Jurnal Pro Hukum:

Jurnal Penelitian Bidang Hukum Universitas Gresik Volume 12 Nomor 3, Maret 2023 pISSN 2089-7146 - eISSN 2615-5567

PERLINDUNGAN HUKUM TERHADAP KEJAHATAN PHISING PADA CHANNEL E-BANKING MELALUI TRANSFER VIRTUAL ACCOUNT (STUDI KASUS PADA PENGGUNA INTERNET BANKING)

Rosalia Herlina Sutanti[1], Markoni[2]
Universitas Esa Unggul[1,2]
Email : nina.waluyo@gmail.com

ABSTRAK

Penelitian ini membahas mengenai perlindungan hukum terhadap kejahatan phising pada channel e-banking melalui transfer Virtual Account, dengan studi kasus pada pengguna internet banking. Produk internet banking yang merupakan salah satu delivery channel perbankan, merupakan "the must have product", bukan saja "nice to have product" bagi kalangan perbankan karena menjawab berbagai kebutuhan nasabahnya. Namun di balik manfaat yang besar bagi nasabah, produk perbankan ini juga memiliki risiko yang tidak kecil bagi penggunanya. Ada beberapa penelitian yang membahsa mengenai phising, namun dalam penelitian ini penulis menitik beratkan pada phising yang dengan menggunakan Virtual Account sebagai sarana transfer dana. Metode yang dipakai adalah penelitian normatif yang didukung dengan data empiris, dengan tujuan untuk mengetahui bagaimana peraturan perundang-undangan melindungi korban phising pada channel e-banking melalui transfer Virtual Account. dengan merujuk pada peraturan lain yaitu UU no 8 tahun 1999 tentang perlindungan konsumen dan UU no 19 tahun 2016 tentang perubahan atas UU no 11/ 2008 tentang ITE dan UU no 27 tahun 2022 mengenai Perlindugan Data Pribadi.

Kata Kunci: Perlindungan Hukum, Kejahatan Phising, Pengguna Internet Banking

ABSTRACT

This research is discusses about legal protection against phishing crimes on e-banking channels through virtual account transfers, with case studies on internet banking users. Internet banking product, which is one of the banking delivery channels, is the must have product for the banking institution, not only as the nice to have product. It's provides convinience features for it users, but also has risks that can harm its users at the same time. There are several studies that discuss phishing, but focus of this study is phising by using a Virtual Account as a transferring funds method. The method used is normative research supported by empirical data, to know how laws and regulations protect victims of phishing on e-banking channels through Virtual Account transfers by reffering Law No. 8 of 1999 concerning Consumer Protection, Law No. 19 of 2016 concerning Amendments to Law No. 11/2008 concerning ITE and Law No 13 of 2022 concerning Privacy Data Protection.

Keywords: Binary Options, Refunds, Crime

Pendahuluan

Memiliki rekening pada suatu bank pada saat ini merupakan suatu keharusan bagi setiap orang. Meskipun data dari bank Indonesia menyebutkan bahwa masih terdapat 91,3 juta penduduk berstatus unbankable, namun bagi sebagian besar orang, produk perbankan merupakan suatu kebutuhan yang sangat mendukung aktivitas sehari-hari (Arkanuddin, Nugroho, & Wijaya, 2022). Kenyataan adanya penduduk yang masih berstatus *unbankable*, tentu saja bukanlah tanpa sebab, dan umumnya mereka tidak mau membuka rekening di bank karena birokrasi yang bertele-tele, kantor bank yang jauh dari tempat tinggal dan sebab lainnya. Sebagian masalah tersebut telah terjawab dengan berbagai inovasi produk perbankan. Salah satunya adalah internet banking. Internet Banking merupakan salah satu produk yang menjadi *"the must*

have product" bagi kalangan perbankan, dan bukan hanya sebuah *"nice to have product"*, apa lagi dengan jumlah pengguna internet yang makin hari makin bertambah banyak. Internet banking tidak hanya dibutuhkan oleh nasabah perorangan, namun jenis produk perbankan ini juga dibutuhkan oleh para pebisnis. Tentu kita tidak bisa membayangkan bagaimana repotnya membawa sejumlah besar uang tunai untuk membayar gaji bulanan karyawan bukan? Dengan teknologi internet banking ini, pengusaha hanya membutuhkan seperangkat gadget untuk melakukan berbagai transkasi untuk mendukung operasional mereka sehari-hari.

Walaupun Pemerintah belum mengatur secara khusus mengenai internet banking, namun kita dapat melihat bahwa kehadiran internat banking dapat tercermin dalam Pasal 4 UU ITE, di mana "Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

a. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
b. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
c. Meningkatkan efektivitas dan efesiensi pelayanan publik;
d. Membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
e. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggaraan teknologi informasi."

Tidak berhenti pada kemudahan dalam transfer dana melalui internet banking, kalangan perbankan pun telah menambah kemudahan bertransaksi dengan adanya fasilitas Virtual Account. Virtual Account adalah nomor identifikasi pelanggan perusahaan yang dibuka oleh Bank atas permintaan perusahaan untuk selanjutnya diberikan oleh perusahaan kepada pelanggannya (perorangan maupun non perorangan) sebagai Nomor Rekening Tujuan penerimaan (collection). Dengan mengirimkan dana melalui Virtual Account, pengirim dana tidak perlu repot mengirimkan bukti transaksi, karena pihak penerima dana dapat mengecek asal dan jumlah dana yang diterima pada rekening penampungan milik nasabah tersebut (Hartanto & Ramli, 2018). Tentu saja hal ini sangat mempermudah pihak pemilik rekening, terutama yang memiliki skala bisnis retail yang besar dengan trafik transaksi yang tinggi. Pada penulisan kali ini pembahasan mengenai internet banking tidak dibatasi pada transaksional berbasis web namun juga yang berbasis mobile.

Teknologi dalam bidang apa pun juga bertujuan untuk mempermudah kehidupan, namun tetaplah memiliki sisi positif dan negatif (Putri et al., 2022). Demikian juga dengan intenet banking. Dengan kepraktisannya, internet banking dapat diakses dan digunakan di mana saja tanpa hambatan ruang dan waktu. Yang dibutuhkan oleh pengguna hanyalah seperangkat gadget yang telah diinstal dengan aplikasi dari bank tempat nasabah menyimpan dananya, dan jaringn intenet untuk mengaksesnya. Sangat simple. Namun kepraktisan tersebut juga dibayangi dengan bahaya yang mengintai penggunanya, utamanya adalah kejahatan dunia maya yang sangat marak, salah satunya adalah phising. Phising, yang merupakan singkatan dari password harvesting phising, adalah suatu aktivitas seseorang untuk mendapatkan informasi rahasia dengan cara menggunakan email, situs web palsu yang di tampilannya

menyerupai web aslinya. Phiser bertindak seolah-olah sebagai perwakilan perusahaan yang menyampaikan informasi undian, pengiriman pulsa gratis, sampai dengan bertindak sebagai customer service dari institusi keuangan yang pada akhirnya menggiring korban untuk memberi atau menginput data pribadi pada web palsu tersebut yang berujung pada kerugian korban.

Maraknya kejahatan phising ini dapat dilihat dari hasil survey yang dilakukan penulis, di mana dari 68 form kuesioner yang disebarkan kepada responden, terdapat 63% orang yang mengalami kejahatan phising, baik pada tahap percobaan maupun telah mengalami kerugian (Zuhri et al., 2020). Mereka mengalami kejahatan tersebut melalui sosial media yang menawarkan hadiah maupun bertindak sebagai otoritas resmi suatu instansi. Dalam kasus phising pada transaksi perbankan, saat ini phiser telah memanfaatkan salah satu cara pembayaran yaitu melalui Virtual Account, yang dapat dieksekusi baik melalui internet banking atau mobile banking maupun ATM. Virtual Account ini bukanlah rekening riil sehingga tidak dapat diblokir secara otomatis pada saat nasabah pemilik dana melaporkan kepada bank. Banyak nasabah yang tidak mendapatkan cara penyelesaian dari pihak Bank sebagai institusi tempat mereka menyimpan dana.

Dalam beberapa kasus Bank terkendala untuk memediasi karena rekening tujuan pada kasus phising adalah rekening Virtual Account yang dibuka oleh institusi untuk pemakainya. Dalam hal ini hubungan antara Bank dengan rekening yang dituju bukanlah hubungan antara Bank dengan nasabah secara langsung. Semakin tinggi teknik dan tingkat kejahatan para phiser, maka para nasabah membutuhkan sistem keamanan tingkat tinggi pula, sebab banyak penyerang atau phiser yang tertarik untuk mengeksploitasi data para nasabah apabila tingkat keamanan rendah. Phiser dapat melakukan tindakannya dengan berbagai media, yaitu email, SMS, WhatsApp text, dan Telegram yang dapat mengarahkan korbannya pada tindakan yang berujung pada kerugian.

Nasabah yang mengalami perpindahan dana tanpa disadari oleh mereka, biasanya mengadukan hal tersebut kepada bank di mana dana mereka disimpan. Pengaduan nasabah adalah bentuk perwujudan dari perlindungan hukum yang dimiliki oleh nasabah yaitu hak untuk untuk didengar. Hak tersebut diatur dalam pasal 4 huruf d Undang Undang no 8 tahun 1999 tentang perlindungan konsumen (UUPK), yang pada sektor jasa keuangan diatur lebih lanjut dalam Peraturan Otoritas jasa Keuangan Nomor 1 /POJK 07/ 2013 tentang Perlindungan Konsumen Setor jasa Keuangan (POJK PK).

Pembahasan mengenai perlindungan hukum sendiri, dijelaskan oleh beberapa ahli antara lain yaitu (Chandra & Syam, 2016) :

a. Teori perlindungan hukum dari Salmond bahwa hukum bertujuan mengintegrasikan dam mengkoordinasikan berbagai kepentingan dalam masyarakat, karena dalam suatu lalulintas kepentingan, perlindungan terhadap kepentingan tertentu dapat dilakukan dengan cara membatasi berbagai kepentingan di lain pihak (Sinaulan, 2018). Kepentingan hukum adalah mengurusi hak dan kepentingan manusia, sehingga hukum memiliki otoritas tertinggi untuk menentukan kepentingan manusia yang perlu diatur dan dilindungi. Perlindungan hukum harus melihat tahapan yakni perlindungan hukum lahir dari suatu ketentuan hukum dan

segala peraturan hukum yang diberikan oleh masyarakat yang pada dasarnya merupakan kesepakatan masyarakat tersebut untuk mengatur hubungan perilaku antara anggota-anggota masyarakat dan antara perseorangan dengan pemerintah yang dianggap mewakili kepentingan masyarakat.

b. Perlindungan hukum adalah adanya upaya melindungi kepentingan seseorang dengan cara mengalokasikan suatu kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut (Rahardjo, 2003).
c. Perlindungan hukum diartikan sebagai tindakan melindungi atau memberikan pertolongan kepada subyek hukum dengan perangkat-perangkat hukum. Bila melihat pengertian perlindungan hukum di atas, maka dapat diketahui unsur-unsur dari perlindungan hukum, yaitu: subyek yang melindungi, obyek yang akan dilindungi alat, instrumen maupun upaya yang digunakan untuk tercapainya perlindungan tersebut (Sahlan, 2016).
d. Hukum dapat difungsikan untuk mewujudkan perlindungan yang sifatnya tidak sekedar adaptif dan fleksibel, melainkan juga prediktif dan antipatif (Rasjidi, Sos, & Putra, 1993).

Dari uraian para ahli di atas dapat dipahami bahwa perlindungan hukum merupakan gambaran dari bekerjanya fungsi hukum untuk mewujudkan tujuan-tujuan hukum, yakni keadilan, kemanfaatan dan kepastian hukum. Perlindungan hukum adalah suatu perlindungan yang diberikan kepada subyek hukum sesuai dengan aturan hukum, baik itu yang bersifat preventif maupun dalam bentuk yang bersifat represif, baik yang secara tertulis maupun tidak tertulis dalam rangka menegakkan peraturan hukum. Perlindungan hukum adalah memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati semua hak-hak yang diberikan oleh hukum atau dengan kata lain perlindungan hukum adalah berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun.

Banyaknya kasus phising akan berakibat negatif, bukan hanya bagi nasabah, namun juga bagi bank sebagai lembaga keuangan dan juga pemerintah. Bank adalah salah satu pemangku regulasi tertinggi karenanya kegagalan bank akan menimbulkan biaya sosial yang tinggi berupa hilangnya peran bank sebagai lembaga intermediasi dan transmisi dalam sistem pembayaran (Sihombing, 2010).

Dengan maraknya kasus phising yang penulis amati, maka penulis tertarik melakukan penelitian yang membahas mengenai perlindungan hukum terhadap kejahatan phising pada channel E-Banking melalui transfer Virtual Account dengan studi kasus pada pengguna internet banking.

Ada beberapa penelitian yang membahas mengenai phising pada internet banking, namun pada penelitian ini penulis berfokus pada transaksi internet banking melalui trasnfer Virtual Account.

Berdasarkan latar belakang yang telah diuraikan di atas, maka rumusan masalah yang diangkat dalam penelitian ini adalah mengenai perlindungan hukum terhadap kejahatan phising pada channel E-Banking melalui transfer Virtual Account dengan studi kasus pada pengguna internet banking, serta bagaimana langkah perlindungannya.

Metode Penelitian

Penelitian ini merupakan penelitian normatif yang didukung dengan data empiris, yaitu gabungan unsur normatif berupa analisis Undang Undang dan didukung dengan data-data lapangan, seperti hasil wawancara dan kuisioner. Penelitian normatif empiris adalah penelitian hukum mengenai pemberlakuan atau implementasi ketentuan hukum normatif secara in action pada setiap peristiwa hukum tertentu yang terjadi dalam masyarakat. Sumber data yang digunakan adalah data yang diperoleh secara langsung dari sumber utama seperti kuesioner yang disebarkan pada warga masyarakat.

Dalam hal ini nasabah pengguna internet banking yang melakukan transaksi internet banking serta pejabat internal Bank merupakan sumber utama dalam penelitian ini, yang pengambilan datanya dilakukan dengan penyebaran kuisioner melalui google form dan wawancara. Jenis wawancara yang penulis gunakan adalah wawancara bebas terpimpin atau bebas terstruktur dengan menggunakan panduan pertanyaan yang berfungsi sebagai pengendali agar proses wawancara tidak kehilangan arah.

Penelitian ini menggunakan peraturan perundang-undangan seperti Undang-Undang No. 10 Tahun 1998 jo Undang-Undang No. 7 Tahun 1992 tentang Perbankan; Undang-undang Nomor 19 tahun 2016 tentang perubahan atas Undang Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-undang No 8 tahun 1999 tentang Perlindungan Konsumen, untuk mengkaji operasional perbankan serta Undang Undang nomor 27 tahun 2022 tentang Perlindung Data Pribadi. Sedangkan data sekundernya berupa buku-buku yang menjadi referensi terhadap tema yang diangkat. yaitu mengenai perbankan, phising, internet banking, perlindungan hukum, dan perlindungan konsumen di Indonesia

Hasil dan Pembahasan

Seperti telah diuraikan di atas, kehadiran teknologi khususnya di bidang IT, diikuti pula dengan peluang kejahatan baru, seperti munculnya tindak kejahatan cyber-crime. Cyber-crime sendiri merupakan istilah yang sangat luas, sehingga cukup banyak penjelasan untuk istilah yang sama. Akan tetapi, secara singkat cyber-crime dapat diartikan sebagai kejahatan yang dilakukan dengan menggunakan komputer dan jaringan internet untuk mencuri suatu data atau informasi. Jika menengok ke belakang, fenomena cyber crime sendiri telah ada sejak awal penemuan internet, saat internet masih disebut sebagai ARPANet.

Kasus kejahatan cyber crime yang pertama di dunia muncul seputar tahun 1970-an, yang teridentifikasi dengan nama virus Creeper. Virus Creeper ini dirancang untuk merusak sistem pada komputer, kemudian pada perangkat yang terinfeksi akan muncul pesan bahwa sistem komputer telah terinfeksi virus disertai tampilan identitas pembuat virus. Kasus cyber crime lain yang disertai penipuan pertama di dunia terjadi pada tahun 1973, yakni ketika seorang kepala teller bank lokal di New York (Union Dime Savings Bank) menggelapkan uang dari perusahaan sebanyak lebih dari $2.000.000 dengan cara memanipulasi data rekening yang ada dalam sistem komputer bank.

Sebagai negara di mana sebagian besar penduduknya merupakan pengguna aktif internet, sudah seharusnya pemerintah memberikan perhatian khusus pada masalah cyber crime ini, karena perkembangan internet yang sangat pesat telah menciptakan banyak celah besar dalam setiap aspek, baik bagi negara maupun penduduknya. Dapat dikatakan

bahwa cyber crime merupakan suatu ancaman yang besar bagi negara. Hal ini sesuai dengan pendapat John Arquilla dan David Ronfeldt bahwa revolusi informasi mengakibatkan terjadinya perubahan besar yang kemudian mendukung tumbuhnya jaringan-jaringan yang memungkinkan berbagai aktor untuk dapat berkomunikasi, berkoordinasi, sampai beroperasi tanpa terbatas akan ruang dan waktu. Arquilla dan Ronfeldt juga menemukan bahwa kemudahan komunikasi ini menimbulkan perubahan keterlibatan masyarakat dalam suatu konflik, serta adanya perubahan peperangan dalam militer. Arquilla dan Ronfeldt menjelaskan netwar dan cyber war mewakili model konflik baru yang akan semakin penting di masa depan. Jika dilihat dari istilahnya, kedua model konflik tersebut merupakan peperangan yang terjadi di dalam ranah cyberspace, akan tetapi hal yang membedakan kedua model konflik tersebut adalah aktornya, di mana netwar sendiri biasanya terjadi pada level society sehingga cenderung bersifat non-military, sedangkan cyberwar terjadi pada level military yang melibatkan penggunaan teknologi informasi dalam operasi militer yang ada.

Phising pada channel internet banking merupakan ancaman dengan menggunakan metode rekayasa sosial untuk menipu pengguna (pelanggan). Biasanya pengguna tertarik dengan penawaran melalui email, pesan singkat, atau panggilan telepon dari penjahat yang menyamar sebagai pejabat bank dan mengajak nasabah untuk memberikan data rahasia terkait data pengguna bank. Salah satu faktor penyebab ancaman serangan phising dalam perbankan online adalah kurangnya kesadaran pengguna. Masih banyak orang yang belum begitu paham mengenai pentingnya data pribadi, sehingga perlu dilindungi. Begitu pentingnya data pribadi, sehingga Pemerintah berkepentingan untuk mengatur Perlindungan Data Pribadi dalam suatu Undang Undang tersendiri. Pasal 1 (2) Undang Undang no 27 tahun 2022 mengenai Perlindungan Data Pribadi menyatakan bahwa Perlindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek data Pribadi. Sedangkan Data Pribadi menurut pasal 4 ayat 2 huruf f Undang Undang ini adalah termasuk data keuangan pribadi, yang memang rawan untuk disalahgunakan oleh pihak lain. Di sisi lain faktor psikologis pengguna layanan jejaring sosial menjadi penyeban lain terjadinya phising yang semakin marak.

Perbankan memiliki berbagai jenis channel dalam pelayannya, baik secara konvensional ataupun melalui media alternatif lainnya seperti internet banking (Nuralam, 2017). Internet banking merupakan suatu bentuk pemanfaatan media internet oleh bank untuk mempromosikan dan sekaligus melakukan transaksi secara online, baik dari produk yang sifatnya konvensional maupun yang baru. Menurut pasal 1 angka 1 Undang-Undang Nomor 10 tahun 1998 perubahan atas Undang-Undang Nomor 7 tahun 1992 tentang Perbankan:

"Perbankan adalah segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha serta cara dan proses dalam melaksanakan kegiatan usahanya".

Khusus berkenaan dengan konsep internet banking, terdapat hal serius yang harus dicermati yaitu mengenai privacy atau keamanan data nasabah. Hal ini dikarenakan karakteristik layanan internet banking yang rawan akan penyalaahgunaan aspek data pribadi nasabahnya, sehingga diperlukan adanya perlindungan hukum.

Ketentuan lain yang dapat dipergunakan untuk menetapkan dan memberikan perlindungan hukum atas data pribadi nasabah dalam penyelenggaraan layanan internet banking dapat dicermati pada Pasal 29 ayat (4) Undang-undang Nomor 10 tahun 1998 yang menyatakan bahwa untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbul resiko kerugian sehubungan dengan transaksi nasabah yang dilakukan oleh bank. Hal tersebut diatur mengingat bank adalah institusi pengumpul dana dari masyarakat yang disimpan atas dasar kepercayaan.

Selanjutnya, ketentuan lain dalam Undang-undang Perbankan adalah ketentuan Pasal 40 ayat (1) dan (2), di mana Bank diwajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44 dan Pasal 44A. Namun prinsip kerahasian bank pada ketentuan tersebut tidak dapat diterapkan secara optimal terhadap perlindungan hukum atas data pribadi nasabah dalam penyelenggara layanan internet banking. Hal ini dikarenakan perlindungan hukum atas data pribadi nasabah yang ada pada ketentuan tersebut terbatas hanya pada data yang disimpan dan dikumpul oleh bank, padahal data nasabah di dalam penyelenggaran layanan internet banking tidak hanya data yang disimpan dan dikumpulkan tetapi termasuk data yang ditransfer oleh pihak nasabah dari tempat komputer di mana nasabah melakukan transaksi.

Oleh karena itu diperlukan seperangkat aturan hukum untuk melindungi konsumen, yang antara lain dapat dilihat pada Undang Undang Perlindungan Konsumen. Menurut Pasal 1 angka 1 Undang-undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Perlindungan Konsumen mempunyai pengertian berupa segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen. Dari pengertian ini dapat diketahui bahwa perlindungan konsumen merupakan segala upaya yang dilakukan untuk melindungi konsumen sekaligus dapat meletakkan konsumen dalam kedudukan yang seimbang dengan pelaku usaha.

Nasabah jika ditilik dari pasal 1 ayat (2) UUPK disini yang dimaksudkan adalah: “Pengguna akhir (end user)” dari suatu produk yaitu setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain maupun makhluk hidup lain dan tidak untuk diperdagangkan. Dalam Undang-undang Dasar 1945 Pasal 28D Ayat (1) yang berbunyi :

“Setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum”

Pasal tersebut pada dasarnya memberikan landasan konstitusional bagi perlindungan hukum konsumen di Indonesia, karena dalam ketentuan itu secara jelas dinyatakan bahwa menjadi hak setiap orang untuk memperoleh keamanan dan perlindungan. Payung hukum yang dijadikan perlindungan bagi konsumen yang dalam hal ini nasabah bank pengguna layanan Internet Banking, yaitu Undang Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, sedangkan aturan perundang-undangan lainnya sebagai pendukung payung hukum yang sudah ada.

Masalah kedudukan yang seimbang secara jelas dan tegas terdapat dalam Pasal 2 yang menyebutkan bahwa perlindungan konsumen berasaskan manfaat, keadilan, kesimbangan, keamanan, dan keselamatan konsumen serta kepastian hukum. Dengan

berlakunya undang-undang tentang perlindungan konsumen, memberikan konsekuensi logis terhadap pelayanan jasa perbankan, oleh karenanya bank dalam memberikan layanan kepada nasabah dituntut untuk:

a. Beritikad baik dalam melakukan kegiatan usahanya;
b. Memberikan informasi yang benar dan jelas, dan jujur mengenai kondisi dan jaminan jasa yang diberikannya;
c. Memperlakukan atau melayani konsumen secara benar dan jujur serta tidak diskriminatif;
d. Menjamin kegiatan usaha perbankannya berdasarkan ketentuan standard perbankan yang berlaku dan beberapa aspek lainnya.

Konsumen memiliki hak untuk memperoleh keamanan, kenyamanan, dalam mengkonsumsi barang dan/atau jasa, serta hak untuk memperoleh ganti rugi. Pasal 7 huruf f Undang-Undang Perlindungan Konsumen menyebutkan tentang adanya penggantian atas kerugian terhadap penggunaan, pemanfaatan barang dan/jasa yang diperdagangkan. Namun sayangnya pengenaan denda ini hanya dapat dikenakan apabila terdapat pelanggaran atas perjanjian, seperti yang disebutkan dalam pasal 7 huruf g. Sedangkan seperti kita ketahui, perjanjian antara Bank dengan nasabahnya dilandasi dengan perjanjian baku yang disediakan oleh bank, sehingga dalam hal ini nasabah tidak memiliki posisi yang sejajar. Oleh karena itu terhadap kerugian tersebut perlu dianalisis apakah karena kelalaian dari pihak nasabah ataukan fraud dari pihak Bank, seperti yang dijelaskan oleh nara sumber dari pihak perbankan. Jika disebabkan oleh pihak Bank, maka Bank bertanggung jawab untuk memberikan ganti rugi.

Konsumen berhak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa. Sebagai pihak penyedia jasa, bank berupaya memberikan yang terbaik dalam pelayanannya kepada nasabah, sedangkan nasabah atau konsumen pengguna berhak mendapatkan fasilitas terbaik, dalam hal ini terutama berkaitan dengan keamanan nasabah sendiri, utamanya data sensitif yang rawan disalahgunakan. Perlindungan terhadap nasabah pengguna internet Banking selanjutnya dapat merujuk pada Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Undang Undang ini dinilai telah cukup mampu mengatur permasalahan- permasalahan hukum dari sistem internet banking sebagai salah satu layanan perbankan yang merupakan wujud perkembangan teknologi informasi. Meskipun dalam pasal-pasal Undang-undang ITE tidak ada pasal-pasal yang spesifik mengatur mengenai Internet Banking itu sendiri, akan tetapi terdapat pasal-pasal yang mengatur mengenai transaksi dengan media Internet.

Setiap penyelenggara sistem elektronik diwajibkan untuk menyediakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Andal artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuahan penggunanya. Aman artinya sistem elektronik terlindungi secara fisik maupun nonfisik. Beroperasi sebagaimana mestinya artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. Selain itu, penyelenggaraan sistem elektroniknya harus bertanggung jawab artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut. Namun

demikian ketentuan tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik.

Undang-undang ITE juga mengatur bahwa sepanjang tidak ditentukan lain oleh Undang-undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut, yaitu:

a. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.
b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaran sistem elektronik tersebut.
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik.
d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik.
e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan dan kebertanggungjawaban prosedur atau produk.

Perlindungan hukum yang diberikan oleh Undang- undang ITE dalam hal perlindungan data pribadi, berhubungan dengan hak pribadi nasabah (privasi). Menurut Pasal 26, kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Phising, apabila ditinjau dari pasal ini, tentu saja merupakan suatu pelanggaran dan tindak kejahatan. Sedangkan dalam KUHP, tindakan tersebut dapat dikategorikan sebagai penipuan.

Pasal 378 KUHP menyatakan bahwa "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun." Sehingga phising termasuk dalam penipuan menurut pasal ini, karena phiser bertindak sebagai pemilik data dan mengubah atau menggunakan data yang bukan miliknya seolah-olah sebagai pemilik yang sah.

Data pribadi dilindungi berdasarkan peraturan perundang-undangan di Indonesia. Oleh karena itu, ketika kerahasiaan terhadap suatu (barang) hak milik tidak lagi sempurna maka membutuhkan perlindungan hukum dalam bentuk perlindungan kepada pihak-pihak yang dirugikan. Seperti kita ketahui, ketika data pribadi berada di tangan pihak lain yang salah, dapat mengakibatkan pembobolan terhadap data tersebut. Contoh yang marak terjadi yaitu ketertarikan pelaku terhadap data kartu kredit dan/atau nomor rekening sehingga dapat membuat kerugian ekonomi bagi korban. Menurut UU ITE bentuk dari pemenuhan hak atas perlindungan bagi para korban dalam sebuah transaksi elektronik atau cyber-crime ini hanya ditandai dengan adanya bentuk penyelesaian perkara berupa ketentuan pemidanaan atas perbuatan-perbuatan yang dilarang dalam undang-undang ini kepada pelaku tindak pidana di mana hal tersebut tercantum dari Pasal 45 sampai

Pasal 52 UU ITE berupa pidana penjara dan/atau pidana denda. Namun sayangnya pengungkapan phising oleh aparat penegak hukum masih terkendala pada minimnya jumlah aparat yang menguasai Teknologi Informasi, sehingga tindak lanjut atas pengaduan kasus phising ini sering kali mengalami kebuntuan.

Di Indonesia, beberapa kasus phising telah diputus pengadilan, di antaranya dapat dilihat pada putusan nomor 30/Pid.Sus/2019/PN Skg dengan terdakwa Suparman Alias Suppa Bin Keteng, yang diadili pada Pengadilan negeri Sengkeng dengan dijatui pidana penjaara selama 2 (dua) tahun dan denda sebesar Rp. 100.000.000 (seratus juta rupiah). Dalam kasus tersebut terdakwa dijerat pasal 51 ayat (1) UU RI no 11 tahun 2008 tentang ITE jo Pasal 55 ayat (1) KUHP. Dalam putusan itu disebutkan bahwa terdakwa membuat web palsu yang mirip dengan web milik Bank Rakyat Indonesia (BRI), di mana korban diarahkan pada web tersebut dan digiring untuk mengirim data berupa user id dan password. Data tersebut kemudian digunakan oleh phiser yang saat ini masih masuk dalam DPO (daftar pencarian orang) untuk menguras dana korban melalui internet banking. Pada kasus tersebut pihak BRI mendapatkan pengaduan dari nasabah yang terkuras dananya setelah mendapatkan tawaran kredit dari pelaku dengan syarat penempatan dana pada rekening BRI sebesar 10% dari pinjaman yang diajukan. Korban juga diharuskan mendaftarkan rekeningnya pada internet banking. Selanjutnya korban diarahkan pada website palsu yang tampilannya menyerupai website internet banking BRI. Pada saat korban melakukan login ke website yang mirip dengan milik BRI tersebut, user id dan password korban direkam dan digunakan phiser untuk memindahkan dana ke rekening penampungan tertentu. Dari pengaduan korban tersebut BRI melakukan penelusuran dan mendapatkan data yang mengarah pada lokasi (berupa longitude dan latitude) di mana website dibuat oleh phiser. Tentu saja dibutuhkan kemapuan dalam bidang IT untuk mengungkap hal tersentu Pada kasus ini pertanggungjawaban BRI adalah menindaklanjuti kasus tersebut dan bekerja sama dengan pihak terkait untuk selanjutnya melakukan penangkapan terhadap terdakwa.

Pemidanaan pada pelaku untuk menegakkan hukum bagi para korban phising merupakan langkah yang tepat sehingga kebanyakan bentuk ketentuan pidana yang tercantum dalam UU ITE maupun KUHP, merupakan rangkaian pemberian sanksi berupa pidana penjara dan pidana denda. Pidana penjara dan pidana denda bagi pelaku phising dirasa kurang cukup untuk melindungi dan memenuhi hak para korban. Oleh karena itu khusus bagi korban cyber crime berbentuk phising dapat diupayakan adanya penggantian kerugian secara materiil karena kerugian tersebut yang tidak sepantasnya ia alami, apalagi bagi korban yang memiliki perekonomian lemah. Berkaitan peraturan yang mengatur secara khusus mengenai perlindungan kepada korban, di Indonesia terdapat peraturan perundang-undangan yang mengaturnya yaitu dalam UU No. 31 Tahun 2014 Tentang Perubahan Atas UU No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban dengan didampingi oleh LPSK atau Lembaga Perlindungan Saksi dan Korban. LPSK yang adalah lembaga aktif untuk membantu saksi dan/atau korban tindak pidana untuk mendapatkan perlindungan dan pemenuhan haknya. Korban phising pada dasarnya memiliki kebutuhan terhadap pemenuhan kerugian material yang dialaminya. Dalam UU

Perlindungan Saksi dan Korban atau disebut dengan UUPSK disebutkan terdapat adanya perlindungan korban dan/atau saksi tindak pidana yaitu tersebut dalam bentuk Kompensasi, Restitusi dan Bantuan. Terhadap kerugian materiil bagi korban tindak pidana cyber crime berbentuk phising ini, Restitusi adalah metode yang tepat, seperti dalam dan Pasal 1 Angka 11 yang disebutkan bahwa "Restitusi adalah ganti kerugian yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga."

Penegakan hukum bagi korban phising khususnya yang terjadi melalui transfer Virtual Account, ternyata banyak mengalami kendala. Kendala tersebut tidak hanya disebabkan karena minimnya jumlah penegak hukum yang memahami Teknologi Informasi, namun dari sisi perbankan sendiri ada keterbatasan dalam menindaklanjuti pembobolan rekening nasabahnya, ketika rekening tujuan transfer pada kasus phising tersebut merupakan rekening Virtual Account. dalam kasus phising di mana korban mentrasfer ke no virtual account, data penerima dana akhir sulit dilacak karena pihak bank berurusan dengan pihak penyelenggara virtual account dan bukan pada pengguna. Biasanya penyalahgunaan Virtual Account ini adalah untuk suatu transaksi deposit, ataupun billing untuk pengguna tertentu yang diterbitkan institusi melalui Bank (Kusuma & SH, 2019).

Seperti diketahui, dalam permohonan pembuatan virtual acccount, pihak Bank memberikan form kepada institusi/ perusahaan, yang berisi data pemohon dan persyaratan yang harus disepakati apabila institusi pemilik Virtual Account akan menggunakan fasilitas tersebut. Dalam kaitannya dengan transfer melalui virtual account, hukum perjanjian menjadi dasar dalam pembuatan VA (Johannes Ibrahim, Sirait, & SH, 2021). Namun perjanjian tersebut adalah antara institusi dengan bank, sehingga apabila terjadi phising, bank hanya bertindak sebagai mediator. Biasanya institusi bekerja sama dengan bank untuk membuat suatu rekening giro penampungan yang akan digunakan intitusi tersebut untuk menampung tagihan ataupun deposit pada wallet untuk pembayaran tertentu melalui Virtual Account. Virtual Account diterbitkan sesuai dengan parameter dan maksud transaksi, sehingga dana yang ditransfer dapat terlihat oleh institusi tersebut, yaitu berupa informasi tujuan transaksinya tanpa perlu bukti pembayaran dari pengirimnya.

Untuk mempermudah gambaran mengenai cara kerja dan hubungan hukum antara bank dengan nasabah korban phising serta institusi penerbit Virtual Accout, dapat digambarkan pada diagram di bawah ini :

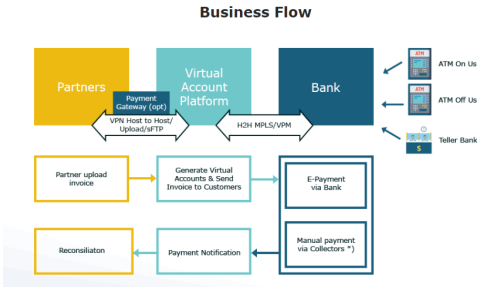

Diagram 1 Alur bisnis flow pada transaksi Virtual Account

Penyalahgunaan Virtual Account pada kasus phising misalnya adalah untuk pembayaran wallet atau deposit untuk transaksi crypto, transaksi forex dan lain sebagainya.

Dari sisi perbankan, menurut nara sumber, yang merupakan kepala departement Quality Assurance salah satu bank Himbara, apabila fraud atau kerugian disebabkan oleh internal perbankan, maka

akan dilakukan ganti rugi, tentu saja setelah dilakukan analisis mendalam, namun apabila terjadinya fraud karena kelalaian nasabah, maka tanggung jawab ada pada nasabah itu sendiri Oleh karena itu dalam pembuatan virtal account seharusnya Bank menyaratkan pada institusi penerbit Virtual account untuk menerapkan KYC (know your customer) kepada pengguna secara ketat serta persetujuan institusi untuk bekerja sama dengan bank sehingga dalam mediasinya Bank dapat membantu nasabah untuk mendapatkan ganti rugi dari phiser. Tentu saja hal tersebut dilakukan setelah melakukan investigasi melalui bantuan institusi penegak hukum dan institusi pemohon Virtual Account.

Pemerintah telah sepakat bahwa pelindungan data pribadi merupakakan hal yang penting yang harus diupayakan secara serius. Sehingga pada tanggal 17 Oktober 2022 pemerintah mengundangkan UU no 27 tahun 2022 tentang perlindugnan Data Pribadi. Menurut pasal 1 (1) UU ini dikatakan bahwa yang dimaksud dengan data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atu dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Selanjitnya pada pasal 4 angka 2 huruf f, data pribadi ini termasuk juga data keuangan pribadi, yang sering menjadi incaran para phiser, di mana penggunaannya harus jelas dan pihak peminta data pribadi pun harus merupakan pihak yang memiliki akuntanbilitas. Jelaskah bahwa phiser bukanlah pihak yang memiliki akuntabilitas yang baik, dan dikategorikan sebagai pelaku penipuan menurut pasal 378 KUHP.

Resiko atas penyelenggaran internet banking tidak hanya dihadapi oleh nasabah, namun juga oleh bank penyenggara, yang pada akhirnya juga mengakibatkan kerugian nasabah. Menurut Sabirin, empat risiko manajemen yang terkait penggunaan internet banking yaitu pertama, technology risk yang berhubungan dengan kehandalan dan keamanan sistem informasi dari berbagai manipulasi atau pembobolan, kedua, reputional risk yang berkaitan dengan corporate image dari bank itu sendiri apabila pelayanan internet banking-nya tidak berjalan dengan baik, ketiga, outsourching risk yaitu bila bank yang bersangkutan sering menggunakan jasa pihak ketiga sebagai ISP sehingga memungkinkan layanan ISP pada suatu waktu dapat mengalami gangguan, keempat, legal risk dimana aspek hukum internet banking saat ini masih belum diatur secara jelas dan lengkap. Ganesh Ramakrishnan menambahkan salah satu risiko-risiko yang dihadapi bank yang menyediakan layanan internet banking adalah: Transaction risk, risiko ini timbul dari adanya kecurangan, kesalahan, kelalaian dan ketidakmampuan untuk mempertahankan tingkat pelayanan yang diharapkan. Tingkat risiko transaksi dapat saja meningkat, karena bank tidak memiliki kontrol penuh atas pihak ketiga. Selain resiko tersebut adapula risiko berupa Reputation risk. Risiko ini muncul dari adanya opini publik yang negatif. Reputasi sebuah bank dapat rusak oleh eksekusi layanan internet banking yang buruk (misalnya, ketersediaan server yang terbatas, performance system lambat). Dan yang terakhir adalah Information security risk, yaitu risiko muncul dari adanya proses keamanan informasi yang longgar, sehingga mengekspos adanya hacker atau serangan insider, virus, pencurian data, kerusakan data dan penipuan. Kecepatan perubahan teknologi dan fakta bahwa saluran internet dapat diakses secara

universal membuat risiko ini sangat penting.

Salah satu faktor penyebab serangan phising di antaranya adalah karena minimnya pengetahuan pengguna akan pentingnya menjaga keamanan data. Pengguna dianggap tidak memiliki pengetahuan yang baik mengenai sistem komputer terutama membedakan domain yang resmi dan palsu (Hasanah, 2014). Faktor mengapa pengguna menjadi korban serangan phising adalah mayoritas pengguna memiliki pengetahuan yang minim terhadap ancaman kriminalitas online, tidak memiliki pengetahuan yang baik mengenai ancaman phising, tidak memiliki strategi yang baik dalam mengenali serangan phising, fokus terhadap konten dibandingkan indikator pada website, dan tidak mengetahui prosedur layanan online yang dipakai sehingga terjebak ketika mendapatkan e-mail dari layanan online yang mereka gunakan terkait informasi maintenance dan informasi- informasi lainnya yang dimanfaatkan phisher untuk mendapatkan data-data sensitif pengguna (Radiansyah, Rusdjan, & Priyadi, 2016).

Dalam perbankan digital, tanggung jawab perlindugnan nasabah juga terdapat pada Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Lnyanan Perbankan Digital Oleh Bank Umum. Peraturan OJK ini menyebutkan, bank penyelenggara layanan perbankan digital wajib menerapkan prinsip perlindungan konsumen.

Pasal 2 Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan mencakup transparansi, perlakuan yang adil, keandalan, kerahasiaan serta keamanan data/informasi nasabah dan penanganan pengaduan serta penyelesaian sengketa nasabah secara sederhana, cepat dan biaya terjangkau.

Kasus phising tidak hanya dialami oleh nasabah di Indonesia, namun terjadi di seluruh dunia. Salah satunya yang dialami oleh nasabah di Singapura. Namun terhadap kasus tersebut telah dilakukan jalan keluar dari kalangan perbankan, seperti yang dilakukan oleh OCBC Bank, di mana Bank tersebut mengganti sejumlah dana kapada nasabah korban phising.23 Hal ini sedikit berbeda dengan penanganan phising di Indonesia, di mana pihak Bank hanya sebatas memberi sosialisasi pada nasabah akan bahaya phising. Lebih lanjut di Singapura, terdapat langkah-langkah baru seperti menghapus tautan yang dapat diklik dalam email dan pesan teks yang dikirim ke pelanggan ritel untuk mengatasi penipuan phishing, seperti laporan media. Otoritas Moneter Singapura (MAS) dan Asosiasi Bank di Singapura (ABS).

Lain halnya dengan Amerika Serikat, yang telah memiliki aturan khusus yaitu Electronic Fund Trasfer Act 1978 (EFTA) yang mengatur kerangka dasar penetapan hak, kewajiban dan tanggung jawab peserta yang terlibat dalam transfer dana elektronik. Istilah "Transfer Dana Elektronik" secara luas meliputi transaksi elektronik yang dimulai melalui terminal, telepon, komputer, atau pita perekam suara yang berisi perintah konsumen bagi lembaga keuangan untuk mendebet atau mengkredit rekening konsumen. Undang-Undang Transfer Dana Elektronik (EFTA) merupakan undang-undang federal yang disahkan pada tahun 1978. Undang-undang ini memberikan perlindungan penting bagi konsumen saat mereka mentransfer dana secara elektronik, termasuk melalui penggunaan kartu debit, mesin teller otomatis (ATM), dan penarikan otomatis dari akun bank. EFTA menyediakan cara untuk meninjau ulang transaksi, dan memperbaiki kesalahan. Ini

juga membatasi tanggung jawab bank jika kartu hilang atau dicuri, selama dilaporkan dalam waktu 60 hari.

EFTA juga membebankan tanggung jawab pada lembaga keuangan, mengharuskan mereka untuk mengungkapkan informasi penting tentang cara mereka mengelola rekening (Suryokumoro & Ula, 2020).

Selain itu Amerika Serikat juga juga memiliki Undang-Undang Anti-phishing tahun 2005, yang mengubah Undang-Undang pidana Federal untuk mengkriminalkan penipuan internet yang melibatkan penipuan untuk mendapatkan informasi pribadi (phishing). Sanksi pidana dalam Undang-undang tersebut terhadap pelaku phising yaitu menjatuhkan denda atau penjara hingga lima tahun, atau keduanya, untuk orang yang dengan sengaja dan dengan maksud untuk terlibat dalam aktivitas yang merupakan penipuan atau pencurian identitas berdasarkan undang-undang Federal atau Negara, yaitu (1) pelaku yang membuat atau membeli pembuatan situs web atau nama domain yang mewakili dirinya sebagai bisnis online yang sah tanpa otoritas atau persetujuan dari pemilik terdaftar dari bisnis tersebut; dan (2) menggunakan situs web atau nama domain tersebut untuk meminta sarana identifikasi dari siapapun. Selain itu, menjatuhkan denda atau penjara selama-lamanya lima tahun, atau keduanya, bagi seseorang yang dengan sengaja dan dengan maksud untuk terlibat dalam kegiatan yang merupakan penipuan atau pencurian identitas berdasarkan undang-undang Federal atau Negara dengan mengirimkan pesan surat elektronik yang: (1) secara palsu menyatakan dirinya dikirim oleh bisnis online yang sah; (2) termasuk alat lokasi Internet yang merujuk atau menghubungkan pengguna ke lokasi online di world wide web yang secara palsu mengaku milik atau terkait dengan bisnis online yang sah; dan (3) meminta alat identifikasi dari penerima.

Kesimpulan

Berdasarkan penelitian ini, maka dapat ditarik suatu kesimpulan bahwa pada dasarnya di Indonesia saat ini eblum ada peraturan yang secara khusus khusus melindungi korban tindakan kejahatan phising pada channel e-banking melalui transfer virtual account. Dengan maraknya kasus phisinng maka lembaga perbankan maupun aparat penegak hukum di Indonesia dapat tunduk aturan dan menggunakan Undang Undang yang berlaku saat ini seperti Undang- Undang Nomor. 8 tahun 1999 Tentang Perlindungan Konsumen dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Terkait prinsip perlindungan kerahasiaan data nasabah bank ketentuannya dapat dilihat pada SE OJK no 14 th 2014. Dalam SEOJK 14 / 2014 disebutkan ketentuan mengenai metode enkripsi dan bagaimana hak akses disesuaikan dengan kewenangan pejabat bank. Selain itu pemerintah juga telah memperketat perlindungan data privasi masyarakat dengan penerbitan Undang Undang no 13 tahun 2022 tentang Perlindungan Data Pribadi. Namun sayangnya penyelesaian atas kasus phising masih terkendala dengan kurangnya mediasi antara Bank dengan Institusi penerbit VA dengan nasabah yang mengalami kejahatan. Di samping itu penegakan hukum terhadap pelaku phising masih terkendala dengan minimnya jumlah personel penegak hukum yang menguasai teknologi informasi sehingga sulit dalam melacak keberadaan phiser. Selain itu, langkah perlindungan hukum terhadap korban phising terdiri dari perlindungan hukum secara represif dan perlindungan

hukum secara preventif. Perlindungan represif diberikan ketika perlindungan secara preventif tidak dapat menghindarkan nasabah dari tindakan phishing. Menurut UUPK, konsumen mempunyai hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan. Disebutkan dalam Pasal 32 POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan bahwa Pelaku usaha jasa keuangan wajib memiliki dan melaksanakan mekanisme pelayanan dan penyelesaian bagi konsumen. Selain perlindungan represif, terdapat pula perlindungan nasabah secara preventif tercantum dalam Pasal 4 Undang-Undang Perlindungan Konsumen, yang menyatakan bahwa pelaku usaha, yang dalam hal ini adalah bank, memiliki kewajiban untuk memberikan pembinaan dan pendidikan bagi nasabah sebagai konsumen. Beberapa case jika terjadi fraud dari pihak bank, maka bank akan bertanggungjawab untuk pengembalian dana atau pengembalian data yang sekiranya dapat dikembalikan kepada nasabah. Sedangkan kelalaian yang dilakukan oleh nasabah tidak menjadi tanggungjawab dari pihak bank dan sepenuhnya menjadi tanggungjawab nasabah.Namum kendala penegakan hukum juga sering terjadi karena minimnya jumlah aparat yang mengusai teknologi informasi guna melacak keberadaan phiser.

Daftar Pustaka

Arkanuddin, Mohammad Fahmi, Nugroho, Bernardus Yuliarto, & Wijaya, Chandra. (2022). *Pengaruh model bisnis canvasing terhadap risiko pada industri fintech P2P lending Indonesia*.

Chandra, Muhammad Alfian, & Syam, Husni. (2016). The Legal Protection for Suspected Malpractice Doctor Cases Based on Law Number 29 of 2004 on Medical Practice (a Case Study of Blind Toddler in Cibabat Hospital, Cimahi). *Prosiding Ilmu Hukum*, 229–234.

Hartanto, Ratna, & Ramli, Juliyani Purnama. (2018). Hubungan Hukum Para Pihak dalam Peer to Peer Lending. *Jurnal Hukum Ius Quia Iustum*, *25*(2), 320–338.

Hasanah, Firda Atsalis Maulidya. (2014). *Ancaman Phising Pada Pengguna Online Banking*.

Johannes Ibrahim, S. H., Sirait, Yohanes Hermanto, & SH, L. L. M. (2021). *Kejahatan Transfer Dana: Evolusi Dan Modus Kejahatan Melalui Sarana Lembaga Keuangan Bank*. Sinar Grafika (Bumi Aksara).

Kusuma, Mahesa Jati, & SH, M. H. (2019). *Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank terhadap Tindak Kejahatan ITE di Bidang Perbankan*. Nusamedia.

Nuralam, Inggang Perwangsa. (2017). *Etika pemasar dan kepuasan konsumen dalam pemasaran perbankan syariah*. Universitas Brawijaya Press.

Putri, Dinda Ameliani, Lahagu, Edita Emilia, Ufmayza, Dara, Adilia, Dina Novita, Ningrum, Ayu Dyah, & Lubis, Kartika Sari. (2022). Pemanfaatan Media Sosial Untuk Berwirausaha Bagi Para Generasi Millenial. *Prosiding Seminar Nasional Sosial, Humaniora, Dan Teknologi*, 797–802.

Radiansyah, Ikhsan, Rusdjan, Candiwan, & Priyadi, Yudi. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1–14.

Rahardjo, Satjipto. (2003). *Sisi-sisi lain dari Hukum di Indonesia*. Penerbit Buku Kompas.

Rasjidi, Lili, Sos, S., & Putra, I. B. Wyasa. (1993). *Hukum sebagai suatu sistem*. Remaja Rosdakarya.

Sahlan, Muhammad. (2016). Unsur Menyalahgunakan Kewenangan dalam Tindak Pidana Korupsi sebagai Kompetensi Absolut Peradilan Administrasi. *Jurnal Hukum Ius Quia Iustum*, *23*(2), 271–293.

Sihombing, Jonker. (2010). *Penjaminan simpanan nasabah perbankan*. Alumni.

Sinaulan, J. H. (2018). Perlindungan Hukum Terhadap Warga Masyarakat. *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya*, *4*(1).

Suryokumoro, Herman, & Ula, Hikmatul. (2020). *Koperasi Indonesia dalam Era MEA dan Ekonomi Digital*. Universitas Brawijaya Press.

Zuhri, Syaifuddin, Fajriah, Nurul, Wibowo, Rheinaldy Thalia Hadi, Prakoso, Ardan Agung Dwi, Indriani, Regina Olvi, Windari, Anyes Tri, Thomas, Christian, Auliya, Ariena Zulfa, Annisa, Megga, & Yusuf, Muhammad. (2020). *Teori Komunikasi Massa dan Perubahan Masyarakat* (Vol. 5). Prodi Ilmu Komunikasi Universitas Muhammadiyah Malang bekerjasama dengan ….