Jurnal Pustaka Cendekia Hukum dan Ilmu Sosial
Volume 1, No. 1, November, pp. 116-127
E-ISSN: 2987-4475
https://pchukumsosial.org/index.php/pchs

Tinjauan Yuridis Tindak Pidana Penipuan *Social Engineering* pada Nasabah Perbankan melalui Aplikasi Chat Whatsapp

Nur Hidayah[1], Amran[2]

[1,2] Universitas Sawerigading Makassar, Jl. Kandea No.127, Bontoala Tua, Kec. Bontoala, Kota Makassar, Sulawesi Selatan
nurhidayahkhaeril@gmail.com[1],Amran@gmail.com[2]

Abstract

The aims of this research are: 1) to find out the practice of social engineering fraud on banking customers via the WhatsApp chat application and 2) to find out the legal sanctions against perpetrators of criminal acts of "social engineering" fraud on the WhatsApp messaging application. This research is a normative-juridical research, namely by examining the legal regulations related to targets related to analysis and construction which are carried out methodologically, systematically and consistently. The data that has been collected and processed will be discussed using a qualitative normative method, namely a discussion that is carried out by interpreting and describing the data that has been obtained and processed, based on legal norms and doctrine. The conclusions of this research are as follows: 1) The soceng or social engeneering mode that is usually carried out by fraudsters via the WhatsApp messaging application is: 1. Making Fake Calls (Fake Caller) 2. Digital Wedding Invitations 3. Sending packages 4. Changes in administration rates for savings fees and finally 5. Ticket notification via What'Sapp chat. 2) The threat of sanctions imposed by soceng fraudsters is regulated in Law no. 3 of 2011 concerning Fund Transfers in articles 81 and 82. Meanwhile, in Law 11 of 2008 concerning Information and electronic transactions, article 32 paragraph 2 with criminal threats in article 48 paragraph 2 and finally the Criminal Code in article 362. The suggestion in this research is that users of messaging applications of any kind, whether from social media or messaging such as WhatsApp, to always be careful and increase vigilance regarding all information provided to other parties. For this reason, increasing literacy, especially banking literacy, is needed to prevent cases of soceng fraud.
Keywords: Social Engineering Mode, Fraud, Banking Customers.

Abstrak

Tujuan penelitian ini yaitu: 1) untuk mengetahui praktek modus penipuan sosial engineering pada nasabah perbankan melalui aplikasi chat WhatsApp dan 2) untuk mengetahui Sanksi hukum terhadap pelaku tindak pidana penipuan " social engineering " pada aplikasi pesan WhatsApp. Penelitian ini merupakan penelitian normatif-yuridis yaitu dengan cara mengkaji melalui aturan-aturan perundangan yang terkait dengan sasaran yang berkaitan dengan analisa dan konstruksi yang dilakukan secara metodologis, sistematis, dan konsisten. Data yang telah terkumpul dan telah diolah akan dibahas dengan menggunakan metode normatif kualitatif, yakni suatu pembahasan yang dilakukan dengan cara menafsirkan dan menjabarkan data yang telah diperoleh dan diolah, berdasarkan dengan norma-norma hukum dan doktrin. Keseimpulan penelitian ini sebagai berikut : 1) Modus soceng atau sosial engeneering yang biasanya dilakukan oleh si penipu melalui aplikasi perpesanan WhatsApp adalah : 1.Melakukan Telepon Palsu (Fake Caller) 2. Undangan Pernikahan Digital 3. Pengiriman paket 4. Perubahan tarif administrasi biaya tabungan dan terkhir adalah 5. Pemberitahuan tilang melalui chat What'Sapp. 2) Ancaman Sanksi yang dikenakan oleh penipu soceng ini di ataur dalam Undang-Undang No. 3 Tahun 2011 tentang Transfer Dana pada pasal 81 dan pasal 82 . Sedangkan pada Undang-Undang 11 Tahun 2008 tentang Informasi dan transaksi elektronik pasal 32 ayat 2 dengan ancaman pidana pada pasal 48 ayat 2 dan terkahir KUHP pada pasal 362. Adapun saran dalam penelitian ini adalah Pengguna aplikasi perpesanan apapun bentuknya baik itu dari media sosial atau perpesanan seperti WhatsApp agar selalu berhati-hati dan meningkatkan kewaspadaannya untuk segala pemberian informasi kepada pihak lain Untuk itu peningkatan literasi khususnya literasi perbankan di butuhkan guna mencegah terhidar dari kasus penipuan soceng
Kata Kunci: Modus Social Engeneering , Penipuan , Nasabah Perbankan.

✉Corresponding author: Nur Hidayah
Email Address: nurhidayahkhaeril@gmail.com (Jl. Kandea No.127, Kec. Bontoala, Kota Makassar, Sulsel)
Received 18 November 2023, Accepted 24 November 2023, Published 30 November 2023

PENDAHULUAN

Globalisasi saat ini memberikan dampak pada berbagai aspek kehidupan manusia, baik dalam pertumbuhan ekonomi maupun teknologi. Perkembangan tersebut mendorong setiap individu untuk terus melakukan pembaruan dan berusaha untuk dapat memenuhi kebutuhan serta kesejahteraan hidupnya. Pesatnya perkembangan teknologi tentunya membuat perubahan pola hidup masyarakat menjadi milenium. Berbagai informasi dapat diketahui secara langsung di berbagai belahan dunia berkat globalisasi, khususnya pada aspek teknologi yang memberikan manfaat pada masyarakat sehingga dapat melakukan sesuatu dengan mudah, cepat, dan efisien hasil dari inovasi yang dibuat.

Manfaat internet semakin dirasakan oleh pengguna sebagai hal yang tidak terpisahkan dari dunia internet ini. Saat ini masyarakat indonesia telah menggunaakan internet sebagai sarana komunikasi , transaksi jual beli, baik secara tatap muka maupun daring. Proses perpindahan ke sebuah sistem digital (digitalisasi) telah mengubah aspek kehidupan manusia .

Pada era internet saat ini, informasi itu sangat mudah diperoleh dan dapat disebarluaskan pula. Oleh karena itu, bagi seseorang, organisasi, pemerintah maupun swasta, informasi itu menjadi aset yang sangat berharga. Informasi memiliki nilai dan harus dilindungi, sehingga menjadi penting bagi individu untuk melakukan perlindungan terhadap informasi. Oleh karena itu dibutuhkan keamanan informasi yaitu melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan operasi organisasi, meminimalisasi kerusakan akibat terjadinya ancaman, serta mempercepat kembalinya proses kerja organisasi.

Pengamanan informasi sangat dibutuhkan agar kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) informasi dapat terjaga sehingga tidak mengganggu kinerja dan operasional organisasi. Serangan terhadap keamanan informasi dapat berasal dari dalam (insider attacks) dan dari luar (outsider attacks). Seperti yang dinyatakan oleh. Mitnick dan Simon (2002) manusia merupakan faktor utama dan penting dalam pengamanan informasi selain teknologi, karena manusia merupakan rantai terlemah dalam rantai keamanan. Oleh sebab itu, dimensi manusia perlu selalu dibina dengan baik agar segala bentuk ancaman dapat dihindari. Salah satu cara yang dapat dilakukan adalah dengan menumbuhkan kesadaran akan pentingnya keamanan informasi

Proses perpindahan ke sebuah sistem digital (digitalisasi) telah mengubah aspek kehidupan manusia seperti sistem pembayaran dan berefek pada sistem perbankan di Indonesia yang dari sistem konvensional menjadi sistem digital. Sistem pembayaran ialah bagian utama dalam suatu negara karena merupakan hal krusial yang mempengaruhi perkembangan serta pertumbuhan ekonomi negara. Keefisiensian sebuah sistem pembayaran dapat dilihat dari kapabilitas sebuah negara dalam menghasilkan biaya minimal untuk memperoleh keuntungan dan kelancaran mekanisme dari aktivitas perdagangan karena melibatkan sebuah alat pembayaran yang dijadikan media transaksi dalam siklus perekonomian.

Dukungan dunia perbankan yang memungkinkan masyarakat dalam menjalanankan transaksi keuangan dengan menggunakan media pembayaran non tunai memberikan efesiensi dalam bertransaksi, akan tetapi dari efesiensi dan kemudahan yang ditawarkan bagaikan pisau bermata dua

karena membuat para hacker berupaya membobol data untuk meretas akun rekening seseorang melalui jaringan internet. Seperti akhir – akhir ini media sosial dihebohkan dengan chat whatsapp dari oknum yang mengatas namakan bank-bank yang mana mengirimkan aplikasi yang meminta untuk nasabah memberikan informasi data dirinya, dengan cara memanipulasi psikologis korban untuk melakukan langkah-langkah tertentu sehingga nasabah memberikan data pribadi atau kunci akses pada 'brankas digital' atau layanan mobile banking yang mereka miliki.

Cara memanipulasi ini di sebut dengan penipuan dalam bentuk social engineering . Sehingga banyak dari kalangan masyarat yang menjadi korban dari kejahatan penipuan seperti ini. Kunci akses ini adalah username, dan password mobile banking yang tanpa sadar, nasabah berikan melalui website palsu. Terbaru, modus penipuan yang marak terjadi, yakni permintaan untuk meng-install aplikasi yang mengatasnamakan jasa ekspedisi atau kurir pengiriman barang.

Dalam hal ini hubungan antara nasabah dan bank di lindungi dengan UU Perlindungan Konsumen No.8 Tahun 1999. Sedangkan untuk pembobol rekening dapat dikenakan Pasal 81 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana yang menguraikan bahwa setiap orang 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 tahun atau denda paling banyak Rp5 miliar.

METODE

Jenis penelitian ini adalah penelitian normatif, dengan cara mengkaji dan mendriskipsikan bahan-bahan yang bersumber dari literatur, perundang-undangan, dan beberapa berita yang berkaitan dengan permasalahan yang dibahas.

Penelitian ini menggunakan dan mengelola data sekunder atau disebut juga dengan penelitian kepustakaan atau studi pustaka (*library research*) yang dikonsepsikan dan dikembangkan dengan kajian-kajian hukum. Pendekatan yang dipakai dalam penelitian ini menggunakan pendekatan konseptual (*conceptual approach*) mengenai modus praktek penipuan dengan *sosial engineering* yang menyasar nasabah perbankan melalui Aplikasi Chat dan sanksi hukum bagi penggunanya serta digunakan peraturan perundang-undangan (*statue approach*) terutama pengaturan dalam Kitab Undang-Undang Hukum Pidana. Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Udang No. 3 Tahun 2011 tentang Transfer Dana dan dan Undang- Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen. Pendekatan dapat dilakukan karena secara logika hukum penelitian hukum normatif didasarkan pada penelitian yang dilakukan terhadap bahan hukum yang ada. Jadi, pendekatan ini dilakukan dengan cara meneliti bahan pustaka atau data sekunder yang terdiri dari bahan hukum primer, sekunder dan bahan hukum tersier dari hukum normatif. Adapun bahan yang digunakan pada penelitian ini sebagai berikut.

Bahan hukum primer

Bahan yang digunakan dalam penelitian ini adalah, Kitab Undang-Undang Hukum Pidana. Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-Undang No. 3 Tahun 2011 tentang Transfer Dana.

Bahan hukum sekunder.

Bahan hukum sekunder yang digunakan antara lain:

1. Buku-buku teks
2. Kamus-kamus hukum
3. Jurnal-jurnal hukum
4. Komentar-komentar atas putusan pengadilan

Bahan hukum tersier

Bahan-bahan tersebut disusun secara sistematis dan dikaji kemudian, ditarik suatu kesimpulan yang ada hubungannya dengan masalah yang diteliti pada saat sekarang berdasarkan fakta yang terlihat atau sebagaimana adanya.

Dalam penelitian ini metode pengolahan data yang digunakan adalah menganalisis dan menggunakan pendekatan analisis data *kualitatif.* Analisis data *kualitatif* adalah upaya yang dilakukan dengan jalan bekerja dengan data, mengorganisasikan data, menyederhanakan menjadi satuan yang dapat dikelola, mensitesiskannya, mencari dan menemukan pola, menemukan apa yang penting dan apa yang dipelajari, dan memutuskan apa yang diberitahukan kepada orang lain.

HASIL DAN DISKUSI

Praktek Modus Penipuan "Social Engineering" Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp.

Seiring dengan perkembangan teknologi di bidang komunikasi berbagai macam aplikasi untuk berkomunikasi berkembang. Dulunya alat untuk saling berkomunikasi hanyalah menggunakan telpon, akan tetapi sekarang orang-orang lebih banyak menggunakan aplikasi percakapan untuk saling berbagi informasi salah satunya adalah aplikasi WhatsApp. Berdasarkan data pengguna WhatsApp di tahun 2023 pengguna WhatsApp mencapai 2,45 miliar secara global. Di Indonesia sendiri pengguna WhatsApp sebanyak 112 juta orang. Hal ini disebabkan karena pada zaman ini penggunaan internet sudah menjadi kebutuhan primer yang dibutuhkan oleh manusia. Segala informasi mudah di dapatkan melalui akses jariangan internet.

Sama halnya dengan dunia komunikasi, saat ini dunia perbankan telah mengikuti perkembangan zaman sehingga penggunan mobile banking menjadi di minati oleh para nasabah, karena tidak perlu lagi ke kantor bank atau ke atm untuk sekedar mentransfer dana. Dari segi pembayaran pun telah mengalami kemajuan pembayaran kini bergeser dengan sistem cashless. Sistem cashless ini merupakan upaya pemerintah dalam transformasi digital. Di Indonesia sendiri transformasi digital dimulai pada tahun 2014 dimana Bank Indonesia mencanangkan Gerakan

Nasional Non Tunai atau disingkat dengan GNNT. Tentunya hal ini dimulai dengan keluarnya peraturan Bank Indonesia mengenai uang elektronik di tahun 2009.

Penyatuan antara komunikasi dan dunia perbankan dalam satu smartphone memberikan celah kepada para peretas untuk mendapatkan keuntungan sendiri. Pada tahun 2022 menjadi awal merebaknya kasus penipuan sosial engineering (soceng). Pemberitaan dihebohkan dengan dibobolnya rekening nasabah BRI di jember. Berdasarkan data pada Tahun 2022 di pertengahan tahun tercatat sebanyak 433 laporan terkait dengan pengaduan Fraud Eksternal (penipuan, pembobolan rekening, Skimming, dan cyber crime yang berhubungan dengan keuangan yang masuk dalam pengaduan OJK dan angka ini terus bertambah karena kurangnya literasi dan kehati-hatian masyarakat dalam penggunaan teknologi perbankan.

Social engineering atau rekayasa sosial merupakan istilah dari bentuk modus penipuan perbankan yang meresahkan akhir-akhir ini. Berdasarkan laman ojk.go.id defenisi sosial engineering adalah rekayasa sosial suatu teknik penipuan yang memanipulasi psikologis korban. Dimana korban di buat senang sekali atau panik. Sehingga korban penipuan tidak bisa berfikir jernih dan memberikan info-info rahasia kepada orang lain. Sehingga dengan informasi yang di dapatkan dengan teknik skimming dapat menguras isi rekening korban

Berdasarkan hasil wawancara bersama ibu Dr. Friderica Widyasari Dewi, S.E., M.B.A anggota Dewan Komisioner Otoritas Jasa Keuangan (DK OJK) periode 2022 -2027 sebagai Kepala Eksekutif Pengawas Perilaku Pelaku Usaha Jasa Keuangan, Edukasi, dan Pelindungan Konsumen melalui media online beliau mengatakan bahwa penipuan social engineering ini tidak hanya menyasar orang-orang yang beredukasi rendah tetapi akan tetapi orang-orang berdukasi tinggi pun bisa terkena social engineering karena metode memanipulasi psikolgis korban dan dengan perpaduan antara penipuan social engineering dan era digital menjadikan dampak luar biasa, rekening nasabah bisa dibobol sampai kosong.

Lebih lanjut lagi beliau menjelaskan bahwa karena soceng atau sosial engineering ini menyasar kondisi psikologi si korban yang mana pada saat lengah si korban bisa dengan mudah dan tanpa berfikir panjang memberikan informasi yang dianggap sepele tetapi ternyata informasi tersebut penting untu meretas akun banknya.

Dulunya kasus soceng ini dilakukan melalui telpon dengan melakukan penipuan dengan modus seseorang memenangkan hadiah atau menyampaikan kenalan seseorang yang terkena musibah sehingga memerlukan dana, sehingga karena kesenangan atau panik orang yang diberitahukan tersebut tanpa berpifikir panjang mentrasfer sejumlah dana kepada penelpon tesebut. Akan tetapi dengan penggunaan aplikasi perpesan seperti WhatsApp , tingkatannya lebih parah lagi karena si penipu bisa meretas langsung ke akun bank korbannya dan menguras habis isi rekening korbannya.

Adapun yang menjadi modus dalam praktek penipuan sosial engineering atau rekaya sosial yang biasa dilakukan melalui aplikasi WhatsApp adalah sebagai berikut :

Fake Caller (Panggilan Telepon Palsu)

Modus pada Fake Caller (Panggilan Telepon Palsu) si penipu menggunakan aplikasi Fake Caller , sehingga yang muncul di bank terlihat seperti nomor kontak Call Center Perbankan dan dengan permainan kalimat yang menyakinkan dapat memancing dan membuat nasabah dengan mudah menyebutkan data-data perbankannya seperti, no kartu kredit, expaired kartu dan OTP .

WhatsApp yang berisi udangan pernikahan digital.

Modus ini menggunakan undangan pernikahan digital. Undangan digital saat ini banyak dilakukan oleh orang-orang yang akan melangsungkan perkawinan. Selain praktis, mengirimkan undangan digital kepada sahabat dan kerabat jauh,ini juga menjadi alternatif bagi orang-orang saat ini karena tidak memakan biaya dan waktu. Hal inilah yang menjadi perhatian penipu dengan melakukan modus penipuan menggunakan aplikasi undangan pernikah digital. Berikut contoh percakapan pada WhatsApp yang mengirimkan udangan pernikahan digital.

Gambar 1. WhatsApp yang berisi udangan pernikahan digital.

Pada undangan digital ini telihat berkas Apk yang apabila di klik akan mengarahkan si pengguna ke aplikasi dan dengan metode phising seseorang bisa secara tidak sengaja memberikan no rekening dan otp kepada si penipu. Hal ini dikarenakan pada Undangan digitital memungkinkan seseorang untuk memberikan isi amplopnya melalui transfer ke orang yang mempunyai acara pernikahan dalam hal ini si mempelai. Jadi si penipu dapat memanipulasi hal tersebut.

WhatsApp yang berisi kiriman paket

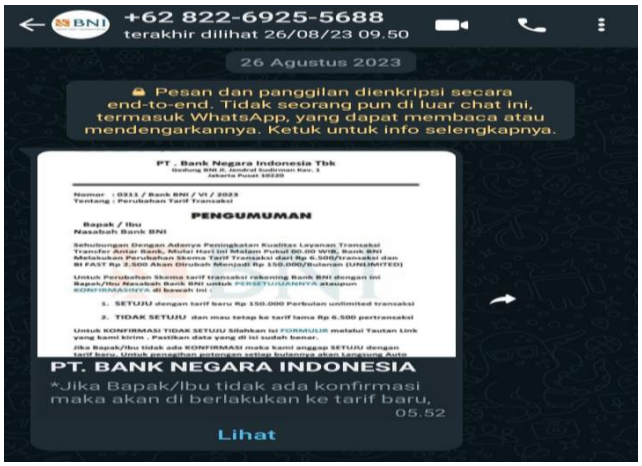
Pengiriman paket saat ini dilakukan dengan mudah dan untuk mengetahui alamat pasti si penerima , atau mengecek ada tidaknya si penerima di alamat tersebut. Biasanya si kurir menghubungi si penerima melalui chat WhatsApp. Hal inilah yang menjadi celah yang menjadikan modus penipuan. Berikut penipuan chat WA dengan modus pengiriman barang.

Gambar 2. WhatsApp yang berisi kiriman paket

Pada chat WA di atas, modusnya ingin mengirimkan paket akan tetapi pengirimnya mengirimkan foto untuk memperlihatkan bukti barangnya. Sama dengan kasus di atas menggunakan APK dan dengan satu klik dapat mengarahkan seseorang untuk mendownload aplikasi yang tidak terdaftar di play store.

WhatsApp pemberitahuan dari pihak Bank

Salah satu yang menjadi viral adalah WA yang mengatasnamakan bank tertentu dalam mengubah tarif admin bank dalam perbulannnya . yang mana apabila si korban tidak setuju dalam pengubahan tarif tersebut si korban di arahkan untuk mengisi formulir. Hal ini bisa menyerang psikologis korban dan secara tidak sadar mengisi data-data yang di harapkan si penipu. Adapun contoh isi percakapannya sebagai berikut :



Gambar 3. WhatsApp pemberitahuan dari pihak Bank

Jika dilihat dari chat what's app di atas dikrim oleh nomor WA biasa hanya profil picture yang bergambarkan bank BNI. Sehingga jika seseorang tidak teliti maka akan mengganggap bahwa chat ini dari bank BNI dan secara tidak langsung memengaruhi psikologis korban untuk mengklik tanda lihat untuk melihat informasi lebih lanjut yang diberikan oleh pesan tersebut. Apabila pesan tersebut di klik lebih lanjut maka akan di arahkan dengan pesan sebagai berikut :

Gambar 4. WhatsApp pemberitahuan dari pihak Bank

Apabila si korban mengklik web tersebut maka, akan di giring untuk mengisi formulir berisikan data dirinya sehingga dengan mudah di retas oleh penipu.

Adapun beberapa jenis teknik/ metode penyerangan dengan *social engineering* yang sering terjadi meliputi:

1. **Phishing**: Penyerang yang mana mengirimkan pesan atau email yang mengelabui orang agar memberikan informasi pribadi atau mengklik tautan yang mengarah ke situs web palsu yang terlihat seperti situs web yang dapat dipercaya.
2. **Baiting**: Penyerang menggunakan janji atau hadiah yang menggoda untuk mengelabui orang agar memberikan informasi pribadi atau mengklik tautan yang tidak aman.
3. **Scareware**: Penyerang menggunakan taktik menakut-nakuti untuk mengelabui orang agar membeli produk atau layanan yang tidak berguna dengan janji bahwa itu akan memperbaiki masalah keamanan yang tidak ada.
4. **Quid pro quo**: Penyerang menawarkan sesuatu kepada orang dalam pertukaran untuk informasi pribadi atau akses ke sistem.
5. **Pretexting**: Penyerang menggunakan dalih yang sah untuk mengelabui orang agar memberikan informasi pribadi atau akses ke sistem.

Sanksi hukum terhadap pelaku tindak pidana penipuan " social engineering " pada aplikasi pesan WhatsApp.

Praktek penipuan soceng atau sosial engineering tentunya sangat merugikan banyak kalangan utamanya si pemilik rekening dan pihak perbankan. Pihak perbankan pun dalam menyikapi fenomena ini secara massif memberikan edukasi ataupun informasi kepada masyarakat khususnya kepada

nasabah untuk lebih meningkatkan kewaspadaan dan kehati-hatiannya dalam memberikan informasi-informasi pribadi kepada orng lain.

Undang-Undang sendiri telah mengatur berbagai peraturan yang berkaitan dengan transaksi perbankan yang di tuangkan dalam Undang - undang No. 3 Tahun 2011 tentang Transfer Dana dimana Undang-undang ini di buat dengan melihat perkembangan transaksi media transfer dana dan permasalahan yang terjadi, Sehingga diperlukan pengaturan yang bertujuan menjamin keamanan dan kelancaran transaksi transfer dana serta memberikan kepastian bagi pihak yang terkait dalam penyelenggaraan kegiatan transfer dana.

Dalam hal pembobolan rekening yang disebabkan oleh pengiriman tautan yang di dalamnya ada modus sosial engineering secara tidak sadar, si korban memberikan "kunci" kepada si penipu untuk mempersilahkan dana dari rekeningnya untuk di transfer ke rekening lain dengan metode dan teknik yang telah di jelaskan sebelumnya. Oleh karena itu transfer dana yang dilakukan dari rekening perlu dianggap tidak sah karean tidak sesuai dengan kesadaran penuh dari pihak yang rekeningnya di bobol. Bahkan mereka tidak mengetahui bahwa ada transaksi yang berlangsung pada saat itu.

Dalam penentuan suatu tindak pidana dalam ilmu hukum pidana kita mengenal istilah kriminalisasi, dimana diuraikan pemahaman kriminalisasi menurut Muladi menyatakan bahwa kriminalisasi sebagai sebuah proses untuk menjadikan suatu perbuatan yang semula bukan merupakan tindak pidana atau belum termasuk tindak pidana dikarenakan tidak diatur secara gamblang dalam aturan pidana tertentu bisa menjadi suatu tindak pidana.

Kriminalisasi berlaku bagi perbuatan-perbuatan yang dinilai sebagai perbutan pidana. Namun, konsep kriminalisasi dalam tindak pidana perbankan berbeda dengan konsep kriminalisasi dibidang ekonomi pada umumnya seperti pencucian uang dan korupsi yang diatur secara khusus didalam undang-undang tersendiri atau khusus. Konsep kriminalisasi perbankan tidak dilakukan dalam satu undang-undang tersendiri malainkan kriminalisasinya tersebar didalam berbagai peraturan perundang-undangan. Kriminalisasi perbankan dapat ditemukan didalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, dan undang-undang lainnya yang mengatur hal-hal yang berhubungan secara langsung dengan perbankan, seperti Undang-Undang Nomor 13 Tahun 1999 tentang Bank Indonesia dan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.Undang-Undang No.3 Tahun 2011 tentang Transfer Dana.

Menurut Ted Honderich, suatu pidana dapat disebut sebagai alat pencegahan yang ekonomis apabila dipenuhi syarat-syarat sebagai berikut:

1. Pidana itu sungguh-sungguh mencegah;
2. Pidana itu tidak menyebabkan timbulnya keadaan yang lebih berbahaya atau merugikan dari pada yang akan terjadi apabila pidana itu tidak dikenakan; dan
3. Tidak ada pidana lain yang umumnya terwujud dalam kepentingankepentingan sosial yang mengandung nilai-nilai tertentu dapat mencegah secara efektif dengan bahaya atau kerugian yang lebih kecil

Dalam Undang –Undang No.3 tahun 2011 tentang transfer dana yang selanjutnya dalam tulisan ini akan di singkat UU No.3 Tahun 2011 transfer dana menyebutkan dalam pasal 1 ayat 1 bahwa :
"*Transfer Dana adalah rangkaian kegiatan yang dimulai dengan perintah dari Pengirim Asal yang bertujuan memindahkan sejumlah Dana kepada Penerima yang disebutkan dalam Perintah Transfer Dana sampai dengan diterimanya Dana oleh Penerima*."

Selanjutnya dalam UU No.3 Tahun 2011 tentang transfer dana pada pasal 8 ayat 1 menyatakan bahwa dalam perintah transfer dana harus sekurang-kurang nya memuat informasi tentang :

1. identitas Pengirim Asal;
2. identitas Penerima;
3. Identitas Penyelenggara Penerima Akhir;
4. Jumlah Dana dan jenis mata uang yang ditransfer;
5. Tanggal Perintah Transfer Dana; dan
6. informasi lain yang menurut peraturan perundangundangan yang terkait dengan Transfer Dana wajib dicantumkan dalam Perintah Transfer Dana.

Selanjutnya pada ayat 3 menyebutkan bahwa :
"Identitas Penerima sebagaimana dimaksud pada ayat (1) huruf b meliputi sekurang-kurangnya nama dan nomor Rekening atau apabila Penerima tidak memiliki Rekening pada Penyelenggara Penerima Akhir, identitas tersebut meliputi sekurang-kurangnya nama dan alamat sesuai dengan ketentuan peraturan perundang-undangan."

Dalam kasus soceng yang merebak melalui aplikasi perpesanan WhatsApp si korban akan di giring untuk mengisi formulir yang berisikan data diri yang di perlukan untuk membuat perintah transfer ke penyelenggra untuk memindahkan dana dari nomor rekening si korban ke nomor rek lain. Terkait dengan perintah transfer dalam undang – undang pasal 7 ayat 1 ini menyatakan bahwa perintah untuk transfer dana dapat di lakukan baik secara tertulis maupun secara elektronik.

Yang di maksud dengan secara tertulis di sini adalah dilakukan perintah transfer secara tertulis yang di tuliskan pada formulir pemindahan dana dan dilakukan langsung ke bank di hadapan teller. Sedangkan yang di maksud secara elektronik adalah yang dilakukan melalui mobile banking, bank application ataupun web banking.

Adapun sanksi dalam undang – undang ini yang dapat di timpakan kepada pelaku pembobolan rek melalui modus soceng adalah pidana penjara paling lama 5 tahun atau denda sebanyak 5 miliar .Sanksi yang tercantum dalam pasal 81 UU No.3 Tahun 2011 yang menguraikan bahwa Setiap orang 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 tahun atau denda paling banyak Rp5 miliar.

Selanjutnya pasal 82 menyebutkan bahwa Penerima yang dengan sengaja menerima atau menampung, baik untuk diri sendiri maupun untuk orang lain, suatu Dana yang diketahui atau patut diduga berasal dari Perintah Transfer Dana yang dibuat secara melawan hukum dipidana dengan

pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Selain itu, Undang-Undang 11 Tahun 2008 tentang Informasi dan transaksi elektronik pasal 32 ayat 2 dengan tegas melarang untuk Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak. Untuk pasal ini di berikan ancaman pidana yang tertuang dalam pasal 48 ayat 2 yang berbunyi bahwa Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

Dalam Kitab Undang-Undang Hukum Pidana (selanjutnya dalam tulisan ini di sebut KUHP) juga di atur tentang pasal pencurian, pembobolan rekening ini bisa di kategorikan pencurian. Pasal yang terkait dengan pencurian ini adalah pasal 362 KUHP pidana dalam pasal ini menyebutkan bahwa *"Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah".*

Dalam hal penipuan yang bermoduskan "*social engineering"* pelaku dapat dijerat dengan ancaman sanksi yang telah dijelaskan di atas. Namun pada kenyataannya kasus penipuan seperti ini masih sulit untuk melacak pelakunya karena mereka menggunakan kartu pra bayar yang berganti-ganti.

Adapun upaya yang dapat dilakukan kepada pengguna aplikasi perpesanan WhatsApp agar tidak menjadi korban soceng adalah sebagai berikut :

1. Selalu menjaga kerahasiaan data pribadi. Seperti *Password*, PIN, atau OTP dilarang untuk dibagikan kepada siapa pun termasuk jika ada yang mengaku dari pihak bank, baik untuk penggunaan ATM dan atau *mobile banking*.
2. Melakuan pembaharuan *password* secara berkala
3. Mengaktifkan fitur notifikasi transaksi, sehingga apabila terjadi transaksi pada rekening, segera di ketahui melalui notifikasi tersebut
4. Cek histori transaksi secara berkala melalui aplikasi *mobile banking*
5. Jangan mudah terhasut pada saat membaca pesan WhatsApp yang berisi pemberitahuan, pengancaman ataupun yang memberitakan kecelakaan terhadap keluarga.

KESIMPULAN

Adapun yang menjadi kesimpulan dalam penelitian ini adalah sebagai berikut. Pertama, modus soceng atau sosial engeneering yang biasanya dilakukan oleh si penipu melalui aplikasi perpesanan WhatsApp adalah : 1.Melakukan Telepon Palsu (Fake Caller) 2. Undangan Pernikahan Digital 3. Pengiriman paket 4. Perubahan tarif administrasi biaya tabungan dan terkhir adalah 5. Pemberitahuan

tilang melalui chat What'Sapp. Ke lima modus ini yang sering kali digunakan penjahat soceng dalam memanipulasi perasaan korbannya sehingga dengan mudah mendaptkan informasi-informasi pribadi yang dinginkan si penipu dalam membobol rekening bank si korban . Kedua, ancaman Sanksi yang dikenakan oleh penipu soceng ini di ataur dalam Undang-Undang No. 3 Tahun 2011 tentang Transfer Dana pada pasal 81 dan pasal 82 . Sedangkan pada Undang-Undang 11 Tahun 2008 tentang Informasi dan transaksi elektronik pasal 32 ayat 2 dengan ancaman pidana pada pasal 48 ayat 2 dan terkahir KUHP pada pasal 362.

REFERENSI

Buku

Adami Chazawi, *Pelajaran Hukum Pidana 1*, PT Raja Grafindo Persada,Jakarta, 2001.

Amir Ilyas, *Asas-Asas Hukum Pidana*, Rangkang Education, Makassar,2012.

Andi hamzah, *Delik-Delik Tertentu (Speciale Delicten) di dalam KUHP*, Sinar Grafika, Jakarta, 2010.

Bastian Bastari, *Analisis Yuridis Terhadap Delik Penipuan*, Makassar,2011.

Mahrus Ali, *Dasar-Dasar Hukum Pidana*, Sinar Grafika, Jakarta Timur,2011.

Muladi & Barda Nawawi Arief, *Teori-teori Dan Kebijakan Pidana*, Bandung:ALUMNI, 2005

P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, PT Citra AdityaBakti, Bandung, 1997.

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, PT Raja Grafindo Persada, Jakarta, 2001.

Subandi Al Marsudi, *Pengantar Hukum Indonesia*, Tanggerang: JelajahNusa, 2014.

Teguh Prasetyo, *Hukum Pidana Edisi Revisi*, PT Raja Grafindo Persada,Jakarta, 2011.

Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana di Indonesia*, RefikaAditama, Bandung, 2003.

Jurnal

Achmad Nur Fuad Chalimi, Siti Herdinawati dan Asadi Asadi,Faktor Kemajuan Teknologi Dan Sumber Daya Manusia Terhadap Peningkatan Pendapatan Umkm Era Revolusi 4.0‟ (2022) 9 , Jurnal Ilmu Manajemen dan Akuntansi .

MA Harahap and S Adeni, „Tren Penggunaan Media Sosial Selama Pandemi Di Indonesia‟ (2020) Professional: Jurnal Komunikasi Dan Administrasi Publik.

Perundang-Undangan

Kitab Undang-undang Hukum Pidana

Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan

Undang-Undang No. 3 Tahun 2011 tentang Transfer Dana

Undang-Undang 11 Tahun 2008 tentang Informasi dan transaksi elektronik