YUSTISIA TIRTAYASA : JURNAL TUGAS AKHIR
Volume 3 Nomor 1, April 2023, hlm. (57-72)
Fakultas Hukum, Universitas Sultan Ageng Tirtayasa, Serang-Banten, Indonesia
P-ISSN: 2807-2863 | E-ISSN: 2807-1565
https://jurnal.untirta.ac.id/index.php/yustisia/index

Perlindungan Hukum terhadap Nasabah BTPN Jenius akibat Tindakan *Phishing* (Studi Kasus Bank Tabungan Pensiunan Nasional Jenius)

Yosefine
Fakultas Hukum, Universitas Sultan Ageng Tirtayasa
Jl. Raya Palka Km 3 Sindangsari, Pabuaran, Serang, Banten
Email: 1111180421@untirta.ac.id

Rani Sri Agustina
Fakultas Hukum, Universitas Sultan Ageng Tirtayasa
Jl. Raya Palka Km 3 Sindangsari, Pabuaran, Serang, Banten
Email: rani@untirta.ac.id

Dede Agus
Fakultas Hukum, Universitas Sultan Ageng Tirtayasa
Jl. Raya Palka Km 3 Sindangsari, Pabuaran, Serang, Banten
Email: de298gus@gmail.com

DOI: http://dx.doi.org/10.51825/yta.v2i1.

Info Artikel
|Submitted: 13 November 2022 **|Revised**: 5 Maret 2023 **|Accepted**: 20 Maret 2023

How to cite: Yosefine, Rani Sri Agustina, Dede Agus, "Perlindungan Hukum terhadap Nasabah BTPN Jenius akibat Tindakan *Phishing* (Studi Kasus Bank Tabungan Pensiunan Nasional Jenius)", *Yustisia Tirtayasa: Jurnal Tugas Akhir*, Vol. 3 No. 1, (April, 2023), hlm. 57-72.

ABSTRACT:

This article discusses phishing activities that have led to allegations of leakage of personal data from Jenius customers, which is one of the digital banking applications from the National Pension Savings Bank (BTPN). This phishing activity causes the loss of customer deposits in the Jenius application. Law Number 10 of 1998 concerning Banking and Law Number 19 of 2016 concerning Information and Electronic Transactions are used as references in this study. The purpose of this study is to identify and analyze legal protection for customers and to identify and analyze the legal responsibilities given by banks to customers. The research method used is normative juridical through legislation approach, conceptual approach, case approach and qualitative descrptive analysis. The source of the data used is secondary data in the form of library research and is supported by primary data obtained by interview. Based on the research results, the legal protection provided to customers is by applying the principle of confidentiality by banks as regulated in Law Number 10 of 1998 concerning Banking, although the Banking Law does not regulate in detail regarding digital banking. Phishing activities themselves have been regulated and threatened in Law Number 19 of 2016 concerning Information and Electronic Transactions. The responsibility given by the bank is to provide complaint services and carry out inspections/investigations as well as assist customers in finding solutions for losses suffered by customers.

Keyword: *Digital Banking, Personal Data Leakage, Phishing, BTPN Jenius*

ABSTRAK:

Jurnal ini membahas mengenai kegiatan phising yang menimbulkan dugaan kebocoran data pribadi dari para nasabah Jenius yang merupakan salah satu aplikasi perbankan digital dari Bank Tabungan Pensiunan Nasional (BTPN). Kegiatan phising ini menimbulkan hilangnya simpanan nasabah dalam aplikasi Jenius. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dijadikan sebagai acuan dalam penelitian ini. Tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis perlindungan hukum bagi nasabah serta untuk mengetahui dan menganalisis tanggung jawab hukum yang diberikan oleh bank kepada nasabah. Metode penelitian yang digunakan adalah yuridis normatif melalui pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus serta analisis deskriptif kualitatif. Sumber data yang digunakan adalah data sekunder berupa penelitian kepustakaan dan didukung dengan data primer yang diperoleh dengan wawancara. Berdasarkan hasil penelitian, perlindungan hukum yang diberikan bagi nasabah adalah dengan penerapan prinsip kerahasiaan oleh bank sebagaimana diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, meskipun Undang-Undang Perbankan tidak mengatur secara rinci mengenai perbankan digital. Kegiatan phising sendiri telah diatur dan diancam dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Tanggung jawab yang diberikan oleh bank adalah menyediakan layanan pengaduan dan melakukan pemeriksaan/penyelidikan serta membantu nasabah dalam mencari solusi atas kerugian yang dialami oleh nasabah.

Kata Kunci: *Perbankan Digital, Kebocoran Data Pribadi, Phising, BTPN Jenius*

Pendahuluan

Perkembangan industri telah memasuki era digial yang mempengaruhi berbagai bidang. Setiap bidang berlomba-lomba untuk memaksimalkan transformasi layanannya guna menarik perhatian konsumennya. Salah satu bidang yang turut melakukan transformasi adalah sektor perbankan dengan memunculkan layanan perbankan berbentuk digital (*digital banking)*. Layanan perbankan digital ini bertujuan untuk memberikan kemudahan bagi nasabah dalam bertransaksi. Perbankan digital adalah suatu kegiatan dengan melakukan layanan atau kegiatan perbankan secara mandiri menggunakan fasilitas elektronik atau digital yang dimiliki oleh bank, serta melalui media digital yang dimiliki oleh nasabah atau calon nasabah. Perbankan digital memungkinkan nasabah untuk melakukan komunikasi, pendaftaran, pembukaan rekening, transaksi, dan penutupan rekening.[1] Selain itu, nasabah juga dapat memperoleh informasi dan melakukan transaksi yang tidak terkait dengan layanan perbankan, seperti penasehat keuangan, investasi, dan e-commerce atau transaksi melalui sistem perdagangan berbasis elektronik.

Transformasi yang dilakukan dalam sebuah perbankan tetap harus memegang prinsip kerahasiaan bank terutama dalam menjaga kerahasiaan data pribadi nasabah. Hubungan hukum antara bank dengan nasabah pada hakekatnya mengikuti asas kepercayaan, dimana nasabah menitipkan dananya untuk disimpan di bank dalam suatu portofolio dan dikelola secara jujur dan aman, dengan pengertian bahwa bank dapat menyediakannya ketika diminta kembali oleh nasabah.[2] Hal ini didukung dengan adanya prinsip kehati-hatian sebagaimana diatur dalam ketentuan Pasal 2 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Prinsip kehati-hatian ini dilakukan dengan tujuan untuk menghindari terjadinya kerugian yang dapat merugikan kepentingan nasabah, mengingat adanya risiko yang besar terutama dalam pemanfaatan teknologi dan informasi.

Bank wajib merahasiakan seluruh informasi yang berkaitan dengan nasabah yang melakukan penyimpanan dan simpanannya dengan menerapkan asas-asas, yaitu asas perlindungan, asas kepastian hukum, asas kemanfaatan, asas kepentingan umum, asas pertanggungjawaban, asas keseimbangan, dan asas kehati-hatian. Penerapan prinsip-prinsip perbankan tersebut pada kenyataannya masih belum terlaksana secara maksimal dalam menjaga data pribadi nasabahnya, sehingga menimbulkan kebocoran data pribadi. Kebocoran data pribadi nasabah tersebut dapat menimbulkan penyalahgunaan data pribadi yang merugikan nasabah. Hal ini dapat dilihat dari masih banyaknya nasabah mendapatkan telepon yang mengatasnamakan pihak bank untuk melakukan penipuan. Sehingga menimbulkan dugaan adanya kebocoran data pribadi dari para nasabah.

Dugaan kebocoran data pribadi ini dialami oleh beberapa nasabah Bank Tabungan Pensiunan Nasional (BTPN) Jenius. Hal ini bermula ketika beberapa nasabah menerima panggilan telepon yang mengatasnamakan Jenius dan menginformasikan adanya pergantian kartu debit. Awalnya tidak ada

[1] Otoritas Jasa Keuangan, "Panduan Penyelenggaraan Digital Branch Oleh Bank Umum," https://www.ojk.go.id/id/kanal/perbankan/Pages/Panduan-Penyelenggaraan-Digital-Branch-oleh-Bank-Umum.aspx., December 2016.

[2] Trisadini P. Usanti and Shomad, *Hukum Perbankan* (Jakarta: Kencana, 2017), hlm.25.

kecurigaan dari para nasabah karena perkataan yang dilontarkan oleh penelepon tersebut memiliki kesamaan dengan ciri khas *customer secrive* Jenius. Nasabah yang tidak memiliki kecurigaan tersebut kemudian mengisi *link* yang diberikan oleh penelepon. Setelah beberapa saat, aplikasi Jenius nasabah sudah ter-*log out* dan tidak bisa melakukan *log in* lagi. Ketika melakukan pengecekan di kantor BTPN, nasabah mendapatkan informasi bahwa uang ratusan juta milik nasabah sudah ditransfer ke rekening orang lain. Hal inilah yang menimbulkan dugaan kebocoran data nasabah BTPN Jenius sehingga terjadi penyalahgunaan data pribadi oleh pihak yang tidak berwenang dan menimbulkan kerugian bagi nasabah.

Prinsip kerahasiaan merupakan salah satu kewajiban bank. Peraturan mengenai rahasia perbankan ini dapat dijumpai di dalam Pasal 40, 41, 41 A, 42, 43, 44, 44A dan Pasal 45 Undang-Undang Perbankan.[3] Keterangan data pribadi seorang nasabah juga sangat penting untuk dijaga kerahasiaannya, hal ini ditegaskan dalam Pasal 40 Undang-Undang Perbankan yang berarti keterangan mengenai nasabah bank tidak hanya mengenai keterangan mengenai keadaan keuangan melainkan segala bentuk keterangan mengenai nasabah penyimpan, dan nomor telepon menjadi sesuatu yang harus dirahasiakan oleh bank penyimpan data nasabah.[4] Meskipun peraturan menganai perlindungan data pribadi belum diatur secara merinci dalam suatu Undang-Undang, namun Pasal 26 Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan landasan perlindungan data pribadi yang diperoleh dengan menggunakan sistem elektronik.[5] Berdasarkan latar belakang masalah tersebut, maka penulis tertarik untuk melakukan sebuah penelitian mengenai bentuk perlindungan hukum yang diberikan kepada nasabah Jenius akibat adanya tindakan *phishing*.

Metode Penelitian

Penelitian ini menggunakan penelitian yuridis normatif, yang membahas norma-norma kemasyarakatan dan hukum yang terdapat dalam undang-undang dan putusan pengadilan.[6] Penelitian ini didukung dengan pendekatan perundang-undangan (*statute approach),* pendekatan konspetual (*conceptual approach),* dan pendekatan kasus (*case approach).* Penulis menggunakan data sekunder dan data primer sebagai sumber data dalam penelitian ini. Data sekunder diperoleh dengan penelitian kepustakaan (*library search)* dari dokumen-dokumen resmi, buku-buku yang berhubungan dengan objek penelitian, hasil penelitian dalam bentuk laporan, skripsi, tesis, disertasi, dan peraturan perundang-undangan.[7] Selanjutnya data primer yang digunakan diperoleh dengan studi lapangan (*field research)* berupa wawancara dengan BTPN Jenius, Nasabah BTPN Jenius, Otoritas Jasa Keuangan, dan Direktorat Jenderal Aplikasi Informatika Kominfo. Semua data yang diperoleh kemudian dianalisis secara deskriptif kualitatif,

[3] Mahesa Jati Kusuma, *Hukum Perlindungan Nasabah Bank, Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE Di Bidang Perbankan* (Bandung: Nusa Media, 2019), hlm. 113.

[4] Marnia Rani, *Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank*, vol. 2, No.1, (2014): 169.

[5] Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 1, no. 1 (2019): 152.

[6] Zainuddin Ali, *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2009), hlm. 105.

[7] Ibid, hlm. 106.

yaitu penulis berpedoman kepada bahan hukum sebagai acuan dalam memberikan penetapan serta dianalisis tanpa menggunakan perhitungan rumus matematika, populasi, sampel, dan data statistika.

Perlindungan Hukum terhadap Nasabah akibat Dugaan Kebocoran Data Pribadi dalam Aplikasi Perbankan Digital

Perbankan digital sebagai suatu pemanfaatan teknologi dalam perbankan telah memberikan perubahan baru bagi nasabah. Setiap pelaku usaha tentunya selalu berusaha untuk memberikan pelayanan terbaiknya bagi nasabah. Sama halnya dengan perbankan digital yang diharapkan dapat lebih memberikan kemudahan bagi nasabah daripada pelayanan secara konvensional. Harapan ini dapat kita lihat dalam Pasal 1 Ayat (4) POJK No.12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum, bahwa layanan perbankan digital adalah layanan perbankan elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah dalam rangka melayani nasabah secara lebih cepat, mudah, dan sesuai dengan kebutuhan (*customer experience*), serta dapat dilakukan secara mandiri sepenuhnya oleh nasabah, dengan memperhatikan aspek keamanan.[8] Pelayanan yang diberikan oleh bank dalam perbankan digital juga didukung dengan layanan-layanan lain yang dapat digunakan oleh nasabah, yaitu:

1. *Internet banking* yang memungkinkan nasabah dapat melakukan berbagai transaksi perbankan dengan menggunakan perangkat elektronik atau komputer yang terhubung dengan jaringan internet, antara lain transfer dana, perubahan rekening, informasi saldo, informasi nilai tukar, pembayaran tagihan, dan pembelian.
2. *Mobile banking* yang memungkinkan nasabah untuk bertransaksi melalui telepon dimana terdapat program khusus yang sudah terpasang pada SIM Card nasabah untuk bisa melakukan transaksi perbankan.
3. *SMS banking* merupakan layanan perbankan digital yang dapat dilakukan nasabah dengan menggunakan fitur SMS yang terdapat dalam telepon seluler.
4. *Phone banking* yang memungkinkan nasabah menghubungi pihak bank untukmenjalankan transaksi nasabah seperti transfer dana, informasi saldo, mutasi rekening, pembayaran tagihan, dan pembelian.

Pelaksanaan perbankan digital pada dasarnya berpedoman pada Undang-Undang Perbankan meskipun belum ada undang-undang yang mengatur secara khusus. Undang-Undang Perbankan memberikan pengaturan yang dapat ditemukan dalam Pasal 5 Ayat (2), yaitu bahwa "Bank umum dapat mengkhususkan diri untuk melaksanakan kegiatan tertentu atau memberikan perhatian yang lebih besar kepada kegiatan tertentu".[9] Pasal 6 huruf a juga menyebutkan bahwa "melakukan kegiatan lain yang lazim dilakukan oleh bank sepanjang tidak bertentangan dengan undang-undang ini dan peraturan perundang-undangan yang berlaku".[10] Berdasarkan ketentuan

[8] "Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum " (n.d.).

[9] "Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 10 Tahun 1998" (n.d.).

[10] Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998.

tersebut, dapat dikatakan bahwa sistem perbankan digital dapat dilaksanakan oleh bank selama tidak bertolak belakang dengan Undang-Undang Perbankan serta peraturan perundang-undangan lainnya yang memiliki keterkaitan. Namun berkembangnya layanan perbankan digital juga meningkatkan resiko yang akan dihadapi oleh bank, untuk itu Peraturan OJK No.12/POJK.03/2018 diharapkan dapat memprioritaskan manajemen risiko dalam penggunaan teknologi informasi dengan tetap menawarkan layanan perbankan digital.[11] Pasal 2 Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum menentukan bahwa:

1. Bank dapat menyelenggarakan Layanan Perbankan Elektronik atau Layanan Perbankan Digital.
2. Bank yang menyelenggarakan Layanan Perbankan Elektronik atau Layanan Perbankan Digital, wajib menerapkan manajemen risiko, prinsip kehati-hatian, dan memenuhi ketentuan dalam Peraturan Otoritas Jasa Keuangan.

Data pribadi seseorang saat ini menjadi hal prioritas yang harus dijaga keamanannya, terutama dalam sistem elektronik seperti perbankan digital. Ketika membicarakan sebuah sistem elektronik, kita tidak bisa mengatakan bahwa data diri seseorang akan aman seutuhnya karena pasti memiliki celah-celah keamanan yang tidak terlihat. Kejahatan dalam dunia perbankan juga semakin canggih mengingat adanya pemanfaatan teknologi informasi dengan memanfaatkan kelemahan keamanan sistem perbankan atau biasa disebut dengan *cyber crime*. Tentunya segala upaya harus dilakukan untuk mengantisipasi terjadinya kebocoran data atau mengamankan data pribadi ketika terjadi kebocoran data.[12] Hal tersebut harus dilakukan baik dari pihak bank maupun nasabahnya untuk mencegah timbulnya kerugian yang tidak diinginkan.

Salah satu tindakan *Cyber crime* yang sering ditemukan dalam perbankan adalah *phising.* Berdasarkan hasil studi literatur yang telah dilakukan sebelumnya, faktor penyebab munculnya ancaman serangan phising ketika pengguna menggunakan layanan online banking adalah minimnya pengetahuan pengguna, psikologis, dan privasi social networking services pengguna.[13] *Phising* merupakan sebuah kegiatan peretasan yang dilakukan oleh seseorang untuk mendapatkan informasi sensitif secara ilegal, seperti data pribadi (nama, usia, alamat), data akun (username, password), dan data finansial (informasi kartu kredit, rekening). Kegiatan phising ini terbilang mudah karena dapat memberikan hasil yang efektif dengan langkah yang mudah yaitu dengan cara meminta calon korban untuk memberikan informasi pribadi dengan cara mengirimkan pesan yang tidak benar dalam bentuk surat elektronik atau komunikasi lainnya.[14]

[11] Herdian Ayu Andreana Beru Tarigan and Darminto Hartono Paulus, "Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital", *Jurnal Pembangunan Hukum Indonesia*, Vol. 1, No. 3, (2019): 301.

[12] "Wawancara Dengan Ajeng Risda Rahmadani, Subkor Edukasi Dan Promosi PDP Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi Dan Informatika", pada 20 Juli 2022, pukul 10.00 WIB, n.d.

[13] Ikhsan Radiansyah and Yudi Priyadi, "Analisis Ancaman Phising Dalam Layanan Online Banking," *Jurnal Ekonomika Bisnis, Universitas Telkom*, Vol.7, No.1, (2016): 4.

[14] Fitri Nur Latifahi, Imron Mawardi, and Bayu Wardhana, "Ancaman Pencurian Data (Phising) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19 (Study

Menggunakan beberapa saran resmi, peretas mengklaim untuk menjaga atau meningkatkan keamanan rekening bank pengguna, pengguna dapat memasukkan kembali nama pengguna dan kata sandi untuk *internet banking* atau rekening bank, dan kemudian menambahkan administrator atau layanan dukungan nomor telepon untuk mengatasi masalah.[15] Kasus hilangnya simpanan nasabah BTPN Jenius merupakan salah satu kegiatan *phising* karena pelaku *phising (phiser)* mendapatkan informasi sensitif korban seperti data pribadi dan data finansial dengan cara memberikan *link* menuju sebiah *website* yang serupa dengan *website* asli BTPN Jenius. Ketika nasabah memasukkan isian data dan kata sandi miliknya ke dalam website tiruan tersebut, maka data tersebut akan diketahui oleh phiser tersebut.

Perlindungan terhadap nasabah sangat diperlukan mengingat risiko yang dapat menimpa nasabah. Menurut menurut Marulak Pardede, perlindungan terhadap data nasabah bank di Indonesia dapat dilakukan melalui 2 cara, yaitu:

1. Perlindungan secara eksplisit (*explicit deposit protection*), yaitu perlindungan dengan membentuk suatu lembaga, yaitu Lembaga Penjamin Simpanan yang diatur berdasarkan Keputusan Presiden RI Nomor 26 Tahun 1998 mengenai Jaminan Terhadap Kewajiban Umum serta Undang-Undang Nomor 24 Tahun 2004 mengenai lembaga tersebut Lembaga Penjamin Simpanan (LPS). Tujuan lembaga LPS ini adalah sebagai penjamin simpanan nasabah yang bertugas sebagai lembaga yang nantinya akan mengganti dana nasabah yang disimpan di bank, ketika bank yang bersangkutan mengalami kegagalan atau biasa disebut dengan bank gagal. LPS juga berperan aktif dalam menjaga stabilitas sistem perbankan sesuai dengan kewenangannya.
2. Perlindungan secara implisit (*implicit deposit protection)*, yaitu diterapkannya pengawasan serta pembinaan bank yang merupakan bentuk penerapan perlindungan secara efektif untuk mencegah terjadinya kebangkrutan bank. Dalam hal perlindungan implisit ini, terdapat beberapa perlindungan yang diperoleh melalui peraturan perundang-undangan di bidang perbankan; perlindungan yang dihasilkan dari pengawasan dan pengarahan yang efisien oleh Bank Indonesia, khususnya dengan memantau kinerja bank dalam mengamankan nasabah dan memberikan pembinaan terhadap yang tidak sehat; upaya menjaga kelangsungan usaha bank sebagai sebuah lembaga pada khususnya dan perlindungan terhadap sistem perbankan pada umumnya; memelihara tingkat kesehatan bank yaitu dengan pembinaan yang dilakukan oleh Bank Indonesia; melakukan usaha sesuai dengan prinsip kehati-hatian sesuai dengan ketentuan Pasal 2 Undang-Undang Perbankan; cara pemberian kredit yang tidak merugikan bank dan kepentingan nasabah; menyediakan informasi risiko pada nasabah bank.

Perlindungan hukum bagi nasabah selaku konsumen mempunyai hak untuk melakukan pengaduan nasabah, serta menggunakan forum mediasi perbankan untuk mendapatkan penyelesaian sengketa di bidang perbankan secara sederhana, murah, dan

Phising Di Indonesia)," *Perisai: Islamic Banking and Finance Journal,* Vol 6 Issue 1, (2022): 80.

[15] Amin Muftiadi, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phisingterhadap Layanan Online Banking," *Hexatech: Jurnal Ilmiah Teknik* 1, no. 2 (2022):. 63.

cepat.[16] Otoritas Jasa Keuangan selaku pengawas pada sektor jasa keuangan juga memberikan perlindungan hukum bagi nasabah Pengawasan OJK terhadap perbankan mencakup seluruh aspek dalan keberjalanan suatu bank, mulai dari aspek kelembagaan, aspek produk dan aktivitas, aspek prudensial, hingga aspek transparasi. Tahapan pengawasan yang dilakukan OJK mencakup memahami bank yang diawasi, melakukan penilaian risiko bank, menyusun rencana pengawasan berdasarkan risiko yang teridentifikasi, melakukan pemeriksaan bank, dan melakukan pemantauan kondisi bank secara berkala.[17] Perlindungan hukum yang diberikan oleh OJK kepada nasabah atau konsumen dalam perbankan berpedoman pada Pasal 2 ayat (1) POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, yaitu dengan menerapkan prinsip:[18]

1. edukasi yang memadai;
2. keterbukaan dan transparansi informasi;
3. perlakuan yang adil dan perilaku bisnis yang bertanggung jawab;
4. perlindungan aset, privasi dan data Konsumen; dan
5. penanganan pengaduan dan penyelesaian sengketa yang efektif dan efisien.

Pemanfaatan akan teknologi dan informasi yang dapat dirasakan dalam berbagai bidang memungkinkan pelaku usaha atau penyelenggara sistem elektronik bisa mengumpulkan data pribadi dari pelanggan atau calon pelanggan secara luring atau daring, dimana data digital dapat diperjualbelikan tanpa sepengetahuan dan seizin pemilik data atau disalahgunakan, bisa juga terjadi data pribadi yang terkoneksi dibajak, dicuri (*hack*) oleh pihak ketiga.[19] Peristiwa inilah yang dapat membuka peluang timbulnya kejahatan dalam perbankan digital atau biasa disebut dengan *cyber crime*. Aplikasi Jenius sendiri sudah terbilang cukup aman karena telah berada di dalam pengawasan Otoritas Jasa Keuangan (OJK) dan simpanannya juga telah dijamin oleh Lembaga Penjamin Simpanan (LPS). Jadi jika terdapat kesalahan dalam Jenius, OJK selaku pengawas akan mendatangkan pengawasnya ke pusat untuk melakukan pengecekan.[20]

Selain itu menurut Haryono, *service point* Jenius, data pribadi nasabah dalam aplikasi Jenius terbilang aman karena dari sisi internal melakukan audit mengenai betul ada atau tidaknya penyimpanan data nasabah, ada atau tidaknya penyalahgunaan data nasabah, ada atau tidaknya keterlibatan internal. Aplikasi Jenius juga tidak mengalami kebocoran data, melainkan nasabah yang memang memiliki kekurangan informasi mengenai perbankan dan tidak tersedukasi. Ketika nasabah tersebut melakukan pembukaan tabungan yang relatif singkat, banyak nasabah yang malas membaca sehingga menimbulkan

[16] David Y. Wonok, "Perlindungan Hukum Atas Hak-Hak Nasabah Sebagai Konsumen Pengguna Jasa Bank Terhadap Risiko Yang Timbul Dalam Penyimpangan Dana", *Jurnal Edisi Khusus* Vol.1, No.2, (2012): 63.

[17] "Wawancara Dengan Direktorat Pengembangan Pengawasan Bank, Otoritas Jasa Keuangan,", pada 6 Juni 2022, pukul 14.00 WIB , n.d.

[18] "Wawancara Dengan Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan,", pada 6 Juni 2022, pukul 14.00 WIB, n.d.

[19] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, Vol. 27 No. 1, (2021): 39.

[20] "Wawancara Dengan Haryono K.P, Service Point Jenius,", pada 6 Juni 2022, pukul 14.00 WIB, n.d.

nasabah tidak mengetahui risiko ketika memberikan data kepada orang lain.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 10 Tahun 1998 tentang Informasi dan Transaksi Elektronik sebagai dasar hukum penyelenggaraan sistem elektronik telah memberikan perlindungan hukum apabila terjadi permasalahan antara bank dengan nasabah dalam pelaksanaan layanan perbankan digital.

Saat ini kegiatan *cyber crime* dalam bentuk *phising* di Indonesia diatur dalam Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik karena dalam kegiatannya *phiser* menirukan website asli yang menimbulkan kerugian bagi nasabah. Pasal 35 jo. Pasal 51 ayat (1) ini manyatakan:

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 51 Ayat (1)

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Phiser juga dapat dikenakan Pasal 30 Ayat (3) jo. Pasal 46 Ayat (3) Undang-Undang Informasi dan Transaksi Elektronik jika pelaku menerobos atau menjebol suatu sistem elektronik dengan menggunakan identitas dan *password* korban dengan tanpa hak. Pasal 30 Ayat (3) jo. Pasal 46 Ayat (3) Undang-Undang Informasi dan Transaksi Elektronik menyebutkan:

Pasal 30 Ayat (3)

(3) "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan".

Pasal 46 Ayat (3)

(3) "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)".

Selain itu kegiatan *phising* juga diatur dalam Pasal 32 ayat (2) jo. Pasal 48 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik atas perbuatan memindahkan atau mentransfer informasi elektronik milik korban seperti isi rekening, kode akses, dan lain sebagainya yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Pasal 32 Ayat (2) jo. Pasal 48 Ayat (2) Undang-Undang Informasi dan Transaksi Elektronik menyebutkan:

Pasal 32 Ayat (2)

(2) "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang Lain yang tidak berhak".

Pasal 48 Ayat (2)

(2) "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah)".

Tanggung Jawab Bank Tabungan Pensiunan Nasional akibat Hilangnya Dana Nasabah dalam Aplikasi Jenius

Pertanggungjawaban bank terhadap kerugian yang dialami oleh

nasabah dapat dilakukan dengan melakukan penyelesaian sengketa. Bank sebagai Pelaku Usaha Jasa Keuangan (PUJK) wajib melakukan penanganan atas aduan dari nasabah selaku konsumen dan menyelesaikan sengketa atas produk dan/atau layanannya. Hal ini sebagaimana diatur dalam Pasal 6 POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Bank BTPN Jenius sendiri telah memberikan tata cara pengaduan yang dapat dilakukan jika sewaktu-waktu nasabah mengalami kerugian sebagaimana dijelaskan dalam website BTPN Jenius yaitu www.jenius.com.

Pengaduan dapat dilakukan oleh nasabah dengan secara lisan maupun tertulis. Pengaduan secara lisan dapat dilakukan oleh nasabah dengan cara menelepon Jenius Help di nomor 1500365 atau datang secara langsung ke Jenius *Service Point* terdekat. Selanjutnya pengaduan akan diverifikasi oleh tim terkait dan jika dibutuhkan Jenius akan meminta dokumen tambahan atau pendukung. Setelah diverifikasi, nasabah akan mendapatkan nomor registrasi untuk memudahkan pihak Jenius maupun nasabah dalam mengecek proses pengaduan. Pengaduan yang telah diajukan akan selesai dalam waktu maksimal 5 hari kerja. Pengaduan secara lisan tidak jauh berbeda dengan pengaduan secara lisan. Perbedaannya terletak pada media yang digunakan dalam pengaduan serta jangka waktu proses pengaduan. Nasabah dapat mengirimkan pengaduan melalui Twitter @jeniushelp, *email* jenius-help@btpn.com, atau live chat di *website* www.jenius.com dan aplikasi Jenius. Jangka waktu yang dibutuhkan untuk memproses aduan nasabah adalah maksimal 20 hari kerja. Dalam kondisi tertentu, penyelesaian pengaduan dapat diperpanjang dalam jangka waktu maksimal 20 hari kerja. Pengaduan ini dapat dilakukan oleh nasabah Jenius sendiri maupun diwakilkan oleh pihak lain dengan surat kuasa khusus. Beberapa dokumen yang diperlukan pada saat melakukan pengaduan adalah kartu identitas nasabah, jenis dan tanggal transaksi yang ingin diadukan, permasalahan yang ingin diadukan, serta kartu identitas dan surat kuasa khusus jika pengaduan diwakilkan oleh pihak lain. Nasabah akan mendapatkan 3 tanda terima sebagai bukti nasabah telah mengajukan pengaduan, yaitu nomor registrasi pengaduan, tanggal penerimaan pengaduan, nomor telepon fungsi/layanan pengaduan yang gapat dihubungi oleh nasabah terkait.

Setelah melakukan pengaduan, nasabah nantinya akan mendapatkan tanggapan pengaduan yaitu diterima atau tidak diterima. Terdapat beberapa hal penyebab tidak diterimanya aduan nasabah, yaitu nasabah dan/atau perwakilan nasabah tidak melengkapi persyaratan dokumen sesuai jangka waktu yang telah ditetapkan, pengaduan sebelumnya telah diselesaikan Jenius sesuai dengan peraturan Otoritas Jasa Keuangan, pengaduan tidak terkait dengan kerugian dan/atau potensi kerugian materil, wajar, dan secara langsung sebagaimana tercantum dalam perjanjian dan/atau dokumen transaksi keuangan, serta pengaduan tidak terkait dengan transaksi keuangan yang dikeluarkan oleh Jenius. Jika nasabah terkait dan/atau perwakilan nasabah menolak tanggapan pengaduan dari Jenius, maka nasabah terkait dapat melakukan upaya penyelesaian sengketa melalui pengadilan atau di luar pengadilan.

Secara umum, setiap PUJK memiliki kewajiban untuk menjaga privasi tiap-tiap konsumennya dan bertanggung jawab atas setiap kerugian konsumennya akibat adanya tindakan kejahatan yang dilakukan oleh pihak yang mewakili kepentingan PUJK terkait ataupun kesalahan dalam pelaksanaan

usaha oleh PUJK terkait.[21] Tahap pertama yang harus dilakukan bank adalah dengan melakukan pemeriksaan atas dana nasabah yang hilang tersebut. Apabila benar-benar hilang, maka nasabah dapat mengajukan tuntutan pertanggungjawaban kepada pihak bank maupun kepada pihak ketiga. Konsumen yang mengalami kerugian dapat menggugat melalui lembaga yang bertugas menyelesaikan sengketa atau melalui peradilan yang berada di lingkungan peradilan umum. Sebagai upaya penyelesaian sengketa di luar pengadilan, pemerintah membentuk Badan Penyelesaian Sengketa Konsumen (BPSK).

Berdasarkan Pasal 52 Undang-Undang Perlindungan Konsumen, penyelesaian sengketa konsumen dapat dilakukan dengan melalui cara mediasi, arbritase atau konsiliasi. BPSK wajib mengeluarkan keputusan paling lambat dalam waktu 21 hari kerja setelah gugatan diajukan oleh korban. Apabila para pihak merasa keberatan dengan putusan BPSK, maka para pihak dapat mengajukan keberatan kepada Pengadilan Negeri paling lambat 14 hari kerja setelah pemberitahuan putusan tersebut. Secara lebih khusus pertanggungjawaban PUJK terhadap kerugian konsumen yang terjadi di sektor jasa keuangan diatur dalam Pasal 8 Ayat (1) POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Berdasarkan ketentuan tersebut, PUJK memiliki tanggung jawab atas kerugian nasabah atau konsumen dalam hal terdapat kesalahan/kelalaian/pelanggaran ketentuan perundang-undangan di sektor jasa keuangan oleh pihak PUJK, dimana hal ini memerlukan penelaahan dan pembuktian yang lebih lanjut. Lebih lanjut pertanggungjawaban bank atau PUJK dijelaskan dalam Pasal 8 Ayat (3) POJK Nomor 6/POJK.7/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Dalam hal ini apabila tidak ditemukan kesepakatan diantara para pihak, maka penyelesaian sengketa dapat dilanjutkan ke pengadilan atau apabila disepakati bersama dapat pula melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS Sektor Jasa Keuangan).[22]

Penyelenggaraan transaksi elektronk secara lebih rinci diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Undang-Undang ini berfungsi sebagai suatu pendekatan terhadap perkembangan telekomunikasi, teknologi informasi dan transaksi elektronik, tetapi yang paling penting adalah berfungsi dan bertujuan sebagai sarana tolok ukur yang dapat menjamin perlindungan hukum, kepastian hukum dan keadilan bagi para pihak, baik perseorangan, pengguna, masyarakat, lembaga-lembaga non pemerintah, pelaku bisnis, penyelenggara, instansi pemerintah dalam penyelenggaran informasi dan transaksi elektronik.[23]

Kegiatan bank didasari oleh kepercayaan dari nasabah untuk menyimpan simpanannya di bank. Sultan Remy Sjahdeini menerangkan bahwa hubungan antara bank dengan nasabah penyimpan dana adalah hubungan pinjam-meminjam uang antara debitur (bank) dan kreditur (nasabah penyimpan dana) yang dilandasi oleh asas kepercayaan, bukan hanya hubungan kontraktual biasa antara debitur dan kreditur, tetapi juga

[21] "Wawancara Dengan Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan"

[22] "Wawancara Dengan Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan."

[23] Abdul Halim Barkatullah, *Hukum Transaksi Elektronik Sebagai Panduan Dalam Menghadapi Era Digital Bisnis E-Commerce Di Indonesia* (Bandung: Nusa Media, 2020), hlm. 19.

hubungan kepercayaan yang diliputi asas kepercayaan.[24] Ketika nasabah telah mempercayakan simpanannya di bank, khususnya dalam perbankan digital, maka bank harus memaksimalkan segala upaya untuk tetap mempertahankan kepercayaan nasabah dengan memberikan pertanggungjawaban hukum kepada nasabah apabila terjadi kesalahan dalam sistemnya. Ketika membicarakan mengenai digital, maka otomatis kita berbicara mengenai sistem elektronik yang harus diperhatikan pengamanannya. Bank yang sudah memutuskan untuk beralih ke digital harus sudah menilai risiko dan juga harus siap terkait dengan pengamanan dalam sisi teknologi dan sumber daya yang mengolah teknologi tersebut. Khususnya data pribadi nasabah yang memiliki kaitan yang erat dengan penyalahgunaan pihak yang tidak berwenang dan dapat merugikan secara materil juga.[25]

Pertanggungjawaban yang diberikan oleh BTPN Jenius tentunya harus melalui tahap pemeriksaan/penyelidikan terlebih dahulu untuk melihat apakah kerugian yang dialami oleh nasabah merupakah kesalahan dari pihak bank, kesalahan dari pihak nasabah, atau kesalahan dari pihak ketiga. Peristiwa hilangnya simpanan nasabah di aplikasi Jenius ini merupakan akibat dari praktik penipuan rekayasa sosial atau lebih dikenal dengan *social engineering* yaitu *phising*. Kegiatan *phising* ini terjadi akibat kurangnya pengetahuan nasabah atas kegiatan *social engingeering* ini sehingga nasabah secara tidak sadar mengakses *link phising* yang diberikan oleh *phiser* dan memberikan informasi data pribadinya. Hal ini mengakibat *phiser* dapat mengakses akun Jenius nasabah dengan info yang telah didapatkan *phiser* melalui *link* yang diberikan kepada nasabah. Apabila informasi rahasia konsumen (seperti *user id, password,* PIN, kode OTP, dll) yang diperlukan untuk melakukan kejahatan dalam ITE diberikan oleh konsumen kepada fraudster, maka konsumen bertanggungjawab atas hal tersebut.[26]

Jenius telah mengatur mengenai keadaan kahar (*force majeure)* dalam syarat dan ketentuan dalam aplikasi Jenius, yaitu:[27]

1. Nasabah akan membebaskan bank dari segala tuntutan, jika bank tidak dapat melaksanakan instruksi dari nasabah, baik sebagian maupun sepenuhnya yang disebabkan oleh kejadian atau sebab yang berada di luar kendali atau kemampuan bank, meliputi tetapi tidak terbatas pada bencana alam, peperangan, kerusuhan, kondisi perangkat keras, kegagalan sistem infrastruktur elektronik atau transmisi, ganguan daya, gangguan telekomunikasi, kegagalan sistem kliring atau hal lainnya yang ditetapkan oleh Bank Indonesia atau lembaga berwenang lainnya.
2. Setelah kejadian yang menyebabkan bank tidak dapat melaksanakan instruksi dari nasabah berakhir, bank akan melanjutkan kembali instruksi tersebut dalam kurun waktu sesuai dengan ketentuan dari Bank Indonesia dan/atau Otoritas Jasa Keuangan.

[24] Andika Persada Putera, "Prinsip Kepercayaan Sebagai Fondasi Utama Kegiatan Perbankan", *Jurnal Hukum Bisnis Bonum Commune*, Vol. 3 No. 1, (2020): 136.

[25] "Wawancara Dengan Ajeng Risda Rahmadani, Subkor Edukasi Dan Promosi PDP Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi Dan Informatika."

[26] "Wawancara Dengan Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan."

[27] Jenius, *https://www.jenius.com/terms-and-conditions*, pada 8 Agustus 2022, pukul 13.27 WIB.

Dasar hukum *force majeure* sendiri telah diatur dalam KUH Perdata Pasal 1244 dan 1245 yang memberikan ketentuan bahwa pihak debitur tidak melakukan penggantian biaya kerugian atau bunga kepada pihak lainnya akibat terjadinya sesuatu hal yang tidak terduga, keadaan memaksa, dan karena perbuatan tersebut dilarang. Selain diatur dalam KUH Perdata, secara khusus keadaan *force majeure* dalam transaksi elektronik diatur dalam Pasal 15 Ayat (3) Undang-Undang Informasi dan Transaksi Elektronik bahwa pertanggungjawaban penyelenggara sistem elektronik tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik.

Keadaan Force majure yang telah ditetapkan oleh Bank BTPN Jenius ini menimbulkan pembatasan dalam pemberian tanggung jawab atau bahkan menghapus sama sekali tanggung jawab yang semestinya dipenuhi. Pertanggungjawaban dengan pembatasan ini dikenal dengan klausula eksonerasi, yaitu ketentuan dalam perjanjian baku yang berisi penambahan, pengurangan, pembatasan secara sepihak atas hak dan kewajiban salah satu pihak oleh pihak lain yang menetapkan isi, bentuk, serta cara penutupan perjanjian baku.[28]

Pertanggungjawaban Bank BTPN Jenius terhadap kerugian yang dialami nasabah adalah dengan membantu proses pengaduan nasabah dan melakukan pemeriksaan/penyelidikan sesuai dengan prosedur bank serta membantu nasabah dalam mencari solusi atas kerugian yang dialami oleh nasabah seperti membuat laporan kepada pihak kepolisian untuk ditangani lebih lanjut. BTPN Jenius juga bertanggungjawab atas pemeliharaan atau maintenance aplikasi Jenius guna menjaga keamanan dan kenyamanan nasabahnya kedepannya. Pertama, BTPN Jenius menonaktifkan akses Jenius melalui situs guna meminimalisir risiko terjadinya upaya rekayasa sosial (social engineering) oleh pelaku tindak kejahatan siber. Selain itu, BTPN juga telah menerapkan kebijakan satu perangkat yang terhubung untuk melindungi akun Jenius nasabah. Ini dilakukan agar pemilik akun Jenius hanya bisa mengakses dan bertransaksi menggunakan akunnya lewat satu perangkat saja yang telah terverifikasi. Kemudian, nasabah yang ingin mengalihkan akun Jenius miliknya ke perangkat lain hanya dapat melakukannya melalui Jenius Help 1500 365 atau Kantor Cabang Sinaya Bank BTPN.[29]

Jika membicarakan pertanggung-jawaban akibat pencantuman klausula eksonerasi, nasabah dapat meminta ganti rugi atas kerugian yang dialaminya. Tanggung jawab yang diberikan oleh bank kepada korban ini dapat dilaksanakan ketika perkara tersebut diproses oleh korban dalam sistem peradilan dan di luar peradilan. Sistem peradilan dapat dilakukan dalam hal konsumen telah mengalami kerugian sebagai akibat perjanjian baku yang mencantumkan klausula eksonerasi, maka untuk memitigasi kerugian yang telah dialaminya, konsumen dapat menggugat ganti rugi melalui badan peradilan. Selanjutnya sebagai alternatif selain melalui badan peradilan, konsumen yang telah dirugikan dapat memitigasi kerugian yang dialaminya dengan melalui badan penyelesaian sengketa konsumen sebagai badan non

[28] Johannes Gunawan, dkk., *Perjanjian Baku Masalah Dan Solusi* (Jakarta, 2021), hlm. 41.

[29] Kompas.com., "Jenius BTPN: Tidak Ada Kasus Nasabah Kehilangan Dana Karena Sistem Keamanan Bank," *https://Money.Kompas.Com/Read/2021/08/26/123152626/Jenius-Btpn-Tidak-Ada-Kasus-Nasabah-Kehilangan-Dana-Karena-Sistem-Keamanan?Page=all,* diakses pada 26 September 2022, pukul 11.05 WIB.

litigasi.[30] Lain hal dengan konsumen yang tidak ingin atau tidak mau berbelit-belit dalam urusan tersebut dan kebanyakan konsumen tidak mengerti semua akan hak-haknya, sehingga tidak melakukan atau mengajukan gugatan ke pengadilan, dan knsumen itu sendiri hanya diam dan menerima apapun yang menjadi pengalihan dari tanggung jawab pelaku usaha.[31]

Penutup

Berdasarkan Uraian tersebut dapat disimpulkan bahwa perlindungan hukum yang diberikan kepada nasabah adalah menerapkan prinsip kerahasiaan sebagaimana diatur dalam Undang-Undang Perbankan dengan memastikan keamanan sistem elektronik yang digunakan dalam perbankan digital. Jenius sebagai salah satu perbankan digital yang telah berjalan dibawah pengawasan Otoritas Jasa Keuangan dan dijamin oleh Lembaga Penjamin Simpananan dapat memastikan bahwa aplikasinya memiliki keamanan berlapis dengan menggunakan teknologi keamanan dan enkripsi data terkini yang berstandar internasional serta menerapkan isolasi dan proteksi data berlapis. Kegiatan phising juga telah diatur dan diancam dalam Undang-Undang Informasi dan Transaksi

Adapun tanggung jawab yang dilakukan oleh BTPN adalah dengan pertanggungjawaban terbatas yaitu dengan menyadiakan layanan pengaduan nasabah secara lisan maupun tertulis. Kasus phising yang dialami oleh beberapa nasabah Jenius ini terjadi akibat kelalaian nasabah yang tidak berhati-hati dalam mengakses link phising yang diberikan oleh phiser, sehingga BTPN tidak memberikan pertanggungjawaban berupa ganti rugi. Selain itu BTPN juga melakukan beberapa tanggung jawab dalam pemeliharaan aplikasi Jenius yaitu dengan menonaktifkan akses Jenius melalui situs guna meminimalisir risiko terjadinya upaya social engineering oleh pelaku tindak kejahatan siber. Jenius juga telah menerapkan kebijakan satu perangkat yang terhubung untuk melindungi akun nasabah. Ini dilakukan agar pemilik akun Jenius hanya bisa mengakses dan bertransaksi menggunakan akunnya lewat satu perangkat saja yang telah terverifikasi. Akses unlink device melalui aplikasi atau situs juga telah ditutup dan mengalihkannya ke Jenius Help 1500365 atau kantor cabang BTPN.

Bagi pihak bank diharapkan untuk meningkatkan sistem keamanan dalam aplikasi perbankan digital serta melakukan pemblokiran situs-situs ilegal yang meniru situs resmi untuk mencegah terjadinya peningkatan kasus pembobolan melalui perbankan digital yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Selain itu bank diharapkan untuk lebih giat lagi dalam memberikan sosialiasi kepada nasabah baik mengenai keamanan data pribadi maupun produk-produk resmi bank. Selain itu, bagi pihak nasabah diharapkan dapat lebih berhati-hati dalam mengakses segala hal yang berkaitan dengan transaksi elektronik serta menambah wawasan mengenai keamanan data pribadi dan informasi mengenai bank yang digunakan.

Daftar Pustaka

Abdul Halim Barkatullah. *Hukum Transaksi Elektronik Sebagai Panduan Dalam Menghadapi Era Digital Bisnis E-Commerce Di Indonesia*. Bandung: Nusa Media, 2020.

Ali, Zainuddin. *Metode Penelitian Hukum*.

[30] Johannes Gunawan, Op.Cit, hlm. 65.

[31] Jein Stevany Manumpil, "Klausula Eksonerasi Dalam Hukum Perlindungan Konsumen Di Indonesia", Lex Privatum, Vol. IV, No.3, 2016, hlm.39.

Jakarta: Sinar Grafika, 2009.

Amin Muftiadi. "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phisingterhadap Layanan Online Banking." *Hexatech: Jurnal Ilmiah Teknik* 1, no. 2 (2022): 60–65.

Andika Persada Putera. "Prinsip Kepercayaan Sebagai Fondasi Utama Kegiatan Perbankan." Surabaya, 2020.

Ayu Andreana Beru Tarigan, Herdian, and Darminto Hartono Paulus. "Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital," 2019.

David Y. Wonok. "Perlindungan Hukum Atas Hak-Hak Nasabah Sebagai Konsumen Pengguna Jasa Bank Terhadap Risiko Yang Timbul Dalam Penyimpangan Dana," 2012.

Jein Stevany Manumpil. "Klausula Eksonerasi Dalam Hukum Perlindungan Konsumen Di Indonesia," 2016.

Jenius. "No Title," n.d.

Johannes Gunawan, dkk. *Perjanjian Baku Masalah Dan Solusi*. Jakarta, 2021.

Kompas.com. "Jenius BTPN: Tidak Ada Kasus Nasabah Kehilangan Dana Karena Sistem Keamanan Bank." https://money.kompas.com/read/2021/08/26/123152626/jenius-btpn-tidak-ada-kasus-nasabah-kehilangan-dana-karena-sistem-keamanan?page=all, n.d.

Latifahi, Fitri Nur, Imron Mawardi, and Bayu Wardhana. "Ancaman Pencurian Data (Phising) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19 (Study Phising Di Indonesia)." *Study Phishing Di Indonesia) 74 Perisai* 6, no. 1 (2022): 73–85. https://doi.org/10.21070/perisai.

Mahesa Jati Kusuma. *Hukum Perlindungan Nasabah Bank, Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE Di Bidang Perbankan*. Bandung: Nusa Media, 2019.

Marnia Rani. "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank." Vol. 2, 2014.

Otoritas Jasa Keuangan. "Panduan Penyelenggaraan Digital Branch Oleh Bank Umum." https://www.ojk.go.id/id/kanal/perbankan/Pages/Panduan-Penyelenggaraan-Digital-Branch-oleh-Bank-Umum.aspx., December 2016.

Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum (n.d.).

Radiansyah, Ikhsan, and Yudi Priyadi. "Analisis Ancaman Phising Dalam Layanan Online Banking." *Bulan Januari Tahun* 7, no. 1 (2016): 1–14.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (March 2021): 38–52. https://doi.org/10.47268/sasi.v27i1.394.

Trisadini P. Usanti, and Shomad. *Hukum Perbankan*. Jakarta: Kencana, 2017.

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 (n.d.).

"Wawancara Dengan Ajeng Risda Rahmadani, Subkor Edukasi Dan Promosi PDP Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi Dan Informatika." n.d.

"Wawancara Dengan Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan." n.d.

"Wawancara Dengan Direktorat Pengembangan Pengawasan Bank, Otoritas Jasa Keuangan." n.d.

"Wawancara Dengan Haryono K.P, Service Point Jenius." n.d.

Yuniarti, Siti. "Perlindungan Hukum Data Pribadi Di Indonesia." *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 1, no. 1 (2019): 147–54. https://doi.org/10.21512/becossjournal.v1i1.6030.