Jurnal MAHUPAS: Mahasiswa Hukum Unpas (Journal MAHUPAS: Law Student of Unpas), Vol. 2 No. 2, Juni 2023

KELALAIAN BANK DALAM MENJAGA RAHASIA BANK PADA PERJANJIAN BAKU TERHADAP TINDAKAN *PHISING* YANG DIALAMI NASABAH AKIBAT *SOCIAL ENGINEERING* DITINJAU DARI HUKUM POSITIF INDONESIA

Fadiah Azzahra Gusti
Fakultas Hukum Universitas Pasundan (UNPAS)

Abstrak

Pertumbuhan ekonomi Indonesia, mendorong bank untuk menciptakan perbankan digital demi memudahkan transaksi nasabah. Dengan masuknya teknologi tersebut, kasus kejahatan digital meningkat, seperti *phising* yang dialami nasabah disertai *social engineering*. Kasus tersebut terjadi akibat nasabah lalai menjaga data pribadinya, Namun, bank juga menjadi salah satu indikator terjadinya *phising*. Penelitian ini dilakukan dengan menggunakan metode penelitian deskriptif analitis,dengan pendekatan yuridis normatif yang menelusuri peraturan dan literatur terkait dengan permasalahan yang diteliti. Hasil penelitian menunjukkan bahwa kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering* adalah tidak ada penyesuaian sistem pengendalian intern dengan tingkat risiko khusunya pada sistem keamanan dan pemerataan sosialisasi kepada nasabah berdasarkan Pasal 15 ayat (1) huruf a UU No. 18 Tahun 2006 Tentang Penerapan Manajemen Risiko Bagi Bank Umum, sehingga prinsip kehati-hatian pada bank tidak berjalan dengan baik. Sedangkan akibat hukum kelalaian bank dalam menjaga rahasia bank terhadap perjanjian baku dalam tindakan *phising* yang dialami nasabah akibat *social engineering* ditinjau dari hukum positif Indonesia adalah batal demi hukum sebab Perbuatan Melawan hukum yang dilakukan bank sebagaimana yang diatur pada Pasal 1365 KUHPerdata. Dan ganti rugi dapat terlaksana apabila pengadilan membuktikan bahwa terjadi overmacht pada nasabah. Upaya penyelesaian terhadap kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering* dapat dilakukan dengan dua cara, yaitu penyelesaian secara non-litigasi dengan pengajuan perkara melalui Lembaga Alternatif Penyelesaian Sengketa dan non-litigasi dengan mengajukan gugatan ke pengadilan.

Kata Kunci : Kelalaian Bank, Perjanjian Baku, Phising

Abstract

Indonesia's economic growth encourages banks to create digital banking to facilitate customer transactions. With the entry of this technology, cases of digital crime are increasing, such as phishing experienced by customers accompanied by social engineering. The case occurred due to customers neglecting to maintain their personal data; however, banks are also an indicator of phishing. This research was conducted using analytical descriptive research methods with a normative juridical approach that traces regulations and literature related to the problem under study. The results showed that the bank's negligence in maintaining bank secrets in the standard agreement against

phishing actions experienced by customers due to social engineering was that there was no adjustment of the internal control system with the level of risk, especially in the security system and equitable distribution of socialization to customers based on Article 15 paragraph (1) letter a of Law No. 18 of 2006 concerning the Application of Risk Management for Commercial Banks, so that the precautionary principle at the bank does not work well. Meanwhile, the legal consequences of bank negligence in maintaining bank secrets against standard agreements in phishing actions experienced by customers due to social engineering in terms of Indonesian positive law are null and void because of unlawful acts committed by banks as stipulated in Article 1365 of the Civil Code. And compensation can be carried out if the court proves that there was overpayment to the customer. Efforts to resolve bank negligence in maintaining bank secrets in standard agreements against phishing actions experienced by customers due to social engineering can be done in two ways: non-litigation settlement by filing a case through an Alternative Dispute Resolution Institution and non-litigation by filing a lawsuit with the court.

Keywords: Bank Negligence, Standard Agreement, Phishing

I. PENDAHULUAN

Pengaruh teknologi pada produk perbankan menjadi tanda dunia perbankan telah memasuki era perbankan digital yaitu disebut sebagai *financial technology*. Hal ini berdampak baik bagi transaksi yang dilakukan masyarakat. Bank menemukan terobosan baru berupa transaksi digital. Dengan adanya temuan ini semua transaksi seperti pembukaan rekening atau penyimpanan dana tabungan, transfer dana dan transaksi *e-commerce* dapat dilakukan dengan media digital (Ginantra dkk., 2020, hlm. 6). Dalam hal penyimpanan dana tabungan secara digital, pelaku usaha bank menyiapkan layanan berupa *m-banking.* Tetapi untuk menggunakan aplikasi *m-banking* nasabah harus menyetujui beberapa syarat dan ketentuan yang akan muncul pada aplikasi (Rifka, 2022). Syarat dan ketentuan ini yang menjadi perjanjian baku yang akan mengikat pihak nasabah dan pihak bank.

Berkembangnya teknologi perbankan pasti akan menimbulkan permasalahan baru. Sebab, bank harus menyesuaikan kebijakan-kebijakan perusahaan dengan perubahan yang ada. Semakin maju teknologi yang digunakan oleb bank, maka tidak menutup kemungkinan terdapat serangan-serangan baru dari pihak luar. Risiko dan kelemahan bank akan semakin tidak terkendali. Sebab, kejahatan pada bidang perbankan juga semakin berinovasi. Kejahatan yang sedang marak terjadi terhadap masyarakat pengguna jasa perbankan adalah *Phising*.

Tindakan *phising* merupakan sebuah tindakan manipulasi oleh pihak di luar bank yang menyamar sebagai pihak terpercaya kepada nasabah bank untuk mendapatkan informasi sensitif berupa nama lengkap, nomor *handphone*, *e-mail*, dan rincian kartu kredit dengan memancing korban untuk menakan *link phising* (Ikatan Bankir Indonesia, 2019, hlm. 370). Kejahatan ini merupakan pelanggaran terhadap Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dikatakan demikian sebab pelaku kejahatan *phising* tersebut memiliki tujuan untuk membobol rekening nasabah yang menjadi target mereka sehingga mereka berusaha untuk menerobos dan menjebol sistem keamanan bank agar mereka dapat menarik seluruh uang yang ada di dalam rekening korban.

Nasabah yang mengalami *phising* hampir tidak mempunyai kekuatan untuk menggugat ganti rugi kepada bank apabila dana nasabah tersebut hilang. Sebab, banyak dari nasabah yang dengan sukarela memberikan data-data pribadi yang sensitif kepada pelaku *phising*. Sehingga bank tidak memiliki tanggung jawab untuk mengganti kerugian nasabah karena kelalaian terdapat pada diri nasabah (Oktavira, 2020)

Tindakan *phising* yang sering terjadi di indonesia, terkadang diikuti dengan adanya manipulasi psikologis (*social engineering).* Pelaku akan melakukan manipulasi dengan menyamar sebagai karyawan sah suatu perusahaan dan menekan kelemahan korban terhadap ketidaktahuannya akan suatu informasi agar korban berada pada posisi yang lemah (Bandig dkk., 2021, hlm. 75). Dengan adanya *social engineering* ini akan membuat nasabah tidak memiliki pilihan selain mengikuti instruksi yang diberikan oleh pelaku *phising*.

Dalam praktiknya, pelaksanaan transaksi perbankan baik secara konvensional ataupun digital, seharusnya dilaksanakan dengan menerapkan prinsip-prinsip perbankan diantaranya adalah prinsip kepercayaan dan prinsip kehati-hatian. Prinsip ini akan membantu menjaga kesehatan usaha perbankan baik itu ancaman dari luar seperti *phising* ataupun risiko kejahatan lainnya. Pihak bank harus menjalankan prinsip tersebut karena dalam menjalankan usahanya pelaku usaha bank sangat bergantung pada

kepercayaan masyarakat (Hermansyah, 2020, hlm. 114). Kepercayaan tersebut berhubungan dengan kerahasiaan data nasabah dan simpanannya atau disebut sebagai rahasia bank di dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Data-data nasabah tersebut harus dirahasiakan untuk mencegah kemungkinan buruk yang akan terjadi. Sehingga nasabah merasa aman dan nyaman melakukan transaksi di bank. Kerahasiaan data nasabah ini merupakan bentuk kewajiban bank yang harus dilaksanakan akibat telah disepakatinya perjanjian oleh kedua belah pihak.

Prinsip lain yang juga penting untuk diterapkan oleh bank adalah prinsip kehati-hatian. Prinsip ini bertujuan untuk menjaga bank agar terus tetap teliti dan benar-benar memperhatikan pelaksanaan kegiatan di perusahaannya agar usaha tetap sehat dan aman dari segala kerugian. Namun, untuk menciptakan usaha yang sehat, bank harus mempunyai keseimbangan antara operasional dan manajemen risiko. Hal ini dilakukan agar bank tidak mudah jatuh ditengah peristiwa yang tidak dapat diperkiraan terutama di era perbankan yang sudah memasuki dunia digital.

Proses manajemen risiko dilakukan oleh bank sesuai dengan kebijakan yang sudah diatur di dalam Peraturan Otoritas Jasa Keuangan Nomor 18 Tahun 2016 tentang Penerapan Manajemen Risiko Bank Umum. Sebagaimana yang diatur dalam Pasal 15 ayat (1) huruf a POJK No. 18 Tahun 2006, dalam pelaksanaan usaha dan operasional, bank memiliki kewajiban untuk melaksanakan sistem pengendalian intern kepada seluruh jenjang organisasi bank dan menyesuaikannya dengan tingkat serta jenis risiko yang melekat pada usahanya. Hal ini dilakukan agar bank mudah mendeteksi kelemahan ataupun penyimpangan yang terjadi.

Pada hakikatnya, dalam penyelenggara sistem elektronik pelaku usaha bank harus menjalankan sistem elektronik dengan bertanggung jawab dan wajib untuk mengoperasikan sistem elektronik sesuai persyaratan salah satunya dapat melindungi keotentikan dan kerahasiaan informasi elektronik. Kewajiban bank dalam melaksanakan sistem elektronik telah diatur di dalam Pasal 15 dan Pasal 16 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pengaturan ini ada untuk memastikan

agar bank tidak lalai dalam menjaga sistem elektronik yang mereka miliki. Namun dalam hal kejahatan *phising*, bank sering kali mengalami kecolongan akibat nasabah yang tidak menjaga data-data dirinya, sehingga sering terjadi pembobolan terhadap sistem perbankan yang akhirnya mengakibatkan dana nasabah hilang di dalam rekening tabungan terutama pada *m-banking*.

Pada praktiknya, didapat bahwa kasus tindakan *phising* disertai dengan *social engineering* ini telah terjadi pada salah satu bank di Indonesia pada tahun 2022. Awalnya masyarakat hingga nasabah Bank X mendapatkan pesan via *Whatsapp* oleh pihak yang mengaku sebagai pegawai Bank X. Dalam pesan tersebut dinyatakan bahwa ada kenaikan biaya transaksi melalui m-banking yang semula Rp 6.500/ transaksi menjadi Rp 150.000/bulan. Pihak yang mengaku sebagai pegawai Bank X tersebut meminta respon oleh pihak penerima pesan mengenai persetujuan mereka terhadap kenaikan tersebut dengan memberikan *link phising* yang nantinya akan meretas semua data nasabah. Pelaku *phising* tersebut memberikan manipulasi dengan mengirimkan informasi bahwa apabila nasabah tidak menjawab pesan tersebut maka nasabah dianggap setuju akan kenaikan biaya transaksi tersebut. Pada Jumat 10 Juni 2022, SA seorang nasabah Bank X sedang berada di kantor imigrasi Padang. SA menerima kiriman pemberitahaun kenaikan tarif transfer dari Bank X melalui chat whatsapp serta link isian. Diketahui bahwa SA menekan *link* yang diberikan oleh pelaku akibat informasi yang disebarkan yang dipicu dari tidak bersedianya SA terhadap kenaikan biaya transaksi. Saat setelah ia menekan *link* yang diberikan pelaku *phising,* SA mengisi data-data pribadi sesuai dengan panduan yang tertera pada *link*. Setelah semua data diperoleh dari *link* tersebut, pelaku *phising* menggunakan data-data tersebut untuk membobol sistem keamanan bank. Dan dikarenakan sistem keamanan bank yang tidak maksimal, maka pelaku *phising* berhasil membobol rekekning milik SA. Setelah peristiwa tersebut, dikabarkan tidak berapa lama uang dalam rekening perusahaan miliknya berkurang karena ada transaksi berupa transfer dari aplikasi *M-Banking* (Putra, 2022). Saat ini kerugian yang dialami SA sebesar Rp 469 Juta. Terhadap kerugian yang dialami oleh SA, dana

yang hilang tidak kembali dikarenakan pihak bank tidak mau mengganti kerugian yang dialami akibat bank menyatakan bahwa kesalahan ada pada nasabah.

Pada kasus diatas, ada kebocoran rahasia bank yang diakibatkan oleh tindakan *phising* disertai dengan *social engineering*. Tindakan tersebut menyebabkan kerugian berupa hilangnya dana nasabah pada rekening tabungan, sehingga dapat dikatakan terdapat kerusakan sistem keamanan pada bank. Mengingat bahwa hubungan antara nasabah dan bank diikat dengan suatu perjanjian maka terhadap hilangnya dana nasabah ditemukan adanya pelanggaran dalam perjanjian tersebut.

Dari penjelasan teori sebelumnya, penulis merumuskan bahwa terdapat kekosongan hukum. Sebab, seharusnya terdapat peraturan yang mengatur mengenai manajemen risiko dan sistem elektronik bank dalam menghadapi kejahatan-kejahatan digital yang disertai manipulasi psikologis agar prinsip perbankan dapat dijalankan dengan baik di dalam kegiatan usaha bank maupun perjanjian antara bank dan nasabahnya.

II. METODE PENELITIAN

Penelitian ini dilakukan secara Deskriptif Analitis. Dimana penelitian dengan data deskriptif merupakan penelitian yang dilakukan dengan mengumpulkan data yang berbentuk kata-kata seperti tulisan atau literatur. Sedangkan Metode Pendekatan yang digunakan adalah Yuridis Normatif, yaitu penelitian dengan meninjau dan meneliti data sekunder atau bahan pustaka lainnya (Soekanto, 2013). Dengan pendekatan ini, penulis akan menelusuri peraturan-peraturan dan literatur yang memiliki sebab akibat dengan permasalahan yang akan diteliti.

III. HASIL PENELITIAN DAN PEMBAHASAN

A. Kelalaian Bank dalam Menjaga Rahasia Bank Pada Perjanjian Baku Terhadap Tindakan *Phising* yang Dialami Nasabah Akibat *Social Engineering*

Usaha yang dimiliki bank berjalan dengan kepercayaan masyarakat. Maka, bank harus memberikan pelayanan yang terbaik kepada masyarakat. Demi meningkatkan pelayanan tersebut, sistem yang dimiliki bank harus andal agar masyarakat dapat merasakan keamanan dan kenyamanan dalam melakukan transaksi. Sebagai bentuk keamanan, bank harus mengupayakan agar rahasia bank seperti data nasabah yang bersifat pribadi dapat terjaga. Hal tersebut dijelaskan dalam Pasal 40 ayat (1) Undang-Undang Nomor 10 tahun 1998 tentang Perbankan, yaitu : “Bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanananya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A”

Kasus *phising* yang saat ini yang marak dialami nasabah berdampak pada bocornya data nasabah. Kebocoran data tersebut disebabkan oleh diri nasabah. Hal ini menyebabkan adanya pelanggaran terhadap kerahasiaan bank. Namun, pada praktiknya, *phising* yang dialami oleh nasabah terjadi karena adanya *social engineering* atau manipulasi psikologis yang pada akhirnya menempatkan nasabah pada posisi yang lemah. *Social engineering* pada nasabah berupa tekanan akibat adanya kenaikan biaya yang cukup besar. Dengan adanya tekanan tersebut nasabah mengakses *link* yang diberikan oleh pelaku *phising* dan mengisi seluruh data-data yang diminta, yaitu *username, password,* pin dan kode OTP. Pada kejadian ini, nasabah memiliki kesalahan karena memberikan data pribadinya kepada pihak bukan bank, namun kesalahan ini terjadi diluar kehendak dari pihak nasabah, sebab tindakan *phising* berhasil dilakukan akibat adanya tekanan psikologis yang dirasakan oleh pihak nasabah.

Pada penelitian yang dilakukan oleh penulis, di dapat sebuah hasil bahwa pada kasus tindakan *phising* yang dialami nasabah akibat *social engineering* telah terjadi sebuah kerugian berupa hilangnya dana nasabah pada rekening. Pada kehilangan tersebut, terdapat kelemahan suatu sistem yang dimiliki oleh bank, sebab, pembobolan rekening nasabah telah berhasil dilakukan oleh pelaku *phising.* Berdasarkan Pasal 15 ayat (1) Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik menegaskan mengenai : “Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem ekeltronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya”.

Pasal tersebut memberikan makna bahwa penyelenggara harus melaksanakan sistem elektronik dengan andal dan aman. Menurut Kamus Besar Bahasa Indonesia, andal memiliki arti dapat dipercaya atau mampu menjalankan tanggung jawabnya dengan baik serta dapat memberikan hasil yang sama dengan uji percobaannya. Sehingga, bank sebagai penyelenggara sistem elektronik harus dapat dipercaya dan dapat menjalankan tanggungjawabnya dalam melaksanakan sistem elektronik yang baik. Demi menjalankan sistem yang baik, bank harus melaksanakan beberapa kewajibannya dalam mengoperasikan sistem elektronik seperti yang disebutkan di dalam Pasal 16 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

1. Dapat menampilkan kembali informasi elektronik yang telah tersimpan;
2. Dapat melindungi kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik;
4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa yang sederhana dan mudah dipahami;
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Dari uraian di atas, maka tanggung jawab bank dalam menjalankan sistem elektronik yang baik merupakan suatu bentuk kehati-hatian yang dimiliki oleh bank agar usahanya tetap terjaga dan sehat. Pada praktiknya, kasus *phising* dengan *social engineering* yang dialami nasabah memang terdapat unsur kesalahan nasabah, namun pada sisi lain juga terdapat kelemahan pada sistem yang dimiliki oleh bank. Dari hasil penelitian, ditemukan bahwa pada layanan bank digital pada salah satu bank yang nasabahnya terkena *phising*, pintu keamanan dikuasai oleh nasabah. Dengan keadaan ini, apabila terjadi kasus seperti *phising* maka kunci keamanan hanya ada pada nasabah. Praktiknya, pintu keamanan nasabah akan efektif apabila nasabah paham akan tanggung jawab dan kejahatan digital yang sering terjadi pada dunia perbankan. Namun, korban-korban yang mengalami *phising* merupakan masyarakat yang awam akan teknologi dan hukum. Sosialisasi yang dilakukan oleh bank nyatanya belum dapat menyentuh segala lapisan nasabah, sehingga masih terdapat nasabah yang tidak paham akan adanya kejahatan digital seperti *phising.*

Keamanan yang hanya memiliki satu pintu tidak dapat berjalan dengan efektif pada era kejahatan digital yang semakin variatif. Pasal 15 ayat (1) huruf a Peraturan Otoritas Jasa Keuangan Nomor 18 Tahun 2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum dijelaskan mengenai sistem pengendalian intern, yaitu harus mencakup kesesuaian antara sistem pengendalian intern dengan jenis dan tingkat risiko yang melekat pada kegiatan usaha bank. Pengendalian intern dibutuhkan oleh suatu bank agar usahanya dapat terus berjalan. Sistem pengendalian intern yang digunakan bank harus mencakup upaya-upaya untuk mengurangi dampak kerugian dan pelanggaran terhadap prinsip kehati-hatian bank.

Pada kasus *phising* yang dialami nasabah, kebocoran data terjadi akibat kurang meratanya sosialisasi kepada nasabah dan lemahnya sistem keamanan yang dimiliki oleh bank. Sistem keamanan yang dimiliki

tidak disesuaikan dengan risiko operasional yang dialami bank. Sehingga sistem elektronik tidak bersifat baru dan berkelanjutan.

Dari uraian di atas, maka dapat disimpulkan bahwa kelalaian bank dapat dilihat dari sifat kurang berhati-hati dalam menerapkan sistem pengendalian intern. Sebab, kurangnya sosialisasi dan lemahnya sistem keamanan bank menjadi salah satu indikator terjadinya tindakan *phising* dan hilangnya dana nasabah pada rekening.

B. Akibat Hukum Kelalaian Bank dalam Menjaga Rahasia Bank Pada Perjanjian Baku Terhadap Tindakan *Phising* yang Dialami Nasabah Akibat *Social Engineering* Ditinjau dari Hukum Positif Indonesia

Perjanjian baku adalah perjanjian yang klausulanya telah ditentukan oleh salah satu pihak yang lebih dominan. Perjanjian ini dibentuk untuk mempermudah pelaksanaannya di dalam dunia bisnis. Adanya perjanjian baku merupakan akibat dari perubahan keadaan sosial dan ekonomi masyarakat (Zakiyah, 2014, hlm. 51). Perjanjian baku memiliki akibat hukum yang sama dengan akibat yang ditimbulkan oleh perjanjian biasa.

Dalam kasus *phising* dengan *social engineering* yang dialami nasabah, terdapat kelalaian dari pihak bank yaitu kurangnya penerapan prinsip kehati-hatian pada sistem pengendalian intern bank. Kelalaian tersebut mengakibatkan hilangnya dana nasabah pada rekening. Hal ini merupakan suatu pelanggaran terhadap pasal 40 ayat (1) Undang-Undang.

Bank dan nasabah memiliki hubungan hukum yang diikat dengan perjanjian baku. Apabila nasabah maupun bank melakukan suatu pelanggaran atau tidak melaksanakan kewajiban yang seharusnya dijalankan, maka akibat yang timbul adalah ingkar janji atau wanprestasi. Namun, apabila kewajiban yang tidak dijalankan olehnya merupakan kewajiban yang tidak dijelaskan dalam perjanjian namun undang-undang mengaturnya, maka hal tersebut merupakan Perbuatan Melawan Hukum. Sebab, hal-hal yang diatur dalam perjanjian ataupun perundang-

undangan akan mengikat dan menimbulkan konsekuensi hukum sebagaimana yang diatur dalam Pasal 1339 jo. Pasal 1347 KUHPerdata yaitu perjanjian tidak hanya mengikat untuk hal yang diperjanjikan saja, namun hal yang menurut kepatutan, kebiasaan atau undang-undang serta hal-hal yang menurut kebiasaan harus dilaksanakan walaupun hal tersebut tidak tegas dinyatakan pada perjanjian.

Termaktub di dalam Buku III KUHPerdata khususnya pada Pasal 1320 KUHPerdata disebutkan bahwa ada 4 (empat) syarat sah perjanjian, yaitu :Kata Sepakat; Kecakapan; Suatu Hal Tertentu, dan Suatu Sebab yang Halal.

Berdasarkan pasal tersebut maka dapat kita lihat suatu perjanjian akan dinyatakan sah apabila telah memenuhi keempat syarat perjanjian. Pada kasus kelalaian bank ini di dapat bahwa ada Perbuatan Melawan Hukum yang dilakukan oleh bank sebab lalainya dia untuk memenuhi kewajibannya sebagaimana diatur di dalam Pasal 15 ayat (1) huruf a POJK No. 18 Tahun 2006 yaitu bank wajib menyesuaikan sistem pengendalian intern dengan tingkat dan jenis risiko yang melekat pada usaha bank. Maka dari uraian tersebut terdapat suatu sebab yang terlarang dalam pelaksanaan perjanjian. Disebabkan suatu sebab terlarang merupakan syarat objektif, maka apabila syarat ini tidak terpenuhi maka perjanjian batal demi hukum yang mengakibatkan perjanjian dianggap tidak pernah ada dan keadaan kembali seperti sebelum perjanjian ada.

Namun, dalam kasus *phising* yang dialami nasabah akibat *social engineering,* terdapat wanprestasi yang dilakukan oleh nasabah. *Phising* terjadi akibat nasabah yang memberikan data pribadi berupa *username, password,* pin, dan kode OTP kepada pelaku *phising,* sehingga wanprestasi dilakukan oleh pihak nasabah. Sehingga ganti kerugian tidak dapat dijatuhkan kepada pihak bank.

Pada pengaturannya, sebuah wanprestasi dapat dibenarkan apabila ada suatu keadaan yang tidak dapat dihindari atau yang disebut

sebagai overmacht. Berdasarkan Pasal 1244 dan Pasal 1245 KUHPerdata.

Dari hasil penelitian yang dilakukan oleh penulis, wanprestasi yang dilakukan oleh nasabah terjadi karena nasabah mengalami *social engineering*. Pelaku *phising* melakukan taktik untuk membuat nasabah merasa tertekan dan berkehendak untuk mengakses *link* yang mereka kirimkan melalui pesan *whatsapp*. Taktik yang digunakan adalah manipulasi berupa kenaikan tarif transaksi yang sangat tinggi. Sehingga, keadaan tersebut membuat nasabah panik dan berakhir mengakses *link phising* tersebut. Nasabah yang terkena *phising* merupakan orang tua atau lanjut usia yang awam akan teknologi, sehingga manipulasi yang dilakukan oleh pelaku *phising* berdampak besar bagi nasabah. Keyakinan nasabah untuk mengakses *link phising* juga dikuatkan dengan formulir beserta laman web yang dibuat layaknya informasi dari instansi resmi. Maka, dengan kurangnya pengetahuan yang dimiliki nasabah dan tekanan yang dihasilkan dari informasi palsu tersebut mengakibatkan nasabah memberikan data-data pribadinya melalui *link phising.*

Apabila dikaitkan dengan overmacht, maka keadaan yang dialami nasabah termasuk peristiwa overmacht relatif yang bersifat subjektif. Hal ini disebabkan tekanan yang dialami nasabah dapat dipandang berbeda oleh pihak lain. Namun nasabah yang terkena *phising* akibat *social engineering* akan merasakan dampak yang besar dan secara terpaksa tidak dapat melaksanakan kewajibannya, bukan karena ia tidak ingin memenuhinya namun dikarenakan untuk memenuhi kewajibannya membutuhkan pengorbanan yang besar. Overmacht tidak dapat dibuktikan sendiri melainkan harus dibuktikan oleh putusan pengadilan. Sebab. Apabila terbukti terdapat keadaan memaksa pada nasabah, maka nasabah tidak dapat diminta pertanggungjawaban atas pemenuhan prestasinya dalam perjanjian.

Terhadap kelalaian yang dilakukan oleh bank akibat tidak diterapkannya prinsip kehati-hatian yang baik di dalam sistem

pengendalian intern, menyebabkan bank melakukan Perbuatan Melawan Hukum. Hal ini dikarenakan hilangnya dana nasabah pada rekening tidak dapat dihindari akibat kurangnya kekuatan sistem keamanan pada layanan bank digital. Mengenai konsekuensi yang timbul akibat Perbuatan Melawan Hukum, bank belum dapat bertanggung jawab hingga nasabah yang menjadi alasan terjadinya *phising* dibuktikan oleh pengadilan bahwa telah memenuhi unsur *overmacht,* sebab tindakan *phising* yang dialami nasabah terjadi akibat adanya *social engineering*. Apabila pengadilan telah membuktikan bahwa benar nasabah telah mengalami overmacht, maka lalainya bank dalam menjalankan kewajibannya dalam perjanjian oleh nasabah tidak dapat dimintai pertanggungjawaban, dan pihak yang akan menanggung kerugian adalah bank sebab telah melakukan Perbuatan Melawan Hukum akibat lalainya dalam menjalankan kewajibannya.

C. Upaya Penyelesaian Terhadap Kelalaian Bank dalam Menjaga Rahasia Bank Pada Perjanjian Baku Terhadap Tindakan *Phising* yang Dialami Nasabah Akibat *Social Engineering*

Penyelesaian kelalaian bank dalam perjanjian baku dapat dilaksanakan melalui dua cara yakni penyelesaian dengan jalur pengadilan (litigasi) dan penyelesaian dengan jalur diluar dari pengadilan seperti mediasi (non-litigasi). Dalam hal penyelesaian sengketa pada lembaga jasa keuangan, Otoritas Jasa Keuangan memberikan dua mekanisme yang dapat ditempuh oleh pelaku usaha keuangan dengan konsumennya, yaitu penyelesaian melalui pengaduan konsumen yang dilakukan oleh Lembaga Jasa Keuangan, dan penyelesaian melalui jalur litigasi seperti peradilan atau non-litigasi.

Terhadap penyelesaian masalah yang disebutkan di atas, para pihak diberikan kebebasan untuk memilih jalur yang akan ditempuh oleh kedua belah pihak. Mengenai penyelesaian jalur non-litigasi dapat dijelaskan sebagai berikut :

1. Penyelesaian melalui jalur non-litigasi

Penyelesaian non-litigasi disebut sebagai penyelesaian sengketa alternatif. Pada sektor jasa keuangan terdapat lembaga yang akan menangani permasalahan yang terjadi antara Lembaga Jasa Keuangan dengan konsumennya. Lembaga tersebut dikenal sebagai Lembaga Alternatif Penyelesaian Sengketa (LAPS). Namun, terdapat lembaga khusus yang akan menangani permasalahan di bidang perbankan. Lembaga ini dibentuk oleh Otoritas Jasa Keuangan (OJK) untuk menjadi wadah penyelesaian sengketa jalur non-litigasi, yaitu Lembaga Alternatif Penyelesaian Sengketa Perbankan Indonesia (LAPSPI).

Berdasarkan Pasal 2 POJK Nomor 1/POJK.07/2014 tentang Lembaga Alternatif Penyelesaian Sengketa di Sektor Jasa Keuangan mengatur, sebelum memasuki tahap penyelesaian melalui LAPSPI penyelesaian harus dilakukan oleh pelaku usaha bank. Peraturan OJK mengenai Perlindungan Konsumen Sektor Jasa Keuangan mengatur bahwa setiap Lembaga Jasa Keuangan khususnya bank harus memiliki pelayanan berupa pengaduan bagi konsumen (Otoritas Jasa Keuangan, 2017). Pengaturan ini diadakan untuk menjamin terlaksananya perlindungan konsumen di dalam pelaksanaan usaha pada sektor jasa keuangan.

Pada Lembaga Jasa Keuangan khususnya bank, layanan pengaduan nasabah dapat diakses oleh setiap masyarakat yang telah menjadi nasabah suatu bank. Layanan pengaduan tersebut dapat dilakukan oleh nasabah dengan cara datang langsung ke kantor cabang bank terdekat ataupun dilakukan melalui aplikasi bank digital yang disediakan oleh bank. Apabila penyelesaian melalui pelayanan pengaduan nasabah tidak ditemukan kesepakatan, maka penyelesaian sengketa diluar pengadilan dilakukan melalui Lembaga Alternatif Penyelesaian Sengketa (LAPS). Adapun layanan yang akan diberikan oleh LAPS adalah berupa (Otoritas Jasa Keuangan, 2017) :

a. Mediasi, yaitu penyelesaian masalah melalui mediator agar mencapai kesepakatan;
b. Ajudikasi, yaitu penyelesaian sengketa melalui ajudikator untuk menjatuhkan putusan yang mengikat bagi para pihak;
c. Arbitrase, yaitu penyelesaian sengketa yang didasarkan pada perjanjian yang dibuat dan disepakati oleh para pihak. Putusan yang dihasilkan dari penyelesaian melalui arbitrase ini bersifat final dan mengikat bagi para pihaknya.

Dalam penyelesaian kelalaian bank dalam perjanjian baku akibat adanya tindakan *phising* yang dialami nasabah akibat *social engineering* dapat dilakukan dengan cara non-litigasi, yaitu nasabah melakukan pengaduan melalui aplikasi layanan bank digital atau langsung mendatangi kantor cabang bank yang terdekat. Dari pengaduan tersebut pihak bank akan melakukan investigasi dan analisis terhadap pengaduan guna untuk membuktikan kelalaian yang dilakukan oleh bank. Namun, apabila putusan bank tidak dapat mencapai kesepakatan bagi pihak nasabah, maka penyelesaian dapat dilakukan melalui LAPS untuk selanjutnya ditindak lanjuti.

2. Penyelesaian melalui jalur pengadilan

Jalur litigasi merupakan upaya terakhir yang dapat ditempuh apabila jalur non-litigasi tidak menghasilkan sepakat. Apabila suatu permasalahan yang memasuki penyelesaian secara litigasi atau pengadilan, maka harus ada pembuktian yang harus diperlihatkan di muka pengadilan, karena berdasarkan Pasal 1865 KUHPerdata dapat disimpulkan bahwa setiap orang yang ingin meneguhkan haknya atau membantah suatu hak orang lain, merujuk pada suatu peristiwa maka orang tersebut wajib membuktikannya.

Adapun alat-alat bukti yang dapat digunakan di pengadilan adalah yang disebutkan oleh Pasal 1866 KUHPerdata, yaitu bukti tertulis, saksi, prasangka, pengakuan, dan sumpah.

Seiring berkembangnya teknologi, pembuktian pada perkara perdata semakin berkembang. Pada kasus perdata pembuktian

dapat berupa alat bukti elektronik seperti yang dijelaskan dalam Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Ekonomi, yaitu informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Dalam penyelesaian kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering,* apabila dilakukan melalui jalur litigasi maka pembuktian berupa dokumen elektronik seperti perjanjian, bukti terjadinya *phising*, bukti kerugian yang dialami, serta bukti transaksi yang berbentuk dokumen elektronik dapat dijadikan bukti di dalam proses pengadilan.

IV. SIMPULAN DAN SARAN

A. SIMPULAN

1. Kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering* adalah tidak ada penyesuaian sistem pengendalian intern dengan jenis dan tingkat risiko khusunya pada sistem keamanan dan pemerataan sosialisasi kepada nasabah berdasarkan Pasal 15 ayat (1) huruf a POJK No. 18 tahun 2006.
2. Akibat hukum kelalaian bank dalam menjaga rahasia bank terhadap perjanjian baku dalam tindakan *phising* yang dialami nasabah akibat *social engineering* ditinjau dari hukum positif Indonesia adalah batal demi hukum dikarenakan adanya Perbuatan Melawan Hukum yang dilakukan oleh bank sebagaimana yang diatur pada Pasal 1365 KUHPerdata. Dan ganti rugi oleh bank dapat terlaksana apabila pengadilan membuktikan bahwa terjadi overmacht pada nasabah.
3. Upaya penyelesaian terhadap kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering* dapat dilakukan dengan dua cara, yaitu penyelesaian secara non-litigasi dengan pengajuan

perkara melalui Lembaga Alternatif Penyelesaian Sengketa dan non-litigasi dengan mengajukan gugatan ke pengadilan.

B. SARAN

1. Mengenai kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering* diharapkan Instansi Otoritas Jasa Keuangan dapat lebih tegas dalam pengawasan sistem keamanan yang dimiliki oleh bank, sehingga bank tetap dapat menjadi instansi yang dapat dipercaya oleh masyarakat.
2. Mengenai akibat hukum kelalaian bank dalam menjaga rahasia bank terhadap perjanjian baku dalam tindakan *phising* yang dialami nasabah akibat *social engineering* ditinjau dari hukum positif diharapkan pemerintah dapat mengoptimalkan Perundang-undangan di Indonesia terkait kejahatan digital yang dialami oleh nasabah seperti *phising* yang disertai *social engineering*, dan diharapkan untuk kedepannya nasabah memiliki hak untuk memasukkan pendapatnya dalam perjanjian antara bank dan nasabah
3. Mengenai upaya penyelesaian terhadap kelalaian bank dalam menjaga rahasia bank pada perjanjian baku terhadap tindakan *phising* yang dialami nasabah akibat *social engineering,* disarankan untuk nasabah dapat melakukan penyelesaian melalui jalur litigasi agar mendapatkan penyelesaian yang adil sehingga dapat memperoleh kepastian hukum.

DAFTAR PUSTAKA

Bandig, M. P., Padliansyah, R., & Shalahuddin. (2021). *Sistem Informasi Manajemen Dalam Perspektif Revolusi Industri 4.0* (M. K. Muchamad, Ed.). Syiah Kuala University Press.

Hermansyah. (2020). *Hukum Perbankan Nasional Indonesia* (Vol. 3). Kencana.

Ginantra, N. L. W. S. R., Simarmata, J., Purba, R. A., Tojiri, M. Y., Duwila, A. A., Siregar, M. N. H., Nainggolan, L. E., Marit, E. L., Sudirman, A., & Siswanti, I. (2020). *Teknologi Finansial Sistem Finansial Berbasis Teknologi di Era Digital* (A. Rikki, Ed.). Yayasan Kita Menulis.

Ikatan Bankir Indonesia. (2019). *Pedoman dan Strategi Audit Intern Bank Modul Sertifikasi Bidang Audit Intern Bank untuk Audit Manager* (Fajarianto, Ed.). PT Gramedia Pustaka Utama.

Oktavira, B. A. (2020, Mei 12). *Tanggung Jawab Bank atas Pembobolan Rekening Nasabah*. Hukumonline. https://www.hukumonline.com/klinik/a/tanggung-jawab-bank-atas-pembobolan-rekening-nasabah-lt5ea6e27adf366

Otoritas Jasa Keuangan. (2017). *Lembaga Alternatif Penyelesaian Sengketa*. Ojk.Go.Id. https://www.ojk.go.id/id/kanal/edukasi-dan-perlindungan-konsumen/pages/lembaga-alternatif-penyelesaian-sengketa.aspx

Putra, P. (2022). Lagi, Uang Rp 469 Juta di Rekening BRI Raib Gara-gara Klik Link Penipu https://regional.kompas.com/read/2022/06/11/153551878/lagi-uang-rp-469-juta-di-rekening-bri-raib-gara-gara-klik-link-penipu?page=all

Rifka, I. (2022, Januari 14). *Cara Daftar dan Mengaktifkan Mobile Banking BRI*. Kompas.Com. https://money.kompas.com/read/2022/01/14/171000626/cara-daftar-dan-mengaktifkan-mobile-banking-bri?page=all

Soekanto, S. (2013). *Penelitian Hukum Normatif, Suatu Tinjauan Singkat* . Raja Grafindo Persada.

Zakiyah. (2014). *Perjanjian Baku dalam Perspektif Perlindungan Konsumen* (taufik Hudayat, Ed.). Aura Pustaka.