Hakim: Jurnal Ilmu Hukum dan Sosial
Vol.2, No.2 Mei 2024
e-ISSN: 2987-7539; p-ISSN: 2987-6737, Hal 367-383
DOI: https://doi.org/10.51903/hakim.v2i2.1829

Analisis Yuridis *Cyber Crime* Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu

Angela Gabriela Bupu
Fakultas Hukum, Universitas Nusa Cendana
Korespondensi penulis: trocigia@gmail.com

Karolus Kopong Medan
Fakultas Hukum, Universitas Nusa Cendana

Heryanto Amalo
Fakultas Hukum, Universitas Nusa Cendana

Abstract*. The purpose of this research is to analyze the juridical cybercrime of breaking into customer funds on mobile banking applications with the mode of breaking into fake wedding invitation lines. This research is an empirical legal research that examines all legal events that have occurred through a case approach. Retrieval is done in two ways, namely interviews and document studies. The data obtained is then presented descriptively qualitative. The results showed that the form of responsibility of the Bank to the victim can be in the form of compensation or refund but if the customer can prove that the money was lost due to the fault of the Bank. The countermeasures taken by the Bank are strengthening the mobile banking security system while the efforts of the NTT Regional Police are conducting socialization, cyber patrols, and making preventive and repressive efforts. The obstacles experienced by the NTT Regional Police are the lack of government supervision in the use of the internet, aspects of evidence, and jurisdiction, as well as the lack of public knowledge of cyber crime. Therefore, suggestions for the results of this study are Suggestions that researchers can put forward are the need for special provisions that explicitly regulate mobile banking. The government should provide legal certainty to create a clean and safe social media environment.*

Keywords*: Cyber Crime, Fake Wedding Invitations, Forms of Responsibility, Countermeasures, Obstacles.*

Abstrak. Tujuan penelitian ini ialah menganalisis yuridis cyber crime pembobolan dana nasabah pada aplikasi mobile banking dengan modus pembobolan jalur undangan pernikahan palsu. Penelitian ini merupakan penelitian hukum empiris yang mengkaji semua peristiwa hukum yang telah terjadi melalui pendekatan kasus. Pengambilan dilakukan dengan dua cara yaitu wawancara dan studi dokumen. Data - data yang diperoleh kemudian disajikan secara deskriptif kualitatif. Hasil penelitian menunjukan bahwa bentuk pertanggung jawaban pihak Bank terhadap korban dapat berupa ganti rugi maupun pengembalian uang namun jika nasabah dapat membuktikan bahwa uang tersebut hilang karena kesalahan pihak Bank. Upaya penanggulangan yang dilakukan oleh pihak Bank yaitu memperkuat sistem keamanan mobile banking sedangkan upaya dari Polda NTT adalah mengadakan sosialisasi, patrol siber, dan melakukan upaya preventif dan represif. Hambatan – hambatan yang dialami pihak Polda NTT adalah kurangnya pengawasan pemerintah dalam penggunaan internet, aspek alat bukti, dan yuridiksi, serta kurangnya pengetahuan masyarakat akan *cyber crime*. Oleh sebab itu, saran terhadap hasil penelitian ini adalah Saran yang dapat peneliti kemukakan adalah perlunya ketentuan khusus yang mengatur secara eksplisit mengenai mobile banking. Seharusnya pemerintah memberikan kepastian hukum guna menciptakan lingkungan media sosial yang bersih dan aman.

Kata Kunci: *Cyber Crime*, Undangan Pernikahan Palsu, Bentuk Pertanggung Jawaban, Upaya Penanggulangan, Hambatan.

Received Februari 10, 2024; Accepted Maret 25, 2024; Published Mei 30, 2024
*Angela Gabriela Bupu, trocigia@gmail.com

LATAR BELAKANG

Lahirnya Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Eleketronik sebagaimana telah diubah oleh Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik didasarkan amanat yang terkandung pada Pasal 28F Undang-undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

Secara yuridis, Undang-undang ini telah mengatur mengenai segala sesuatu yang berkaitan dengan kegiatan internet, perangkat komputer, dan instrumen elektronik lainnya serta dibentuk oleh lembaga yang berwenang yakni Dewan Perwakilan Rakyat selaku legislator. Secara, masyarakat memang memerlukan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik untuk mengatur berbagai aktivitas yang mereka lakukan selama berinteraksi di cyber space.

Sampai saat ini, Indonesia belum memiliki undang – undang khusus yang mengatur tentang cyber crime. Namun demikian, terdapat beberapa hukum positif yang berlaku umum dan dapat dikenakan kepada pelaku cyber crime yang menggunakan sarana internet. Karena tindak pidana cyber crime melibatkan beberapa perbuatan sekaligus, maka Pasal–Pasal dalam KUHP dapat digunakan beberapa pasal sekaligus yaitu, pasal 362 KUHP tentang pencurian, pasal 378 KUHP tentang Perbuatan Curang, Pasal 369 KUHP tentang Pemerasan dan Pengancaman, Pasal 372 KUHP tentang Penggelapan, Pasal 506 KUHP tentang Pelanggaran Ketertiban Umum (Akub, M. S., 2020).

Penegak hukum sering kali masih menggunakan ketentuan dalam KUHP padahal sudah ada Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik pada kasus carding. Hal ini membuat terdakwa dengan mudah lepas dari jeratan hukum karena unsur-unsur pasal yang didakwakan tidak dapat dibuktikan. Kesalahan dalam menggunakan undang-undang memang sudah sering kali terlihat dalam kasus-kasus yang ditangani oleh penegak hukum dalam kasus kejahatan cyber.

Kecenderungan mengglobalnya karakteristik teknologi informasi yang semakin akrab dengan pengguna, akhirnya menjadikan Indonesia harus mengikuti pola tersebut. Karena teknologi informasi (khususnya dalam dimensi cyber) tidak akan mengkotak- kotak dan membentuk signifikasi karakter. Namun selalu ada gejala negatif dari setiap fenomena teknologi, salah satunya adalah aktifitas kejahatan.

Bentuk kejahatan (crime) secara otomatis akan mengikuti untuk kemudian beradaptasi pada tingkat perkembangan teknologi. Salah satu contoh terbesar saat ini adalah kejahatan maya atau biasa disebut cyber crime "Cyber crime" (kejahatan di dunia maya) secara hukum bukanlah kejahatan sederhana karena tidak menggunakan media konvensional, tetap menggunakan komputer dan internet. Sebuah data informal mensinyalir bahwa Indonesia adalah negara "hacker" terbesar ketiga di dunia.

Kemajuan teknologi informasi yang hadir saat ini juga dapat membantu menyokong dunia perbankan dalam keberhasilan pada sistem operasional bank. Melalui sebuah jaringan internet yang mudah digunakan pada kehidupan sehari-hari, membuat masyarakat sebagai nasabah pada bank dapat melakukan berbagai transaksi keuangan, salah satu nya adalah mobile banking (Styarini, F. & Riptiono, S., 2020).

Mobile banking merupakan layanan yang memudahkan nasabah bank melakukan transaksi perbankan melalui ponsel atau smartphone. Layanan mobile banking dapat digunakan dengan menggunakan menu yang sudah tersedia melalui aplikasi yang dapat diunduh dan diinstal oleh nasabah. Mobile banking menawarkan kemudahan jika dibandingkan dengan SMS banking karena nasabah tidak perlu mengingat format pesan SMS yang akan dikirimkan ke bank dan juga nomor tujuan SMS banking. Fitur-fitur layanan mobile banking antara lain layanan informasi (saldo, mutasi rekening, suku bunga, dan lokasi cabang/ATM terdekat); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, internet), pembelian pulsa, dan berbagai fitur lainnya (Nasution, D. S., 2019).

Selain mempunyai banyak keunggulan atau kemudahan lewat fitur - fiturnya yang canggih, system mobile banking juga memiliki kelemahan yang wajib di waspadai pengguna yaitu tergantung pada jaringan internet, diperlukan ponsel dengan spek tertentu, dan terkoneksinya aplikasi mobile banking dengan Handphone seringkali memunculkan masalah proteksi data pribadi, aspek keamanan cyber.

Salah satu contoh kelemahan penggunaan internet adalah kasus penipuan yang terbaru adalah pelaku kejahatan sniffing yaitu dengan cara mengirimkan file undangan pernikahan digital kepada korban melalui personal chat. Alih-alih berisi undangan, lampiran file tersebut

memiliki format apk atau APK (Application Package File), bukan file foto yang menggunakan format jpg, jpeg, png, atau pdf.

Sniffing adalah modus penipuan online dengan cara mengendus atau menyadap melalui jaringan internet pada perangkat korban lalu mengakses aplikasi yang menyimpan data penting pengguna. Data penting itu bisa berupa username, password mobile banking, informasi kartu kredit, password e-mail, hingga informasi penting lainnya. Modus sniffing berkedok undangan nikah digital pun sudah memakan korban yakni Derasmus Kenlopo, warga Kelurahan Naimata, Kecamatan Maulafa, Kota Kupang, Nusa Tenggara Timur (NTT), yang kehilangan Rp. 14,000.000. Menurut pengamat keamanan cyber, Alfons Tanujaya, ketika korban sudah klik undangan nikah digital berformat apk tersebut, maka otomatis terpasang aplikasi.

Jika sudah ter-install, aplikasi APK bakal meminta akses ke berbagai data seperti SMS, media, dan lain sebagainya. Jika diabaikan memperbolehkan akses tersebut, aplikasi APK akan dapat mengakses SMS, termasuk membaca kode OTP dari pihak bank yang biasanya dikirimkan via SMS. Walau kode OTS tak cukup ampuh untuk membobol rekening korban, pelaku bisa mendapatkan data tambahan lainnya seperti ID pengguna, password mobile banking, PIN persetujuan, dan data transaksi.

Tujuan penelitian ini adalah menganalisis yuridis cyber crime pembobolan dana nasabah pada aplikasi *mobile banking* dengan modus pembobolan jalur undangan pernikahan palsu.

METODE PENELITIAN

Jenis penelitian yang digunakan oleh peneliti adalah penelitian yuridis empiris yaitu dilakukan dengan melihat kenyataan yang ada dalam praktik atau kenyataan di lapangan. Lokasi penelitian di dua tempat yaitu di Bank BRI Cabang Kupang dan Kepolisian Daerah Nusa Tenggara Timur (POLDA NTT).

Jenis data yang digunakan dalam penelitian ini adalah data primer dan data sekunder. Data primer diperoleh langsung berupa keterangan-keterangan dan pendapat dari para responden yaitu staff di Bank BRI Cabang Kupang dan dari pihak kepolisian melalui wawancara. Data Sekumder diperoleh dari studi kepustakaan dan mempunyai kekuatan hukum yang mengikat, yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Teknik pengumpulan data digunakan untuk mengumpulkan data primer dan data sekunder dengan cara dilakukan dengan wawancara, observasi, dan dokumentasi. Teknik pengolahan data melalui *editing, coding, dan tabulasi*.

HASIL DAN PEMBAHASAN

Bentuk pertanggung jawaban pihak bank terhadap nasabah yang kehilangan uang

Penggunaan teknologi informasi dan komunikasi dalam perbankan nasional relative lebih maju daripada sektor usaha lainnya. Perkembangan teknologi membuat semua sector usaha termasuk bank harus bersaing dengan kebutuhan teknologi agar tidak tertinggal dengan sektor usaha lainnya. Adapun beberapa pihak yang terkait dalam penyelenggaraan layanan mobile banking yaitu bank. Bank adalah suatu badan usaha berbadan hukum yang bergerak di bidang jasa keuangan. Bank sebagai badan hukum berarti secara yuridis adalah merupakan subyek hukum yang berarti dapat mengikatkan diri dengan pihak ketiga (Sembiring, S., 2000).

Pasal 1 Angka 16 Undang- Undang perbankan menyebutkan bahwa nasabah adalah pihak yang menggunakan jasa bank. Nasabah perbankan dibagi menjadi dua yaitu nasabah penyimpan dan nasabah debitur. Internet Server Provider (ISP) Pada pasal 1 Angka 12 Undang – Undang No. 36 Tahun 1999 Tentang Telekomunikasi menyebutkan bahwa penyelenggaraan telekomunikasi adalah kegiatan penyedia dan pelayanan telekomunikasi sehingga memungkinkan terselenggaranya telekomunikasi Internet Server Provider (ISP) yang merupakan perusahaan yang menjual koneksi internet kepada pelanggan.

Menurut Ass. Manager ops dan layanan bank bri cabang kupang yaitu hendrianto trijono, terdapat ketentuan yang menegaskan bahwasannya beban tanggung jawab tergantung pada kesalahan pihak yang melakukannya.

Hal inilah yang menjadi alasan mengapa dalam ketentuan Peraturan Perundang-Undangan lebih cenderung mengharuskan pihak bank dalam konteks ini adalah produsen untuk lebih memperkuat sistem yang dimiliki serta memberikan penjelasan terkait resiko yang akan muncul kepada nasabah. Sehingga apabila di kemudian hari terdapat kejadian yang merugikan nasabah, tidak memberikan beban tanggung jawab tersebut kepada pihak bank.

Selain itu, dalam konteks terjadinya kerugian yang diakibatkan oleh pihak eksternal yang dalam hal ini tidak termasuk nasabah dan bank melainkan pelaku cyber crime, juga lebih jelas telah diatur dalam Pasal 27 Undang-Undang Nomor 11 Tahun 2008 Tentang ITE yang menyatakan:

“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik yang memiliki muatan yang melanggar kesusilaan.”

Kemudian pada Pasal 30 Undang-Undang ITE tersebut juga menegaskan:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3) 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 system pengamanan.

Pasal di atas menguraikan beberapa delik tindak pidana dalam Undang-Undang Nomor 11 Tahun 2008 Tentang ITE yang merupakan lex specialis dari KUHP. Undang-undang ini bertujuan melengkapi KUHP sehingga apabila perbuatan tersebut tidak diatur di dalam KUHP, maka undang-undang tersebut dapat diterapkan.

Mengenai perbuatan destruktif dari pihak luar yang berdampak kerugian, tentu saja bukan hanya akan menyasar nasabah melainkan juga pihak bank itu sendiri. Sebab selain mengalami kerugian materiil, pihak bank juga akan mendapat citra yang buruk dari masyarakat bahwa bank yang bersangkutan tidak berkompeten untuk mengelola dan menyalurkan dana masyarakat yang dikelolanya.

Secara keseluruhan dapat disimpulkan, bahwa bila mengacu pada ketentuan perundang-undangan, pertanggung jawaban atas kerugian yang dialami nasabah dalam penggunaan layanan internet banking masih menggunakan konsep pihak yang melakukan “kelalaian”.

Ganti rugi dapat berupa pengembalian uang atau penggantian barang dan/atau jasa yang sejenis atau setara nilainya, atau perawatan kesehatan dan/atau pemberian santunan yang sesuai dengan ketentuan peraturan Perundang-Undangan yang berlaku.

Ketentuan ini tidak berlaku apabila pihak bank (pelaku usaha) dapat membuktikan bahwa kerugian tersebut merupakan atau sebagai akibat kesalahan nasabah (konsumen). Sehingga, pembuktian terhadap ada tidaknya unsur kesalahan dalam gugatan- gugatan ganti rugi, merupakan beban dan tanggung jawab pelaku usaha (Pasal 28 UUPK).

Nasabah akan mengalami kesulitan untuk membuktikan unsur ada tidaknya kesalahan atau kelalaian pihak bank (pelaku usaha). Untuk itulah dianut doktrin productliability, dimana tergugat dianggap telah bermasalah kecuali nasabah mampu membuktikan bahwa nasabah tidak melakukan kelalaian atau kesalahan. Maka nasabah harus memikul resiko kerugian yang dialami pihak lain.

Menurut Asisten Manager Operasional PT.Bank Rakyat Indonesia, Tbk Kantor Cabang Kupang, Hendrianto H. Trijono berbicara tentang tanggungjawab bank terhadap nasabah yang dirugikan, pihak bank sangat bertanggungjawab atas kejadian yang dialami nasabah yang dirugikan tersebut.

Pihak bank akan mengganti rugi apabila nasabah tersebut membuat surat pengaduan tentang kejadian yang dialami dan tidak merupakan kelalaian nasabah itu sendiri serta melengkapi dokumen yang dibutuhkan dan membuktikan bahwa kerugian tersebut bukan karena kelalaian nasabah itu sendiri.

Bentuk Penyalahgunaan dan resiko Transaksi melalui mobile Banking

Mobile banking merupakan salah satu bentuk layanan perbankan tanpa cabang, yaitu fasilitas yang akan memudahkan nasabah untuk melakukan transaksi perbankan tanpa perlu datang ke kantor cabang. Layanan yang diberikan mobile banking kepada nasabah berupa transaksi pembayaran tagihan, informasi rekening, pemindah bukuan antar rekening, informasi terbaru mengenai suku bunga dan nilai tukar valuta asing, administrasi mengenai perubahan personal identification number (PIN), alamat rekening atau kartu, data pribadi dan lain-lain, terkecuali pengambilan dan penyetoran uang.

Dalam kenyataan dilapangan masih banyak terjadi penyalahgunaan aplikasi mobile banking yang seharusnya menjadi alat yang efisien karena menghemat waktu dalam proses transaksinya. Berbagai macam serangan bagi pihak pengguna dan bagi pihak penyedia layanan mobile banking adalah sebagai berikut:

1. Typo Site

   Dalam kejahatan ini, pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada nasabah yang salah mengetikkan alamat dari situs palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi user dan password nasabah dan dapat dimanfaatkan untuk merugikan nasabah.

2. Keylogger

   Keylogger merupakan suatu program yang diciptakan dengan tujuan untuk parental control agar para orangtua yang bekerja siang dan malam dapat mengontrol apa saja yang dilakukan oleh anaknya dalam jaringan komputer. Pada perkembangannya program ini justru disalahgunakan. Dalam kejahatan ini program digunakan untuk merekam karakter apa saja yang diketikkan oleh pengguna komputer.

Hal ini sering terjadi pada tempat mengakses internet umum seperti di warnet. Program ini akan merekam karakter-karakter yang diketika oleh user dan berharap akan mendapatkan data penting seperti user id maupun password. Semakin sering mengakses internet di tempat umum semakin rentan pula terkena modus operandi yang dikenal dengan istilah keylogger atau keystroke di komputer-komputer umum sehingga akan merekam semua tombol keyboard yang ditekan oleh pengguna berikutnya. Karena itu, pihak bank dalam melakukan edukasi kepada

nasabah, selalu memberitahukan untuk tidak melakukan transaksi internet banking di komputer-komputer umum.

1. Sniffing

   Usaha untuk mendapatkan user ID dan password dengan jalan mengamati paket data yang diunggah maupun diunduh pada jaringan komputer. Kejahatan ini biasanya dilakukan oleh orang yang sudah sangat ahli.

2. Brute Force Attacking

   Upaya untuk mendapatkan password atau key dengan mencoba semua kombinasi angka, huruf, tanda baca dan simbol lainnya.

3. Web Deface

   Sistem ecpploitation dengan tujuan mengganti tampilan halaman muka suatu situs persis dengan tampilan halaman muka situs internet banking suatu bank. Pelaku mengelabui nasabah dengan membuat situs yang berbeda dengan situs asli dari suatu bank. Namun, pelaku membuat halaman muka situs yang dibuat olehnya sama dengan halaman muka situs suatu bank. Jadi pelaku meng-hyperlink situs tersebut sehingga apabila nasabah tidak memperhatikan situs tersebut dan tertipu oleh tampilan halaman muka yang mirip dengan situs asli suatu bank, maka nasabah tersebut akan masuk jebakan si pelaku.

4. Email Spamming

   Mengirimkan junk e-mail berupa iklan produk dan sejenisnya pada alamat e-mail seseorang. Pelaku mengirimkan e-mail yang mengatas namakan situs suatu bank yang seolah-olah e-mail tersebut dikirimkan oleh pihak bank. E-mail tersebut biasanya berupa penawaran iklan produk bank atau meminta nasabah tersebut untuk mengkonfirmasi ulang data-datanya dengan alasan untuk keperluan bank sehingga jika ada nasabah yang tertipu dan mengikuti pesan dari e-mail palsu tersebut maka pelaku dapat mengetahui data-data yang dimiliki oleh nasabah tersebut.

5. Denial of Service

   Membanjiri data dalam jumlah yang sangat besar dengan maksud untuk melemahkan sistem sasaran. Jika data yang sudah dimasukkan melebihi dari kapasitas sistem tersebut maka sistem tersebut akan terganggu, sehingga saat sistem terganggu maka pelaku akan lebih mudah menerobos sistem tersebut.

6. Virus, Worm Trojan

   Menyebarkan virus, worm maupun trojan dengan tujuan untuk melemahkan sistem komputer, memperoleh data-data dari sistem korban dan untuk mencemarkan

nama baik pembuat perangkat lunak tertentu (Direktorat Hukum Bank Indonesia dan Fakultas Hukum Universitas Gadjah Mada).

Dari bentuk-bentuk penyalahgunaan yang telah dijabarkan, mengharuskan pihak penyelenggaran mobile banking untuk memberi perlindungan yang ekstra demi kepercayaan dan kenyamanan nasabah. Dalam upaya menjaga keamanan dan kerahasiaan data pribadi, keuangan dan transaksi nasabah, penyelenggara mobile banking sudah membuat beberapa perlindungan yaitu, Pertama User ID dan PIN (Personal Identification Number) yang merupakan kode rahasia dan kewenangan penggunaan yang diberikan kepada nasabah, yaitu setiap kali login ke internet banking nasabah harus memasukkan User ID dan PIN.

Kedua, Automatic Log Out, yaitu jika tidak ada tindakan yang dilakukan lebih dari 10 menit, Internet Banking secara otomatis akan mengakhiri dan kembali ke menu utama. Ketiga, dengan menggunakan kode otp (*one time password*), yaitu kode satu waktu yang akan langsung hangus dan tidak dapat digunakan lagi. Keempat, fitur Safety Mode BRImo, fitur ini mempunyai kegunaan untuk melindungi akun pengguna dari penyalahgunan atau kecurangan yang mungkin terjadi dalam proses transaksi. Kelima, teknologi biometric yang dipunyai oleh aplikasi BRImo adalah dapat login menggunakan keamanan sidik jari dan face recognition atau pengenalan wajah.

Bentuk kerugian nasabah dalam penggunaan mobile banking

Dari bentuk penyalahgunaan serta resiko yang muncul dari penggunaan mobile banking, berdampak secara langsung kepada nasabah. Secara garis besar, kerugian yang dialami nasabah terdiri dari: Pertama, pencurian data pribadi. Kasus ini merupakan yang paling marak terjadi terutama di Indonesia. Secara keseluruhan menurut Gemalto, jumlah data yang dibobol perharinya mencapai 6,9 juta data. Hal ini berdasarkan laporan pencurian data sejak 2013 hingga 2018 yang jumlahnya sebanyak 146 miliar dan hanya 4 persen dari jumlah tersebut yang dilindungi enkripsi oleh pemiliknya (Aaswandi, R.).

Sementara, menurut Digital Forensic Indonesia (DFI) menduga ada sekitar 7,5 miliar data pribadi pengguna internet di seluruh dunia diretas pihak ketiga dalam 15 tahun terakhir. Sumber kebocoran data di seluruh sektor tersebut berasal dari peretasan pihak luar (malicious outsider) dan pihak dalam (malicious insider), kebocoran data yang tidak disengaja akibat sistem tidak aman (accidental loss), hacktivist, gawai atau ponsel yang raib, perangkat pemeras (ransomware), dan beragam sumber yang tidak dapat ketahui, akibatnya data pribadi bisa diperjual belikan.

Pembobolan terjadi karena ada kerja sama antara orang dalam dan nasabah “Kasus pembobolan itu 90%-93% selalu melibatkan orang dalam dan/atau nasabah, yang sukarela

misalnya mencuri sendiri. Terakhir, pada tahun 2017 silam, Bareskrim Polri menangkap jaringan penjual data tersebut, menurut Direktur Pengawasan Bank II Otoritas Jasa Keuangan Anung Herlianto.

Direktur Perlindungan Konsumen Otoritas Jasa Keuangan Agus Fajri mengungkapkan ada keterlibatan mantan pegawai penyelenggara usaha jasa keuangan dalam hal ini bank. Menurutnya, dari temuan penjualan informasi nasabah tersebut terungkap praktik dan oknum mantan pegawai yang terlibat.

Padahal, jaminan perlindungan data sudah diatur dalam Pasal 15 ayat (1) UU ITE yang mengharuskan setiap penyelenggara sistem elektronik termasuk mobile banking untuk menjaga keamanan platform (Aswandi, R.).

Kasus pembobolan data dan informasi pribadi merupakan hal yang harus menjadi perhatian pemerintah Indonesia, karena dengan melalui kebocoran atau pembobolan data dan informasi seseorang, maka pihak-pihak yang tidak bertanggungjawab akan menyalahgunakan data dan informasi pribadi seseorang tersebut. Opsi pertama dari pencurian data biasanya merujuk pada penjualan data secara online. Ini merupakan penghasilan bagi para telemarketer dan pelaku kejahatan.

Bagi telemarketing, data pribadi nasabah digunakan untuk menawarkan produk bank atau asuransi. Ini sebabnya banyak nasabah yang kemudian kerap mendapatkan telepon tawaran produk bank atau asuransi. Namun yang patut disayangkan, beberapa riset membuktikan bahwa kesadaran masyarakat Indonesia terhadap perlindungan data personal mereka di internet masih rendah. Akibatnya masyarakat Indonesia kurang menanggapi serius kasus pelanggaran terhadap perlindungan data personal ini.

Belum spesifiknya regulasi atau aturan tentang kejahatan siber dan juga kejahatan pada penyalahgunaan data dan informasi merupakan salah satu penyebab tingginya kasus penyalahgunaan data dan informasi di Indonesia, barulah ketika terjadi kerugian materill dianggap sebagai kerugian yang berarti.

Demikian ini akan menjadi bentuk kerugian nasabah yang kedua, yaitu kerugian keuangan. Dalam konteks ini, terdapat beberapa kasus kejahatan dengan menggunakan layanan mobile banking dengan mencuri uang nasabah.

Penyelesaian Sengketa Nasabah Dengan Pihak Bank

Disatu sisi internet banking memberikan banyak kemudahan sebagai jawaban perkembangan teknologi namun rupanya tetap menyisakan ruang terjadinya perselisihan antara nasabah dan bank. Hal ini terutama karena banyaknya resiko dari penggunaan layanan internet

banking tersebut. sementara itu, bentuk pertanggung jawaban yang ditentukan dalam perundang-undangan sangat berpatokan dengan penggunaan konsep kesalahan.

Demikian hal ini dapat membuat nasabah berada pada posisi yang lemah terutama dihadapkan pada perjanjian baku yang mengikatnya. Sebenarnya telah dikembangkan prinsip strict liability guna tercapainya perlindungan dan meningkatkan kedudukan nasabah dengan cara menerapkan tanggung jawab produsen dalam hal ini adalah pihak bank. Pihak bank pada posisi ini sebagai produsen penyedia jasa layanan transaksi elektronik moile banking sudah sewajarnya dibebani dengan tanggung jawab mutlak oleh karena resiko dalam transaksi mobile banking ini sangat tinggi dan bermacam-macam jenisnya. Sehingga bank diberikan tekanan agar dapat lebih menerapkan prinsip kehati-hatian dalam melaksanakan penggunaan mobile banking oleh penggunanya.

Namun dengan pemberlakuan prinsip strict liability dalam hukum terhadap produknya terutama terhadap pihak bank, bukan berarti pihak bank tidak mendapat perlindungan hukum melainkan pihak bank diberi kesempatan untuk membebaskan dirinya dari tanggung jawab ketika nasabah tidak dapat membuktikan bahwa memang betul kesalahan dilakukan oleh sistem pihak bank, adanya keadaan yang memaksa ataupun kelalaian dari pihak bank.

Dalam proses pembuktian pihak yang dinyatakan melakukan kesalahan, merujuk pada Pasal 19 Ayat 3 dan Pasal 45 Ayat 1 serta Pasal 47 Undang- Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen menyebutkan bahwa nasabah dalam hal ini sebagai konsumen dapat melakukan sengketa yang diselesaikan di luar maupun melalui pengadilan.

Menurut Pasal 48 Undang-Undang ini, penyelesaian sengketa melalui pengadilan dapat dilakukan oleh nasabah yang telah dirugikan atau ahli waris yang bersangkutan, sekelompok konsumen yang mempunyai kepentingan yang sama, pemerintah dan/atau instansi terkait ataupun lembaga perlindungan konsumen swadaya masyarakat.

Sementara dalam Pasal 19 Ayat (1) dan (3) UUPK ini menegaskan bahwa konsumen yang merasa dirugikan dapat menuntut secara langsung penggantian kerugian kepada produsen dan produsen harus memberi tanggapan dan/atau penyelesaian dalam jangka waktu 7 hari setelah transaksi berlangsung.

Upaya penanggulangan yang dilakukan oleh pihak bank dan Kepolisian terhadap kejahatan cyber di Nusa Tenggara Timur

Penanggulangan Kejahatan Siber Mengingat pelaku kejahatan siber terus berkembang dan memperbaharui virus, malware, atau piranti yang digunakan untuk menghindari deteksi, penanggulangan kejahatan siber merupakan persaingan persenjataan (armrace) yang tak

berkesudahan antara pelaku kriminal dan pihak-pihak yang berupaya melindungi korban potensial serangan kejahatan siber.

Berdasarkan hasil wawancara dengan kasubdit v siber ditreskrimsus ipda risky,SH, mengungkapkan bahwa faktor-faktor yang menyebabkan terjadinya tindak pidana cyber crime, yaitu:

1. Pelaku biasanya sudah mengetahui akan ancaman dari perbuatannya namun karena aturan yang mengatur hukuman atau ganjaran tidak begitu kuat, maka mereka tetap menjalankan aksinya.
2. Faktor ekonomi menjadi salah satu faktor mengapa orang cenderung melakukan jalan pintas agar mendapatkan uang dengan cara apapun asalkan cepat didapat.
3. Faktor penasaran dari pelaku, orang yang cenderung terlalu pintar dengan teknologi yang semakin maju akan melakukan eksperimen agar dapat menyalurkan bakat yang mereka punya walaupun dengan cara yang salah dan bukan pada wadahnya.

Dari faktor penyebab yang telah dijabarkan terdapat pula upaya penanggulangan dan solusi yang dilakukan Polda NTT dalam menanggulangi kejahatan cyber crime, berdasarkan hasil wawancara peneliti dengan kasubdit v siber ditreskrimsus ipda risky banyak metode penanggulangan yang sudah dilakukan untuk mengurangi tindak pidana cyber crime yang sedang marak dikalangan masyarakat yaitu:

1. Mengadakan sosialisasi mengenai kewaspadaan akan kejahatan siber

   Upaya penanggulangan yang dilakukan Polda NTT dalam menanggulangi kejahatan siber yaitu dengan sosialisasi kepada masyarakat mengenai etika dalam menggunakan kemajuan teknologi sehingga dapat dipergunakan dengan bijak oleh masyarakat.

   Selain itu, sosialisasi akan bermuatan tentang peraturan perundang-undangan yang berlaku agar korban dari kejahatan siber tidak merasa tidak mempunyai perlindungan akan kejadian yang menimpa mereka dan dapat membuat laporan kepada pihak berwajib.

   Sosialisasi ini bertujuan agar masyarakat ikut andil berpartisipasi dalam upaya menanggulangi kejahatan siber yang marak terjadi. Sosialisasi ini sudah mulai gencar dilakukan dalam satu bulan sekurang-kurangnya 2 kali dengan sasaran sosialisasi yaitu, pelajar atau mahasiswa, kalangab pemuda-pemudi, dan tokoh agama atau tokoh masyarakat.

2. Patroli siber

Patroli yang dilakukan di dalam kepolisian dalam pelaksanaannya, patroli siber sendiri patroli siber bertujuaan untuk mengawasi segala macam bentuk pelanggaran terhadap hukum di dalam internet terkhusus aplikasi media sosial biasanya dilakukan pada aplikasi seperti instagram, whatsapp, twitter. Patroli siber dilakukan untuk menciptakan ruang internet yang aman serta melindungi masyarakat dari kejahatan.

Dari Hasil wawancara dengan Ipda risky,SH, selaku kasubdit Ditreskimsus siber v NTT, Patroli siber dilakukan setiap hari selama 1x24 jam untuk memantau semua aktivitas yang terjadi di media sosial di wilayah hukum Polda NTT. Patroli siber dilakukan di kantor dengan menggunakan sarana dan prasarana berupa laptop atau PC (Personal Computer) inventaris Subdit siber Polda NTT dan pada waktu - waktu tertentu saat personil sedang di lapangan tetap melakukan patrol siber dengan menggunakan smartphone. Selama proses patroli selain memberikan himbauan proses patroli juga melakukan teguran terhadap perilaku buruk di media sosial.

3. Melakukan upaya preventif dan upaya represif

Selain upaya sosialisasi upaya preventif juga dilakukan dengan cara penyebaran dilakukan melalui media sosial Polda Nusa Tenggara Timur dalam bentuk foto dan video berisis himbauan agar masyarakat menggunakan media sosial dengan bijak dan lebih waspada kepada kejahatan siber yang terus terjadi.

Dalam melakukan upaya represif, pihak kepolisian Daerah Nusa Tenggara Timur telah mengambil tindakan dengan memproses setiap kasus Tindak Pidana Siber yang ditangani sesuai dengan aturan yang berlaku. Pihak kepolisian bekerja sama dengan stakeholder yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus Tindak Pidana Siber, setelah dilakukan penangkapan kemudian diproses dikepolisian sebelum dilimpahkan berkas perkaranya ke kejaksaan.

Tidak hanya pihak kepolisian saja yang wajib memberikan penanggulangan tetapi pihak perbankan juga ikut andil dalam kejahatan yang sering membuat pihak perbankan mengalami kerugian dan juga citra dari bank BRI menjadi buruk.

Melalui wawancara dengan Ass. Manager ops dan layanan bank bri cabang kupang yaitu hendrianto trijono, mengungkapkan pihak perbankan sudah membuat keamanan secanggih mungkin yang bahkan sulit ditembus oleh orang – orang awam

seperti yang pertama User ID dan PIN (Personal Identification Number) . Kedua, Automatic Log Out. Ketiga, dengan menggunakan kode otp (one time password). Keempat, fitur Safety Mode BRImo. Kelima, teknologi biometric yang dipunyai oleh aplikasi BRImo.

Hambatan Yang Dialami Pihak Kepolisian Dan Pihak Bank Terhadap Penanggulangan Yang Diberikan

Dalam menanggulangi Tindak Pidana siber berikut adalah kendala-kendala yang dialami kepolisian daerah NTT dalam menanggulangi tindak pidana siber yaitu :

1. Kendala Internal
   a. Lemahnya Pengawasan Pemerintah dan Kepolisian dalam penggunaan internet berpotensi besar akan menciptakan peluang terjadinya kejahatan cyber crime (dunia maya).

      Karena kejahatan dengan menggunakan teknologi terjadi jika ada akses internet yang cukup memadai. Fasilitas internet Di indonesia bisa dikatakan sudah memadai baik dari segi kecepatan akses dan kemudahan pemasangan jaringan akses internet. Dalam hal pengawasan pemerintah dan kepolisian harus mengontrol dan melakukan pengawasan terhadap trafic konten negative internet yang dapat diakses di indonesia. Seperti pemblokiran situs-situs porno, SARA, kekerasan dan situs-situs website yang dianggap menyalahi norma kesusilaan.

   b. Aspek Alat Bukti

      Alat bukti dalam kasus tindak pidana siber berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media cyber crime merupakan data-data atau system komputer / internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan. Selain itu saksi korban dalam kasus tindak pidana siber berperan sangat penting dimana jarang sekali terdapat saksi dalam kasus tindak pidana siber dikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan.

   c. Aspek Yuridiksi

      Penanganan tindak pidana siber tidak akan berhasil jika aspek yurisdiksi diabaikan. Karena pemetaan yang menyangkut kejahatan dunia maya menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Sehingga penetapan yurisdiksi yang mutlak diperlukan.

2. Kendala Eksternal

a) Kurangnya Kesadaran Hukum Masyarakat

Sampai saat ini, kesadaran hukum masyarakat Indonesia akan fungsi-fungsi tersebut dan dalam hal merespon aktivitas kejahatan mayantara (cybercrime) khususnya tindak pidana siber masih dirasakan kurang. Hal ini disebabkan karena kurangnya pemahaman dan pengetahuan masyarakat terhadap apa saja jenis-jenis kejahatan mayantara. Kurangnya pengetahuan ini menyebabkan upaya penanggulangan kejahatan mayantara mengalami kendala yang berkanaan dengan penataan hukum dan pengawasan (controlling) masyarakat terhadap setiap kegiatan atau aktivitas yang diduga berkaitan dengan tindak pidana siber.

b) Minimnya Respon Masyarakat

Kurangnya Respon Masyarakat terhadap sosialisasi atau penyuluhan yang dilakukan pihak Kepolisian, kendala yang dihadapi pihak Kepolisian dalam melakukan sosialisasi atau penyuluhan tentang tindak pidana siber yaitu kurangnya respon masyarakat terhadap apa yang dilakukan pihak Kepolisian ini membuktikan bahwa masyarakat masih minim pengetahuan tentang peraturan Undang-undang tentang cyber crime karena masyarakat menganggap bahwa teknologi itu merupakan hiburan semata dan menganggap tidak ada peraturan yang mengikat yang akan diberi sanksi ketika dilanggar.

c) Kurangnya Laporan Masyarakat

Kurangnya laporan masyarakat terhadap yaitu ketika terjadi tindak pidana siber di lingkungan masyarakat, mereka seakan tidak peduli dengan kegiatan tersebut. Hal ini berpengaruh terhadap kurangnya laporan yang masuk di kepolisian terkait tindak pidana siber. Dari keterangan beberapa masyarakat, mereka tidak melaporkan adanya tindak pidana siber karena kurangnya pengetahuan masyarakat tentang tindak pidana siber dan masyarakat cenderung menanggap hal tersebut biasa-biasa saja, mereka takut berurusan dengan kepolisan dan tidak mau memperpanjang masalah, sehingga untuk pelaporan kecil kemungkinan dilakukan oleh masyarakat.

KESIMPULAN

Berdasarkan hasil dan pembahasan diperoleh bahwa Bentuk pertanggung jawaban dari pihak bank menggunakan prinsip kelalaian ditimbulkan oleh pihak yang melakukan maka wajib bertanggung jawab atas tindakannya. Dalam kasus undangan pernikahan palsu yang diklik oleh nasabah pengguna mobile banking tanggung jawab sepenuhnya jatuh kepada

nasabah karena nasabah tidak menjaga dengan baik dan kurang berhati-hati dalam menggunakan media sosial. Upaya penanggulangan yang dilakukan oleh pihak kepolisian daerah NTT masih belum efektif, selain karena kurangnya alat untuk mencegah hal - hal seperti itu dapat masuk dan menimbulkan kerugian, penangkapan pelaku juga sulit dilakukan karena pelaku langsung menghapus akun yang dipakai untuk membuat tindak kejahatan. Hambatan pihak kepolisian dalam menanggulangi kejahatan siber sepatutnya menjadi tanggung jawab bersama baik pemerintah dalam hal menyediakan fasilitas yang lebih memadai dan canggih maupun dari sisi masyarakat yang kurang menyadari pentingnya kesadaran akan kejahatan siber yang kian hari makin bertambah banyak dengan berbagai modus kejahatan, sehingga dapat terjadinya kesinambungan dalam bahu – membahu menanggulangi kejahatan siber.

DAFTAR REFERENSI

Adami Chazawi. *Tindak Pidana Mengenai Kesopanan*, Rajagrafindo Persada, Jakarta.2005.

Akub, M Syukri. "Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia." Al-Ishlah : Jurnal Ilmiah Hukum 21, no. 2 (2020): 85–93.

Andi Hamzah, *Asas-Asas Hukum Pidana Edisi Revisi*, (Jakarta: Rineka Cipta, 2004).

Andi Hamzah, *Asas-Asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2010).

Alfitra, *Hukum Pembuktian dalam Beracara Pidana, Perdata dan Korupsi di Indonesia,* Raih Asa Sukses, (Penebar Swadaya Grup), 2002.

Arif Mansyur M, Dikdik dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, Bandung: PT. Refika Aditama.2005.

Bank Indonesia. "Peraturan Bank Indonesia Nomor 2/19/PBI/2000 Tentang Persyaratan Dan Tata Cara Pemberian Perintah Atau Izin Tertulis Membuka Rahasia Bank" (2000).

Besar."Kejahatan Dengan Menggunakan Sarana Teknologi Informasi"https://business-law.binus.ac.id/2016/07/31/kejahatan-dengan-menggunakan-sarana-teknologi-informasi.

Deris Setiawan. *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta. 2005.

Erdianto Effendi, *Hukum Pidana Indonesia Suatu Pengantar*, (Bandung: PT. Refika Aditama, 2014).

Fitri Wahyuni, *Dasar-Dasar Hukum Pidana Indonesia*, PT Nusantara Persada Utama, 2017.

Imron, Dkk. *Hukum Pembuktian*. *Jurnal Hukum & Pembangunan*. Vol. 16, 2017. https://www.mendeley.com/catalogue/63f3e7de-995c-3eda-b6af-edfdb1e480ed/?utm_source=desktop&utm_medium=1.19.8&utm_campaign=open_catalog&userDocumentId=%7Bc35be639-9b37-4493-a96e-8c0ade7a02e4%7D.

Indriyanto Seno Adji, Korupsi dan Hukum Pidana, (Jakarta: Kantor Pengacara dan Konsultasi Hukum "Prof. Oemar Seno Adji & Rekan, 2002).

Munir Fuady, *Teori Hukum Pembuktian,* Bandung, PT. Citra Aditya, 2006.

Nasution, Dewi Sartika, M Ec, Muhammad Muhajir Aminy, and Lalu Ahmad Ramadani.

"Ekonomi Digital." Mataram: Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Mataram, 2019.

P.A.F Lamintang, S.H., *Hukum Pidana Indonesia*, Bandung: Sinar Baru, cetakan ketiga, 1990.

Parenrengi, Sudarmin, and Tyahya Whisnu Hendratni. "Pengaruh Dana Pihak Ketiga, Kecukupan Modal Dan Penyaluran Kredit Terhadap Profitabilitas Bank." *Jurnal Manajemen Strategi dan Aplikasi Bisnis* 1, no. 1 (2018): 9–18.

Pujiyono, Agung Budiarto; ' "Perlindungan Hukum Nasabah Pengguna Mobile Banking." *Jurnal Privat Law* 9, no. Vol 9, No 2 (2021): JULI-DESEMBER (2021): 300–308. https://jurnal.uns.ac.id/privatlaw/article/view/60038/34997.

Rehulina, Hatialum, B R Silalahi, Yayasan Kesejahteraan, Pendidikan Dan, Fakultas Hukum, Program Studi, and Ilmu Hukum. "Analisis Yuridis Kejahatan Cyber Crime Dalam Pembobolan Mesin Atm Bank." Universitas Pembangunan Nasional "Veteran" Jawa Timur Fakultas Hukum, 2012.

Roeslan *Saleh, Perbuatan Pidana dan Pertanggungan Jawab Pidana Dua Pengertian Dasar Dalam Hukum Pidana*, (Jakarta: Aksara Baru, 1981), hlm.9.

Rondonuwu, Sabrina M. D. "Artikel Skripsi Mahasiswa Pada Fakultas Hukum Unsrat, NIM. 14071101110." *Lex Et Societatis* 6, no. 5 (2020): 42–49.

Sabartua Tambubolon.*Domain Name: Nama Domain*, Universitas Pelita Harapan, Jakarta.2002.

S.R Sianturi, *Asas-Asas Hukum Pidana dan Penerapannya di Indonesia* Cetakan Ke-2, Alumni AHAEM PTHAEM, Jakarta, 1998.

Soetandyo Wingjosoebroto, "*Penelitian Hukum: Sebuah Tipologi Majalah Masyarakat Indonesia"*, tahun ke-I, No.2,1974.

Styarini, Fitria, and Sulis Riptiono. "Analisis Pengaruh Customer Trust Terhadap Keputusan Menggunakan Mobile Banking Melalui Perceived Risk Dan Perceived Usefulness Sebagai Variabel Intervening." *Jurnal Ilmiah Mahasiswa Manajemen, Bisnis dan Akuntansi (JIMMBA)* 2, no. 4 (2020): 670–680.

Tofik Yanuar Chandra, SH., MH. *Hukum Pidana*. Edited by SH Yasmon Putra. *Nucl. Phys.* Vol. 13. PT. Sangir Multi Usaha, 2022.

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang dirubah dengan Undang-undang Nomor 19 Tahun 2016.

Wahyuni, Dr.Fitri. *Dasar-Dasar Hukum Pidana Indonesia*. *Perpustakaan Nasional*, 2017.

Wa Ode Nony Fauziah, " Penegakkan Hukum Pidana Terhadap Pelaku *Cyber Pornography* Wilayah Hukum Kepolisian Nusa Tenggara Timur", (Universitas Nusa Cendana Nusa Tenggara Timur Fakultas Hukum), 2022.

Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, (Bandung: Eresco, 1986).

Yurizal, S.H.M.H. *Penegakan Hukum Tindak Pidana Cyber Crime Di Indonesia*. 1. Media Nusa Creative (MNC Publishing), 2018. https://books.google.co.id/books?id=y8dGEAAAQBAJ. "Modus Penipuan Sniffing, Terbaru Bentuknya Undangan Digital." https://sampaijauh.com/modus-penipuan-sniffing-29007.