ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 5154-5159
Volume 8 Nomor 1 Tahun 2024

Pertanggung Jawaban Bank terhadap Pencurian Data Personal Nasabah dengan Menggunakan Teknik *Phising*

M Widya Pangestika[1], S Alfi Kamilatakhir[2], A Ul Hosnah[3]

[1,2,3] Program Studi Ilmu Hukum Fakultas Hukum Universitas Pakuan

e-mail: pangestikamiranti@gmail.com[1], salfikt321@gmail.com[2], asmak.hosnah@unpak.ac.id[3]

Abstrak

Teknologi dan informasi saat ini sangat berkembang pesat. Dengan berkembang nya teknologi memudahkan orang untuk mengakses dan mendapatkan informasi dimana pun. Termasuk dalam bidang perbankan, salah satu nya data pribadi nasabah mudah diretas oleh oknum tidak bertanggung jawab. Kejahatan di sektor perbankan menggunakan teknik *phising* sudah banyak terjadi khususnya di Indonesia yang disebut dengan kejahatan siber. menurut Anti Phising Data Exchange (IDADX) terdapat 26.000 domain phising pada kuartal I-2023. Kejahatan siber di Indonesia diatur dalam pengaturan UU ITE, KUHP dan juga UU Perbankan. Dalam jurnal ini penulis menggunakan metode hukum normatif yaitu deskriptif analitis, dengan berdasarkan data sekunder selaku data pokok dengan teknik pengumpulan data pustaka.

Kata Kunci : *Teknologi, Perbankan, Kejahatan Siber.*

Abstract

Technology and information are currently developing very rapidly. With the development of technology, it makes it easier for people to access and get information anywhere. Including in the banking sector, customer personal data is easily hacked by irresponsible individuals. Crimes in the banking sector using phishing techniques have often occurred, especially in Indonesia, which are called cyber crimes. according to IDADX there are 26,000 phishing domains in the first quarter of 2023. Cyber crime in Indonesia is regulated in the ITE Law, Criminal Code and also the Banking Law. In this journal the author uses a normative legal method, namely analytical descriptive, based on secondary data as main data with library data collection techniques.

Keywords: *Technology, Banking, Cyber Crime*

PENDAHULUAN

Dampak dari pesatnya perkembangan teknologi menyentuh segala aspek kehidupan manusia, khususnya internet berpengaruh pada proses bisnis di industri perbankan. Lembaga keuangan yaitu bank adalah sektor utama dalam keuangan dalam suatu negara. Perbankan di Indonesia diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Apabila dilihat dari kasus-kasus yang sudah terjadi, dan apabila hal ini dikaitkan dengan menggunakan syarat aturan hukum pidana umum, kenyataannya bahwa dari sudut pandang hukum kejahatan komputer dan kejahatan dunia maya tidak bisa dikatakan sebagai tindak kejahatan yang ringan (david I. Bainbridge, 1993 ; 161).

Kemajuan teknologi dan informasi melalui dunia maya, adalah suatu cara media untuk membagikan informasi secara cepat dan masif yang berdampak negatif karena ada oknum yang menyalahgunakan dan tidak bertanggung jawab untuk menghasilkan keuntungan melalui cara meretas data pribadi nasabah untuk mendapatkan *password*

dengan menggunakan teknik *phising.* Lembaga keuangan merupakan salah satu target utama eksploitasi bagi pelaku *cyber crime.*

Kecanggihan alat informasi dan komunikasi memiliki dampak positif yaitu mempermudah pekerjaan manusia untuk mengakses informasi dari seluruh dunia hanya, meningkatkan produktivitas dan sangat membantu dalam menjalankan bisnis. Namun, terdapat juga dampak negatif, seperti ketergantungan yang berlebih pada alat komunikasi tersebut serta semakin mudah oknum untuk meretas data-data pribadi jika tidak berhati-hati dalam menggunakan fasilitas tersebut. Sehingga penting untuk menjadi pengguna yang bijak.

Teknik *phising* adalah upaya untuk memperoleh informasi atau data pribadi dengan upaya pengelabuan. Data yang diperoleh dengan teknik *phising* tersebut merupakan data personal milik nasabah yang di input oleh korban pada laman palsu seperti e-mail atau website. Pencurian data dengan *Phising* memang dimaksudkan untuk memancing korban agar memberi data pribadi nya secara tidak sadar. Pelaku yang melakukan *phising* biasanya mengaku sebagai pihak atau institusi lain. Hal ini bukan hanya merugikan korban saja tetapi juga merugikan bank yang telah diakui oleh pelaku Karena berdampak buruk pada kepercayaan masyarakat.

Menurut Pelaksana Nama Domain Internet (PANDI) bahwa sudah berlangsung 26.675 tindakan *phising* pada kuartal I - 2023. Mayoritas mengutamakan pada sektor keuangan. “Dari jumlah tersebut, kebanyakan terjadi pada sektor bisnis keuangan” jelas Deputi Pengembangan, Riset Terapan, Inovasi dan Teknik. Masyarakat harus lebih waspada pada ancaman phising ini karena pada saat ini nama domain phising menggunakan protocol HTTPS. Pada tahun 2023 telah terjadi sebesar 99% yang menggunakan HTTPS.

Terjadi peningkatan laporan domain phising pada tahun 2023. Hal tersebut mungkin disebabkan oleh peningkatan jumlah penggunaan domain biz.id pada tahun 2022. Dengan adanya inisiasi anti phising IDADX bertujuan untuk meningkatkan keamanan siber nasional dengan memberikan fasilitas respon global terhadap kejahatan siber disektor pemerintahan, hukum, industri dan yang lainnya.

Kejahatan *cyber crime (phising)* telah diatur dalam Undang - Undang Nomor 11 Tahun 2008 Tentang informasi dan transaksi elektronik Pasal 35 jo. Pasal 51 ayat (1) dijerat ancaman maksimal 12 tahun penjara dengan unsur delik dimana setiap orang yang melakukan manipulasi, menciptakan, merubah atau mentransmisikan, menghilangkan serta melakukan pengrusakan data atau sistem informasi elektronik dengan sengaja melakukan tindakan melawan hukum dengan tujuan dokumen atau informasi elektronik tersebut dianggap dari pihak resmi,

Dalam penulisan ini mencakup uraian singkat yang berasal dari penelitian terdahulu. Penelitian terdahulu tersebut sebagai bahan perbandingan dan acuan dalam penulisan. Dan juga untuk menambah teori yang digunakan dalam penulisan artikel ini. Sehingga, penulis mampu menghindari kesamaan judul pada penelitian yang sejenis. Penelitian terdahulu hanya menjadi acuan dan perbandingan dengan penelitian yang lainnya. Berikut ini merupakan beberapa penelitian terdahulu yang menjadi acuan bagi penelitian yang sedang penulis lakukan.

Penelitian ini dilakukan oleh Erwin Ginting, dkk (2023) dengan judul *“Analisis Ancaman Phising Terhadap Layanan Online Perbankan”.* Penelitian ini bertujuan untuk mengetahui cara kerja phising, teknik phising, dan dampak phising dari pada kasus bank. Dari penelitian ini dapat diketahui bahwa phising merupakan kejahatan dunia maya dengan menyamar sebagai pihak terkait.

Tujuan dari penulisan ini untuk mengetahui sejauh mana hukum di Indonesia berlaku untuk mengatasi permasalahan pencurian data pribadi nasabah dengan teknik phising yang sudah marak terjadi. Apakah sudah terlaksana dengan baik atau tidak. Serta pencegahan terhadap peretasan data pribadi nasabah bank.

METODE

Dalam penulisan menggunakan metode penulisan hukum normatif dengan menganalisis permasalahan hukum yang telah terjadi didasarkan pada undang-undang. Dan mengumpulkan data dari penelitian terdahulu sebagai bahan referensi.

HASIL DAN PEMBAHASAN

Penjelasan mengenai kejahatan siber

Cyber crime adalah suatu bentuk kejahatan dengan pemanfaatan teknologi informasi yaitu jaringan komputer dan para pengguna nya. Cyber Crime atau kejahatan dunia maya merupakan jenis kejahatan dengan cara yang biasa dilakukan dari jarak jauh. Hal ini tidak lepas dari perkembangan teknologi digital yang semakin canggih di segala aspek kehidupan manusia sehingga memudahkan kejahatan siber terjadi. *Cyber Crime* menggunakan kecanggihan teknologi komputer dan internet untuk mencuri data pribadi seseorang untuk kepentingan pribadi. *Cyber Crime* berdampak buruk bagi korban karena hal tersebut merugikan korban secara materiil dan nonmaterial.

Kejahatan siber ini memiliki ruang lingkup sangat luas yang dapat menembus ruang dan waktu, nasional maupun global serta dapat dilakukan dimana pun dan kapan pun. Teknologi yang berkembang pesat ini memberikan efisiensi dan mengurangi biaya operasional pada perusahaan. Namun disisi lain, kejahatan dengan menggunakan jaringan komputer sangat rentan karena kemudahan dalam mengakses tersebut.

Cyber Crime ini seringkali terjadi bukan karena kelalaian pihak bank melainkan karena minimnya pemahaman tentang perkembangan teknologi dan informasi masa kini. Sehingga sangat penting diadakan sosialisasi pada masyarakat bagaimana pentingnya untuk tidak mudah memberikan data pribadi di situs tidak resmi.

Sedangkan pengertian dari Cyber law merupakan sekumpulan peraturan dari suatu negara tertentu, aturan jika sudah disahkan oleh negara tersebut hanya berlaku untuk masyarakat Negara tersebut. Dapat dikatakan hukum siber merupakan hukum yang diperuntukkan di dunia maya, pada dasarnya menggunakan internet.

Penjelasan mengenai Teknik *Phising*

Phising ditemukan sekitar tahun 1996, cara yang digunakan pertama kali pada teknik *phising* ini adalah dengan mengacak nomor kartu kredit nasabah. *Phising* juga disebut "*Brand Spoofing"* atau "*carding".* Dalam sektor perbankan phising merupakan tindak kejahatan siber dengan modus operandi yang mengakibatkan *fraud. Fraud* adalah tindakan melanggar hukum oleh sekelompok orang untuk meraup keuntungan finansial berasal dari pemakaian kartu kredit yang bukan hak miliknya. *Fraud* biasanya menyerang online banking dan kartu kredit nasabah. Kasus fraud dalam kartu kredit biasanya oknum tersebut mengincar 4 digit angka terakhir pada kartu kredit dan nomor PIN-nya. Kemudian pelaku mempergunakan informasi tersebut untuk bertransaksi atas nama nasabah.

Phising adalah suatu upaya untuk menghasilkan data personal seperti nama pengguna, *PIN,* nomor rekening, nomor kartu kredit secara ilegal melalui e-mail palsu atau website tidak resmi dengan menyatakan bahwa pengirim dari institusi yang sah. Data pribadi nasabah bank merupakan hal privasi sehingga harus dirahasiakan dan perlu mendapat perlindungan dari pihak bank.

Data Pribadi nasabah yang memuat nama, alamat, tanggal lahir, *e-mail* dan nomor ponsel harus dijaga kerahasiaannya dan tidak dapat diretas oleh siapapun sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 26 ayat (1) bahwa kecuali diwajibkan oleh undang-undang, bahwa pemakaian setiap informasi apapun pada media elektronik yang berkaitan dengan data personal seseorang harus dibuat dengan kesepakatan antara kedua belah pihak. Tetapi kenyataannya, hal ini belum mendapat perlindungan penuh dari pihak perbankan, sehingga masih sering terjadi kebocoran data pribadi nasabah bank.

Berikut beberapa teknik *phising* yang dilakukan oleh phiser dalam melakukan aksinya:

1. Manipulasi tautan link
   Manipulasi link merupakan teknik yang dilakukan phiser dengan cara mengirim link palsu. Seperti yang terjadi baru-baru ini dengan mengirim link undangan, ketika link tersebut dibuka otomatis terhubung dengan phiser sehingga saldo atau data pribadi korban diretas.
2. Rekayasa Sosial
   Untuk modus penipuan rekayasa sosial yaitu menyalahgunakan data pribadi dengan mengatasnamakan lembaga pemerintahan misalnya dinas sosial mengadakan rekrutmen relawan, lalu korban diminta untuk mengisi data pribadi seperti e-mail, nomor telepon, alamat, dan lain-lain.
3. Phising Telepon
   Pelaku *phising* telepon biasanya mengaku sebagai pegawai bank dan meminta korban untuk menyebutkan kode rahasia atau OTP. Ketika kode OTP diberikan maka phiser dapat mengakses data pribadi dan menyalahgunakannya.

Pengaturan pencurian data pribadi nasabah bank

Peraturan perundang-undangan mengenai data personal dan data diri nasabah tercantum dalam Undang-Undang Nomor 24 Tahun 2013 jo. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, menyatakan data perorangan adalah salah satu data yang di amankan, dirawat, dan terjaga kebenarannya dan harus diberikan perlindungan terhadap kerahasiaannya.

Identitas personal nasabah memiliki kegunaan untuk membuka layanan perbankan bagi nasabah. Seperti membuka rekening, kartu kredit, deposito, dan lain sebagainya. Dalam pengisian data pribadi bisa dilakukan secara online menggunakan aplikasi maupun secara langsung. Sehingga bisa dikatakan hubungan hukum nasabah dengan pihak bank didasarkan simbiosis mutualisme. Dimana nasabah kedudukannya sebagai konsumen.

Nasabah sebagai konsumen perbankan yang telah tercantum pada Undang-Undang Nomor 8 tahun 1999 tentang perlindungan konsumen. Tetapi dalam UU tersebut tidak dikhususkan untuk mengatur perlindungan pada data personal nasabah dalam transaksi bank. Tindak pidana pencurian adalah suatu tindakan kejahatan seperti tercantum pada Pasal 362 KUHP 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 dan denda paling banyak enam puluh rupiah”.

Perlindungan data personal dalam bidang perbankan telah dijelaskan dalam Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Berdasarkan pada pasal tersebut dijelaskan yaitu bank mengharuskan menjaga kerahasiaan data nasabah yang tersimpan.

D. Pertanggungjawaban Lembaga keuangan yaitu bank terhadap Pencurian Data Diri pada Nasabah Bank dengan *Phising*

Perbankan merupakan sektor keuangan yang dipercaya masyarakat untuk bertransaksi dan menyimpan dana. Masyarakat mempercayai bank karena memiliki prinsip kehati-hatian dan manajemen resiko dalam penyelenggaraan transaksi. Tetapi semakin canggih teknologi memperbesar kemungkinan adanya oknum yang tidak bertanggung jawab untuk meretas. Penjelasan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik yang sebetulnya bisa memperkuat kenyamanan serta keamanan pada pengguna bank ketika berlangsungnya aktivitas perbankan dengan sistem teknologi yang difasilitasi oleh pihak bank. Tetapi, berbagai pengaturan yang tercantum pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik harus disertai dengan aturan hukum yang lebih mendalam dengan berkolaborasi dengan peraturan pemerintahan.

Contoh kejahatan pencurian data nasabah bank yaitu dengan teknik *phising.* Menurut penelitian cyber war dan security inspection menyatakan, phising merupakan tindakan dalam penipuan dengan cara memakai surat elektronik yang bertujuan agar memperoleh

username, password, dan informasi pribadi lain yang dikirim melalui laman palsu. Penipuan ini melalui surel phising yang seakan-akan dari lembaga di mana pengguna adalah anggota dari lembaga tersebut.

Pencurian data menggunakan Teknik *phising* marak terjadi dalam industri perbankan yang tentu dapat menyebabkan kerugian pada nasabah sebagai konsumen layanan perbankan. Kemudian dalam masalah ini timbul pertanyaan, siapa saja yang akan menanggung kerugian yang dialami nasabah? Sebenarnya pertanggungjawaban dimulai sejak adanya ikatan hukum antara masing-masing melalui ikatan. Pihak bank dan pengguna memiliki hubungan hukum yang menimbulkan hak dan kewajiban diantara mereka. Dalam upaya perlindungan konsumen, Undang-Undang Informasi dan Transaksi Elektronik memuat pengaturan yang mengatur tentang teknologi netral yang berguna untuk transaksi elektronik, dengan syarat terdapat persetujuan untuk menggunakan sistem elektronik. Tetapi aturan hukum itu sudah daluarsa berkaitan dengan terdapat bukti telah mengalami keadaan mendesak, kesalahan, dan/atau kelalaian dari orang yang memakai sistem elektronik (Pasal 15 UU ITE).

Pada saat melakukan transaksi, pihak yang menanggung segala risiko yang akan terjadi dalam melakukan transaksi elektronik yaitu:

1. Apabila dilakukan tanpa melibatkan pihak lain (seorang diri) maka segala resiko hukum akan ditanggung oleh diri sendiri bukan pihak bank.
2. Apabila dilakukan dengan perantara agen elektronik, maka apapun risiko hukum pada saat transaksi dilakukan maka menjadi pertanggungjawaban agen tersebut.
3. Dalam hal kerugian dalam melakukan transaksi elektronik terjadi akibat atas kesalahan agen elektronik dampak dari tindakan langsung pihak lain pada sistem elektronik, mengakibatkan semua akibat hukum ditanggung oleh pihak agen. Sebaliknya, apabila kerugian dalam suatu transaksi elektronik menyebabkan tidak berfungsinya agen elektronik dampak kelalaian dari konsumen jasa, demikian seluruh sanksi hukum ditanggung oleh konsumen jasa. Kecuali ketentuan tersebut dapat dibuktikan apabila terdapat paksaan, kesalahan atau kelalaian pihak pengguna.

Selanjutnya, industri perbankan tetap bertanggung jawab pada kerugian yang telah terjadi pada nasabah saat menggunakan jasa keuangan bank, jika terdapat bukti yang menyatakan pelanggaran menyangkut pada kelalaian bocornya data personal nasabah penyebabnya kesalahan oleh industri terkait. Kemudian Bank akan memberikan perlindungan hukum kepada nasabah yang telah dirugikan berdasarkan yang telah diatur dalam Undang-undang Nomor 10 Tahun 1998 tentang perbankan dan UU ITE.

Dalam kasus ini bagi kami terlihat bahwa kurangnya penegakan hukum yang diberikan oleh pemerintah sehingga para pelaku masih banyak melakukan hal seperti ini dan hukuman yang diterima oleh pelaku masih belum cukup untuk membuat jera. Bahkan tak jarang bahwa para pelaku tidak dapat tertangkap atau sulit dicari karena berkembangnya teknologi sehingga mereka melakukan aksinya dengan teknologi yang canggih juga. Bahkan terkadang aparat pemerintahan terutama kepolisian sulit untuk melacak pelaku yang dimana biasanya pelaku akan berhati hati terhadap identitasnya sendiri. Pelaku juga terkadang menyimpan uang hasil curian tersebut di bank luar negeri sehingga uang tersebut tidak dapat disita oleh pihak yang berwajib. Biasanya juga uang yang dihasilkan dari pencurian tersebut bukanlah jumlah yang kecil dan hal ini sangat membuat kerugian bagi pihak korban. Terlebih jika kejadian ini dilakukan atas kelalaian pribadi bukan kelalaian pihak bank sehingga pihak bank merasa tidak perlu untuk mengganti rugi.

SIMPULAN

Pencurian data personal nasabah bank menggunakan teknik *phising* merupakan tindak pidana kejahatan yang muncul karena dampak buruk dari perkembangan teknologi dan informasi yang semakin pesat. Sedangkan masih ada saja segelintir orang yang tidak mengikuti perkembangan teknologi masa kini. Apabila tidak dilakukan himbauan atau sosialisasi kepada masyarakat maka semakin besar peluang oknum tidak bertanggungjawab untuk menjalankan aksinya. Dengan demikian tentunya tidak hanya menyebabkan dampak

negatif berupa kerugian pada nasabah bank tetapi juga merugikan pihak bank terkait. Kasus pencurian data pribadi nasabah bank merupakan kejahatan pidana pencurian tercantum pada Pasal 362 KUHP sedangkan tentang perlindungan data nasabah bank tercantum dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Sejatinya bahwa teknik *phising* ini masih sulit dihindari bagi masyarakat terutama untuk kalangan lanjut usia yang tidak begitu mengetahui teknologi. Maka dari itu perlu sekali kerjasama yang baik antara masyarakat dan pemerintah dalam menanggulangi permasalahan ini. Salah satu caranya adalah dengan mengadakan sosialisasi terhadap masyarakat yang dilakukan secara langsung untuk masyarakat bukan melalui sosial media karena permasalahan utamanya adalah kurangnya edukasi dalam pemakaian teknologi yang bijak sehingga memudahkan pelaku kejahatan dalam melakukan aksinya. Dan juga memperkuat akibat hukum bagi pelaku yang melakukan pelanggaran dan perlindungan hukum bagi pengguna bank. Namun, tetap saja bahwa kejahatan dalam perbankan ini masih sulit dihindari maka dariitu sebaiknya kita sebagai pengguna bank terutama *online banking* lebih waspada dalam melakukan transaksi yang mencurigakan.

DAFTAR PUSTAKA

Ginting Erwin,dkk, *Analisis Ancaman Phising terhadap Layanan Online Perbankan (Studi kasus pada Bank BRI),* Vol 8, UNES Journal Of Scientech Research, 1 Juni 2023.

Kitab Undang-Undang Hukum Pidana (KUHP)

Pratiwi Fuji, "*Ada 26 ribu Phising Domain pada Kuartal I 2023",* https://ekonomi.republica.co.id

Suparni Niniek, *Masalah Cyber Space,* Fortun Mandiri Karya, Jakarta 2001.

Wahyu Putri, *Tindak Pidana Pencurian Data Nasabah dalam Bidang Perbankan Sebagai Cyber Crime,* Vol 2 No. 2, Jurnal Hukum dan Perundang-Undangan, 20 juli 2022.