TANGGUNG JAWAB BANK DALAM MENGANTISIPASI DAN MENANGANI KERUGIAN NASABAH AKIBAT SCAM MELALUI LINK PHISING PADA MOBILE BANKING

Vanya Agatha Hendarto, Endang Prasetyawati
vanyaagatha11@gmail.com, endang_pras@untag-sby.ac.id
Fakultas Hukum Universitas 17 Agustus 1945 Surabaya, Indonesia

Abstract

Currently, mobile banking services are increasingly popular among the public. Advances in internet technology can help the banking sector run its business better. In fact, in addition to the advantages, there are disadvantages, namely cybercrime. Phishing attacks are one of the most common attack techniques used to threaten security, mobile banking. This study analyzes the responsibility of banks in anticipating and handling losses experienced by customers due to fraud through phishing links or links in mobile banking services. Phishing attacks are increasing along with the increasing use of digital banking technology, which increases the risk of financial loss for customers. This study looks at what banks should do to protect customer data and what they should do to reduce the risk of fraud. This study is a normative legal study using a statutory approach and a conceptual approach. The results of this study indicate that banks must not only ensure technical security, but must also inform customers about how to reduce the risk of attacks. To ensure comprehensive protection, banks, governments, and other related parties must work together. Increased regulation, which regulates consumer protection against cybercrime and increased use of security technologies such as two-factor authentication and data encryption are some of the suggestions given. To make customers more aware of phishing, banks are also advised to regularly update their fraud prevention systems and create educational materials.

Keywords *: Responsibility, Bank, Customer, Phishing, Mobile Banking*

Abstrak

Saat ini, layanan mobile banking yang semakin populer di kalangan masyarakat. Kemajuan dalam teknologi internet yang dapat membantu sektor perbankan dalam menjalankan bisnisnya dengan lebih baik. Faktanya, selain kelebihan terdapat kekurangan yaitu adanya kejahatan *cyber*. Serangan phishing adalah salah satu teknik serangan yang paling umum yang digunakan untuk mengancam keamanan perbankan mobile. Penelitian ini menganalisis tanggung jawab bank dalam mengantisipasi dan menangani kerugian yang dialami nasabah akibat penipuan melalui tautan atau *link* phising di layanan mobile banking. Serangan phishing meningkat seiring dengan meningkatnya penggunaan teknologi perbankan digital, yang meningkatkan risiko kerugian finansial bagi nasabah. Penelitian ini melihat apa yang harus dilakukan bank untuk melindungi data nasabah juga apa yang wajib mereka laksanakan guna mengurangi risiko penipuan. Penelitian ini ialah penelitian hukum normatif dan

memakai pendekatan undang-undang juga pendekatan konseptual. Hasil penelitian ini memperlihatkan bahwasanya bank tidak hanya harus memastikan keamanan teknis, tetapi juga harus memberi tahu nasabah terkait cara mengurangi risiko serangan. Untuk memastikan perlindungan yang komprehensif, bank, pemerintah, dan pihak lain yang berkaitan harus bekerja sama. Peningkatan regulasi yang mengatur perlindungan konsumen terhadap kejahatan *cyber* dan peningkatan penggunaan teknologi keamanan seperti autentikasi dua faktor dan *enkripsi* data adalah beberapa saran yang diberikan. Untuk membuat pelanggan lebih waspada terhadap phishing, bank juga disarankan untuk memperbarui sistem pencegahan penipuan secara teratur dan membuat materi pendidikan.

Kata Kunci : Tanggung Jawab, Bank, Nasabah, Phising, Mobile Banking

PENDAHULUAN

Masyarakat mendapatkan banyak manfaat dari teknologi internet yang terus berkembang dengan pesat. Ini membuat orang percaya bahwa kemajuan teknologi dapat membuat kegiatan sehari-hari lebih mudah, terutama dalam urusan keuangan. Akibatnya, layanan yang disediakan secara online ini telah masuk ke banyak pasar bisnis, terutama sektor perbankan. Saat ini, kemajuan teknologi internet dapat membantu sektor perbankan menjadi lebih baik dalam menjalankan bisnisnya. Sebagai nasabah, mereka memiliki kemampuan untuk melakukan berbagai jenis transaksi keuangan dengan cepat melalui internet dan kemajuan dalam sistem informasi perbankan telah menghasilkan berbagai inovasi, salah satunya adalah Mobile Banking.[1] Mobile Banking ialah layanan perbankan yang bisa dipakai kapan saja dalam hitungan jam dan memungkinkan nasabah mengakses data keuangan dari bank melalui smartphone, ponsel, dan komputer mereka. Layanan transaksi termasuk pembayaran tagihan melalui internet, air, listrik, pulsa, tiket, dan informasi seperti mutasi rekening, saldo, dan suku bunga.

Bagi pelaku usaha skala besar yang menginginkan solusi hemat biaya, fleksibel, dan aman, mobile banking sangat membantu. Meski demikian, e-banking tidak diatur secara spesifik oleh peraturan apapun. Dengan demikian landasan penerapan mobile banking adalah UU No 10 Tahun 1998 terkait Perubahan Atas UU No 7 Tahun 1992 terkait Perbankan. Bank umum dapat memusatkan perhatian pada kegiatan tertentu ataupun memberi perhatian lebih atas bidang usaha tertentu, sesuai dengan ayat 2 Pasal 5 UU tersebut. Selain itu, selama tidak berlawanan atas peraturan perUUan ini atau peraturan perUUan lain yang ada, bank umum diperbolehkan melakukan kegiatan tambahan yang lazim dilakukan oleh bank, sesuai atas Pasal 6 Huruf A. Sebagaimana

[1] Cut Mutia and Rayyan Firdaus, "Analisis Penipuan Digital Teknik Phishing Terhadap Layanan Mobile Banking," *Jurnal Transformasi Bisnis Digital* 1, no. 4 (June 22, 2024): 05–10, https://doi.org/10.61132/jutrabidi.v1i4.191.

tercantum dalam ketentuan ini, bank diperbolehkan untuk mengadopsi sistem Mobile Banking selaras atas ketentuan yang ada.[2]

Faktanya, meskipun ada keuntungan juga ada kekurangan yaitu potensi ancaman kejahatan digital dalam bentuk serangan kejahatan siber. Menurut laporan terbaru perusahaan keamanan siber Kaspersky, dari Januari hingga Maret tahun ini, pihaknya berhasil memblokir 5.863.955 ancaman online, turun 23,37% dari 7.651.841 deteksi atas waktu yang sama tahun sebelumnya. Sebagian besar serangan siber ini ada saat pengguna mengunjungi situs web yang terinfeksi. Bahkan tanpa sepengetahuan pemakai, serangan terjadi. Metode ini, seperti malware atau Phising tanpa file. Malware ini mempunyai kode berbahaya yang mempertahankan diri dengan memakai langganan registri ataupun WMI, tidak meninggalkan apa pun guna analisis statis atas disk. Dengan menyeluruh, ancaman yang disebarkan melalui web menyerang 21,2 persen pengguna selama Q1 2024; ini memposisikan Indonesia atas peringkat ke-96 di dunia terkait hal ancaman penjelajahan web. Pengguna dalam negeri tetap menjadi sasaran penjahat siber. Pada tahun 2023, Kaspersky menemukan 97,226 deteksi ransomware, 16,4 juta insiden lokal, 11,7 juta serangan RDP, serta 97,465 serangan phishing finansial.[3]

Phishing ialah kejahatan peretasan yang berkembang selaras atas jalannya waktu pada bidang perbankan.[4] Phishing pada dasarnya adalah aktivitas ilegal di mana penjahat mengirim pesan elektronik dengan berpura-pura menjadi orang atau organisasi yang dapat diandalkan dalam upaya mendapatkan informasi pribadi. Teknik ini sering dikaitkan dengan strategi rekayasa sosial. Adalah ilegal bagi siapa pun untuk secara sengaja juga tanpa izin, ataupun melanggar hukum, mengakses komputer dan/atau sistem elektronik melalui teknik apa pun yang dapat menyebabkan pelanggaran, penetrasi, penghindaran, ataupun pembobolan sistem keamanan, selaras atas UU No 19 Tahun 2016. mengenai Perubahan Atas UU No 11 Tahun 2008 mengenai Informasi juga Transaksi Elektronik. Oleh sebab itu, phishing dikenal atas tindak pidana yang melawan hukum juga sesuai pasal ini diancam atas pidana penjara paling lama delapan tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah). Oleh karena itu, hal ini menunjukkan beratnya hukuman yang bisa dipakai guna mempertahankan integritas juga keamanan sistem elektronik atas pelanggaran contohnya phishing.

Atas banyak sudut pandang, phishing adalah permasalahan yang kompleks. Hal ini karena kepercayaan konsumen terhadap lembaga keuangan dan uang mereka mungkin terganggu akibat aktivitas phishing. Pelanggan yang tertipu penipuan phishing

---

[2] Ramadhanti Achlina Tri Putri Putri and Heru Sugiyono, "Tanggung Jawab Bank Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking (Studi : Kasus Phising Pada Pt . Bank Rakyat Indonesia (PERSERO) TBK)," *Jurnal Interpretasi Hukum* 4, no. 3 (2023): 682–90.

[3] CNN Indonesia, "Indonesia Digempur 6 Juta Ancaman Siber Di Awal 2024, Cek Modusnya," 2024, https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya.

[4] Alhuseen Omar Alsayed, "E-Banking Security: Internet Hacking, Phishing Attacks, Anlaysis and Prevention of Fraudelent Activities," *(International Journal of Emerging Technology and Advanced Engineering* 7, no. 1 (2017): 110.

berisiko kehilangan uangnya. Sebagai organisasi keuangan, bank mungkin mengalami masalah serius dengan reputasinya. Oleh karena itu, bank harus bertanggung jawab atas aktivitas phishing dan melindungi nasabahnya dari aktivitas tersebut. Konsekuensinya, penelitian ini mempunyai implikasi praktis yang penting dan krusial bagi pengembangan teori hukum. Hal ini akan meningkatkan kepercayaan konsumen terhadap layanan perbankan seluler dan membantu lembaga keuangan termasuk bank, badan pengatur, dan pengacara dalam melindungi klien dari meningkatnya ancaman phishing. Tujuan atas penelitian ini ialah guna menganalisis kewajiban bank saat memberikan kompensasi kepada konsumen yang kehilangan uang akibat penipuan link phishing pada mobile banking.

METODE PENELITIAN

Hukum normatif, yang mendefinisikan hukum atas apa yang terdapat pada UU atau peraturan yang menetapkan norma-norma perilaku manusia yang dapat diterima, merupakan metodologi kajian yang digunakan. Standar hukum saat ini dianalisis menggunakan metodologi penelitian ini. Dua metodologi penelitian yang dipakai ialah pendekatan konseptual (Conceptual Approach) juga pendekatan Undang-Undangan (Statute Approach). Dengan mengkaji peraturan perUUan terkait, pendekatan legislasi memberikan landasan hukum atas kewajiban bank untuk memberikan kompensasi kepada konsumen yang menderita kerugian akibat penipuan link phishing pada mobile banking. Teks hukum primer dan sekunder dimasukkan dalam repositori penelitian ini. UU No 8 Tahun 1999 terkait Perlindungan Konsumen, UU No 10 Tahun 1998 terkait Perubahan Atas UU No 7 Tahun 1992 terkait Perbankan, serta UU No 19 Tahun 2016 terkait Perubahan Atas UU No 11 Tahun 2008 terkait Informasi dan Transaksi Elektronik merupakan contoh naskah hukum primer. Buku, artikel, makalah, dan doktrin merupakan contoh bahan hukum sekunder. Konten ini menawarkan wawasan yang diperoleh dari pengetahuan khusus dan memfasilitasi analisis tambahan. Pengelompokan dokumen hukum berdasarkan rumusan masalah, sistematisasi, interpretasi, analisis, dan kesimpulan merupakan salah satu komponen analisis penelitian.

HASIL DAN PEMBAHASAN

1. Perlindungan Hukum Terhadap Nasabah Akibat Scam Melalui Link Phising Pada Mobile Banking

Perkembangan baru dalam layanan perbankan adalah transaksi elektronik seperti mobile banking, yang menghubungkan kebutuhan jasa keuangan dan kebutuhan nasabah dalam rangka percepatan layanan perbankan.[5] Namun seiring dengan kemajuan sektor jasa keuangan, bank juga harus menghadapi lebih banyak bahaya. Oleh sebab itu, POJK No. 12/POJK.03/2018 yang mengatur terkait bagaimana bank umum

[5] Mirza Yuniar Isnaeni Nasser Atorf, Agus Sugiarto, Irnal Fiscallutfi, "Internet Banking," *Manajemen Teknologi* 1 (2002): 10.

menerapkan layanan perbankan digital bertujuan untuk memotivasi bank guna mengutamakan manajemen risiko teknologi informasi. Oleh karena itu, guna menyelenggarakan layanan perbankan digital secara efisien, bank harus menyertakan kebijakan dan prosedur manajemen risiko teknologi informasi. Resiko-resiko disini disebutkan adalah Phising, phising merupakan salah satu jenis pelanggaran siber atau kejahatan siber yang terjadi pada platform digital perbankan, termasuk layangan mobile banking.

Modus ini biasanya melibatkan penggunaan tautan yang terlihat seperti benar yang dikirimkan melalui pesan singkat, email, atau media sosial, yang bertujuan untuk mencuri data pribadi, informasi keuangan, atau detail login pengguna. Dengan mengklik link tersebut, pelanggan seringkali secara tidak sadar memberikan informasi penting kepada penjahat siber yang dapat mengakses rekening bank mereka. Fenomena ini memiliki konsekuensi finansial dan psikologis yang signifikan, serta menimbulkan masalah dalam dunia hukum terkait perlindungan nasabah. Sementara itu, bank juga disemogakan guna mematuhi peraturan keamanan juga privasi tersebut.[6] Keamanan data pribadi nasabah juga sangat utama, terlebih pada sistem elektronik contohnya e-banking. Nasabah bank yang menggunakan mobile banking dapat terkena dampak negatif dari peretas keamanan. Ini didukung oleh modus kejahatan perbankan yang semakin canggih dan berkembang, salah satunya adalah phising.

Perlindungan informasi pribadi konsumen diatur dalam UU No 19 Tahun 2016 terkait Perubahan Atas UU No 11 Tahun 2008 yang didasarkan pada UU No 8 Tahun 1999 terkait Perlindungan Konsumen. Oleh sebab itu, konsumen secara hukum memiliki hak atas perlindungan informasi pribadi mereka, dan lembaga keuangan diwajibkan untuk melakukannya. Dalam situasi ini, phishing dapat dihindari dengan mengambil tindakan preventif dan represif. Sejumlah tindakan preventif dilakukan sebelum kejahatan terjadi guna melindungi nasabah bank yang menjadi korban phishing di sistem mobile banking Indonesia. Ini memberi klien nasihat dan informasi terkait hak-hak hukum mereka. Kenali hak dan tanggung jawab Anda sebagai nasabah di industri keuangan. Karena mereka ingin melindungi konsumen dan mendidik mereka terkait hak-hak mereka, termasuk hak guna dilindungi atas praktik berbahaya seperti phishing, bank diwajibkan untuk mendidik juga memberikan nasihat atas nasabah mereka terkait hak-hak mereka. Hal ini menyoroti betapa pentingnya mendidik klien mengenai hak-hak hukum mereka.

Bank dan pelaku usaha jasa keuangan lainnya wajib berdasarkan Pasal 9 POJK No. 1/POJK.07/2013 terkait Perlindungan Konsumen Sektor Jasa Keuangan untuk memberitahukan hak dan tanggung jawab nasabah. Hal ini mencakup pemberian informasi akurat kepada konsumen terkait keamanan akun, bahaya penggunaan layanan

[6] Herdian Ayu Andreana Beru Tarigan and Darminto Hartono Paulus, "Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital," *Jurnal Pembangunan Hukum Indonesia* 1, no. 3 (2019): 294–307, https://doi.org/10.14710/jphi.v1i3.294-307.

mobile banking, dan tindakan pencegahan yang mungkin mereka ambil. Memberikan informasi menyeluruh kepada klien membantu mereka memahami bahaya dan cara mempertahankan diri dari phishing. Akibatnya, hal ini menumbuhkan suasana yang lebih aman juga memotivasi klien guna menentukan tindakan pencegahan yang proaktif. Klausul ini juga memberikan klien cara yang sah untuk mendapatkan informasi dan perlindungan yang mereka perlukan saat memanfaatkan layanan keuangan. Selain itu, nasabah bank yang menjadi korban penipuan melalui tautan phishing di mobile banking terlindungi dari penindasan. [7]

Perlindungan dengan represif untuk nasabah bank yang memperoleh akibat scam melalui link phising pada mobile banking, melibatkan tindakan penyelesaian setelah terjadinya tindakan kejahatan.[8] Nasabah bank mempunyai hak untuk menyuarakan pendapatnya dan mengajukan pengaduan terhadap produk dan jasa yang digunakannya, sebagaimana tertuang dalam UU No 8 Tahun 1999 terkait Perlindungan Konsumen. Nasabah yang menjadi korban phishing berhak mengajukan pengaduan atas jasa keuangan yang diterimanya seperti tertulis atas Pasal 4 Huruf D. Bank juga pelaku korporasi lain di sektor jasa keuangan wajib mampu mengawasi sistem yang memberikan layanan dan solusi. kepada nasabah sebagaimana tercantum atas Pasal 32 POJK No. 1/POJK.07/2013 terkait Perlindungan Konsumen Sektor Jasa Keuangan. Hal ini memberikan ketenangan pikiran bagi klien bahwa masalah apa pun yang mereka hadapi akan ditangani secara efektif dan transparan.

Berdasarkan Pasal 39 dan 40 POJK No. 1/POJK.07/2013, Otoritas Jasa Keuangan (OJK) memberihak kepada nasabahnya untuk menyelesaikan perselisihannya baik di dalam ataupun di luar pengadilan jika nasabahnya tidak dapat mencapai kesepakatan. Konsumen yang mengalami pelanggaran layanan perbankan wajib mengajukan pengaduan ke OJK. OJK bisa bertindak atas perantara juga menentukan apakah terdapat pelanggaran yang nantinya ditindaklanjuti. Pelanggan dapat menangani pelanggaran phishing dengan berbagai cara berkat tindakan pencegahan ini. Mereka dapat menyelesaikannya dengan bank, dengan OJK atau lembaga pengatur keuangan lainnya, atau melalui sistem peradilan. [9] Oleh karena itu, nasabah bank yang yakin bahwa mereka telah dirugikan oleh phishing dalam sistem mobile banking berhak mendapatkan perlindungan hukum. Hak pelanggan untuk melaporkan phishing adalah salah satu perlindungan ini.

---

[7] Ahmad Jahri, "Perlindungan Nasabah Debitur atas Perjanjian Baku Yang Mengandung Klausula Eksonerasi di Bank Umum Di Bandarlampung," *FIAT JUSTISIA:Jurnal Ilmu Hukum* 10, no. 1 (2017): 125–48, https://doi.org/10.25041/fiatjustisia.v10no1.651.

[8] Anugrah I Kadek Duta, I Made Minggu Widyantara, and Desak Gde Dwi Arini, "Perlindungan Hukum atas Nasabah Bank Atas Tindak Pidana Pencatatan Palsu pada Dokumen Perbankan," *Preferensi Hukum* 3, no. 2 (2019): 294–99.

[9] Febbyanti Rahmadian, Muhammad Maksum, and Mara Sutan Rambe, "Perlindungan Nasabah Bank atas Tindakan Phishing Studi di PT Bank Rakyat Indonesia (Persero) Tbk," *JOURNAL of LEGAL RESEARCH* 2, no. 2 (2021): 351–72, https://doi.org/10.15408/jlr.v2i2.17933.

Konsumen mempunyai hak untuk menyampaikan keluhannya kepada bank atau lembaga keuangan yang bersangkutan dengan menggunakan forum mediasi keuangan. menggunakan prosedur penyelesaian sengketa alternatif yang memungkinkan bank dan konsumen mencapai penyelesaian tanpa harus melalui proses hukum yang berlarut-larut agar dapat menyelesaikan perselisihan di sektor perbankan dengan cepat, sederhana, dan terjangkau.[10] Selain itu, otoritas pengawas di sektor jasa keuangan (OJK) melindungi nasabah secara hukum. OJK memantau juga mengawasi aspek kelembagaan, produk, serta operasi, dan kehati-hatian. serta kejelasan terkait cara bank bekerja. OJK mengawasi bank dengan memahami bank yang bersangkutan, menilai risikonya, membuat strategi pemantauan berdasarkan risiko, memeriksa bank, dan secara teratur memverifikasi kondisi mereka. Langkah-langkah ini diambil guna memastikan bahwasanya bank beroperasi secara aman juga sesuai dengan peraturan.

2. Tanggung Jawab Bank Terhadap Nasabah Akibat Scam Melalui Link Phising Pada Mobile Banking

Kepercayaan nasabah sangat penting bagi perbankan. Phishing merupakan salah satu jenis kejahatan yang dapat membahayakan keamanan simpanan nasabah di industri perbankan. Selain itu, upaya bank untuk mempertahankan citranya dan memenangkan hati nasabah mungkin terhambat oleh risiko keamanan ini. Menjaga hubungan positif antara bank dan nasabahnya sangat bergantung pada rasa aman dan kepercayaan mereka. Bank harus mengambil langkah-langkah untuk mencegah dan mengatasi phishing guna menjaga keamanan dan mengurangi risiko yang dapat membahayakan nasabah. Menjaga keamanan memerlukan penerapan teknologi keamanan mutakhir, bersikap transparan, dan mengajari klien terkait prosedur keamanan. Sudah menjadi tugas bank untuk membela nasabahnya baik secara represif maupun preventif. Salah satu tugas pencegahannya adalah menerapkan kebijakan untuk menghentikan phishing. Konsumen menerima informasi terkait bahaya phishing dan cara mempertahankan diri terhadap bahaya tersebut. Menangani dan menyelesaikan masalah setelah serangan phishing adalah salah satu tugas represif mereka jika mereka menjadi korbannya.

Salah satu contoh tugas preventif bank adalah dengan menggunakan media sosial, khususnya Twitter, dan mengirimkan email berulang kepada konsumen yang memberitahukan mereka terkait keamanan transaksi mobile banking. Hal ini ialah satu diantara langkah yang dilaksanakan bank guna membuat transaksi mobile banking lebih aman. Selain itu, bank terus memberikan waktu, ruang, dan kesempatan kepada kliennya untuk menghubungi mereka secara pribadi jika mereka memiliki pertanyaan atau kekhawatiran mengenai layanan mobile banking. Dalam setiap aspek operasional bisnisnya, bank memberikan pertimbangan yang cermat terhadap manajemen risiko. Hal ini mencakup penggunaan teknik manajemen risiko serta efisiensi tugas manajemen yang dilakukan secara rutin sesuai dengan spesifikasi. Pengendalian Risiko Secara

[10] David Y. Wonok, "Perlindungan Hukum terkait Hak-Hak Nasabah atas Konsumen pemakai Jasa Bank atas Risiko Yang ada pada Penyimpangan Dana," *Jurnal Hukum Unsrat* 1, no. 2 (2013): 60.

Menyeluruh Manajemen risiko teknologi informasi yang efektif diperlukan karena adanya kebijakan, kemajuan teknis, dan ketersediaan mobile banking. Pedoman ini berisi panduan dan pengamanan yang diperlukan untuk menerapkan manajemen risiko teknologi informasi.[11]

Bank menyatakan bahwa serangan phising juga dapat disebabkan oleh kelalaian nasabah, yang mencakup tindakan oleh nasabah yang menciptakan celah untuk serangan phishing. Bank menyarankan agar dalam proses memberikan tanggung jawab secara represif, guna mencegah laporan yang serupa terulang juga memastikan prosedur pengaduan berjalan lancar, nasabah yang mengajukan pengaduan tidak mengajukan laporan lebih dari satu kali. Jika hasil penyelidikan menunjukkan bahwa kejadian phishing tersebut merupakan akibat dari kecerobohan konsumen, maka nasabah bertanggung jawab penuh. Karena dianggap berada di luar kendali bank, jadi bank tidak memberi ganti rugi kepada nasabah. Menurut UU No 19 Tahun 2016 terkait ITE, persepsi nasabah tentang keamanan juga kenyamanan layanan perbankan digital, contohnya mobile banking, dipengaruhi.[12] Sebaliknya, pelanggan juga memiliki tanggung jawab untuk menjaga keamanan data mereka dan menghindari mengungkapkan informasi sensitif kepada pihak yang tidak bertanggung jawab. Menurut Pasal 26 UU ITE (Informasi dan Transaksi Elektronik), pelanggan memiliki alasan hukum untuk tidak membayar kerugian jika mereka membuat kesalahan atau tidak menginformasikan data mereka kepada pihak yang tidak bertanggung jawab.

Nasabah dapat menuntut bank jika terjadi kasus phising dan bank dianggap tidak melindungi data atau sistem keamanannya agar mudah ditembus. Pertanggungjawaban ini biasanya memerlukan bukti bahwa bank tidak menerapkan protokol keamanan yang cukup atau gagal memberi tahu pelanggan terkait bahaya phising. Bank harus melengkapi dengan teknologi anti-phising yang dapat mengurangi serangan siber, dan mereka juga harus secara teratur mengajarkan pelanggan mereka bagaimana menghindari jebakan phising. Kampanye digital, peringatan, dan panduan keamanan di aplikasi dan situs web bank dapat menjadi contoh pendidikan digital. Dengan langkah-langkah ini, bank menunjukkan bahwa mereka telah berusaha untuk menghindari pelanggaran siber dan melindungi klien mereka.[13] Bank sangat bertanggung jawab untuk melindungi data pelanggan, terutama karena layanan mobile banking semakin populer. Berdasarkan Pasal 29 UU No 21 Tahun 2011 terkait Otoritas Jasa Keuangan, bank dikenakan tanggung jawab untuk memastikan bahwa informasi pelanggan tetap aman. Bank harus menggunakan teknologi seperti autentikasi berlapis, enkripsi data, dan notifikasi keamanan untuk mengidentifikasi aktivitas yang mencurigakan untuk melindungi data nasabah mereka.

---

[11] "PT BRI Multifinance Indonesia," 2023.

[12] Kadek Yogi Pratama Putra, A Agung Sagung Laksmi Dewi, and Luh Putu Suryani, "Perlindungan Hukum Korban Penipuan Undian Berhadiah sesuai UU No 11 Tahun 2008 mengenai Informasi juga Transaksi Elektronik," *Jurnal Interpretasi Hukum* 2, no. 3 (2021): 673–77, https://doi.org/10.22225/juinhum.2.3.4195.673-677.

[13] Alfred Yetno, Kata Kunci, and Keamanan Kerahasiaan, "Tanggung Jawab Bank saat Menjaga Keamanan juga Kerahasiaan Data Nasabah Perbankan Di Indonesia" 10, no. 1 (2024): 67–76.

KESIMPULAN

Melalui upaya preventif dan represif, nasabah yang menjadi korban upaya penipuan melalui URL phishing di mobile banking dilindungi secara hukum. Memahami hak-hak konsumen dan menghindari phishing merupakan contoh upaya preventif, sedangkan mengadu ke OJK dan menyelesaikan konflik di luar pengadilan merupakan contoh upaya represif. Konsumen berhak secara hukum atas perlindungan konsumen. UU No 8 Tahun 1999 terkait Perlindungan Konsumen juga UU No 19 Tahun 2016 terkait Perubahan UU No 11 Tahun 2008 mengatur perlindungan data pribadi nasabah, memberikan landasan hukum untuk melindungi nasabah dari phishing. Oleh karena itu, nasabah berhak secara hukum atas privasi data mereka, dan lembaga keuangan diharuskan untuk memastikan hal itu. Dalam sistem pembayaran mobile banking, bank bertugas untuk menjaga dan memerangi penipuan phishing. Nasabah terlebih dahulu dididik terkait bahaya phishing dan cara membela diri terhadap serangan tersebut. Nasabah yang menjadi korban serangan phishing juga diberi kewajiban yang bersifat represif. Ini meliputi tahapan guna menangani juga memperbaiki permasalahan sesudah serangan phishing. Peningkatan manajemen risiko, keamanan teknologi informasi, serta layanan pengaduan pelanggan atas pusat kontak juga media sosial semuanya mendukung hal ini. Jika konsumen kehilangan uang akibat phishing, bank diharuskan untuk mengganti kerugian mereka. Jika tidak, klien dapat mengajukan gugatan terhadap bank di pengadilan jika tanggapan bank terhadap kasus phishing tidak memenuhi harapan mereka. Nasabah juga dapat mendaftarkan pengaduan ke OJK apabila mereka merasa penanganan atas bank tidak memadai. OJK bisa mempercepat prosedur pengaduan klien untuk kerusakan mengenai phishing. Akibatnya, bank menggunakan tindakan pencegahan dan hukuman. Mereka juga bertanggung jawab untuk memastikan bahwa perbankan seluler aman dan mengelola insiden phishing.

DAFTAR PUSTAKA

"Keamanan E-Banking: Peretasan Internet, Serangan Phishing, Analisis dan Pencegahan Aktivitas Penipuan," oleh Alsayed dan Alhuseen Omar. (Jurnal Internasional Teknik Lanjutan dan Teknologi Baru, 7, no. 1 (2017): 110).

"Analisis Teknik Penipuan Digital Phishing pada Layanan Mobile Banking" oleh Cut Mutia dan Rayyan Firdaus. 22 Juni 2024, Jurnal Transformasi Bisnis Digital 1, no. 4: 05–10. https://doi.org/10.61132/jutrabidi.v1i4.191.

Perlindungan Hukum Hak Nasabah Sebagai Pengguna Jasa Bank Terhadap Risiko Terkait Pencurian Dana, David Y. Wonok. Jurnal Hukum Unsrat 1, no. 2 (2013): 60.

Desak Gde, I Made Minggu Widyantara, Duta, dan Anugrah I Kadek Pembelaan Hukum Nasabah Bank Terhadap Tindak Pidana Pencatatan Palsu dalam Dokumen Perbankan, Dwi Arini. 294–99 dalam UU Preferensi 3, no. 2 (2019).

CNN, Indonesia. "Cek Modusnya: 6 Juta Ancaman Siber Menghantam Indonesia di Awal 2024." 2024. Cek Modusnya: https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-diserang-oleh-6-juta-ancaman-siber-di-awal-2024.

Jahri, Ahmad. "Perlindungan Nasabah Debitur Bank Umum di Bandarlampung Terhadap Perjanjian Baku yang Memuat Klausul Pembebasan." Jurnal Ilmu Hukum, FIAT JUSTISIA, 10, no. 1 (2017): 125–48. https://doi.org/10.25041/fiatjustisia.v10no1.651.

Mirza Yuniar Isnaeni, Agus Sugiarto, Irnal Fiscallutfi, dan Nasser Atorf. Manajemen Teknologi 1 (2002): 10. "Internet Banking."

Tahun 2023 "PT BRI Multifinance Indonesia."

Kadek dan Putra Luh Putu Suryani, A Agung Sagung Laksmi Dewi, dan Yogi Pratama. "Perlindungan Hukum Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Bagi Korban Penipuan Pengundian Hadiah." Jurnal Interpretasi Hukum, Volume 2, Edisi 3, 2021: 673–77. .2.3.4195.673-

677 https://doi.org/10.22225/juinhum.

Ramadhanti Putri Achlina "Tanggung Jawab Bank Atas Aksi Phishing Pada Sistem E-Banking (Studi : Kasus Phishing Pada PT Bank Rakyat Indonesia (PERSERO) TBK)" oleh Tri Putri dan Heru Sugiyono. Jurnal Interpretasi Hukum edisi ke-4 (2023): 682–90.

Muhammad Maksum, Rahmadian, Mara Sutan Rambe, dan Febbyanti. "Investigasi Perlindungan Nasabah Bank dari Aktivitas Phishing di PT Bank Rakyat Indonesia (Persero) Tbk." Jurnal Penelitian Hukum 2, no. 2 (2021): 351–72. https://doi.org/10.15408/jlr.v2i2.17933.

Herdian Tarigan Darminto Hartono Paulus dan Ayu Andreana Beru. "Melindungi Hak Hukum Konsumen sekaligus Menawarkan Layanan Perbankan Digital." 1, tidak. 3 (2019): 294–307, Jurnal Perkembangan Hukum Indonesia. https://doi.org/10.14710/jphi.v1i3.294-307.

Alfred Yetno, "Tanggung Jawab Bank Dalam Menjaga Keamanan dan Kerahasiaan Data Nasabah Perbankan di Indonesia" 10, no. 1 (2024): 67–76. Kata Kunci dan Keamanan Kerahasiaan.