Hakim: Jurnal Ilmu Hukum dan Sosial
Vol.2, No.1 Februari 2024
e-ISSN: 2987-7539; p-ISSN: 2987-6737, Hal 01-16
DOI: https://doi.org/10.51903/hakim.v2i1.1535

Perlindungan Hukum Terhadap Nasabah atas Kejahatan *Phising* dan *Hacking* pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia

Salsabila Chairunnisa
Fakultas Hukum, Universitas Padjadjaran
Email: salsabila19015@mail.unpad.ac.id

Tarsisius Murwadji
Fakultas Hukum, Universitas Padjadjaran
Email: t.murwadji@unpad.ac.id

Nun Harrieti
Fakultas Hukum, Universitas Padjadjaran
Email: nun.harrieti@unpad.ac.id

Abstract*. Phishing and hacking crimes are cybercrimes that often occur in banking. Therefore, the purpose of this research is to examine the responsibility of digital banks and legal protection for phishing and hacking crimes of customers in digital bank services. Researchers have concluded that the responsibility of digital banks for phishing and hacking crimes to customers in using digital banks service is reviewed based on Indonesia's Positive Law. Digital banks are responsible in this case for confirming phishing and hacking crimes, making customer complaint handling services accessible to customers in 24 hours. Banks compensate for losses suffered by customers to always maintain the principle of customer trust in them. However, if the customer is unsatisfied with the internal settlement with the digital bank, then the customer is not followed up by the bank concerned. The customer's legal protection for phishing and hacking crimes is reviewed based on Indonesian Positive Law. The government as a regulator provides legal protection to customers in order to achieve order and legal certainty.*

Keywords*: Legal Protection, Consumer, Digital Banking Services, Phishing, Hacking.*

Abstrak. Kejahatan phising dan *hacking* merupakan kejahatan siber yang sering terjadi pada perbankan. Oleh karena itu, tujuan dari penelitian ini menemukan bentuk pertanggungjawaban bank digital dan perlindungan hukum atas kejahatan phising dan hacking terhadap nasabah pada layanan bank digital. Penelitian ini menggunakan metode pendekatan yuridis normatif. Penulis melakukan penelitian secara studi kepustakaan data sekunder berupa bahan hukum primer, sekunder, dan tersier, dan studi lapangan yang berkorelasi dengan objek penelitian ini. Penelitian ini menyimpulkan bahwa pertanggungjawaban bank digital atas kejahatan phising dan hacking kepada nasabah dalam penggunaan layanan bank digital ditinjau berdasarkan Hukum Positif Indonesia, bank digital bertanggungjawab dalam hal ini melakukan konfirmasi terhadap kejahatan phising dan hacking, membuat layanan pengaduan nasabah yang dapat diakses nasabah dalam 24 jam sehari. Bank mengganti kerugian yang dialami oleh nasabah untuk selalu mempertahankan kepercayaan nasabah terhadap bank. Akan tetapi, apabila nasabah kurang puas dengan penyelesaian internal dengan bank digital, maka nasabah dapat menyelesaikan sengketa melalui LAPS apabila komplain yang diajukan tidak ada tindak lanjut dari bank digital. Perlindungan hukum nasabah atas kejahatan phising dan hacking ditinjau berdasarkan Hukum Positif Indonesia sudah cukup memadai. Pemerintah sebagai regulator memberikan perlindungan hukum kepada nasabah agar dapat mencapai ketertiban dan kepastian hukum.

Kata kunci: Hacking, Layanan Bank Digital, Nasabah, Perlindungan Hukum, Phishing.

Received Oktober 30, 2023; Revised November 22, 2023; Accepted Desember 01, 2023
*Salsabila Chairunnisa, salsabila19015@mail.unpad.ac.id

LATAR BELAKANG

Perkembangan teknologi informasi sangat berkembang pesat dan kita dihadapkan pada era revolusi industri 4.0 yang memiliki ciri, yaitu munculnya inovasi – inovasi baru. Adanya perkembangan terhadap teknologi informasi sangat berpengaruh terhadap industri ekonomi khususnya perbankan (Radiansyah et al., 2016). Terdapat beberapa aspek yang mendorong perubahan pandangan terhadap perbankan seiring dengan era revolusi industri ini, diantaranya nasabah sebagai konsumen memiliki harapan lebih terhadap perubahan produk dan layanan perbankan yang mudah dan aman, tidak ketinggalan zaman, dan memberikan kemudahan bagi para nasabah, dan juga perspektif terhadap perubahan model perbankan, dari model operasional, menuju model bisnis digital, yang dirasa akan efektif dan efisien dalam bertransaksi (Jati, 2019).

Industri perbankan menghadirkan inovasi baru berupa bank digital untuk memberikan pelayanan yang terbaik kepada nasabah. Bank digital merupakan inovasi dari bank umum untuk menghadapi perkembangan teknologi informasi dan masyarakat yang sudah mulai memasuki era digital (Tasman & Ulfanora, 2023). Landasan hukum beroperasinya bank digital adalah Undang – Undang Nomor 7 Tahun 1992 sebagaimana diubah oleh Undang – Undang Nomor 10 Tahun 1998 tentang Perbankan sebagaimana diubah oleh Undang – Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Jasa Keuangan.

Bank digital harus memastikan model bisnis yang digunakan tidak merugikan nasabah. Data nasabah terjamin kerahasiaan dan keamanan datanya yang sangat penting dalam dunia perbankan (Munir, 2017). Sebagaimana diatur dalam Pasal 23 ayat (1) dan Pasal 24 ayat (1) poin a dan e Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank **Umum ("POJK Bank Umum")** Keuntungan dapat dirasakan nasabah, ketika nasabah telah meletakkan kepercayaannya kepada bank.

Diatur lebih lanjut dalam Peraturan Otoritas Jasa Keuangan Nomor 06/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan mengenai ketentuan Pelaku Usaha Jasa Keuangan ("PUJK") dalam hal ini bank digital, untuk menggunakan teknologi informasi yang aman dan andal dan menjamin keamanan dan/atau informasi nasabah.

Keuntungan dapat dirasakan oleh kedua belah pihak. Bagi nasabah tanpa disadari dengan adanya bank digital memudahkan para nasabah untuk bertransaksi dalam kegiatan perbankan. Seiring berkembangnya teknologi, terdapat perkembangan dalam layanan perbankan secara digital, dimana layanan bank digital, dapat dimungkinkan calon nasabah dan/atau nasabah bank dapat melakukan transaksi seperti, pembukaan rekening, menabung.

Meletakkan dana deposito, pengelolaan keuangan, kredit/pinjaman, pembayaran transaksi *e-commerce*, dan masih banyak lagi.

Pemanfaatan teknologi yang semakin canggih ini bukan tanpa kekurangan. Akan sangat riskan terhadap kejahatan – kejahatan siber yang timbul. Kejahatan siber tersebut dapat berupa *phising* dan *hacking*. *Phishing* dan *hacking* merupakan kejahatan siber yang saling berkaitan. *Phishing* merupakan kejahatan dimana pelaku melakukan penyebaran tautan melalui media sosial atau dapat melakukan kejahatan melalui saluran telepon, dengan meminta nasabah bank digital untuk memberikan kode rahasia *On Time Password* (OTP). Sedangkan *hacking* apabila diterjemahkan ke dalam Bahasa Indonesia berarti peretasan.

Mengutip pendapat Tarsisius Murwadji, mutu hukum adalah kesesuaian apa yang semestinya *"das Sollen"* dan apa yang terlihat dalam kenyataan *"das Sein"*. Das Sollen diartikan sebagai regulasi atau peraturan perundang – perundangan, sedangkan das Sein merupakan standarisasi mutu hukum. (Murwadji, 2017). Kejahatan *phising* dan *hacking* yang terjadi pada bank digital menunjukkan bahwa adanya kesenjangan antara *das Sein* dengan *das Sollen*. Perbuatan melawan hukum, seperti *hacking* sebagai salah satu bentuk kejahatan siber telah melanggar peraturan perundang – undangan, diantaranya Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah oleh Undang – Undang Nomor 19 Tahun 2016 tentan Informasi dan Transaksi Elektronik ("UU ITE"), Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, dan juga peraturan terkait pada Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan. Tidak menutup kemungkinan banyak kejahatan – kejahatan siber lainnya yang masuk ke dunia bank digital, seperti kejahatan *phising* dan *hacking*.

Kejahatan dalam dunia siber bersifat *borderless*. Dengan adanya kejahatan *phising* dan *hacking* sebagai salah satu kejahatan siber dapat mengganggu pertumbuhan perbankan. Diperlukan pengaturan yang sangat kuat agar kedepannya tidak terjadi kejahatan – kejahatan dalam kegiatan siber dan bank digital (Mansur & Gultom, 2005).

KAJIAN TEORITIS

Teori yang digunakan Penulis dalam penelitian ini adalah teori hukum Pembangunan yang dipaparkan oleh Mochtar Kusumaatmadja. Mochtar menyatakan bahwa definisi hukum merupakan keseluruhan asas – asas dan kaidah – kaidah yang mengatur kehidupan manusia dalam masyarakat, meliputi Lembaga – Lembaga dan proses – proses yang mewujudkan berlaku kaidah tersebut dalam kenyataan. Dalam definisi hukum tersebut, sudah terkandung

fungsi dan tujuan hukum itu sendiri. Teori Mochtar Kusumaatmadja (2016), memodifikasi teori Roscoe Pound. Mochtar menyatakan bahwa hukum diciptakan sebagai sarana untuk membangun masyarakat kepada ketertiban dan keteraturan seperti yang diharapkan oleh Pembangunan dan pembaharuan tersebut. Mochtar menyatakan bahwa hukum pula merupakan suatu alat untuk memelihara ketertiban masyarakat. Selaras pula dengan penelitian yang Penulis lakukan, dengan adanya hukum, nasabah akan merasakan keteraturan terhadap transaksi perbankan yang dilakukan nasabah. Dengan adanya hukum pula, diharapkan nasabah akan menjadi tertib ketika nantinya terjadi suatu hal yang tidak diinginkan.

METODE PENELITIAN

Metode penelitian yang digunakan penulis dilakukan dengan menggunakan pendekatan yuridis normatif. Pendekatan yuridis normatif meneliti dengan cara melakukan penelitian pada data sekunder. Merujuk pula kepada konsep yang tertuang dalam peraturan perundang – undangan (Amiruddin dan Zainal Asikin, 2017). Berdasarkan metode tersebut, penulis melakukan penelitian terhadap data sekunder yang berhubungan dengan perlindungan hukum terhadap nasabah atas kejahatan *phising* dan *hacking* pada layanan bank digital.

Penulis melakukan penulisan tugas akhir dengan pendekatan yuridis normatif yang berupa pendekatan terhadap konsep, teori, dan peraturan perundang – undangan yang berkorelasi dengan penelitian Penulis (Ali,2009). Penelitian ini, penulis menggunakan metode penelitian secara deskriptif analitis. Menganalisis data yang telah diperoleh pada praktik di lapangan dengan mengaitkan suatu peraturan perundang – undangan dan teori – teori hukum yang berkaitan. Kemudian, diolah secara kualitatif, dengan cara menganalisis aturan – aturan yang terkait sebagai hukum positif secara kualitatif dan tidak menggunakan rumus atau statistika.

HASIL DAN PEMBAHASAN

Pertanggungjawaban bank terhadap nasabah atas kejahatan *phising* dan *hacking* ditinjau berdasarkan hukum positif Indonesia

Bank digital sebagai pihak penyelenggara sistem elektronik, terdapat kewajiban – kewajiban yang harus dipatuhi dan dipenuhi. Mengacu kepada Pasal 15 UU ITE, mengatur sebagai berikut:

" (1) Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem secara **andal** dan **aman** serta **bertanggungjawab** terhadap beroperasinya sistem elektronik sebagaimana mestinya;

(2) penyelenggara sistem elektronik bertanggungjawab terhadap pengguna sistem elektronik; (3) Ketentuan pada ayat (2) tidak berlaku apabila dapat dibuktikan adanya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik."

Andal berarti memiliki kemampuan yang sesuai dengan kebutuhan nasabah. Nasabah berharap akan mendapat kemudahan – kemudahan dan keuntungan atas dananya.

Aman berarti Nasabah dapat merasa aman ketika meletakkan dananya pada bank digital. Sistem elektronik harus aman, yaitu terlindungi secara fisik dan nonfisik. Sistem elektronik yang diselenggarakan memiliki kemampuan sesuai dengan spesifikasinya. Seperti tidak mudah dicuri dan/atau dibobol, secara fisik. Secara non fisik, harus disediakan sistem keamanan yang memberikan jaminan kepada nasabah, sehingga tidak adanya kekhawatiran pada nasabah, karena seluruh informasi pribadi serta dana simpanannya telah dipercayakan kepada bank digital.

Bank digital sebagai subjek hukum wajib bertanggungjawab terhadap penyelenggaraan sistem elektronik yang dipergunakan untuk memberikan layanan. Tanggung jawab ini dilakukan dengan penyediaan sistem yang handal dengan keamanan tingkat tinggi. Bank digital telah menyiapkan mekanisme *business continuity plans* seperti penyediaan lokasi *server backup* yang ditempatkan lokasi yang berbeda.

Pengaturan pada Pasal 2 dan Pasal 21 POJK Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi ("POJK Penyelenggaraan Teknologi Informasi") bentuk tanggungjawab yang dapat dilakukan bank digital adalah **wajib** menerapkan tata Kelola teknologi informasi yang baik serta menjaga sistem dari ketahanan siber. Bank yang melanggar aturan tersebut, akan mendapat sanksi administratif berupa teguran tertulis, bank digital tidak diperbolehkan untuk meluncurkan produk baru, pembekuan pada kegiatan usaha tertentu, hingga penurunan nilai faktor tata Kelola yang berpengaruh pada tingkat kesehatan bank. Dalam artian, bank digital bertanggungjawab untuk membuat layanan bank digital sedemikian rupa aman, andal, dan bertanggung jawab sebagai bentuk upaya preventif kejahatan *phising* dan *hacking*.

Bentuk pertanggungjawaban lainnya, sesuai dengan ketentuan Pasal 6 POJK Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan, bank digital sebagai pelaku usaha jasa keuangan **wajib** mempunyai dan menerapkan kebijakan serta prosedur terkait perlindungan konsumen untuk nasabah yang terkena masalah akibat layanan yang dibuat oleh bank digital. Dalam Pasal 21 ayat (1) POJK Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, bank digital wajib menerapkan prinsip perlindungan konsumen sebagaimana diatur dalam POJK Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan. Pasal 21

ayat (2) mengatur pola, tanggungjawab bank digital untuk menangani setiap pertanyaan dan/atau pengaduan dari nasabah selama 24 (dua puluh empat) jam sehari.

Bank digital saat ini sudah banyak yang menerapkan kebijakan hingga prosedur dengan mencantumkan tata cara pengaduan nasabah apabila dikemudian hari nasabah mengalami masalah dalam penggunaan layanan bank digital. Bank digital membuka jalan melalui pengaduan tertulis dan lisan. Nasabah dapat mengunjungi kantor fisik terbatas nasabah untuk pengaduan secara lisan. Sedangkan, secara tertulis dapat melaporkan melalui *website*, *e – mail* hingga media sosial bank digital resmi. Kemudian, pengaduan tersebut akan diproses sesuai dengan ketentuan yang berlaku pada masing – masing bank digital.

Pengaduan nasabah yang telah masuk kepada bank digital terbaik akan dikonfirmasi kepada nasabah. Kemudian, dilakukan pemeriksaan dan penyelidikan terkait sebab adanya kerugian tersebut. Apakah penyebab *phising* dan *hacking* hingga hilangnya dana pada layanan bank digital disebabkan oleh sistem keamanan bank atau terdapat unsur kesalahan dari nasabah yang memberikan informasi pribadi kepada *phisher* dan *hacker*.

Bentuk pertanggungjawaban terhadap *phising* dan *hacking* terdapat perbedaan. Kejahatan *phishing* merupakan kejahatan dengan merupakan kejahatan diawali dengan memancing nasabah untuk dapat mengakses tautan apabila *phishing* dilakukan melalui aplikasi atau memancing nasabah untuk memberikan data pribadi ketika *phishing* datang melalui saluran telepon. Dalam hal ini, terdapat unsur kelalaian nasabah. Sebagaimana diatur dalam Pasal 8 ayat (2) POJK Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan, apabila bank digital sebagai PUJK dalam pembuktiannya mampu membuktikan bahwa kesalahan, kelalaian, dan/atau perbuatan yang bertentangan dengan peraturan perundang – undangan datang dari nasabah itu sendiri, maka bank tidak dapat bertanggungjawab.

Bank sebagai *agent of trust*, bank menganut asas kepercayaan dalam kegiatan usahanya. Nasabah yang kehilangan dananya dapat berasumsi bahwa tidak adanya keseriusan bank digital dalam penanganan kasus yang menimpa nasabah. Bank digital yang ingin tetap mempertahankan kepercayaan nasabah, maka dapat melakukan kesepakatan terkait tindak lanjut kerugian nasabah, diantaranya dengan melakukan pemantauan atas dana yang diambil atau dapat mengembalikan dananya sesuai kesepakatan berdasarkan ketentuan yang berlaku pada masing – masing bank digital.

Bentuk pertanggungjawaban pada kejahatan *hacking.* Merujuk kepada definisi *hacking*, merupakan pembobolan sistem elektronik yang digunakan. Pembobolan sistem ini dilakukan oleh *hacker* dengan teknologi yang dimilikinya tidak ada unsur kesalahan nasabah. Kejahatan *hacking* merupakan kejahatan yang tidak dapat dihindari. Nasabah terkena serangan siber

berupa *hacking*, maka bentuk pertanggungjawaban bank akan berbeda dengan nasabah terkena serangan *phishing* akibat kelalaian nasabah.

Berdasarkan Pasal 8 ayat (1) dan Pasal 11 ayat (5) POJK Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan, bank digital perlu melakukan pengecekan kelayakan dan/atau keamanan secara berkala ketika menggunakan teknologi informasi untuk mengelola data dan/atau informasi nasabah, untuk menjaga keamanan data nasabah. Bank wajib bertanggung jawab dari adanya kejahatan *hacking*. Bank digital lalai dalam menjaga keamanan layanan yang diluncurkannya tersebut. Bank digital wajib mengganti seluruh kerugian nasabah akibat serangan siber berupa *hacking* kepada nasabah.

Pertanggungjawaban bank yang dapat diberikan kepada nasabah tidak hanya berupa pertanggungjawaban secara materiil, tetapi bank berdasarkan POJK Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan, bank digital dapat bertanggung jawab atas edukasi keuangan kepada nasabah. Pasal 3 ayat (1) dan Pasal 10 ayat (1) POJK Nomor 3 Tahun 2023 tentang Peningkatan Literasi dan Inklusi Keuangan, memberikan kewajiban kepada bank digital sebagai salah satu bagian dari PUJK untuk melakukan literasi keuangan dan termasuk ke dalam program tahunan yang bertujuan meningkatkan literasi nasabah terkait produk atau layanan bank yang terkait. Bentuk edukasi keuangan yang dapat dilakukan berupa sosialisasi dengan bekerjasama dengan instansi pemerintah, instansi akademik, *Non Governmental Organization ("NGO")* terkait atau pihak lain yang memiliki kepentingan yang sama.

Perlindungan hukum terhadap nasabah atas kejahatan *phising* dan *hacking* pada layanan bank digital ditinjau berdasarkan Hukum Positif Indonesia

Nasabah sebagai warga negara berhak mendapat kepastian dan kedudukan yang sama di mata hukum. Sebagaimana tercantum dalam Pasal 28D ayat (1) UUD 1945 yang menyatakan bahwa setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil dan perlakuan yang sama dihadapan hukum.

Mochtar Kusumaatmadja menyampaikan pendapatnya bahwasanya hukum sudah sepatutnya melindungi masyarakat untuk mencapai ketertiban dan kepastian hukum. Mengacu kepada Penelitian ini, hukum dapat mengatur mengenai kejahatan *phising* dan *hacking* dari berbagai aspek, maka dapat dipastikan bahwa aturan hukum tersebut memiliki maksud untuk mencapai ketertiban dan kepastian hukum. Dalam hal ini, nasabah berhak untuk mendapat perlindungan hukum.

Pelaku kejahatan *phising* dan *hacking* dapat diberi sanksi pidana, sanksi terhadap bank digital yang lalai dalam pemanfaatan sistem elektronik dan perlindungan data nasabah. Dengan adanya hukum yang berjalan sebagaimana mestinya, nasabah akan merasa terlindungi oleh

hukum dan bank digital akan sepatutnya bertanggung jawab atas kejahatan *phising* dan *hacking* tersebut akan terpenuhinya asas kepercayaan yang dimana bank pula menjadi *agent of trust*.

Perlindungan hukum kepada nasabah sudah selayaknya diberikan atas adanya kejahatan *phising* dan *hacking* karena sangat merugikan nasabah. Kejahatan tersebut dapat berakibat tersebarnya informasi pribadi nasabah yang kemudian bisa saja disalahgunakan oleh pelaku. Penyalahgunaan tersebut dapat menyebabkan tidak dapat diaksesnya layanan bank digital nasabah hingga kondisi fatalnya dana nasabah dapat hilang karena kejahatan tersebut.

Peraturan perundang – undangan perlu mengakomodir kejahatan – kejahatan siber pada aturan hukum saat ini dikarenakan kejahatan *phising* dan *hacking* sangat menyebar dan merajalela pada saat ini dan diperkirakan akan terus dikembangkan pada tahun yang akan datang sejalan dengan perkembangan teknologi.

Menurut Mochtar Kusumaatmadja, hukum memiliki fungsi dan tujuan untuk mencapai ketertiban dan kepastian hukum. Peraturan yang ada diharapkan dapat menciptakan rasa aman bagi nasabah dalam penggunaan layanan bank digital dan menjamin ketertiban pengelolaan bank digital sehingga bank digital di kemudian hari dapat menciptakan produk – produk yang aman, andal, dan bertanggungjawab. Nasabah yang sudah ragu atau bahkan tidak percaya kepada bank digital akibat adanya kejahatan *phising* dan *hacking* yang menimpanya, maka dikhawatirkan akan menimbulkan penarikan dana secara besar – besaran *(rush)* dan berdampak kepada ekonomi Indonesia. Sri Mulyani, Menteri Keuangan Indonesia menyatakan bahwa penarikan dana besar – besaran tersebut berakibat rusaknya perekonomian Indonesia (Ariyani, 2016).

Mochtar juga memberikan pendapat bahwa tujuan hukum pada akhirnya untuk menciptakan kepastian hukum. Sebagai subjek hukum, nasabah perlu mendapatkan kepastian hukum, apabila kejahatan *phising* dan *hacking* menimpa nasabah. Nasabah memiliki hak atas dananya, dana tersebut merupakan hak dari nasabah ketika melakukan transaksi pada layanan bank digital. Nasabah berharap agar tidak terjadi kejahatan serupa yang menimpanya dikemudian hari.

Kejahatan – kejahatan siber pada dasarnya merupakan kejahatan konvensional. Hanya saja dalam pelaksanaannya kejahatan siber seperti *phising* dan *hacking* menggunakan teknologi internet. Maksud dan tujuan *phishing* untuk mendapatkan data diri nasabah, agar nantinya bisa dilanjutkan oleh para pelaku *hacking* untuk menerobos sistem elektronik yang digunakan nasabah dengan tujuan mengambil keuntungan dari nasabah secara ilegal (Chotimah, 2019).Kejahatan konvensional yang dapat di padu dengan *phishing* dan *hacking* merupakan kejahatan penipuan dan penerobosan secara ilegal. Hal mengenai tindak pidana penipuan diatur

dalam Pasal 378 Kitab Undang – Undang Hukum Pidana ("KUHP"). Unsur dalam penipuan ingin menguntungkan diri sendiri, dapat dilihat dari pelaku yang melakukan tindakan *phising* dan *hacking* bertujuan untuk meraup keuntungan secara melawan hukum menggunakan identitas suatu instansi bank digital agar dapat dipercaya oleh nasabah untuk secara cuma – cuma memberikan data pribadi yang tidak boleh disebarluaskan seperti, nomor kartu, PIN, OTP, dan CVV.

UU Pengembangan dan Penguatan Sektor Jasa Keuangan mengatur perlindungan hukum pada nasabah. Ketentuan mengenai perlindungan hukum menjelaskan mengenai rahasia bank yang tercantum pada Pasal 40 ayat (1), bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Aturan ini menyatakan bahwa bank digital wajib menjaga data dan dana milik nasabah. Bank digital sebagaimana pada Pasal 40A untuk memberikan informasi nasabah untuk keperluan peradilan dalam perkara perdata, penyelesaian piutang bank, permintaan, persetujuan, atau kuasa nasabah. Rahasia bank dapat dikecualikan apabila diperlukan untuk mengetahui kondisi keuangan seseorang sebagai nasabah pada suatu bank yang nantinya akan diserahkan kepada pejabat pajak, makna Otoritas Jasa Keuangan berhak mengeluarkan perintah tertulis kepada bank. Bank diperkenankan untuk membuka rahasia bank serta memberikan dan memperlihatkan keterangan terkait keadaan keuangan nasabah.

Sanksi yang dapat diterapkan apabila bank digital tidak mengindahkan aturan tersebut, berdasarkan Pasal 47 dan 47 A UU Pengembangan dan Penguatan Sektor Jasa Keuangan, dimana yang mengungkapkan rahasia bank tersebut tanpa alasan, sebagai berikut :

Badan hukum atau seseorang yang tidak mengantongi izin atau perintah secara tertulis dari Otoritas Jasa Keuangan atau tanpa kewenangan sebagaimana dimaksud dalam undang – undang ini hingga adanya pemaksaan kepada pihak bank digital atau pihak yang terafiliasi dengan bank digital untuk membuka mengenai rahasia bank, maka dapat dikenakan sanksi pidana. Sanksi pidana sekurang – kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta sanksi material berupa denda sekurang – kurangnya Rp 10.000.000.000 (sepuluh miliar rupiah) dan paling banyak Rp 200.000.000.000 (dua ratus miliar rupiah).

Anggota dewan komisaris, direksi, pegawai bank, dan pihak yang terafiliasi dengan bank digital merupakan pihak yang turut wajib menjaga kerahasiaan bank. Apabila diketahui pihak – pihak tersebut melanggar ketentuan mengenai rahasia bank dengan sengaja, maka dikenakan sanksi pidana sekurang – kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta denda sekurang – kurangnya Rp 4.000.000.000 (empat miliar rupiah) dan sebanyak – banyaknya sebanyaknya Rp 8.000.000.000 (delapan miliar rupiah).

UU ITE mengatur pula mengenai perlindungan hukum bagi nasabah terhadap kejahatan *phising* dan *hacking*, UU ITE dapat menjerat pelaku kejahatan *phising* dan *hacking*. Kepastian hukum dapat ditemukan oleh nasabah dalam UU ITE apabila ditemukan permasalahan antara nasabah dengan bank digital terkait dengan layanan bank digital. Kejahatan *phising* dan *hacking* mengawali kejahatannya dengan mengirimkan tautan atau berpura – pura menjadi bank digital yang bersangkutan.

Akses yang dimiliki *phisher* dan *hacker* merupakan akses ilegal untuk dapat masuk ke dalam sistem bank untuk memperoleh data diri nasabah sebagai bentuk informasi elektronik yang tersimpan pada perangkat elektronik nasabah. Pelaku yang dapat menjangkau sistem elektronik nasabah berupa layanan bank digital yang digunakan merupakan suatu bentuk kejahatan *phising* dan *hacking*. Unsur – unsur tersebut memenuhi pasal 30 UU ITE. Sebagai nasabah, perlu mendapatkan perlindungan secara hukum dari adanya tindak kejahatan tersebut. Bentuk perlindungan hukum terdapat dalam Pasal 46 ayat 1 – 3, dimana penyalahgunaan dapat dikenai sanksi maupun denda. Pengaturan pada Pasal 46 ayat (1) hingga ayat (3) menyatakan bahwa setiap orang yang memenuhi unsur sebagaimana dimaksud pada Pasal 30 ayat (1) hingga ayat (3), maka pelaku telah terbukti memenuhi unsur tersebut dapat dipidana dengan penjara berupa penjara paling lama 6 (enam) tahun hingga paling lama 8 (delapan) tahun dan/atau dapat dikenakan denda sebesar paling banyak Rp 600.000.000 (enam ratus juta rupiah) hingga Rp 800.000.000 (delapan ratus juta rupiah).

Kejahatan *phising* dan *hacking* pada pelaksanaannya, pelaku menyebarkan tautan melalui *e – mail*, aplikasi perpesanan seperti *whatsapp imessenger*, dapat pula melalui saluran telepon yang seolah pelaku tersebut merupakan bank digital resmi. Nasabah yang terkecoh dan mengakses tautan tersebut akan mengakibatkan pelaku dapat melakukan penyadapan terhadap informasi elektronik secara tanpa hak. Pengaturan atas tindakan tersebut diatur dalam Pasal 31 jo. Pasal 47 UU ITE dimana pelaku dapat dijerat dengan sanksi pidana hingga 10 tahun dan/atau sanksi denda hingga Rp 800.000.000 (delapan ratus juta rupiah).

Phisher yang telah melakukan penyadapan terhadap sistem elektronik nasabah, maka *phisher* dapat mengakses sistem elektronik milik nasabah dan mengetahui data – data sensitif nasabah dengan cara melawan hukum. Tindakan tersebut dapat dikelompokkan dalam kegiatan melawan hukum, yaitu melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. UU ITE mengatur tindakan tersebut sebagai kegiatan akses ilegal terhadap sistem elektronik milik orang lain diatur pada Pasal 32. Apabila pelaku memenuhi unsur – unsur tindak pidana pada Pasal 32 UU ITE, maka sanksi yang dapat dikenakan pada pelaku adalah sanksi pidana

penjara paling lama 8 (delapan) tahun dan/atau sanksi denda sebanyak Rp 2.000.000.000 (dua miliar rupiah).

Phisher yang telah berhasil memasuki sistem elektronik nasabah, mengambil alih kendali pada sistem elektronik nasabah. Nasabah tidak dapat mengakses aplikasi layanan bank digital hingga akses terhadap dana simpanan yang dimilikinya. Kondisi terganggunya sistem elektronik yang digunakan berakibat sistem elektronik yang dimiliki tidak bekerja sebagaimana mestinya diatur dalam UU ITE mengatur hal tersebut pada Pasal 33 beserta dengan sanksinya yang terdapat dalam Pasal 49, Pasal 33 dikenal dengan *computer system interference*

Sanksi yang dikenakan terhadap tindakan melawan hukum tersebut adalah sanksi pidana dan/atau denda. Ancaman sanksi yang diberikan sangat tinggi, hal ini semata – mata merupakan upaya untuk memberikan perlindungan kepada nasabah dan memberikan peringatan kepada oknum yang tidak bertanggung jawab (Siahaan,2018). Ancaman pidana pada *phisher* dan *hacker* yang memenuhi unsur yang dimaksud dalam pasal 33, maka akan dikenakan pidana penjara paling lama 10 (sepuluh) tahun dan/atau ancaman denda paling banyak Rp 10.000.000,00 (sepuluh miliar rupiah).

Pasal 1 UU ITE mengatur mengenai informasi elektronik, bahwa informasi elektronik tidak terbatas hanya pada tulisan, gambar, suara ,peta, rancangan foto, elektronik data, *interchange, e – mail*, telegram, teleks, telecopy atau sejenisnya. Huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Nomor telepon, akun e – mail serta media sosial dapat menjadi perantara dari bentuk informasi elektronik para *phisher* dan *hacker* untuk dapat melakukan kejahatan *phising* dan *hacking*. Sanksi yang dapat diberikan kepada pelaku *phising* dan *hacking* akibat dilanggarnya Pasal 35 UU ITE, diancam dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000 (dua belas miliar rupiah).

Selanjutnya dari sisi pengaturan dalam POJK Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum. Dalam POJK tersebut juga memberikan perlindungan hukum kepada nasabah. Dalam POJK tersebut mengatur bahwa setiap bank wajib menerapkan prinsip pengendalian pengamanan terhadap data dan transaksi yang terjadi pada layanan bank digital yang digunakan nasabah. Hal ini diatur dalam Pasal 6 POJK Penyelenggaraan Perbankan Digital oleh Bank Umum sebagai berikut:

“Bank wajib menerapkan prinsip pengendalian pengamanan data dan transaksi nasabah dari layanan perbankan elektronik pada setiap sistem elektronik yang digunakan oleh bank.”

Prinsip pengendalian pengamanan data dan transaksi nasabah pada setiap sistem elektronik layanan bank digital turut pula mencakup prinsip kerahasiaan (*confidentiality*). Nasabah berhak mendapat kepastian hukum apabila terdapat permasalahan dalam penggunaan layanan pada bank digital (Agus & Riskawati,2016). Sebagaimana diatur pada Pasal 9 ayat (2) poin f bank setidaknya memiliki unit atau fungsi untuk memantau kendala dan permasalahan yang timbul dari penyelenggaraan layanan perbankan. Oleh karena itu, nasabah berhak mendapat penanganan dari setiap permasalahan yang muncul, termasuk kejahatan phising dan hacking apabila dialami oleh nasabah.

Bank digital sebagai penyelenggara layanan perbankan elektronik dan/atau layanan perbankan digital, wajib mematuhi peraturan perundang – undangan mengenai perlindungan konsumen sektor jasa keuangan terkait prinsip perlindungan konsumen. Bagi Bank yang tidak patuh POJK mengenakan sanksi administratif berupa teguran tertulis, penurunan tingkat kesehatan berupa penurunan peringkat faktor tata kelola dalam penilaian tingkat kesehatan bank, larangan untuk menerbitkan produk atau melaksanakan aktivitas baru, pembekuan kegiatan usaha tertentu, dan/atau pencantuman anggota direksi, dewan komisaris, dan pejabat eksekutif dalam daftar tidak lulus melalui mekanisme uji kemampuan dan kepatutan apabila bank yang bersangkutan tidak mematuhi peraturan pada pasal 6 dan pasal 21 b.

Bank digital merupakan entitas yang sama dengan bank umum, dimana pelaksanaan kegiatan usahanya tidak jauh berbeda dengan bank umum konvensional. Bank digital merupakan pengembangan bentuk dari bank umum dengan memanfaatkan kemajuan teknologi dalam kegiatan usahanya. Oleh karena pengaturan pembentukkan bank hingga pelaksanaan kegiatan usahanya, bank digital wajib mematuhi peraturan perbankan yang berlaku. Bank digital dapat menjalankan kegiatan usaha sebagaimana undang - undang memberikan kesempatan kepada bank umum. Pengaturan lebih lanjut mengenai syarat - syarat pembentukkan bank umum diatur dalam Pasal 24 POJK Bank Umum sebagai berikut:

1. Memiliki model bisnis dengan penggunaan teknologi yang inovatif dan aman dalam melayani kebutuhan nasabah;
2. Memiliki kemampuan untuk mengelola model bisnis perbankan digital yang prudent dan berkesinambungan;
3. Memiliki manajemen risiko secara memadai;
4. Memenuhi aspek tata kelola termasuk pemenuhan Direksi yang mempunyai kompetensi di bidang teknologi informasi dan kompetensi lain sesuai dengan ketentuan OJK mengenai penilaian kemampuan dan kepatutan bagi pihak utama lembaga jasa keuangan;

5. Menjalankan perlindungan terhadap data nasabah
6. Memberikan upaya yang kontributif terhadap pengembangan ekosistem keuangan digital dan/atau inklusi keuangan.

Berdasarkan ayat ini pada poin a dan e ditekankan kepada bank umum yang akan beroperasi menjadi bank digital, maka wajib menggunakan teknologi yang aman yang akan diterapkan pada layanan bank digital. Nasabah sebagai konsumen pada bank digital berlandaskan asas kepercayaan wajib dilindungi keamanan data pribadi serta dana simpanan yang ada pada bank digital. Nasabah dalam menggunakan layanan bank digital tidak perlu khawatir akan kejahatan phising dan hacking,karena peraturan di Indonesia sudah menjamin adanya kepastian hukum terhadap data dan/atau informasi pribadi nasabah.

POJK Perlindungan Konsumen dan Sektor Jasa memberikan kepastian hukum terhadap data diri nasabah berupa larangan terhadap PUJK untuk memberikan informasi data pribadi kepada pihak lain, dan mengatur penggunaan data-data pribadi hanya untuk keperluan yang diperjanjikan dengan nasabah. Pengaturan dalam Pasal 11 ayat (1) tersebut adalah sebagai berikut:

a. Memberikan data dan/atau informasi pribadi mengenai konsumen kepada pihak lain
b. Mengharuskan konsumen setuju untuk membagikan data dan/atau informasi pribadi sebagai syarat penggunaan produk dan/atau layanan;
c. Menggunakan data dan/atau informasi pribadi konsumen yang telah mengakhiri perjanjian produk dan/atau layanan;
d. Menggunakan data dan/atau informasi pribadi calon konsumen yang permohonan penggunaan produk dan/atau layanan ditolak oleh PUJK;
e. Menggunakan data dan/atau informasi pribadi calon konsumen yang menarik permohonan penggunaan produk dan/atau layanan.

Berdasarkan POJK tersebut data dan/atau informasi pribadi sebagaimana dimaksud dalam ayat (1) mencakup nama, NIK, alamat, tanggal lahir dan/atau umur; nomor telepon; nama ibu kandung; dan/atau data lain yang diserahkan atau diberikan akses oleh nasabah kepada PUJK untuk keperluan yang yang diperjanjikan dan terbatas, serta tidak diperkenankan untuk diberikan kepada pihak lain termasuk penyalahgunaan.

Dalam kasus yang Penulis temukan, terdapat kelalaian yang dilakukan oleh pihak bank digital sehingga hilangnya dana nasabah hingga bahkan nasabah diminta untuk membayar tagihan pada layanan peminjaman kredit yang nyatanya nasabah tersebut tidak menggunakan layanan kredit pada bank digital tersebut. Kondisi ini tentunya perlu penyelidikan lebih lanjut,

sehingga dapat diketahui apakah kelalaian dari nasabah atau penyalahgunaan dari pihak perbankan yang tidak bisa menjaga keamanan dan kerahasiaan data.

POJK Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum juga berlaku untuk setiap bank digital yang menerbitkan aplikasi mobile banking yang dapat diunduh pada perangkat elektronik milik nasabah. Berdasarkan pasal 2 POJK Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, bank dapat menyelenggarakan layanan perbankan elektronik atau layanan perbankan digital dalam bentuk aplikasi mobile banking yang mengakomodir seluruh kegiatan usaha bank digital pada satu aplikasi tersebut. Dalam penyelenggaraannya juga diatur kewajiban perbankan agar menerapkan prinsip kehati - hatian, manajemen risiko, dan memenuhi ketentuan yang diatur dalam POJK.

Prinsip kehati - hatian diperlukan bank digital dalam menjalankan kegiatan usahanya, karena seyogyanya bank dalam menjalankan kegiatan usaha memegang data-data rahasia yang sangat besar. Kegiatan utama perbankan adalah menghimpun dana dan menyalurkan dana masyarakat dalam bentuk kredit. Ketika nasabah melakukan pembukaan rekening pertama kali yang dilakukan adalah memberikan data pribadi untuk dilakukan otorisasi. Kemudian, apabila nasabah hendak menggunakan layanan bank digital untuk menyimpan dana dalam bentuk tabungan dan/atau deposito, maka nasabah perlu meletakkan dananya pada simpanan tersebut.

Data diri dan dana simpanan nasabah merupakan hal terpenting untuk dilindungi keamanannya oleh bank digital, dikarenakan pada bank digital sangat bergantung kepada sistem elektronik dan pemanfaatan teknologi informasi. Sistem pada bank digital telah memuat data penting nasabah yang sudah seyogyanya tidak dapat tersebar kepada pihak yang tidak bersangkutan.

KESIMPULAN

Berdasarkan hasil dan pembahasan diperoleh kesimpulan bahwa pertanggungjawaban bank digital terhadap nasabah atas kejahatan *phising* dan *hacking* ditinjau berdasarkan Hukum Positif Indonesia adalah dengan melakukan konfirmasi terkait dugaan kejahatan *phising* dan *hacking* yang terjadi pada nasabah. Kemudian, bank digital juga dapat memfasilitasi nasabah berupa adanya pelayanan pengaduan nasabah yang beroperasi selama 24 jam sehari. Pada saat kelalaian dilakukan oleh bank digital, maka bank digital bertanggung jawab sepenuhnya atas kerugian nasabah tersebut. Apabila nasabah yang lalai, maka sekurang – kurangnya bank digital dapat memfasilitasi nasabah untuk mengamankan rekening dan dana nasabah sebagai bentuk upaya bank digital untuk mengamankan data dan dana nasabah pada saat terjadi dugaan kejahatan *phising* dan *hacking*.

Perlindungan hukum terhadap nasabah atas kejahatan *phising* dan *hacking* ditinjau berdasarkan Hukum Positif Indonesia belum diatur secara khusus pada UU Pengembangan dan Penguatan Sektor Jasa Keuangan. Akan tetapi, undang – undang serta peraturan perundang – undangan terkait mengacu kepada pengertian bank secara umum. Pengaturan tersebut terdapat pada UU Pengembangan dan Penguatan Sektor Jasa Keuangan, POJK Bank Umum, POJK Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum, POJK Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan. Selain peraturan pada lingkup perbankan, terdapat UU ITE mengatur perlindungan hukum terhadap nasabah dari sisi teknologi informasi, yaitu mencakup kejahatan *phising* dan *hacking.* Ancaman yang diberikan kepada pihak yang tidak bertanggungjawab dan perbankan yang menyalahgunakan kewenangan dapat berupa sanksi administratif, sanksi pidana, dan denda yang sangat berat. Hal ini diharapkan dapat mencegah kejahatan *phising* dan *hacking* terjadi pada nasabah. Nasabah dapat merasa aman ketika menggunakan layanan bank digital.

DAFTAR REFERENSI

Agus, A. A. dan Riskawati., 2016, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), Jurnal Supremasi, Vol. 10, No. 1.

Ali, Z. 2009. *Metode Penulisan Hukum*, PT Sinar Grafika, Jakarta.

Chotimah, H. C., 2019, Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara, Jurnal politica, Vol. 10, No. 2.

Amiruddin., & Asikin. Z. 2012. *Pengantar Metode Penelitian Hukum*. PT RajaGrafindo Persada, Jakarta.

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

Kusumaatmadja, M., & Siddharta, A.2016. *Pengantar Ilmu Hukum: Suatu Pengenalan Pertama Ruang Lingkup Berlakunya Ilmu Hukum*, PT Alumni, Bandung.

Munir, N.2017. Pengantar Hukum Siber Indonesia, Depok: Rajawaji Per

Mansur, D. M. A., dan Gultom, E.2005. cyber law aspek hukum teknologi informasi, Bandung: PT Refika Aditama

Murwadji, T.2017. Integrasi Ilmu Mutu ke dalam Audit Mutu Hukum di Indonesia. *Jurnal Hukum POSTITUM*.

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

Siahaan, A. P. U., 2018, Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia, Jurnal Teknik Dan Informatika, Vol. 5, No. 1.

Soemitro, R. H. (1998). *Metodologi Penelitian Hukum dan Jurimetri*. Ghalia Indonesia, Semarang.

Fiki Ariyani. (2016). Sri Mulyani Ungkap Dampak Penarikan Dana Besar – Besaran di Bank. Available at: https://www.liputan6.com/bisnis/read/2655456/sri-mulyani-ungkap-dampak-penarikan-dana-besar-besaran-di-bank, diakses tanggal 22 November 2023.

Undang – Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana diubah Undang – undang Nomor 10 Tahun 1998 tentang Perbankan sebagaimana diubah oleh Undang – Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Jasa Keuangan.

Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah oleh Undang – Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum

Peraturan Otoritas Jasa Keuangan Nomor 06/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan

Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi