut Pasal 30 ayat (3) ini.

Perbuatan RI dan DV dalam mengakses Komputer dan/atau Sistem Elektronik dilakukan dengan menerobos sistem pengamanan, karena untuk mengakses akun *mobile banking* korban dilakukan dengan serangkaian cara yaitu RI berperan sebagai pencari data nasabah yang menjadi target kejahatannya. Setelah itu, RI mencari data nasabah yang mengaktifkan layanan *mobile banking* yang terhubung dengan *simcard*. Lalu RI mengerucutkan pencariannya pada nasabah yang masa berlaku *simcard* nya sudah tidak aktif tetapi masih terhubung dengan layanan *mobile banking*. Setelah itu pelaku akan berusaha mengaktifkan kembali kartu tersebut di gerai provider. Akhirnya *mobile banking* dalam kartu yang sudah tidak aktif tersebut dapat aktif kembali tetapi masih atas nama korban. RI dan DV mengakses rekening korbannya dengan cara mengaktifkan kembali *simcard* milik korban yang pernah terhubung dengan *mobile banking* namun saat ini sudah tidak aktif. Setelah *simcard* tersebut diaktifkan, RI dan DV kemudian berusaha menerobos masuk ke sistem *mobile banking* korban. Dalam upaya mengakses *mobile banking* korbannya, RI dan DV mencoba menggunakan tanggal lahir korban, dan ternyata berhasil.

Secara yuridis dalam penjelasan Pasal 30 ayat (3) UU ITE bahwa sistem pengamanan adalah sistem yang membatasi akses komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klarifikasi pengguna beserta tingkatan kewenangan yang ditentukan. Sistem pengamanan dalam aplikasi *mobile banking* bagi nasabah adalah *username* dari *simcard* nasabah serta *password* untuk dapat mengakses akun *mobile banking* yang dimiliki seorang nasabah.

Sistem pengamanan dalam suatu sistem elektronik merupakan kewajiban dari Penyelenggara Sistem Elektronik. Seperti halnya diatur dalam Pasal 23 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang menyatakan bahwa: "Penyelenggara Sistem Elektronik wajib melakukan pengamanan terhadap komponen Sistem Elektronik." dan Pasal 24 ayat (2) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang menyatakan bahwa: "Penyelenggara Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian."
Dari penjelasan diatas berarti dalam hal ini Bank selaku penyedia aplikasi *mobile banking* wajib melakukan pengamanan terhadap Sistem Elektronik yang dimiliki. Dalam hal ini adalah aplikasi *mobile banking*

Sistem pengamanan transaksi elektronik terdapat dalam Pasal 34 ayat (3) Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 11 Tahun 2018 tentang

Penyelenggaraan Sertifikasi Elektronik yang menyatakan bahwa:
Terhadap orang perseorangan sebagaimana dimaksud dalam ayat (2), verifikasi identitas dilakukan melalui kombinasi 2 (dua) faktor autentikasi berupa:

a. login akun daring dari layanan yang bersangkutan, berupa *user name*, *password*, *Personal Identification Number* (PIN) atau lainnya yang memenuhi unsur "*what you know*", dan;
b. penguasaan atas kartu magnetis, *chip*, token, *One-Time-Password* (OTP), atau lainnya yang memenuhi unsur "*what you have*".

Berdasarkan penjelasan diatas bahwa Bank selaku penyedia aplikasi *mobile banking* melakukan sistem pengamanan terhadap orang perseorangan yaitu verifikasi identitas dilakukan melalui 2 (dua) faktor autentikasi berupa *user name*, *password*, *Personal Identification Number* (PIN) atau lainnya yang memenuhi unsur "*what you know*", dan penguasaan atas kartu magnetis, *chip*, token, *One Time Password* (OTP), atau lainnya yang memenuhi unsur "*what you have*". Berarti apabila dikaitkan dengan modus ini, Bank telah melakukan pengamanan terhadap aplikasi *mobile banking* yang tersedia. Maka dari itu, RI dan DV dapat dikatakan telah melakukan akses ilegal terhadap suatu akun *mobile banking* korban hingga mengalami kerugian yang besar.

Secara konkrit dalam penerapan sistem pengamanan *mobile banking* adalah misal pada layanan *mobile banking* bank BCA seperti yang terdapat dalam laman BCA (Bca.co.id, 2020) bahwa:
BCA menggunakan 3 (tiga) lapis sistem pengamanan untuk melindungi akses dan transaksi nasabah di *mobile banking* BCA yaitu:

1) *Secure Socket Layer* ("SSL") SSL adalah teknologi pengamanan yang "mengacak" jalur komunikasi antar komputer sehingga tidak dapat dibaca oleh pihak lain.
2) *User ID* dan *Personal Identification Number* (PIN)
3) *One Time Password* yang dihasilkan oleh *KeyBCA One Time Password* adalah teknologi pengamanan yang selalu menghasilkan *password* yang berbeda setiap kali alat/token pengamannya digunakan.

Berdasarkan penjelasan diatas artinya secara konkrit telah ada pengamanan oleh masing-masing Bank terhadap aplikasi *mobile banking* yang disediakan. Artinya, RI dan DV melakukan akses ilegal terhadap suatu akun *mobile banking* korban hingga mengalami kerugian yang besar dengan menerobos akun tersebut yang dilakukan dengan mengetahui *password* yang merupakan tanggal lahir korban.

Suatu perbuatan yang dilarang dalam UU ITE apabila menimbulkan kerugian terhadap orang lain juga dapat dikenakan dengan Pasal 36 UU ITE yang menentukan: "Setiap Orang dengan sengaja melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain." Serta sanksi pidana apabila memenuhi unsur-unsur yang ada pada Pasal 36 UU ITE terdapat pada Pasal 51 ayat (2) UU ITE yang menentukan bahwa: "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Unsur-unsur pada Pasal 36 UU ITE dapat diuraikan sebagai berikut:

1. Setiap Orang;
2. Dengan sengaja;
3. Tanpa hak atau melawan hukum;
4. Melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34;
5. Mengakibatkan kerugian bagi orang lain.

Masing-masing unsur tersebut dijabarkan sebagai berikut:

Unsur setiap orang yang dimaksud yaitu orang perorangan, baik Warga Negara Indonesia, Warga Negara Asing, maupun badan hukum tercantum pada Pasal 1 angka 21 UU ITE. Apabila melihat dari modus yang terjadi, unsur ini telah dipenuhi oleh RI dan DV karena RI dan DV adalah orang perorangan serta RI dan DV adalah Warga Negara Indonesia, dan ditangkap oleh pihak kepolisian di tempat tinggalnya yang beralamatkan di daerah Palembang, Sumatera Selatan.

Unsur yang selanjutnya adalah dengan sengaja. Perbuatan RI dan DV termasuk dalam kesengajaan sebagai maksud, dikarenakan RI dan DV telah menghendaki akibat dari perbuatan yang dilakukan dimana akibat dari perbuatannya tersebut dapat dikenakan ancaman pidana.

Unsur yang selanjutnya adalah tanpa hak atau melawan hukum.

Menurut Adami Chazawi (2005, hal. 87) bahwa:

> Setiap perbuatan yang ditetapkan sebagai dilarang dengan mencantumkannya dalam peraturan perundang-undangan (menjadi tindak pidana), tanpa melihat apakah unsur melawan hukum itu dicantumkan ataukah tidak dalam rumusan, maka pidana itu sudah mempunyai sifat melawan hukum, dalam kata lain melawan hukum adalah unsur mutlak dari tindak pidana.

Menurut Teguh Prasetyo dan Abdul Halim Barkatullah (2005, hal. 34-35) terdapat dua ajaran sifat melawan hukum yaitu ajaran sifat melawan hukum formal dan ajaran sifat melawan hukum material:

1. Ajaran sifat melawan hukum formal apabila suatu perbuatan telah memenuhi semua unsur yang termuat dalam rumusan tindak pidana, perbuatan tersebut adalah tindak pidana. Ajaran ini berpegang pada asas legalitas bahwa perbuatan yang diancam pidana di dalam undang-undang yang tertulis.
2. Ajaran sifat melawan hukum materiil menyatakan bahwa sifat melawan hukum tidak hanya terdapat di dalam undang-undang (yang tertulis), tetapi harus dilihat berlakunya asas-asas hukum yang tidak tertulis juga. Sifat melawan hukum dapat dihapuskan berdasarkan ketentuan undang-undang atau aturan yang tidak tertulis.

Perbuatan yang dilakukan RI dan DV memenuhi unsur melawan hukum seperti yang dijelaskan oleh Adami Chazawi dan Ardi Ferdian, serta Teguh Prasetyo bahwa telah melanggar ketentuan hukum yang berlaku yang ada di dalam UU ITE. Hal tersebut termasuk dalam ajaran sifat melawan hukum formal. Ditunjukkan pada RI dan DV cara mengakses akun *mobile banking* tersebut dengan menerobos sistem pengaman.

Unsur yang selanjutnya adalah melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34. Adami Chazawi dan Ardi Ferdian dalam bukunya (2011, hal. 206) menjelaskan bahwa: "Pasal 36 ini dapat dipandang baik sebagai tindak pidana yang berdiri sendiri maupun sebagai dasar pemberatan pidana pada tindak pidana yang dirumuskan Pasal 27 sampai dengan Pasal 34." Perbuatan RI dan DV telah memenuhi unsur-unsur pada Pasal 30 ayat (3) UU ITE maka perbuatan RI dan DV dapat dikenakan dengan Pasal 36 UU ITE juga.

Unsur yang selanjutnya adalah mengakibatkan kerugian bagi orang lain. Adami Chazawi dan Ardi Ferdian dalam bukunya (2011, hal. 206) menjelaskan bahwa: "Dalam Pasal 36 terdapat unsur akibat konstitutif yakni mengakibatkan kerugian bagi orang lain. Unsur tersebut tidak terdapat (tertulis) dalam tindak pidana Pasal 27 sampai dengan Pasal 34." Adami Chazawi dan Ardi Ferdian juga menjelaskan dalam bukunya (2011, hal. 207) bahwa: "Oleh karena itu tindak pidana ITE Pasal 27 sampai dengan Pasal 34 juga menimbulkan suatu kerugian bagi

kepentingan hukum suatu pihak/orang. Baik kerugian materiil yang dapat dinilai dengan uang, maupun kerugian immateriil." Adami Chazawi dan Ardi Ferdian menjelaskan dalam bukunya (2011, hal. 208) bahwa:

> Yang dimaksud dengan "kerugian bagi orang lain" dalam Pasal 36 pastilah bukan kerugian yang dimaksudkan seperti Pasal 27 ayat (3) UU ITE berupa kerugian immateriil tersebut. Berdasarkan penafsiran logis (*logische interpretatie*), maka kerugian yang dimaksud Pasal 36 adalah kerugian materiil yang dapat dinilai dengan uang, dapat diperhitungkan nilai rupiahnya. Orang yang menderita kerugian akibat tindak pidana ITE Pasal 27 sampai dengan Pasal 34 yang dimaksud Pasal 36 jo. Pasal 51 ayat (2), adalah semua orang, tidak ditentukan kualitasnya. Batasannya tidak terletak pada kualitas orangnya (korban), hanya terletak pada adanya hubungan kausalitas antara akibat kerugian dengan penyebab tindak pidana mana yang menimbulkan kerugian tersebut.

Perbuatan RI dan DV termasuk mengakibatkan kerugian bagi orang lain. Karena dalam kejahatan yang dilakukan oleh RI dan DV, korban mengalami kerugian sebesar Rp1.100.000.000,00 (satu koma satu miliar rupiah) maka RI dan DV memenuhi unsur tersebut dan dapat dikenakan pemberatan pidana dengan Pasal 36 jo. Pasal 51 ayat (2) UU ITE.

Pasal 81 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana menyatakan bahwa: "Setiap orang yang secara melawan hukum mengambil atau memindahkan sebagian atau seluruh Dana milik orang lain melalui Perintah Transfer Dana palsu dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah)." Unsur-Unsur dari Pasal 81 UU Transfer Dana dapat diuraikan sebagai berikut:

1. Setiap orang;
2. Secara melawan hukum;
3. Mengambil atau memindahkan sebagian atau seluruh Dana milik orang lain;
4. Melalui Perintah Transfer Dana palsu.

Masing-masing unsur tersebut dapat dijabarkan sebagai berikut:

Setiap orang adalah dalam hukum pidana modern, ancaman pidana ditujukan kepada orang perseorangan (*natuurlijke persoon*) atau korporasi (*korporatie*) (BPHN, 2008). Apabila melihat dari modus yang terjadi, unsur ini telah dipenuhi oleh RI dan DV karena RI dan DV adalah orang perorangan.

Unsur yang selanjutnya adalah secara melawan hukum. Menurut Adami Chazawi (2005, hal. 87) bahwa:

> Setiap perbuatan yang ditetapkan sebagai dilarang dengan mencantumkannya dalam peraturan perundang-undangan (menjadi tindak pidana), tanpa melihat apakah unsur melawan hukum itu dicantumkan ataukah tidak dalam rumusan, maka pidana itu sudah mempunyai sifat melawan hukum, dalam kata lain melawan hukum adalah unsur mutlak dari tindak pidana.

Menurut Teguh Prasetyo dan Abdul Halim Barkatullah (2005, hal. 34-35) terdapat dua ajaran sifat melawan hukum yaitu ajaran sifat melawan hukum formal dan ajaran sifat melawan hukum material:

1. Ajaran sifat melawan hukum formal apabila suatu perbuatan telah memenuhi semua unsur yang termuat dalam rumusan tindak pidana, perbuatan tersebut adalah tindak pidana. Ajaran ini berpegang pada asas legalitas bahwa perbuatan yang diancam pidana di dalam undang-undang yang tertulis.
2. Ajaran sifat melawan hukum material menyatakan bahwa sifat melawan hukum tidak

Jurnal Yustika
Vol. 23 No. 02, Des 2020



hanya terdapat di dalam undang-undang (yang tertulis), tetapi harus dilihat berlakunya asas-asas hukum yang tidak tertulis juga. Sifat melawan hukum dapat dihapuskan berdasarkan ketentuan undang-undang atau aturan yang tidak tertulis.

Perbuatan yang dilakukan RI dan DV memenuhi unsur melawan hukum yang dijelaskan oleh Adami Chazawi dan Ardi Ferdian, serta Teguh Prasetyo bahwa telah melanggar ketentuan hukum yang berlaku yang ada di dalam UU Transfer Dana. Hal tersebut termasuk dalam ajaran sifat melawan hukum formal.

Unsur yang selanjutnya adalah mengambil atau memindahkan sebagian atau seluruh Dana milik orang lain. Menurut Kamus Besar Bahasa Indonesia, unsur mengambil sendiri berarti memegang sesuatu lalu dibawa. Unsur memindahkan sendiri berarti menempatkan ke tempat lain; membawa berpindah. Unsur sebagian sendiri berarti satu bagian. Unsur seluruh sendiri berarti semua; menunjukkan suatu keutuhan (KBBI Daring, 2016). Unsur Dana milik orang lain dijelaskan dalam penjelasan Pasal 81 UU Transfer Dana yang memiliki arti: "Yang dimaksud dengan "Dana milik orang lain" termasuk dana milik Penyelenggara Pengirim." Terkait dengan Dana dapat melihat penjelasan mengenai Dana sudah dijelaskan diatas. Perbuatan RI dan DV yang mentransferkan Dana dalam kasus ini yaitu Dana yang ada pada rekening akun *mobile banking* korbannya dalam kata lain Dana milik orang lain. RI dan DV hampir menguras Dana yang ada pada rekening akun *mobile banking* korbannya yaitu mencapai 1,1 Miliar Rupiah.

Unsur selanjutnya adalah melalui Perintah Transfer Dana palsu. Pengertian Perintah Transfer Dana terdapat pada Pasal 1 angka 5 bahwa: "Perintah Transfer Dana adalah perintah tidak bersyarat dari Pengirim kepada Penyelenggara Penerima untuk membayarkan sejumlah Dana tertentu kepada Penerima." Menurut tesaurus Kamus Besar Bahasa Indonesia, unsur palsu sendiri berarti kepura-puraan (KBBI Daring, 2016). Menurut Johanes Ibrahim dan Yohanes Hermanto Sirait (2018) dalam Pasal 1 angka 6 UU Transfer Dana dijelaskan terkait pengertian Pengirim termasuk di dalam pengertiannya terdapat Pengirim asal. Dalam Pasal 1 angka 7 ditegaskan juga bahwa Pengirim Asal adalah pihak yang pertama kali mengeluarkan perintah transfer dana. Dalam keadaan normal, dapat dikatakan pengirim asal adalah pemilik rekening sebenarnya yang melakukan transfer dana atau orang yang dipercayakan dan diberikan kuasa untuk melakukan transfer. Sementara itu dalam keadaan tidak normal, pengirim asal adalah siapa saja yang memegang fisik rekening ATM, *mobile banking*, PIN, atau siapa saja yang dengan cara-cara tertentu dapat melakukan transfer dana, padahal bukan pemilik rekening.

Perbuatan RI dan DV dapat dikatakan melakukan Perintah Transfer Dana palsu. Berdasarkan penjelasan diatas, RI dan DV bertindak sebagai pengirim asal dalam keadaan tidak normal. Karena RI dan DV memegang fisik rekening akun *mobile banking* tersebut serta mengetahui *password* dari akun tersebut, sehingga RI dan DV dapat melakukan transfer dana, padahal bukan pemilik rekening yang sebenarnya.

Berkaitan dengan perintah transfer dana palsu. Pendapat hakim dalam putusan Pengadilan Negeri Surakarta Nomor: 108/Pid.sus/2014/PN.Skt. sebagaimana Widianika Durani dalam jurnalnya (2016, hal. 5) menyebutkan bahwa menurut hakim bahwa:

Perintah transfer dana palsu adalah perintah tidak bersyarat dari pengirim kepada penyelenggara penerima untuk membayarkan sejumlah dana tertentu kepada penerima atau suatu kegiatan yang dimulai dengan perintah dari pengirim asal yang bertujuan memindahkan sejumlah dana kepada penerima yang disebutkan dalam perintah transfer dana sampai dengan diterimanya yang dilakukan oleh bukan pemilik yang sah atas dana tersebut.

Dari penjelasan di atas, artinya RI dan DV bukan pemilik yang sah atas Dana yang ada dalam

rekening akun *mobile banking* tersebut. Namun, RI dan DV dapat melakukan transfer dana ke rekening yang telah disiapkan oleh RI dan DV serta aplikasi Sakuku.



## 4. Kesimpulan

Berdasarkan uraian beserta penjelasan , modus akses akun *mobile banking* dengan mengaktifkan *simcard* yang sudah tidak aktif untuk mentransfer dana dapat dikenakan ketentuan pidana Pasal 30 ayat (3) jo. Pasal 46 ayat (3) jo. Pasal 36 jo. Pasal 51 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Pasal 81 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana.Perbuatan akses akun *mobile banking* dengan mengaktifkan *simcard* yang sudah tidak aktif untuk mentransfer dana dapat dikenakan dengan perbuatan berlanjut yaitu Pasal 30 ayat (3) UU ITE dengan pemberatan pidana Pasal 36 UU ITE dan Pasal 81 UU Transfer Dana. Yang mana sanksi pidana Pasal 30 ayat (3) UU ITE terdapat pada Pasal 46 ayat (3) UU ITE dan sanksi pidana Pasal 81 UU Transfer Dana terdapat pada Pasal 81 UU Transfer Dana juga.

## Daftar Referensi

*Buku*

Arief, Barda Nawawi (2006). *Tindak Pidana Mayantara*. Jakarta: Raja Grafindo Persada.

Chazawi, Adami dan Ardi Ferdian (2011). *Tindak Pidana Informasi & Transaksi Elektronik (Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik)*. Malang: Banyumedia.

Hardinanto, Aris (2019).*Akses Ilegal Dalam Perspektif Hukum Pidana*. Malang: Setara Press.

Ibrahim, Johanes dan Yohanes Hermanto Sirait (2018).*Kejahatan Transfer Dana: Evolusi danModus Kejahatan Melalui Sarana Lembaga Keuangan Bank*. Jakarta: Sinar Grafika.

Indradi, Ade Ary Syam (2006). *CARDING (Modus Operandi, Penyidikan, dan Penindakan)*. Jakarta: Pensil 324.

Moeljatno (2008). *Asas-asas Hukum Pidana*. Jakarta: Rineka Cipta.

Prasetyo, Teguh (2010). *Hukum Pidana*. Jakarta: Raja Grafindo Persada.

Riswandi, Budi Agus (2005). *Aspek Hukum Internet Banking*. Jakarta: Raja Grafindo Persada.

Samudra, Anton Hendrik and Julius, Andrian. (2017). *Online Transaction Fraud Methods In Indonesia And The Norm Of Deterrence: The Challenges And Obstacles*. In: *Tackling Financial Crimes: Various International Perspectives*. Genta Publishing, Yogyakarta, pp. 165-172. ISBN 978-602-1500-89-7

Sanusi, Arsyad (2011). *Cyber Crime*. Jakarta: Milestone.

*Artikel Jurnal*

Chintia, Ervina, et. al. (2018). Kasus Kejahatan Siber di Indonesia yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *JIEET*, 02 (02), 65-69. doi: http://dx.doi.org/10.26740/jieet.v2n2.p65-69

Muhammad Khairul Faridi (2018). Kejahatan Siber dalam Bidang Perbankan. *Cyber Security dan Forensik Digital*, 1 (2). 57-61.

Nani Widya Sari (2018). Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan*, 5(1), 577-593. doi: http://dx.doi.org/10.32493/SKD.v5i2.y2018.2339.

Samudra, Anton Hendrik. (2019). Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring, *Mimbar Hukum*, 31(1), 59-74, doi: https://doi.org/10.22146/jmh.34786

S., Anton Hendrik and Qisthi K., Nian (2018) Tightening Loose Ends in Eradicating Card Fraud (Reviewing card skimming case verdict in Denpasar, Indonesia). In: *Proceedings of the Social and Humaniora Research Symposium (SoRes 2018). Advances in Social Science, Education and Humanities Research, 307 . Atlantis Press*, pp. 588-593. ISBN 978-94-6252-693-8. Doi: https://doi.org/10.2991/sores-18.2019.134

Supanto (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy. *Yustisia, 5(1), 52-70.* doi: https://doi.org/10.20961/yustisia.v5i1.8718.

Widianika Nurani, (2014). Tindak Pidana Transfer Dana Melalui Perintah Transfer Dana Palsu YangDilakukan Oleh Nasabah Pt Bank International Indonesia Tbk (Studi Putusan PN Surakarta Nomor: 108/Pid.SUS/2014/PN.Skt.). *Recividive, 3(3), 356-363.*

*Artikel Internet*

Jawa Pos (2019). Dua Pembobol Akun *E-Banking* Ditangkap. https://www.jawapos.com/nasional/hukum-kriminal/09/08/2019/duo-pembobol-akun-e-banking-ditangkap/. (Diakses pada 29 Desember 2019).

Bank Central Asia. (2020). https://www.bca.co.id/bcamobile (Diakses pada 20 Mei 2020).

*Peraturan Perundang-Undangan*

Undang-UndangDasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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

Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik