Locus: Jurnal Konsep Ilmu Hukum
E-ISSN : 2809-9265
Volume 5, Nomor 3, December 2025

Pertanggungjawaban Bank Terhadap Kerugian Nasabah Akibat Pencurian Dana Melalui *Phising*

[a,*]Ni Putu Julietta Maheswari Putri Widjana, [b.]Putu Eva Ditayani Antari, [c.]I Gede Agus Kurniawan, [d.]Bagus Gede Ari Rama.

[a.b.c.d.] Fakultas Hukum, Universitas Pendidikan Nasional.
[*]*corresponding author, email: liettaputri@gmail.com*

https://doi.org/10.56128/jkih.v5i3.649

A B S T R A K

Penelitian ini membahas pertanggungjawaban bank terhadap kerugian nasabah akibat pencurian dana melalui phishing sebagai bentuk kejahatan siber di sektor perbankan. Tujuan penelitian adalah untuk menganalisis pengaturan hukum mengenai perlindungan data pribadi nasabah dan tanggung jawab bank dalam kasus pencurian dana. Metode yang digunakan adalah yuridis normatif dengan pendekatan peraturan perundang-undangan, seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan POJK No.12/POJK.03/2018.Hasil penelitian menunjukkan bahwa pengaturan mengenai perlindungan data pribadi masih bersifat umum dan belum mengatur secara tegas batas tanggung jawab antara bank dan nasabah. Tanggung jawab bank bersifat relatif, bergantung pada letak kelalaian yang menyebabkan kerugian. Oleh karena itu, diperlukan pembaruan regulasi dan peningkatan literasi digital guna menciptakan perlindungan hukum yang seimbang di era perbankan digital.

Kata kunci: Pertanggungjawaban Bank, *Phishing*, Data Pribadi, Perlindungan Hukum, Perbankan Digital.

A B S T R A C T

This study discusses the bank's responsibility for customer losses resulting from fund theft through phishing as a form of cybercrime in the banking sector. The purpose of this research is to analyze the legal regulation of customer personal data protection and the bank's liability in cases of fund theft. The research method used is a normative juridical approach, referring to legal instruments such as Law Number 10 of 1998 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, and OJK Regulation No.12/POJK.03/2018. The results show that the regulation regarding personal data protection remains general and does not clearly define the boundaries of liability between banks and customers. The bank's liability is relative, depending on the degree of negligence causing the loss. Therefore, regulatory reform and improved digital literacy are needed to create balanced legal protection in the digital banking era.

***Keywords**: Bank Liability, Phishing, Personal Data, Legal Protection, Digital Banking.*

Article History
Received: November 14, 2025 --- **Revised**: November 21- December 15, 2025 --- **Accepted**: December 17, 2025

1. Pendahuluan

Evolusi teknologi menghadirkan dampak ganda, yakni sisi positif dan negatif yang berjalan beriringan. Di satu sisi, teknologi menyajikan berbagai kemudahan yang signifikan dalam aktivitas sehari-hari, seperti komunikasi, transaksi komersial, dan berbagai kegiatan lainnya. Manfaat ini telah mendorong masyarakat modern ke tingkat

ISSN 2809-9265 **Locus: Jurnal Konsep Ilmu Hukum**
Vol.5, No.3, December 2025, 451-459

ketergantungan yang semakin tinggi terhadap teknologi. Namun, di sisi lain, kemudahan yang sama juga membuka celah bagi munculnya dampak negatif, terutama dalam bentuk aktivitas kriminal yang memanfaatkan teknologi sebagai instrumen utamanya (Antari, 2022).

Salah satu manifestasi konkret dari penyalahgunaan teknologi ini adalah merebaknya kejahatan siber (*cybercrime*). Spektrumnya luas, mencakup pencurian identitas dan data pribadi, berbagai modus penipuan yang dilakukan secara daring (*online*), hingga pembobolan sistem krusial seperti perbankan. Modus operandi kejahatan ini terus berkembang, menjadi semakin kompleks, canggih, dan sulit untuk dilacak. Data dari berbagai laporan menunjukkan bahwa insiden peretasan dan pencurian data elektronik mengalami eskalasi yang konsisten dari tahun ke tahun. Tren ini menjadi sebuah indikator bahwa kerangka kerja preventif dan represif yang ada saat ini, yang diterapkan oleh negara, kemungkinan besar belum beroperasi secara optimal untuk membendung ancaman tersebut (Firdaus, 2022).

Pada aspek konteks perbankan, hubungan antara nasabah dan bank dilandasi oleh kepercayaan, di mana nasabah mengharapkan adanya jaminan atas tiga aspek utama: keamanan dana, kemudahan layanan, dan kepastian hukum atas seluruh aktivitas transaksinya. Ketika terjadi insiden seperti kegagalan sistem, kebocoran data, atau bentuk kejahatan digital misalnya pencurian dana yang dimediasi oleh manipulasi data pribadi secara elektronik insiden tersebut berpotensi besar menimbulkan kerugian substansial bagi nasabah. Padahal, nasabah adalah pihak yang seharusnya memperoleh perlindungan hukum secara penuh (Sindy Ariyaningsih, et.all, 2023). Oleh karena itu, berbagai instrumen hukum, mulai dari Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, hingga yang terbaru Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, menjadi fondasi yuridis untuk mengukur dan menetapkan tanggung jawab pihak bank saat terjadi pelanggaran yang merugikan nasabah.

Di antara berbagai jenis kejahatan siber, *Phising* (pengelabuan) merupakan salah satu ancaman yang paling sering dihadapi oleh nasabah perbankan. Kejahatan ini secara spesifik menggunakan teknik manipulasi psikologis atau rekayasa sosial (*social engineering*) dengan tujuan untuk mengelabui korban agar menyerahkan data-data pribadi mereka secara tidak sah. Data kredensial yang diperoleh pelaku kemudian digunakan untuk mengambil alih akses ke rekening nasabah, yang pada akhirnya berujung pada kerugian finansial yang signifikan. Padahal, industri perbankan memiliki kewajiban fundamental untuk beroperasi berdasarkan prinsip kehati-hatian. Sebagaimana diamanatkan dalam Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, khususnya pada Pasal 29 Ayat (2), bank "wajib memelihara Tingkat Kesehatan bank sesuai dengan ketentuan kecukupan modal, kualitas asset, kualitas manajemen, likuiditas, rentabilitas, solvabilitas, dan aspek lain yang berhubungan dengan usaha bank, wajib melakukan kegiatan usaha sesuai dengan prinsip kehati-hatian".

Sebagai langkah mitigasi risiko di era digital, Peraturan Otoritas Jasa Keuangan (POJK) No.12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum telah menetapkan kewajiban bagi perbankan. Regulasi ini mengharuskan bank untuk mengimplementasikan manajemen risiko secara ketat, menjamin keamanan serta kerahasiaan data nasabah, dan menyediakan mekanisme perlindungan yang bersifat preventif maupun represif.

Perlindungan tersebut mencakup beberapa elemen penting, seperti transparansi informasi produk dan layanan, pengamanan data yang kuat, ketersediaan mekanisme pengaduan yang efektif, hingga proses pemberian ganti rugi bagi nasabah yang terdampak (Herdian Ayu Andreana Beru Tarigan, 2019). Meskipun demikian, tantangan di lapangan masih tetap ada. Hingga kini, belum ada satu ketentuan hukum yang secara eksplisit dan tegas membatasi tanggung jawab antara bank dan nasabah ketika terjadi kasus kejahatan siber spesifik seperti *phising*. Ketiadaan demarkasi yang jelas ini mengakibatkan munculnya kekaburan norma (norma kabur) dalam implementasinya di ranah hukum. Mandat dalam Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan pada Pasal 29 Ayat (2) dinilai masih bersifat terlalu umum dan tidak memberikan penjelasan rinci mengenai batasan tanggung jawab bank atas kerugian nasabah yang disebabkan oleh serangan *phising*.

Ironisnya, pada tahun 2024, tingkat adopsi atau melek teknologi di Indonesia telah mencapai angka 79,5% dari total populasi. Namun, tingginya angka adopsi ini tidak diimbangi dengan edukasi yang memadai mengenai penggunaan teknologi yang aman, baik, dan benar. Kesenjangan antara adopsi dan edukasi inilah yang diyakini menjadi salah satu faktor utama suburnya praktik *Phising* di Indonesia (Soffa Zahara, et.all, 2024).

Fakta ini didukung oleh data laporan dari Indonesia *Anti-Phishing Data Exchange* (IDADX), yang mencatat tren *phising* di Indonesia menunjukkan peningkatan pada level yang mengkhawatirkan. Tercatat, jumlah laporan kasus melonjak secara drastis dari 3.180 kasus pada tahun 2022 menjadi 26.675 kasus pada tahun 2023.

Sebuah fenomena relevan yang menyoroti kompleksitas masalah ini adalah kasus hilangnya dana milik Perseroan Terbatas Varash Saddan Nusantara (PT VSN) senilai Rp1,8 miliar pada tahun 2025, yang tersimpan di Bank Rakyat Indonesia (BRI). Dalam kasus ini, pihak bank secara tegas menyatakan bahwa kerugian yang dialami nasabah tidak bersumber dari kegagalan sistem internal perbankan. Sebaliknya, BRI mengidentifikasi penyebabnya adalah adanya peretasan (*hacking*) terhadap *server* yang dimiliki oleh nasabah (PT VSN) sendiri. Pelaku kejahatan kemudian memanfaatkan akses ilegal tersebut untuk melakukan pencurian data dan akhirnya pencurian dana secara elektronik. Kasus ini menjadi preseden penting yang menunjukkan bahwa, sekalipun sistem bank diklaim aman, nasabah sebagai pengguna tetap berada dalam posisi rentan terhadap serangan siber. Peristiwa ini secara langsung memicu perdebatan hukum mengenai seberapa jauh batasan pertanggungjawaban hukum yang dimiliki bank atas kerugian yang diderita nasabah dalam situasi semacam itu.

ISSN 2809-9265 **Locus: Jurnal Konsep Ilmu Hukum**
Vol.5, No.3, December 2025, 451-459

Berdasarkan klarifikasi resmi dari pihak BRI, yang juga diberitakan oleh radarbali jawapos, insiden ini menjadi viral di media sosial. Pihak bank menegaskan bahwa hilangnya dana tersebut tidak dipicu oleh gangguan atau celah keamanan pada sistem BRI. Investigasi internal bank menemukan fakta bahwa transaksi finansial tersebut dieksekusi secara sah, artinya menggunakan *username* dan *password* resmi milik nasabah (PT VSN). Lebih lanjut, transaksi tersebut berasal dari alamat IP yang terdaftar sebagai IP publik milik perusahaan tersebut. Dengan demikian, BRI menyimpulkan bahwa telah terjadi penyusupan pada *server* internal PT VSN. Atas dasar temuan ini, BRI menegaskan pendiriannya bahwa tanggung jawab penggantian kerugian oleh bank hanya berlaku apabila terbukti kesalahan atau kelalaian berasal dari sistem perbankan, dan bukan akibat dari kelalaian di sisi nasabah.

2. Metode

Penelitian ini adalah penelitian yuridis normatif dengan fokus pada analisis regulasi sektor perbankan terkait perlindungan data pribadi dan pertanggungjawaban bank dalam kasus *phising*. Data dikumpulkan melalui studi kepustakaan yang mencakup bahan hukum primer berupa UUD 1945, regulasi perbankan, dan Peraturan OJK, serta bahan hukum sekunder seperti jurnal ilmiah, buku, laporan lembaga terkait, dan publikasi berita. Analisis dilakukan dengan pendekatan perundang-undangan untuk menilai keselarasan regulasi dan pendekatan konseptual untuk mengkaji teori tanggung jawab hukum, perlindungan hukum, dan prinsip kehati-hatian perbankan. Seluruh bahan hukum dianalisis secara kualitatif dengan teknik deskriptif-analitis dan interpretatif guna menafsirkan norma yang ambigu, khususnya terkait batas pertanggungjawaban bank atas kerugian nasabah akibat *phising*, dengan studi kasus hilangnya dana PT Varash Saddan Nusantara di BRI sebagai konteks analisis.

3. Hasil & Pembahasan

3.1. Regulasi Perlindungan Data Pribadi Pada Perbankan

Transformasi digital telah mengubah secara fundamental sistem pelayanan perbankan di Indonesia, menggeser proses transaksi dari metode konvensional ke platform digital yang memungkinkan aktivitas perbankan kapan saja dan di mana saja. Kendati demikian, modernisasi ini membawa konsekuensi negatif berupa peningkatan risiko tindak pidana yang memanfaatkan teknologi sebagai sarananya (Antari, 2022). Salah satu risiko terbesar adalah terbukanya peluang bagi kejahatan siber seperti *phishing*, yang didefinisikan sebagai metode pencurian data pribadi melalui rekayasa sosial atau manipulasi psikologis.

Berdasarkan perspektif yuridis, akuisisi data pribadi nasabah secara ilegal merupakan pelanggaran langsung terhadap hak privasi, sebuah prinsip yang kini dikukuhkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 2 Undang-Undang Perlindungan Data Pribadi secara eksplisit memberikan hak kepada setiap individu atas proteksi data miliknya, dan mewajibkan pihak manapun yang

memproses data untuk mendapatkan persetujuan. Dalam ekosistem perbankan, data seperti nama, nomor rekening, dan kredensial *login* dikategorikan sebagai data pribadi sensitif, sehingga bank memiliki kewajiban hukum mutlak untuk melindungi kerahasiaannya.

Landasan hukum ini diperkuat oleh regulasi sektoral yang lebih dulu ada, yakni Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Secara spesifik, Pasal 40 ayat (1) Undang-Undang Perbankan memberlakukan larangan bagi bank untuk memberikan informasi yang tercatat pada rekening nasabah kepada pihak ketiga, kecuali dalam kondisi yang diatur secara ketat oleh undang-undang. Ini menegaskan bahwa bank memegang tanggung jawab hukum penuh untuk memproteksi data nasabah, baik dari ancaman internal maupun serangan siber eksternal.

Akan tetapi, realitas di lapangan menunjukkan bahwa insiden kebocoran dan pencurian data nasabah masih marak terjadi. Data dari Indonesia *Anti-Phishing Data Exchange* (IDADX) mengilustrasikan urgensi masalah ini, dengan lonjakan laporan serangan *phishing* dari 6.106 kasus pada kuartal IV 2022 menjadi 26.675 kasus pada kuartal I 2023. Keterlibatan institusi keuangan, termasuk perbankan, dalam insiden-insiden ini mengindikasikan adanya kelemahan dalam sistem keamanan untuk mencegah serangan siber atau penyalahgunaan data (Dahlan & Hasan, 2025).

Lonjakan kasus peretasan dan pencurian data elektronik ini, seperti yang diamati (Firdaus, 2022), menjadi sinyal bahwa mekanisme preventif dan represif dari negara belum beroperasi secara optimal. Minimnya upaya ini menjadi salah satu faktor pendorong maraknya kejahatan siber. Di sisi lain, faktor dari masyarakat juga berkontribusi (Soffa Zahara, et.all, 2024) menyoroti bahwa rendahnya tingkat literasi digital di Indonesia menjadi penyebab utama kerentanan terhadap *phising*, karena banyak pengguna belum mampu mengidentifikasi tautan palsu atau situs resmi.

Terkait dengan tinjauan hukum positif, kerangka regulasi yang mengatur perlindungan data nasabah dalam transaksi perbankan digital masih terfragmentasi di berbagai peraturan, seperti Undang-Undang Perbankan, Undang-Undang Perlindungan Data Pribadi, dan POJK No.12/POJK.03/2018. Permasalahan utamanya adalah belum tersedianya satu regulasi yang secara komprehensif dan terpadu mengatur mekanisme pertanggungjawaban serta penyelesaian sengketa ketika pencurian data mengakibatkan kerugian finansial. Kondisi ini menciptakan adanya kekosongan norma (*legal vacuum*) yang berimplikasi pada ketidakpastian hukum. Dengan kata lain, meskipun secara normatif pengaturan telah ada, sifatnya masih parsial dan belum terintegrasi. Oleh karena itu, mendesak diperlukan adanya harmonisasi regulasi antara undang-undang sektor perbankan dan perlindungan data pribadi agar bank dan nasabah memiliki pedoman yang jelas.

3.2. Tanggung Jawab Bank terhadap Kerugian Nasabah Akibat Phising

Bank berbeda dengan lembaga keuangan *non-bank* karena hanya bank yang diberi kewenangan hukum untuk menghimpun dana masyarakat dalam bentuk simpanan. Lembaga keuangan lain seperti perusahaan asuransi, *leasing*, atau dana pensiun tidak

ISSN 2809-9265 **Locus: Jurnal Konsep Ilmu Hukum**
Vol.5, No.3, December 2025, 451-459

memiliki fungsi penghimpunan dana publik, sehingga standar pengawasan dan prinsip kehati-hatian yang dikenakan kepada bank jauh lebih ketat (Fadlan, 2022)

Bank secara yuridis adalah lembaga keuangan yang memiliki fungsi utama menghimpun dan menyalurkan dana masyarakat sebagaimana diatur dalam Pasal 1 angka 2 Undang-Undang Nomor 10 Tahun 1998. Bank tidak hanya berperan sebagai tempat penyimpanan dana, tetapi juga sebagai lembaga intermediasi yang menjalankan berbagai kegiatan usaha seperti menghimpun dana (*funding*), menyalurkan dana (*lending*), serta menyediakan jasa-jasa perbankan termasuk layanan digital. (Anwar, 2022)

Seseorang dikatakan secara hukum bertanggung jawab untuk suatu perbuatan tertentu adalah bahwa dia dapat dikenakan suatu sanksi dalam kasus perbuatan yang berlawanan. Normalnya, dalam kasus sanksi dikenakan terhadap pelaku adalah karena perbuatannya sendiri yang membuat orang tersebut harus bertanggung jawab (Ridwan HR, 2016). *Phishing* secara konseptual adalah bentuk kejahatan siber yang menyasar pengguna layanan digital melalui teknik penipuan, dengan tujuan akhir membuat korban secara sukarela menyerahkan data kredensial rahasia (seperti nomor kartu, PIN, atau sandi). Dalam konteks perbankan, data yang diperoleh pelaku ini dieksploitasi untuk mengakses rekening korban dan melakukan transfer dana secara ilegal. Fenomena pencurian dana melalui metode ini telah memunculkan isu hukum yang kompleks dalam industri perbankan modern. Kerugian nasabah dapat berupa kerugian materiil dan immateriil yang disebabkan oleh kesalahan sistem, kelalaian bank, atau tindak melawan hukum melalui akses digital (Putra, 2020).

Apabila terjadi pencurian dana melalui teknik phising, bank tetap memiliki kewajiban untuk membuktikan bahwa sistem yang digunakan telah menerapkan prinsip kehati-hatian secara optimal. Hal ini sejalan dengan pandangan Munir Fuady yang menyatakan bahwa "Tanggung jawab lembaga keuangan tidak hanya terbatas pada pengelolaan dana secara sehat, tetapi juga pada kewajiban melindungi kepentingan nasabah dari risiko sistemik dan risiko teknologi informasi termasuk dengan kejahatan *phising*. (Fuady, 2013)

Kewajiban bank untuk beroperasi berdasarkan prinsip kehati-hatian (*prudential principle*) merupakan amanat sentral dari Pasal 29 ayat (2) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Prinsip ini secara inheren mewajibkan bank untuk mengimplementasikan manajemen risiko dan sistem keamanan data yang memadai guna melindungi kepentingan nasabah. Wujud perlindungan ini mencakup transparansi informasi, jaminan keamanan data, mekanisme penanganan pengaduan, hingga penyediaan ganti rugi bagi nasabah yang dirugikan (Tarigan, 2019).

Tanggung jawab ini diperjelas lebih lanjut dalam Peraturan Otoritas Jasa Keuangan (POJK) No.12/POJK.03/2018. Regulasi ini secara spesifik mewajibkan penyelenggara layanan perbankan digital untuk menjamin keamanan sistem, menjaga kerahasiaan data nasabah, dan memiliki mekanisme pengaduan yang siap menangani kerugian akibat kegagalan sistem. Konsekuensi logisnya adalah, apabila dapat dibuktikan bahwa pencurian

dana terjadi akibat adanya kelemahan pada sistem keamanan internal bank, maka bank dapat dimintai pertanggungjawaban hukum.

Meskipun demikian, dalam implementasinya, tidak semua kerugian akibat *phishing* secara otomatis menjadi beban bank. Kasus antara Perseroan Terbatas Varash Saddan Nusantara (PT VSN) dan Bank Rakyat Indonesia (BRI) pada tahun 2025 menjadi contoh nyata. Dalam insiden tersebut, dana sebesar Rp1,8 miliar milik PT VSN hilang setelah *server* internal perusahaan tersebut disusupi oleh peretas. Investigasi mengungkap fakta krusial: transaksi pengalihan dana dieksekusi menggunakan *username* dan *password* yang sah milik nasabah, serta berasal dari alamat IP publik yang terdaftar atas nama perusahaan (Radarbali.jawapos.com, n.d.). Berdasarkan temuan ini, BRI mengambil sikap bahwa tanggung jawab penggantian kerugian oleh bank hanya timbul jika kesalahan terbukti berasal dari sistem perbankan, dan bukan karena kelalaian yang terjadi di pihak nasabah.

Situasi ini menyoroti adanya benturan ekspektasi. Nasabah, dalam praktiknya, menyerahkan dana mereka kepada bank dengan landasan kepercayaan penuh akan jaminan keamanan, kemudahan layanan, dan kepastian hukum. Oleh karena itu, ketika terjadi insiden yang merugikan baik itu kegagalan sistem, kebocoran data, atau pencurian dana melalui manipulasi elektronik hal tersebut mencederai rasa aman nasabah yang seharusnya dilindungi oleh hukum (Sindy Ariyaningsih, et.all, 2023).

Dari sudut pandang hukum perdata, relasi antara bank dan nasabah adalah hubungan kontraktual yang melahirkan hak serta kewajiban timbal balik. Tanggung jawab bank dapat dikategorikan sebagai tanggung jawab kontraktual. Jika bank terbukti gagal memberikan perlindungan sesuai yang diperjanjikan atau diamanatkan regulasi, bank dapat digugat atas dasar wanprestasi untuk memberikan ganti rugi, sebagaimana diatur dalam Pasal 1243 KUHPerdata. Sebaliknya, jika kerugian terbukti timbul akibat kesalahan atau kelalaian nasabah, maka tanggung jawab bank secara hukum menjadi terbatas.

Secara tanggung jawab hukum, bank juga terikat oleh tanggung jawab moral dan sosial yang diwujudkan melalui penerapan prinsip *Good Corporate Governance* (GCG). Prinsip GCG menuntut bank untuk selalu bertindak secara transparan, akuntabel, dan bertanggung jawab dalam setiap kebijakan yang berdampak pada nasabah. Implementasi GCG yang konsisten sangat esensial untuk memperkuat kepercayaan publik terhadap lembaga perbankan sekaligus mencegah penyalahgunaan wewenang internal.

Berdasarkan analisis tersebut, dapat ditarik kesimpulan bahwa konstruksi tanggung jawab bank atas kerugian nasabah akibat *phishing* pada dasarnya bersifat kondisional dan proporsional. Bank diwajibkan bertanggung jawab penuh jika kerugian terbukti timbul dari kelemahan sistem atau kegagalan pengawasan internal bank. Akan tetapi, jika kerugian terjadi murni karena kelalaian nasabah, tanggung jawab hukum akan beralih kepada nasabah itu sendiri. Untuk ke depannya, sangat diperlukan pembaruan regulasi yang lebih tegas dan komprehensif untuk mengatur pembagian tanggung jawab (*liability sharing*) ini, demi menciptakan kepastian hukum dan perlindungan yang adil bagi kedua belah pihak di era perbankan digital.

ISSN 2809-9265 **Locus: Jurnal Konsep Ilmu Hukum**
Vol.5, No.3, December 2025, 451-459

4. Penutup

Pertanggungjawaban bank atas kerugian nasabah akibat kejahatan *phishing* merupakan kewajiban hukum yang melekat dan fundamental dalam penyelenggaraan perbankan digital. Kewajiban tersebut diwujudkan melalui penerapan prinsip kehati-hatian dan tata kelola perusahaan yang baik guna menjamin keamanan sistem serta perlindungan data pribadi nasabah. Bank berkewajiban memberikan ganti rugi apabila kerugian terbukti timbul akibat kelalaian sistem yang berada dalam pengawasannya, sebagaimana sejalan dengan ketentuan Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi. Penegakan tanggung jawab hukum ini menjadi instrumen penting untuk menjaga kepercayaan publik dan stabilitas sistem keuangan nasional, termasuk melalui pengenaan sanksi administratif maupun pidana terhadap bank yang lalai. Ke depan, penguatan perlindungan nasabah perlu dilakukan secara terpadu melalui peningkatan keamanan siber dan kapasitas sumber daya manusia di sektor perbankan, serta penyusunan batasan tanggung jawab hukum yang lebih tegas oleh regulator guna mencegah kekaburan norma. Di sisi lain, peningkatan literasi dan kesadaran digital masyarakat juga menjadi faktor kunci agar nasabah mampu melindungi data pribadinya dan memahami hak hukumnya. Sinergi antara bank, regulator, dan masyarakat diharapkan mampu mewujudkan ekosistem perbankan digital yang aman, transparan, dan berkeadilan.

Referensi

Antari, P. E. D. (2022). Pemidanaan Terhadap Pekerja Seks Komersial Melalui Aplikasi Michat the Liability of Prostitute on Michat. *Jurnal Selat*, *9 (2)*.

Anwar, S. S. (2022). *Bank Dan Lembaga Keuangan*.

Dana Rp 1,8 Miliar PT VSN Raib, BRI Tegaskan Bukan Salah Sistem Bank, Melainkan Server Nasabah Disusupi Hacker. (n.d.). Radarbali.Id. https://radarbali.jawapos.com/ekonomi/706170217/dana-rp-18-miliar-pt-vsn-raib-bri-tegaskan-bukan-salah-sistem-bank-melainkan-server-nasabah-disusupi-hacker

Fadlan, A. F. (2022). *Bank & Lembaga Keuangan Lainnya*.

Firdaus, I. (2022). *upaya perlindungan hukum hak privasi terhadap data pribadi dari kejahatan peretasan*.

Fuady, M. (2013). *Hukum Perbankan Modern: Berdasarkan Teori, Praktik, dan Hukum Positif di Indonesia*. 56.

Herdian Ayu Andreana Beru Tarigan, D. H. P. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indoensia*, *Volume 1 N*.

Putra, G. N. G. G. (2020). Perlindungan Hukum Terhadap Kerugian Nasabah Akibat Error System. *Jurnal Analisis Hukum*.

Ridwan HR. (2016). *Hukum Administrasi Negara*.

Sindy Ariyaningsih, A Ari Andrianto, Adri Surya Kusuma, Rina Arum Prastyanti. (2023). *kolerasi kejahatan siber dengan percepatan digitalisasi di indonesia*.

Soffa Zahara, Mimin Fatchiyatur Rochmah, Yanuarini Nur Sukmaningtyas, Atika Isnaining Dyah, R. M. A. (2024). *Peningkatan Literasi Digittal Safety Sebagai Upaya Pencegahan Penipuan Digital Pada Masyarakat*. *5 Nomor 2*.

Syahadat Dahlan, Yulia A Hasan, Almusawir Almusawir. (2025). *pelaksanaan perlindungan data pribadi nasabah melalui lembaga perbankan di makasar*.
