JURNAL INTERPRETASI HUKUM | ISSN: 2746-5047
Vol. 4 No 3 – Desember 2023, Hal. 682-690| Tersedia online di https://www.ejournal.warmadewa.ac.id/index.php/juinhum
DOI: https://doi.org/10.55637/juinhum.5.1.8318.682-690

TANGGUNG JAWAB BANK TERHADAP TINDAKAN *PHISING* DALAM SISTEM PENGGUNAAN *E-BANKING* (STUDI: KASUS *PHISING* PADA PT. BANK RAKYAT INDONESIA (PERSERO) TBK)

Ramadhanti Achlina Tri Putri[1], Heru Sugiyono[2]
[1,2]Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
[1]dhantiachlina@gmail.com, [2]herusugiyono@upnvj.ac.id

ABSTRAK

Phishing adalah kejahatan peretasan yang berkembang seiring berjalannya waktu di sektor perbankan, terlebih dengan hadirnya sistem *e-banking*. Metode penelitian yang digunakan adalah yuridis normatif melalui pendekatan perundang-undangan *(statue approach)* dan pendekatan kasus *(case approach)*. Dalam pendekatan perundang-undangan digunakan dengan menganalisis undang-undang yang relevan untuk dijadikan dasar hukum, seperti UU No. 10 Tahun 1998 tentang Perubahan Atas UU No.7 Tahun 1992 tentang Perbankan, UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang ITE. Sedangkan, pendekatan kasus digunakan dengan menginterpretasikan undang-undang dalam tanggung jawab bank terhadap tindakan *phising* dalam sistem *e-banking*. Berdasarkan hasil penelitian disimpulkan bahwa perlindungan hukum yang diberikan kepada nasabah terkait tindakan *phising* dalam penggunaan sistem *e-banking* dilakukan melalui prinsip kerahasiaan bank. Prinsip ini melibatkan upaya preventif dan represif. Upaya preventif merupakan tindakan pencegahan dilakukan dengan memberikan pemahaman mengenai langkah pencegahan sebelum tindakan *phising* terjadi. Sementara itu, upaya represif melibatkan penyelesaian masalah, baik melalui proses hukum di pengadilan maupun di luar pengadilan. Tanggung jawab PT. Bank Rakyat Indonesia (Persero) Tbk terhadap tindakan *phising* dalam sistem penggunaan *e-banking* yaitu melalui penyediaan layanan pengaduan, adanya upaya pemeriksaan dan penyelidikan, serta memberikan dukungan kepada nasabah dalam menemukan solusi terkait kerugian yang mungkin timbul. Dalam menghadapi tindakan *phising* dalam sistem penggunaan *e-banking* maka diharapkan Pemerintah segera membuat regulasi terkait *e-banking* serta peningkatan pengawasan yang optimal dari berbagai pihak, diantaranya bank, OJK, dan nasabah. Hal ini mengingat tindakan *phising* memiliki risiko pada perlindungan data milik nasabah dan reputasi bank terkait.

Kata Kunci : *Phising, E-Banking*, PT. Bank Rakyat Indonesia (Persero) Tbk

ABSTRACT

Phishing is a hacking crime that has developed over time in the banking sector, especially with the presence of e-banking systems. The research method used is normative juridical through a statutory approach and a case approach. In the legislative approach, it is used to analyze relevant laws to be used as a legal basis, such as Law no. 10 of 1998 concerning Amendments to Law No. 7 of 1992 concerning Banking, Law no. 8 of 1999 concerning Consumer Protection, Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning ITE. Meanwhile, the case approach is to illustrate the application and interpretation of law in the bank's responsibility for phishing acts in the e-banking system. Based on the research results, it is concluded that the legal protection provided to customers regarding phishing when using the e-banking system is carried out through the principles of bank secrecy. This principle involves preventive and repressive efforts. Preventive efforts are preventative measures carried out by providing an understanding of preventive measures before phishing occurs. Meanwhile, repressive efforts involve solving problems, either through legal processes in court or outside court. PT's responsibility. Bank Rakyat Indonesia (Persero) Tbk against phishing acts in the e-banking system, namely by providing complaint services, carrying out inspection and investigation efforts, as well as providing support to customers in finding solutions related to losses that may arise. In dealing with phishing actions in the e-banking system, it is hoped that the Government will immediately make regulations related to e-banking and increase optimal supervision from various parties, including banks, OJK, and customers. This is because phishing acts pose a risk to the protection of customer data and the reputation of the bank concerned.

Keywords : *Phising, E-Banking, PT. Bank Rakyat Indonesia (Persero) Tbk*

I. PENDAHULUAN

Peralihan ke era digital dalam perkembangan industri membawa dampak pada beberapa bidang yang berpengaruh pada kehidupan sehari-hari. Salah satu sektor industri yang mengalami perkembangan adalah sektor perbankan. Sehingga, agar perubahan dalam sektor perbankan dapat memberikan dampak positif terhadap masyarakat dan perekonomian secara keseluruhan, perubahan tersebut harus dikelola secara hati-hati (Stefanie & Suherman, 2021). Perbankan mencakup seluruh elemen diantaranya aspek kelembagaan, aktivitas bisnis, dan metode serta proses yang diterapkan dalam pelaksanaan kegiatan bank, sebagaimana dijelaskan dalam Pasal 1 Ayat (1) UU No. 10 Tahun 1998 tentang Perubahan Atas UU No. 7 Tahun 1992 tentang Perbankan. Bank adalah entitas bisnis yang menerima dana dari masyarakat dalam bentuk simpanan yang kemudian mengalokasikannya kembali kepada masyarakat melalui penyediaan kredit atau layanan keuangan lainnya, sebagaimana dijelaskan dalam Pasal 1 Ayat (2) UU No. 10 Tahun 1998 tentang Perubahan Atas UU No. 7 Tahun 1992 tentang Perbankan. Dengan demikian, bank memiliki peran yang cukup signifikan dalam perekonomian suatu negara dengan kontribusinya dalam meningkatkan kesejahteraan masyarakat secara luas (Pratama et al., 2021)

Transaksi elektronik dalam bentuk electronic banking *(e-banking)* mencerminkan implementasi perkembangan teknologi informasi dalam sektor perbankan. Pada masa sekarang, layanan *e-banking* memberikan aksesibilitas yang signifikan bagi nasabah, memungkinkan mereka untuk melakukan transaksi keuangan tanpa harus mengunjungi kantor fisik bank. Hal ini terutama bermanfaat bagi pelaku usaha skala besar yang membutuhkan sistem yang ekonomis, mudah diadaptasi, aman, otomatis, terintegrasi, dan dapat diandalkan, tanpa terikat oleh batasan ruang dan waktu (Soetarto & dkk, 2008). Meskipun demikian, belum ada undang-undang yang secara spesifik mengatur mengenai *e-banking.* Oleh karena itu, UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 7 Tahun 1992 tentang Perbankan dijadikan landasan penerapan *e-banking*. Pasal 5 Ayat (2) dari undang-undang tersebut menyatakan bahwa bank umum memiliki kemampuan untuk mengkhususkan diri dalam pelaksanaan kegiatan tertentu atau memberikan perhatian yang lebih besar kepada sektor kegiatan tertentu. Selain itu, Pasal 6 huruf a menegaskan bahwa bank umum berhak untuk melakukan kegiatan lain yang umumnya dilakukan oleh bank, selama tidak bertentangan dengan undang-undang ini dan peraturan perundang-undangan yang berlaku. Klausul-klausul ini menunjukkan bahwa bank dapat menerapkan sistem *e-banking* selama sesuai dengan ketentuan yang berlaku.

Pasal 2 dalam UU No. 10 Tahun 1998 tentang Perubahan Atas UU No. 7 Tahun 1992 Tentang Perbankan menetapkan bahwa bank wajib menjalankan setiap layanan keuangan yang ditawarkannya kepada nasabah sesuai dengan standar kehati-hatian. Meskipun pasal ini tidak memiliki penjelasan resmi, dapat diartikan bahwa bank dan pihak-pihak terkaitnya diharuskan menjalankan tugas mereka dengan hati-hati, menyeluruh, dan secara profesional untuk mendapatkan kepercayaan masyarakat, terutama dalam penawaran layanan perbankan. Bank juga diwajibkan untuk menetapkan kebijakan dan menjalankan operasionalnya dengan konsisten dan beritikad baik sesuai dengan peraturan perundang-undangan yang berlaku (Sugiyono, 2017). Meski demikian, seiring dengan perkembangan industri di sektor keuangan, terjadi juga peningkatan risiko kejahatan kriminal di sektor perbankan. Akan tetapi, Menurut Johanes Gunawan, bank memiliki kemampuan untuk memberikan perlindungan hukum atau tanggung jawab kepada nasabah sebagai konsumen baik sebelum maupun setelah terjadinya kejahatan selama proses transaksi (Gunawan, 1999).

Keberadaan *e-banking* membawa sejumlah keuntungan bagi nasabah dan bank, namun juga membawa risiko dan dampak negatif. Salah satu kelemahan utama *e-banking* adalah potensi terjadinya kejahatan terhadap perbankan, seperti pencurian data pribadi milik nasabah. Informasi yang diperoleh kemudian dimanfaatkan oleh pihak yang tidak berkepentingan. Salah satu tanggung jawab utama bank adalah menjaga prinsip kerahasiaan, dan hal ini diatur oleh berbagai pasal dalam UU No. 10 Tahun 1998 Tentang Perubahan Atas UU No. 7 Tahun 1992 Tentang Perbankan (Kusuma, 2019). Pasal 40 khususnya menekankan pentingnya menjaga kerahasiaan data pribadi nasabah, menunjukkan bahwa informasi mengenai nasabah mencakup lebih dari sekadar data keuangan. Sebaliknya, nasabah bank juga diharapkan untuk menerapkan prinsip kerahasiaan dengan menjaga informasi yang berkaitan dengan diri mereka, termasuk nomor telepon. Hal ini menegaskan komitmen pada prinsip kerahasiaan sebagai langkah untuk mengatasi potensi risiko kejahatan terhadap perbankan dalam lingkungan *e-banking* (Rani, 2014).

Phishing adalah kejahatan peretasan yang berkembang seiring berjalannya waktu di sektor perbankan (Alsayed, 2017). Pada dasarnya, *phishing* melibatkan kegiatan kriminal di mana pelaku menyamar sebagai individu atau entitas tepercaya dalam pesan elektronik dengan tujuan memperoleh data pribadi yang bersifat rahasia. Metode ini sering kali terkait dengan taktik rekayasa sosial (S et al., 2016). UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bahwa setiap orang dilarang dengan sengaja dan tanpa hak, atau melawan hukum, mengakses komputer dan/atau sistem elektronik dengan cara apa pun yang melibatkan pelanggaran, penetrasi, melewati, atau membobol sistem keamanan. Oleh karena itu, *phishing* dianggap sebagai tindakan kriminal yang melanggar hukum, dan menurut pasal ini, dapat dikenai hukuman penjara hingga 8 tahun dan/atau denda sebesar Rp800.000.000,00 (delapan ratus juta rupiah). Dengan demikian, menunjukkan adanya keseriusan sanksi yang dapat diterapkan untuk melindungi keamanan dan integritas sistem elektronik terhadap kejahatan seperti *phishing.*

Jika melihat dari berbagai aspek, *phishing* bukanlah masalah yang ringan. Hal ini dikarenakan, dampak dari *phising* bisa sangat merugikan, baik secara finansial maupun dari segi kepercayaan nasabah terhadap lembaga keuangan. Nasabah yang menjadi korban *phishing* dapat kehilangan dana mereka, dan bank sebagai lembaga keuangan dapat menghadapi risiko reputasi yang serius. Oleh karena itu, tanggung jawab bank selaku lembaga keuangan terhadap tindakan phising serta perlindungan nasabah dari serangan phishing adalah suatu prioritas. Sehingga, urgensi penelitian ini bukan hanya menjadi kontribusi penting dalam pengembangan teori hukum, tetapi juga memiliki implikasi praktis yang signifikan. Hal ini akan membantu lembaga keuangan seperti hal nya bank, otoritas pengawas, dan praktisi hukum dalam memberikan upaya melindungi nasabah dari ancaman *phishing* yang terus berkembang dan memperkuat kepercayaan nasabah dalam penggunaan layanan *e-banking*.

Bank BRI, sebagai Badan Usaha Milik Negara (BUMN) yang beroperasi di sektor perbankan dengan pengalaman lebih dari 120 tahun memiliki komitmen untuk memberikan kemudahan dan respon cepat terhadap beragam kebutuhan nasabahnya. BRI Mobile atau BRImo adalah aplikasi terkini dari Bank BRI, berbasis pada konektivitas internet, telah dirancang untuk memberikan kemudahan bagi nasabah. Aplikasi ini dilengkapi dengan fitur-fitur canggih seperti login dengan *face recognition* dan *fingerprint*, memungkinkan pengisian saldo Gopay, pembayaran menggunakan QR code, serta sejumlah fitur menarik lainnya. Tujuan utama dari pengembangan aplikasi terbaru BRI Mobile atau BRImo adalah untuk mempersiapkan model bisnis yang lebih adaptif terhadap perkembangan masa depan. Dalam konteks pergeseran kebiasaan nasabah yang sebelumnya melakukan transaksi melalui unit kerja BRI, kemudian beralih ke layanan ATM dan SMS Banking, aplikasi ini diharapkan akan mendorong seluruh nasabah untuk mulai bertransaksi melalui platform *e-banking* ini.

BRI Cabang Tabing di Koto Tengah Kota Padang mengalami kejadian phising pada Mei 2022. Salah satu nasabah Bank BRI mengklik link pengumpulan data nasabah di pesan WhatsApp agar terhindar dari dikenakan biaya transaksi sebesar Rp. 150rb per bulan dengan transaksi unlimited, alhasil tanpa sadar rugi Rp. 1,1 miliar di rekening tabungannya. Ketika korban mencoba menggunakan salah satu ATM untuk menarik uang tunai dan menemukan bahwa hal itu tidak dapat dilakukan lagi karena PIN telah diubah, dia menyadari bahwa dia telah menjadi korban *phishing*. Dalam hal ini, korban sempat melakukan upaya dengan mendatangkan Kantor BRI Tabing, namun uang dalam rekening korban yang dapat terselamatkan hanya Rp. 14 Juta. Sedangkan, saldo senilai Rp. 1,1 Miliar berhasil diambil oleh pelaku *phising* (Nugraha, 2022).

Silvia Yap, nasabah prioritas BRI KCP Lawang, Malang, Jawa Timur, menjadi korban serangan *phishing* di Bank BRI pada Mei 2023. Dalam kejadian tersebut, saldo rekening Silvia Yap berkurang Rp 1.446.000.000 dalam waktu singkat. Di layanan pesan WhatsApp, korban menerima pesan berisi undangan dalam format apk, dari sinilah kejadian ini bermula. Begitu korban mengklik dan membuka undangan tersebut, beberapa iklan mulai muncul di ponselnya. Kejadian penurunan jumlah tabungan dan pemindahan dana melalui fitur transfer antar rekening pada *e-banking* menjadi perhatian serius ketika korban menyadari bahwa saldo di rekeningnya habis dan hanya tersisa Rp 2 juta. Keesokan harinya, korban menghubungi Bank BRI KCP Lawang untuk menanyakan masalah keamanan dan meminta pengembalian dana. Namun, sayangnya, permintaan korban tidak dapat dipenuhi oleh BRI KCP Lawang. Bank tersebut menyatakan bahwa pihak bank hanya akan mengganti kerugian nasabah jika disebabkan oleh kesalahan dari layanan perbankan. Situasi ini menunjukkan bahwa bank mengambil posisi bahwa kejadian tersebut bukanlah hasil dari kesalahan dalam layanan perbankan yang

mereka sediakan, sehingga tanggung jawab atas kerugian tersebut tidak dapat ditangani oleh bank (Ali, 2023).

Penelitian ini memiliki tujuan untuk memberikan analisa mengenai perlindungan hukum terhadap nasabah bank terkait serangan *phishing* dalam penggunaan sistem *e-banking* di Indonesia. Penelitian ini berfokus untuk memahami bagaimana kerangka hukum di Indonesia dalam memberikan perlindungan kepada nasabah bank dari risiko *phishing*, terutama dalam konteks transaksi perbankan digital. Kemudian, penelitian ini juga memberikan analisa mengenai tanggung jawab PT. Bank Rakyat Indonesia (Persero) Tbk terhadap tindakan *phishing* dalam penggunaan sistem *e-banking*. Ini mencakup pemeriksaan apakah bank memenuhi standar keamanan yang diperlukan, langkah-langkah preventif yang diambil, serta respons dan tanggung jawab yang diambil jika nasabah menjadi korban tindakan *phishing*.

II. METODE PENELITIAN

Metode penelitian yang digunakan adalah yuridis normatif yang memandang hukum sebagai apa yang terkandung dalam peraturan perundang-undangan atau aturan yang menetapkan standar perilaku manusia yang dapat diterima. Metode penelitian ini memberikan fokus pada analisis terhadap norma-norma hukum yang ada (Amiruddin & Asikin, 2021). Pendekatan penelitian yang digunakan adalah pendekatan undang-undang *(statute approach)* dan pendekatan kasus *(case approach)*. Dalam pendekatan perundang-undangan digunakan dengan menganalisis undang-undang yang relevan untuk dijadikan dasar hukum terkait dengan tanggung jawab bank terhadap tindakan *phising* dalam sistem penggunaan *e-banking*. Sedangkan, pendekatan kasus digunakan dengan menginterpretasikan undang-undang dalam tanggung jawab bank terhadap tindakan *phising* dalam sistem *e-banking*. Sumber penelitian mencakup bahan-bahan hukum primer, sekunder, dan tersier. Bahan hukum primer berupa UU No. 10 Tahun 1998 tentang Perubahan Atas UU No. 7 Tahun 1992 tentang Perbankan, UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Bahan hukum sekunder berupa pendapat hukum, doktrin, teori-teori yang diperoleh dari literatur hukum, hasil penelitian, artikel ilmiah, dan informasi dari website yang relevan dengan topik seperti tanggung jawab, perlindungan hukum, bank, dan *phishing.* Bahan ini mendukung analisis lebih lanjut dan memberikan pandangan-pandangan berdasarkan pemahaman para ahli. Sedangkan, bahan hukum tersier yaitu kamus bahasa Indonesia, yang digunakan untuk memahami definisi tertentu. Analisis penelitian melibatkan klasifikasi bahan-bahan hukum sesuai dengan rumusan masalah, sistematisasi, interpretasi, analisis, dan simpulan.

III. HASIL DAN PEMBAHASAN

3.1 Perlindungan Hukum Terhadap Nasabah Bank Atas Tindakan Phising Dalam Sistem Penggunaan E-Banking Di Indonesia

Dalam rangka percepatan pelayanan perbankan, transaksi elektronik berupa internet banking atau *e-banking* merupakan perkembangan baru dalam layanan bank. Hal-hal tersebut menghubungkan tuntutan jasa keuangan dan tuntutan nasabah (Atorf & dkk, 2002). Namun seiring dengan berkembangnya layanan perbankan, bank juga akan menghadapi peningkatan risiko. Oleh karena itu, berdasarkan POJK No. 12/POJK.03/2018 yang membahas Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum bertujuan mendorong bank untuk memberikan prioritas pada manajemen risiko informasi teknologi. Dengan demikian, bank diharapkan untuk secara efektif mengintegrasikan kebijakan dan praktik pengelolaan risiko informasi teknologi dalam penyelenggaraan layanan perbankan digital mereka. Hal ini termasuk tindakan pencegahan terhadap risiko-risiko seperti *phishing*, kebocoran data, dan serangan siber lainnya yang dapat mengancam keamanan informasi nasabah. Selain itu, bank diharapkan untuk mematuhi standar keamanan dan privasi yang diatur dalam peraturan tersebut (Tarigan & Paulus, 2019). Terlebih lagi bahwa keamanan data pribadi nasabah sangatlah penting, terutama dalam sistem elektronik seperti *e-banking*. Pelanggaran data yang dilakukan oleh peretas keamanan berdampak negatif pada nasabah bank yang memanfaatkan *e-banking*. Hal ini didukung oleh semakin canggih dan berkembangnya modus kejahatan perbankan, salah satunya adalah *phishing*.

Phishing adalah suatu metode peretasan di mana penipu berusaha untuk memperoleh informasi sensitif atau rahasia dari individu, seperti nama pengguna, nomor PIN, nomor kartu kredit, data akun, serta informasi pribadi seperti nama, usia, dan alamat. Metode ini biasanya melibatkan pengiriman

pesan palsu, baik melalui surat, format elektronik, atau bentuk komunikasi lainnya. Dalam praktiknya, penipu seringkali berpura-pura menjadi entitas atau organisasi yang tepercaya, seperti bank, lembaga pemerintah, atau platform *online*, untuk mengecoh korban. Pada umumnya, pesan yang dikirim meminta korban untuk memberikan data pribadi secara tidak langsung atau mengklik tautan yang tanpa korban ketahui bahwa tautan tersebut mengarah ke situs web palsu yang dirancang untuk mencuri data-data pribadi (Latifahi et al., 2022). Berdasarkan UU No. 8 Tahun 1999 tentang Perlindungan Konsumen memberikan dasar hukum untuk melindungi nasabah dari praktik *phishing* yang merugikan. Kemudian, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 mengatur perlindungan data pribadi nasabah. Sehingga, disimpulkan bahwa nasabah memiliki hak hukum untuk privasi data mereka, dan lembaga keuangan harus memastikan perlindungan data pribadi nasabah. Dalam hal ini, perlindungan nasabah terhadap tindakan *phising* dapat dilakukan secara preventif dan represif.

Perlindungan preventif terhadap nasabah bank yang mengalami tindakan *phishing* dalam sistem penggunaan *e-banking* di Indonesia mencakup serangkaian tindakan pencegahan sebelum terjadinya kejahatan. Ini melibatkan informasi dan nasihat kepada nasabah mengenai hak-hak hukum mereka sebagai konsumen, serta pemberitahuan hak dan kewajiban di sektor keuangan. Bank wajib memberitahukan dan memberikan nasihat kepada nasabah mengenai hak-hak hukumnya sebagai konsumen. Hal tersebut sesuai dengan tujuan perlindungan konsumen untuk memberdayakan konsumen dengan pengetahuan tentang hak-hak mereka, termasuk hak-hak hukum. Hal ini menekankan pentingnya memberikan informasi kepada nasabah mengenai hak-hak mereka, termasuk hak untuk dilindungi dari praktik-praktik yang dapat merugikan, seperti tindakan *phishing.*

Sedangkan, Pasal 9 POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan yaitu Pelaku Usaha Jasa Keuangan menetapkan kewajiban bagi Pelaku Usaha Jasa Keuangan, termasuk bank, untuk memberitahukan kepada konsumen mengenai hak dan kewajiban mereka dalam sektor keuangan. Ini mencakup penyediaan informasi yang jelas mengenai cara mengamankan akun, risiko keamanan dalam penggunaan layanan *e-banking*, serta langkah-langkah pencegahan yang dapat diambil oleh nasabah. Dengan memberikan informasi yang komprehensif, nasabah dapat lebih memahami risiko dan cara melindungi diri mereka dari tindakan *phishing*. Dengan demikian, hal ini menciptakan lingkungan yang lebih aman dan membantu nasabah untuk mengambil tindakan preventif secara proaktif. Selain itu, ketentuan-ketentuan ini juga memberikan dasar hukum bagi nasabah untuk mendapatkan perlindungan dan informasi yang diperlukan dalam penggunaan layanan perbankan digital.

Selain itu, bagi nasabah bank yang mengalami tindakan *phising* juga mendapatkan perlindungan secara represif (Jahri, 2016). Perlindungan secara represif bagi nasabah bank yang mengalami tindakan *phishing* melibatkan tindakan penyelesaian setelah terjadinya tindakan kejahatan (Anugrah et al., 2022).

Beberapa aspek yang mencakup perlindungan ini dapat dilihat pada UU No. 8 Tahun 1999 Tentang Perlindungan Konsumen yaitu nasabah bank selaku konsumen memiliki hak untuk menyatakan pendapat dan mengajukan keluhan terkait dengan produk dan/atau layanan yang mereka gunakan. Hal ini didasarkan pada Pasal 4 huruf D. Dengan demikian, nasabah yang menjadi korban *phishing* dapat menggunakan hak ini untuk menyampaikan pengaduan atau keluhan terkait layanan perbankan yang mereka terima.

Selanjutnya, Pasal 32 POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan yaitu para pelaku usaha di industri jasa keuangan, termasuk bank diharapkan mampu mengelola sistem yang memberikan layanan dan solusi bagi konsumen. Ini menciptakan harapan bahwa penyelesaian atas masalah yang dihadapi oleh nasabah akan dilakukan dengan transparan dan efektif. Sedangkan, dalam Pasal 39 POJK tersebut dijelaskan apabila nasabah belum mencapai kesepakatan, mereka memiliki opsi untuk menyelesaikan tuntutannya di dalam atau di luar pengadilan. Kemudian, berdasarkan Pasal 40 pada POJK tersebut juga dijelaskan bahwa OJK memberikan kewenangan kepada nasabah untuk mengajukan pengaduan ke OJK dengan alasan adanya kesalahan pada layanan perbankan. OJK dapat berperan sebagai mediator dan menilai apakah ada pelanggaran yang perlu ditindaklanjuti. Dengan demikian, mekanisme perlindungan represif ini memberikan nasabah berbagai opsi untuk menyelesaikan permasalahan yang muncul akibat tindakan *phishing*, baik melalui penyelesaian langsung dengan bank, melalui jalur hukum, atau dengan melibatkan otoritas pengawas keuangan seperti OJK (Rahmadian et al., 2020).

Dengan demikian, bagi nasabah bank yang merasa dirugikan dengan terjadinya tindakan *phising* dalam sistem penggunaan *e-banking* berhak untuk mendapatkan perlindungan hukum, diantaranya

adalah nasabah memiliki hak untuk mengajukan pengaduan terkait tindakan *phishing*. Hak ini memberikan sarana bagi nasabah untuk menyampaikan keluhan mereka terhadap bank atau lembaga keuangan terkait. Selanjutnya, nasabah dapat memanfaatkan forum mediasi keuangan untuk menyelesaikan sengketa di industri perbankan secara cepat, mudah, dan murah. Ini menciptakan mekanisme penyelesaian sengketa alternatif yang dapat membantu nasabah dan bank mencapai kesepakatan tanpa melibatkan proses hukum yang panjang (Wonok, 2012). Selain itu, nasabah juga diberikan perlindungan secara hukum oleh OJK, yang merupakan otoritas pengawas di sektor jasa keuangan. OJK memantau dan mengawasi aspek kelembagaan, produk dan operasional, kehati-hatian, serta transparansi dalam operasional bank. OJK melakukan pengawasan terhadap bank melalui berbagai langkah seperti pemahaman bank yang bersangkutan, penilaian risiko bank, penyusunan strategi pemantauan berdasarkan risiko, pemeriksaan bank, dan verifikasi kondisi bank secara berkala. Langkah-langkah ini bertujuan untuk memastikan bahwa bank beroperasi dengan mematuhi standar keamanan dan peraturan yang berlaku.

3.2 Tanggung Jawab PT. Bank Rakyat Indonesia (Persero) Tbk Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking

Pada akhir Maret 2023 atau hanya dalam waktu 3 bulan sejak awal tahun, BRI menyebutkan 225 juta transaksi keuangan telah tercatat di super app perbankan digital miliknya, yaitu BRImo. Saat ini, pengguna BRImo dengan jumlah 26,3 juta nasabah dan terus meningkat (Mayasari, 2023). Dalam konteks layanan perbankan, nasabah adalah individu atau entitas yang memanfaatkan layanan yang disediakan oleh lembaga perbankan. Definisi ini sesuai dengan Pasal 1 Angka 16 UU No. 10 Tahun 1998 Tentang Perubahan Atas UU No. 7 Tahun 1992 Tentang Perbankan.

Rasa kepercayaan nasabah terhadap bank menjadi faktor penting dalam menjalankan layanan perbankan. *Phishing*, sebagai bentuk kejahatan dalam sektor perbankan, memiliki dampak serius terhadap keamanan simpanan nasabah. Ancaman terhadap keamanan ini juga dapat menghambat upaya BRI untuk menjaga reputasi dan memperoleh kepercayaan nasabah. Rasa keamanan dan kepercayaan nasabah adalah aspek-aspek kunci dalam mempertahankan hubungan yang baik antara bank dan nasabah. Upaya pencegahan dan penanggulangan terhadap *phishing* menjadi suatu keharusan bagi bank untuk menjaga keamanan dan meminimalisir risiko yang dapat merugikan nasabah. Transparansi, edukasi terhadap nasabah mengenai praktik keamanan, dan implementasi teknologi keamanan yang canggih menjadi strategi penting dalam menghadapi ancaman *phishing*.

Dalam menjalankan layanan perbankannya, BRI menerapkan prinsip perlindungan konsumen. Hal ini mencakup tanggung jawab untuk memberikan perlindungan secara preventif dan represif terhadap nasabah. Tanggung jawab preventif BRI yaitu dengan adanya prosedur yang dirancang untuk mencegah terjadinya *phishing*. Salah satu prosedur pertama adalah meningkatkan pengetahuan nasabah mengenai ancaman *phishing* dan cara melindungi diri dari serangan tersebut. Sedangkan, tanggung jawab represif diberikan kepada nasabah yang telah terkena serangan *phishing*. Ini mencakup langkah-langkah untuk menanggulangi dan menyelesaikan masalah yang timbul setelah serangan *phising* terjadi.

Tanggung jawab BRI dalam bentuk perlindungan preventif diantaranya adalah menggunakan media sosial, khususnya Twitter, dan pesan email untuk secara berkala menginformasikan nasabah tentang keamanan transaksi *e-banking*. Hal ini mencerminkan upaya bank untuk meningkatkan kesadaran nasabah terhadap ancaman keamanan dan memberikan panduan untuk transaksi yang aman. Selain itu, BRI tidak membatasi bagi nasabah yang memiliki kekhawatiran tentang *e-banking* dengan tetap memberikan ruang, waktu, dan kesempatan untuk berbicara langsung. Ini menciptakan saluran komunikasi yang terbuka antara bank dan nasabah untuk menanggapi kekhawatiran atau pertanyaan secara langsung.

Dalam menjalani layanan operasional perbankan, BRI melakukan secara komprehensif terkait dengan manajemen risiko dalam seluruh layanan operasionalnya. Ini mencakup penggunaan metodologi dan efektivitas aktivitas manajemen risiko secara berkala, sesuai dengan ketentuan Kebijakan Umum Manajemen Risiko. Hal ini mengingat perkembangan teknologi dan hadirnya *e-banking* maka diperlukan pengelolaan yang baik dalam mengendalikan risiko teknologi informasi. Ini mencakup arahan dan pengendalian yang diperlukan dalam menjalankan manajemen risiko terkait teknologi informasi (PT. BRI Multifinance Indonesia, 2022). Secara keseluruhan, BRI memiliki pendekatan untuk melindungi nasabah terhadap ancaman *phishing* dan mengelola risiko operasional terkait teknologi informasi.

BRI menjelaskan bahwa kelalaian nasabah juga dapat menjadi penyebab serangan *phishing*. Ini mencakup tindakan-tindakan yang mungkin dilakukan nasabah yang membuka celah bagi serangan *phishing*. Pada proses memberikan tanggung jawab secara represif, BRI memberikan himbauan agar nasabah yang melakukan pengaduan tidak menyampaikan laporan secara berulang. Hal ini untuk mencegah pengulangan laporan yang sama dan memastikan efisiensi dalam penanganan pengaduan. Kemudian, jika selama proses penyelidikan ditemukan bahwa kejadian *phishing* disebabkan oleh kelalaian nasabah maka nasabah bertanggung jawab atas seluruhnya. Sehingga, bank tidak memberikan ganti rugi kepada nasabah karena dianggap bukan kesalahan dari pihak bank.

UU No. 19 Tahun 2016 tentang ITE berdampak terhadap persepsi nasabah terkait dengan rasa aman dan nyaman dalam menggunakan layanan perbankan digital, seperti hal nya dengan *e-banking* (Putra et al., 2021). Hal ini dikarenakan dalam undang-undang tersebut menjelaskan bahwa bank memiliki tanggung jawab secara hukum apabila terjadi kerugian pada nasabah yang menggunakan layanan dari bank tersebut. Akan tetapi, jika kerugian disebabkan oleh nasabah itu sendiri seperti hal nya kelalaian atau keadaan *force majeure* maka bank tidak bertanggung jawab. Dengan demikian, BRI melakukan pendekatan yang seimbang antara memberikan perlindungan kepada nasabah dan menegakkan tanggung jawab nasabah dalam upaya mencegah serangan *phishing.*

Kemudian, tanggung jawab BRI dalam bentuk represif diantaranya adalah nasabah memiliki hak untuk menggugat BRI di pengadilan jika hasil penyelesaian yang ditawarkan oleh bank terkait kasus *phising* tidak sesuai dengan yang diharapkan. Gugatan dapat diajukan dengan dasar bahwa BRI menyebabkan kerugian nasabah akibat serangan *phising* dalam penggunaan sistem *e-banking.* Selain itu, sebagai alternatif untuk mengajukan gugatan di pengadilan, nasabah juga dapat meminta bantuan OJK. OJK dapat membantu mempercepat proses pengaduan nasabah yang mengalami kerugian akibat *phising*. Langkah ini menunjukkan adanya mekanisme di luar pengadilan untuk menyelesaikan sengketa dan mendapatkan penyelesaian.

Akan tetapi, Bank BRI melakukan upaya semaksimal mungkin untuk memilih penyelesaian secara damai. Upaya untuk menyelesaikan secara damai dapat mencakup negosiasi, mediasi, atau penyelesaian di luar pengadilan. Upaya damai dilakukan untuk mempertahankan hubungan baik dengan nasabah dan menghindari dampak negatif terhadap reputasi bank. Reputasi bank dan kepercayaan nasabah dianggap sebagai faktor krusial dalam penanganan kasus *phising.* BRI berusaha menjaga kepercayaan nasabah dengan menawarkan penyelesaian yang memadai dan menghindari proses pengadilan yang dapat merugikan hubungan tersebut (Indonesia, 2016).

IV. SIMPULAN DAN SARAN

4.1 Simpulan

Nasabah yang terkena serangan *phising* dalam penggunaan sistem *e-banking* mendapatkan perlindungan hukum melalui upaya preventif dan represif. Upaya preventif mencakup pemahaman hak-hak nasabah dan pencegahan *phising.* Upaya represif mencakup penyelesaian sengketa di dalam atau di luar pengadilan serta pengajuan pengaduan ke OJK. Nasabah memiliki hak hukum untuk mendapatkan perlindungan dalam hal perlindungan konsumen. UU No. 8 Tahun 1999 tentang Perlindungan Konsumen memberikan dasar hukum untuk melindungi nasabah dari praktik *phishing* yang merugikan. Kemudian, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 mengatur perlindungan data pribadi nasabah. Sehingga, disimpulkan bahwa nasabah memiliki hak hukum untuk privasi data mereka, dan lembaga keuangan harus memastikan perlindungan data pribadi nasabah.

Tanggung jawab BRI atas terjadinya tindakan *phising* dalam sistem penggunaan *e-banking* yaitu tanggung jawab untuk memberikan perlindungan secara preventif dan represif terhadap nasabah. Tanggung jawab preventif BRI yaitu dengan adanya prosedur yang dirancang untuk mencegah terjadinya *phishing*. Salah satu prosedur pertama adalah meningkatkan pengetahuan nasabah mengenai ancaman *phishing* dan cara melindungi diri dari serangan tersebut. Sedangkan, tanggung jawab represif diberikan kepada nasabah yang telah terkena serangan *phishing*. Ini mencakup langkah-langkah untuk menanggulangi dan menyelesaikan masalah yang timbul setelah serangan *phising* terjadi. Hal ini didukung dengan melengkapi manajemen risiko, memastikan teknologi informasi yang aman, dan menawarkan layanan pengaduan nasabah melalui *call center* dan media sosial. Dalam situasi di mana nasabah mengalami kerugian akibat tindakan *phishing* yang disebabkan oleh BRI maka bank dijamin akan menggantikan dengan kompensasi yang sesuai. Nasabah memiliki hak untuk menggugat BRI di pengadilan jika hasil penyelesaian yang ditawarkan oleh bank terkait kasus *phising* tidak sesuai dengan

yang diharapkan. Selain itu, nasabah memiliki opsi untuk mengajukan pengaduan kepada OJK jika merasa penyelesaian dengan bank tidak memuaskan. OJK dapat mempercepat proses pengaduan nasabah terkait kerugian akibat *phising.* Dengan demikian, ada upaya konkret yang dilakukan oleh bank dalam melibatkan nasabah dalam langkah-langkah preventif dan represif, serta tanggung jawab bank terhadap keamanan *e-banking* dan penanganan kasus *phising*.

4.2 Saran

Dalam menghadapi tantangan yang muncul seiring dengan perkembangan layanan perbankan, khususnya layanan *e-banking* maka Pemerintah Indonesia perlu segera membuat undang-undang yang tegas dan komprehensif yang mengatur penggunaan layanan *e-banking* oleh nasabah bank dengan mencakup tanggung jawab nasabah, bank, dan pemerintah dalam melindungi nasabah dari ancaman *phishing* dan perlu memberikan hukuman yang tegas untuk pelaku *phishing.* Tujuannya agar nasabah selaku korban mendapatkan perlindungan hukum yang jelas dan memberikan dasar hukum bagi pelaku dalam penanganan kasus *phising* yang menyebabkan kerugian pada nasabah. Bagi BRI perlu meningkatkan kapabilitasnya menangani proses penanganan dan pengaduan dari nasabah yang mengalami kerugian akibat tindakan *phishing.* Hal ini mencakup percepatan proses penyelesaian dan komunikasi yang efektif dengan nasabah. Selain itu, BRI perlu terus meningkatkan sistem keamanan dan pengawasan dalam memberikan pelatihan kepada nasabah untuk meningkatkan kesadaran mereka tentang ancaman *phishing*.

Bagi OJK perlu meningkatkan sistem pengawasannya terhadap kegiatan komersial di sektor jasa keuangan, khususnya perbankan, termasuk layanan *e-banking.* Seperti halnya, melakukan pemantauan terhadap keamanan transaksi dan perlindungan kepentingan nasabah. Selain itu, OJK juga memberikan panduan kepada bank-bank tentang praktik terbaik dalam mengatasi tindakan *phishing*. Hal ini dapat membantu bank dalam memahami cara yang lebih efektif untuk melindungi nasabah mereka. Kemudian, bagi nasabah dan masyarakat umum perlu meningkatkan kesadaran terhadap risiko *phising.* Selain itu, nasabah dan masyarakat umum lainnya juga berperan dalam meningkatkan pengawasan dengan melaporkan aktivitas mencurigakan atas terjadinya *phising* kepada bank atau otoritas terkait. Dengan langkah-langkah ini, diharapkan dapat menciptakan penggunaan *e-banking* yang lebih aman, transparan, dan responsif terhadap kebutuhan dan keamanan nasabah.

DAFTAR PUSTAKA

Ali, A. (2023). *Nasabah Prioritas Bank BRI Kehilangan Rp 1,4 Miliar Akibat Phising, Sambangi Polda Jatim*. Berita Satu.

Alsayed, A. O. (2017). E-Banking Security: Internet Hacking, Phishing attacks, Anlaysis and Prevention of Fraudelent Activities. *International Journal of Emerging Technology and Advanced Engineering*, *7*(1).

Amiruddin, & Asikin, Z. (2021). *Pengantar Metode Penelitian Hukum*. Rajawali Pers.

Anugrah, I. K. D., Widyantara, I. M. M., & Arini, D. G. D. (2022). Perlindungan Hukum Terhadap Nasabah Bank Atas Tindak Pidana Pencatatan Palsu Dalam Dokumen Perbankan. *Jurnal Preferensi Hukum*, *3*(2).

Atorf, N., & dkk. (2002). Internet Banking di Indonesia. *Jurnal Manajemen Teknologi*, *2*(1).

Gunawan, J. (1999). *Hukum Perlindungan Konsumen*. Universitas Katolik Parahyangan.

Indonesia, I. B. (2016). *Strategi Manajemen Risiko* . Gramedia Pustaka Utama.

Jahri, A. (2016). Perlindungan Nasabah Debitur Terhadap Perjanjian Baku yang Mengandung Klausula Eksonerasi pada Bank Umum di Bandar Lampung. *Fiat Justisia Journal Of Law*, *10*(2).

Kusuma, M. J. (2019). *Hukum Perlindungan Nasabah Bank, Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE Di Bidang Perbankan*. Nusa Media.

Latifahi, F. N., Mawardi, I., & Wardhana, B. (2022). Ancaman Pencurian Data (Phising) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19 (Study Phising Di Indonesia). *Perisai: Islamic Banking and Finance Journal*, *6*(1).

Mayasari, S. (2023). *Sampai Akhir Maret 2023, Jumlah Transaksi BRImo Melonjak hingga 154,63%*. Keuangan Kontan.

Nugraha, H. S. (2022). *Nasabahnya jadi Korban Link Pishing Hingga Rugi Rp 1,1 Miliar, BRI lakukan Investigasi*. Zona Sumbar.

Pratama, A. A. N. B. K., Mahendrawati, N. L. M., & Ujianti, N. M. P. (2021). Perlindungan Hukum Bagi Konsumen Pada Bank Beku Operasi. *Jurnal Interpretasi Hukum*, *2*(1).

PT. BRI Multifinance Indonesia. (2022). *Kebijakan Manajemen Risiko*. BRI Finance.

Putra, K. Y. P., Dewi, A. A. S. L., & Suryani, L. P. (2021). Perlindungan Hukum Korban Penipuan Undian Berhadiah Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Interpretasi Hukum*, *2*(3).

Rahmadian, F., Maksum, M., & Rambe, M. S. (2020). Perlindungan Nasabah Bank Terhadap Tindakan Phishing; Studi pada PT Bank Rakyat Indonesia (Persero) Tbk. *Journal Of Legal Research*, *2*(2).

Rani, M. (2014). Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank. *Jurnal Selat*, *2*(1).

S, E., Mule, & U, P. (2016). Phishing Attacks and Its Preventions. *Imperial Journal of Interdisciplinary Research*, *2*(12).

Soetarto, & dkk. (2008). *Teknologi E-Banking di Kalangan Smart Customer: Kasus di Kota Solo*. Fakultas Ekonomi Universitas Muhamadiyah Solo.

Stefanie, E., & Suherman. (2021). Urgensitas Pengoptimalan Peraturan Otoritas Jasa Keuangan Terkait Financial Technology. *Jurnal Yuridis Fakultas Hukum, UPN "Veteran" Jakarta*, *8*(1).

Sugiyono, H. (2017). Perlindungan Hukum Terhadap Pihak Ketiga Sebagai Pemilik Jaminan Ketika Tidak Dilaksanakannya Prinsip Kehati -Hatian Oleh Bank Dalam Perjanjian Kredit Dengan Memakai Jaminan. *Jurnal Yuridis Fakultas Hukum UPN "Veteran" Jakarta*, *4*(1).

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia*, *1*(3).

Wonok, D. Y. (2012). Perlindungan Hukum Atas Hak-Hak Nasabah Sebagai Konsumen Pengguna Jasa Bank Terhadap Risiko Yang Timbul Dalam Penyimpangan Dana. *Jurnal Edisi Khusus* , *1*(2).