



DOI: <https://doi.org/10.38035/jgsp.v4i1>
<https://creativecommons.org/licenses/by/4.0/>

Tanggung Jawab Hukum Pihak Bank Atas Kerugian Nasabah Akibat Kejahatan Phising

Roza Mulyadi¹, Diding Rahmat², Rizky Pratama K³.

¹Universitas Dirgantara Marsekal Suryadarma Jakarta, roza.mulyadi@untirta.ac.id.

²Universitas Dirgantara Marsekal Suryadarma Jakarta, didingrahmat@unsurya.ac.id.

³Universitas Dirgantara Marsekal Suryadarma Jakarta, rizkykarokaro@unsurya.ac.id.

Corresponding Author: roza.mulyadi@untirta.ac.id¹

Abstract: *The development of information technology in digital banking systems has enhanced transaction efficiency; however, it has also generated risks of cybercrime, such as phishing. This study aims to analyze the regulatory framework and the legal basis of banks' liability for customer losses resulting from phishing crimes within the perspective of Indonesian positive law. The research employs a normative legal method with a statutory approach and descriptive qualitative analysis, utilizing both primary and secondary legal materials. The findings indicate that the regulation of bank liability is dispersed across various legal regimes, including the Law on Electronic Information and Transactions, the Personal Data Protection Law, the Consumer Protection Law, the Civil Code, as well as regulations issued by the Financial Services Authority and Bank Indonesia. Normatively, bank liability is not solely based on fault liability but also tends toward risk-based liability, considering that banks, as electronic system operators, are obligated to ensure the security and reliability of their systems. The determination of bank liability depends on the existence of negligence in applying the prudential principle, weaknesses in security systems, or inadequate responses to customer reports. Therefore, although phishing is committed by third parties, banks may still be held proportionally liable if a causal relationship can be established between the bank's negligence and the customer's loss.*

Keyword: *Phishing; Bank Liability, Consumer Protection, Digital Banking, Cybercrime.*

Abstrak: Perkembangan teknologi informasi dalam sistem perbankan digital meningkatkan efisiensi transaksi, namun juga memunculkan risiko kejahatan siber seperti phishing. Penelitian ini bertujuan untuk menganalisis pengaturan dan letak pertanggungjawaban hukum bank atas kerugian nasabah akibat kejahatan phishing dalam perspektif hukum positif Indonesia. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan analisis kualitatif deskriptif, menggunakan bahan hukum primer dan sekunder. Hasil penelitian menunjukkan bahwa pengaturan pertanggungjawaban bank tersebar dalam berbagai rezim hukum, antara lain Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Undang-Undang Perlindungan Konsumen, Kitab Undang-

Undang Hukum Perdata, serta regulasi Otoritas Jasa Keuangan dan Bank Indonesia. Secara normatif, tanggung jawab bank tidak hanya berbasis kesalahan (fault liability), tetapi juga mengarah pada tanggung jawab berbasis risiko (risk-based liability), mengingat bank sebagai penyelenggara sistem elektronik wajib menjamin keamanan dan keandalan sistemnya. Letak pertanggungjawaban bank ditentukan berdasarkan adanya kelalaian dalam penerapan prinsip kehati-hatian, kelemahan sistem keamanan, atau respons yang tidak optimal terhadap laporan nasabah. Dengan demikian, meskipun phishing dilakukan oleh pihak ketiga, bank tetap dapat dimintai pertanggungjawaban secara proporsional apabila terdapat hubungan kausal antara kelalaian bank dan kerugian nasabah.

Kata Kunci: Phishing, Pertanggungjawaban Bank, Perlindungan Konsumen, Perbankan Digital, Kejahatan Siber.

PENDAHULUAN

Pada negara hukum, setiap aspek kehidupan warga Indonesia harus diatur oleh hukum karena orang-orang di Indonesia setiap saat akan menghadapi masalah hukum. Setiap manusia pasti ingin hidup yang damai, aman, dan sejahtera. Akan tetapi, tindak kejahatan di tengah masyarakat juga semakin meningkat seiring dengan kemajuan hukum dan modernisasi dalam segala aspek kehidupan, termasuk di Indonesia.

Setiap tindakan yang bertentangan dengan norma, melanggar kesusilaan, mengganggu, dan menimbulkan ketidaknyamanan dalam masyarakat dapat dikategorikan sebagai kejahatan. Kejahatan tidak hanya mencakup pelanggaran hukum, tetapi juga melanggar hak-hak sosial, ekonomi, dan lainnya. Pelanggaran hukum berkaitan juga dengan pelanggaran dan penyalahgunaan perkembangan teknologi tinggi (Hekawati, D, 2018).

Kemajuan teknologi yang sangat pesat ini juga memiliki sisi gelap yang dapat menimbulkan peluang bagi para pelaku kejahatan dunia maya atau cybercrime (Lekahena, dkk, 2023). Penggunaan teknologi informasi yang semakin meluas juga membuka peluang bagi terjadinya tindak pidana informasi dan transaksi elektronik, seperti penipuan online, penyebaran informasi palsu, dan pelanggaran privasi data (Altansa, dkk, 2024). Kemajuan teknologi dan informasi khususnya dalam media internet sebagai salah satu media penyebaran informasi secara masif membawa berbagai dampak dalam bentuk penyalahgunaan media internet untuk memperoleh keuntungan dengan melakukan perbuatan mengambil data identitas guna memperoleh user ID atau password dengan menggunakan teknik Phishing (Julianti & Sugiantari, 2021).

Fenomena kasus phishing terjadi di Kota Makassar dialami oleh Rafiel Baharuddin yang menggugat Bank Sulselbar ke PN Makassar setelah dana sebesar sekitar Rp131 juta hilang dari rekeningnya. Dalam proses persidangan terungkap bahwa nasabah sempat memberikan kode OTP kepada pihak yang diduga pelaku phishing karena tergoda hadiah melalui media sosial Instagram. Meski demikian, majelis hakim tetap mengabulkan sebagian gugatan penggugat dan menyatakan pihak bank bertanggung jawab atas kerugian tersebut (Detik.com, 2023). Selain itu, kasus phishing juga terjadi pada Makan Bergizi Gratis (MBG) di Satuan Pelayanan Pemenuhan Gizi (SPPG) Pangauban, Bandung merupakan contoh nyata atas ada tindak kejahatan berupa penipuan digital atau phishing. Kronologi kejadian bermula pada Kamis, 31 Oktober 2025, ketika Kepala SPPG Pangauban berinisial MC menerima notifikasi dari sistem BNI Direct yang meminta penggantian kata sandi. Tanpa menaruh curiga, ia menghubungi layanan chat yang dikira resmi milik bank. Selanjutnya, seseorang yang mengaku sebagai petugas BNI menghubungi MC dan mengirimkan tautan untuk mengganti kata sandi. Dalam proses tersebut, MC diminta menyerahkan sejumlah data penting rekening dan mengikuti seluruh instruksi karena

khawatir rekening akan diblokir. Tidak lama kemudian, kontak tersebut tidak bisa dihubungi lagi. Saat saldo rekening diperiksa, dana operasional sebesar Rp1 miliar telah terkuras dan hanya tersisa sekitar Rp12 juta. Akibatnya, operasional dapur Program Makan Bergizi Gratis di SPPG Pangauban dihentikan total (Kompas.com, 2025).

Menurut Julianti & Sugiantari (2021) Teknik phishing adalah sebuah tindakan memperloleh informasi pribadi seperti user id atau password (yang merupakan tanda pengenal untuk masuk dan mengakses internet), PIN (merupakan angka sandi rahasia antara pengguna dan sistem), nomor rekening, nomor kartu kredit anda secara tidak sah melalui e-mail palsu kepada seseorang atau suatu perusahaan atau suatu organisasi dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah. Informasi inilah yang digunakan untuk kemudian melakukan tindakan kejahatan perbankan untuk mengakses rekening, melakukan penipuan kartu kredit, atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

Menurut Helndarto & Prasetyawati (2024) Model ini sering kali berkaitan dengan pelanggaran rekayasa sosial. Adalah melanggar hukum bagi siapapun untuk dengan sengaja, tanpa izin, atau melanggar hukum lain, mengakses sistem komputer dan/atau sistem elektronik menggunakan model yang dapat menyebabkan pelanggaran, penetrasi, penghindaran, ataupun pelepasan sistem keamanan, sesuai dengan UU No 19 Tahun 2016 yang mengubah UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penyelbaran konten negatif dan kejahatan siber diatur dalam UU ITE untuk melindungi masyarakat dari kerugian (Karo, 2022). Sebagai akibatnya, phishing diakui sebagai tindak pidana yang bertentangan dengan hukum, dan berdasarkan pasal ini dapat dijatuhi hukuman penjara hingga delapan tahun dan/atau denda maksimum sebesar Rp. 800.000.000,00 (delapan ratus juta rupiah). Hal ini menunjukkan betapa seriusnya sanksi yang dapat diterapkan untuk melindungi integritas dan keamanan sistem elektronik terhadap pelanggaran seperti phishing.

Sepanjang tahun 2023, Kaspersky mencatat lonjakan serangan phishing sebesar 40%, dengan lebih dari 709 juta upaya yang berhasil digagalkan. Para pelaku memanfaatkan platform cloud buatan, pertukaran aset kripto, dan aplikasi pesan seperti Telegram untuk menipu pengguna. Lonjakan signifikan terjadi pada Mei dan Juni, bertepatan dengan musim liburan, di mana penipuan terkait perjalanan seperti tiket pesawat dan penawaran hotel palsu marak terjadi. Kaspersky menekankan pentingnya kewaspadaan dan skeptisisme sebagai pertahanan utama terhadap ancaman phishing yang terus berkembang (CNN Indonesia, 2024).

Pengumpulan dan penyaluran dana publik adalah tugas strategis bank. Bank harus mengelola dan melindungi dana masyarakat dengan baik sehingga pelanggan dapat bertransaksi dengan nyaman dan aman tanpa mengganggu sistem ekonomi negara. Undang-undang Nomor 10 Tahun 1998 tentang Perbankan, bersama dengan peraturan perundang-undangan lainnya, mengatur aktivitas perbankan. Berdasarkan peraturan tersebut, bank harus mematuhi undang-undang dan menerapkan prinsip kehati-hatian.

Pencurian data pribadi nasabah dalam bidang perbankan merupakan salah satu bentuk tindak pidana yang pada akhirnya merugikan nasabah dan memerlukan adanya pertanggungjawaban dari pihak perbankan untuk mengganti kerugian nasabah yang diakibatkan dari pencurian data nasabah. Hingga saat ini pihak kepolisian maupun pihak perbankan masih sangat sulit untuk menemukan pelaku kejahatan pencurian data pribadi nasabah karena belum adanya aturan yang jelas dan pasti yang mengatur mengenai data pribadi (Julianti & Sugiantari, 2021).

Berdasarkan dari uraian diatas, dapat di rumuskan permasalahan pokok yang dapat diteliti dan dituangkan dalam penulisan ini adalah sebagai berikut :

1. Bagaimana pengaturan leltak pelrtanggungjawaban hukum pihak bank atas kerugian nasabah akibat kejahatan phishing saat ini?
 2. Bagaimana leltak pelrtanggungjawaban hukum pihak bank atas kerugian nasabah akibat kejahatan phishing ?
- Tujuan pelnellitian ini telrdiri dari tujuan objektkif dan subjelktif, selbagai belrikut:

Tujuan Objektif

Adapun tujuan objektkif pelnellitian ini adalah:

1. Untuk melngeltahui dan melnganalisis bagaimana pelngaturan leltak pelrtanggungjawaban hukum pihak bank atas kerugian nasabah akibat kejahatan phishing saat ini.
2. Untuk melngeltahui bagaimana leltak pelrtanggungjawaban hukum pihak bank atas kerugian nasabah akibat kejahatan phishing.

Tujuan Subjektif

Adapun tujuan subjelktif pelnellitian ini adalah:

1. Untuk melingkatkan pelmahaman pelnelliti telrhada pelkanismel kelamanan data pribadi dalam sistelm pelrbankan digital.
2. Untuk melnumbuhkan kelsadaran dan tanggung jawab eltis telrhada pelntingnya pelrlindungan data pribadi dalam transaksi keuangan.

METODE

Pelnellitian ini melnggunakan pelndelkatan pelrundang-undangan (statutel approach) untuk mellakukan pelnellitian hukum normatif. Analisis data dalam pelnellitian hukum normatif mellibatkan analisis kualitatif delskriptif. Pelnellitian ini melnggunakan dua katelgori bahan hukum: primelr dan selkundelr.

Bahan hukum primelr telrmasuk undang-undang telntang kejahatan sibelr dan pelrlindungan data pribadi, selpelrti Undang-undang Nomor 11 Tahun 2008 telntang Informasi dan Transaksi ELlelkrtonik (UU ITEl) delngan pelrubahannya melnjadi Undang-Undang Nomor 1 Tahun 2024 dan Undang-undang Nomor 27 Tahun 2022 telntang Pelrlindungan Data Pribadi, selrta belrbagai undang-undang telrkait kelamanan pelrbankan ylang dikelluarkan oleh bank Indonelsia dan Otoritas Jasa Keuangan (OJK). Bahan hukum selkundelr telrmasuk buku, jurnal ilmiah, laporan pelnellitian, dan seljumlah artikell ylang melmbahas aspelk hukum dan telknis dari kejahatan phishing.

HASIL DAN PEMBAHASAN

Hasil

Pengertian Bank

Perkembangan sistem perbankan yang semakin kompleks mengakibatkan meningkatnya kebutuhan akan keberadaan suatu lembaga yang berperan dalam menjaga dan menstabilkan perekonomian (Yuhelson, 2019). Bank adalah suatu lelmbaga pelrantara keuangan (financial intelrmediaryl) antara pihak-pihak ylang melmiliki kellelbiha dana (surplus of funds) delngan pihak-pihak ylang melmelrlukan dana (delficit of funds) (Otoritas Jasa Keuangan, 2019). Yang termasuk dalam istilah bank adalah perusahaan seperti bank umum (commercial bank), lembaga tabungan dan pinjaman (savings and loan associations), bank tabungan bersama (mutual savings banks), dan koperasi kredit (credit unions) (Mishkin & Stanley, 2011).

Bank Umum (commercial bank) merupakan lembaga perbankan yang menghimpun dana masyarakat dalam bentuk simpanan giro dan deposito, serta dalam kegiatan usahanya terutama menyalurkan dana melalui pemberian kredit jangka pendek (Thamrin & Wahjusaputri, 2018). Karena perbankan memainkan peran yang sangat besar dalam menyalurkan dana kepada pihak-

pihak yang memiliki peluang investasi produktif, aktivitas keuangan ini sangat penting untuk memastikan bahwa sistem keuangan dan perekonomian berjalan dengan lancar dan efisien (Mishkin, 2007).

Pengertian dan Karakteristik Kejahatan Phising

Keljahatan phishing adalah salah satu jenis kejahatan siber yang bertujuan untuk mendapatkan informasi pribadi korban, seperti nama pengguna, kata sandi, dan data finansial lainnya, dengan menipu korban untuk membelikannya (Nervia, dkk, 2025). Menurut Bank Muamalat phishing adalah suatu bentuk penipuan yang bertujuan untuk mendapatkan informasi pribadi dan sensitif seseorang, seperti user ID, password, PIN, dan data lainnya, dengan cara menyamar sebagai individu atau organisasi yang berwenang. Model ini sering dilakukan melalui email, pesan teks, atau media elektronik lainnya.

Keljahatan ini biasanya dilakukan dengan mengelabui korban yaitu dengan mengirimkan pesan yang terlihat seperti berasal dari lembaga resmi seperti bank atau lembaga keuangan lainnya. Phishing berasal dari kata "fishing", dan mengacu pada upaya pelaku untuk mendapatkan informasi pribadi dari korban dengan menggunakan model penipuan online yang terlihat jelas (Sitorus, 2024).

Phishing dalam dunia perbankan digital biasanya dilakukan melalui tautan palsu, juga dikenal sebagai "link penipuan", yang mengarahkan korban ke situs web palsu yang terlihat seperti halaman login asli perusahaan perbankan. Tautan ini dapat dikirim ke saluran melalui berbagai jenis komunikasi, seperti email, pesan teks (SMS), aplikasi pesan instan, dan media sosial. Pelaku dapat melakukan transaksi ilegal dan mengakses rekening bank korban setelah korban memberikan informasi mereka ke situs web palsu (Sitorus, 2024).

Bentuk-Bentuk Kejahatan Phising

Phishing merupakan salah satu bentuk kejahatan siber yang paling marak terjadi di era digital, khususnya dalam sistem perbankan. Keljahatan ini dilakukan dengan cara menipu korban agar secara sukarela memberikan informasi sensitif seperti username, password, dan data finansial lainnya, melalui komunikasi elektronik yang menyamar sebagai pihak resmi, seperti bank. Salah satu model yang paling sering digunakan adalah menyebarkan scam link atau tautan berbahaya yang tampak seperti situs perbankan resmi.

Terdapat lima bentuk utama kejahatan phishing dalam konteks perbankan digital (Nervia, dkk, 2025):

a. Email Phishing

Pelaku mengirimkan email yang seolah-olah berasal dari institusi keuangan resmi. Email ini biasanya berisi peringatan palsu atau iming-iming promosi, lalu mengarahkan korban untuk mengklik tautan tertentu yang sebenarnya menuju situs palsu. Di situs ini, korban diminta untuk memasukkan data pribadi yang kemudian disalahgunakan oleh pelaku.

b. SMS dan WhatsApp Phishing (Smishing)

Modus ini memanfaatkan pesan singkat atau aplikasi pesan instan seperti WhatsApp. Pesan biasanya menginformasikan adanya masalah pada akun korban atau transaksi mencurigakan, yang harus segera dikonfirmasi melalui tautan. Setelah diklik, korban diarahkan ke situs tiruan dan diminta memasukkan data login perbankan.

c. Voice Phishing (Vishing)

Pelaku melakukan panggilan telepon dengan menyamar sebagai pegawai bank atau otoritas keuangan. Mereka menciptakan situasi mendesak agar korban

panik dan melmbelrikan informasi pribadi selpelrti nomor kartu, kodel OTP, atau data login.

d. Situs Welb Tiruan

Pellaku melmbuat situs welb palsu ylang sangat melnylelrupai situs relsmi bank. Situs ini dapat muncul mellalui pelncarian di intelrnelt atau diselbarluaskan lelwat elmail dan meldia sosial. Korban ylang tidak waspada akan melngisi informasi selnsitif melrelka pada situs palsu telrselbut.

e. Social Meldia Phishing

Dalam modus ini, pellaku melnggunakan akun meldia sosial palsu ylang melnylelrupai akun relsmi bank. Akun ini digunakan untuk melnghubungi korban, melnawarkan bantuan, atau melnylelbarkan tautan belrbahayla ylang melnuju situs phishing.

Pengaturan Hukum di Indonesia Terkait Kejahatan Phising

Phishing dalam sistelm pelrbankan digital delngan melnggunakan link scam belrbahayla tellah melnjadi salah satu ancaman sibelr ylang selmakin marak di Indonelsia. Untuk melmelrangi pellanggaran ini, pelmelrintah tellah melneltapkan belrbagai undang-undang, telrmasuk undang-undang ylang melngatur selcara khusus transaksi ellelektronik dan undang-undang ylang melngatur pelrlindungan konsumeln di selktor pelrbankan digital (Yustitiana, 2021; Nervia. dkk, 2025). Belbelrapa aturan ylang belrlaku untuk melmelrangi phishing antara lain adalah:

1. Undang-undang Nomor 11 Tahun 2008 telntang Informasi dan Transaksi ELlelektronik (UU ITE) dan Pelrubahannyla dalam Undang-Undang Nomor 19 Tahun 2016 UU ITE melrupakan dasar hukum utama dalam melngatur aktivitas di dunia sibelr, telrmasuk kejahatan phishing. Dalam Pasal 28 aylat (1) UU ITE, diselbutkan bahwa seltiap orang dilarang delngan selngaja dan tanpa hak melnylelbarkan informasi ellelektronik ylang belrsifat melnylelsatkan dan dapat melrugikan konsumeln dalam transaksi ellelektronik. Sellain itu, Pasal 35 UU ITE melngatur bahwa seltiap orang ylang delngan selngaja dan tanpa hak melmanipulasi, melngubah, atau melnciptakan informasi ellelektronik atau dokumeln ellelektronik delngan tujuan agar dianggap selolah-olah data ylang asli dapat dikelnakan sanksi pidana.
2. Undang-undang Nomor 27 Tahun 2022 telntang Pelrlindungan Data Pribadi (UU PDP). UU PDP melngatur pelrlindungan data pribadi masyarakat agar tidak disalahgunakan olelh pihak ylang tidak belrtanggung jawab. Kejahatan phishing selring kali mellibatkan pelncurian data pribadi, selpelrti nama, nomor relkelning, selrta kreldeinsial login nasabah pelrbankan. Dalam undang undang ini, pihak ylang melnylalahgunakan atau melngaksels data pribadi selseorang tanpa izin dapat dikelnakan sanksi pidana.
3. Pasal 215 UU Nomor 4 Tahun 2023, penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK) wajib menerapkan manajemen risiko serta keamanan dan keandalan sistem informasi, termasuk ketahanan siber, sebagai upaya pencegahan phishing. Selanjutnya, Pasal 227–229 menegaskan kewajiban pelaku usaha sektor keuangan dalam melindungi aset, privasi, dan data konsumen. Ketentuan ini diperkuat oleh Pasal 239 yang mewajibkan pelaku usaha menjaga kerahasiaan dan keamanan data pribadi konsumen. Dengan demikian, pencegahan phishing merupakan kewajiban hukum penyelenggara layanan keuangan digital sebagai bagian dari pelindungan konsumen dan pengelolaan risiko teknologi.
4. Kitab Undang-undang Hukum Pidana (KUHP) Melskipun KUHP tidak selcara elksplisit melngatur kejahatan sibelr, belbelrapa pasalnya dapat ditelrapkan dalam

kasus phishing. Pasal 378 KUHP tentang penipuan, misalnya, dapat digunakan untuk menjelrat pelaku yang dengan sengaja menggelabui korban guna mendapatkan keuntungan yang tidak sah. Selain itu, Pasal 362 KUHP tentang pencurian juga dapat diterapkan apabila kejahatan phishing menyebabkan hilangnya uang atau aset korban.

5. Pelraturan Bank Indonelsia (PBI) dan Pelraturan Otoritas Jasa Keuangan (OJK) Dalam konteks perbankan digital, Bank Indonelsia (BI) dan Otoritas Jasa Keuangan (OJK) memiliki pelraturan yang bertujuan untuk melindungi konsumen dan menjaga keamanan transaksi elektronik. Salah satu regulasi yang relevan adalah:
 - 1) PBI Nomor 22/20/PBI/2020 tentang Keamanan Sistem Pembayaran, yang mewajibkan bank dan penyedia layanan keuangan digital untuk menerapkan sistem keamanan yang ketat guna mencegah penyalahgunaan data nasabah.
 - 2) POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang mengatur kewajiban lembaga keuangan untuk memberikan edukasi serta perlindungan kepada nasabah terkait risiko kejahatan digital. Sebagaimana POJK Nomor 1/POJK.07/2013 diganti dengan POJK Nomor 6 /POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan yang mewajibkan lembaga keuangan untuk mengamankan sistem dan data, menangani pengaduan, bertanggung jawab atas kerugian akibat kelalaian, serta meningkatkan edukasi konsumen. Phishing tidak dipandang semata kesalahan konsumen, tetapi juga sebagai indikator kepatuhan PUJK terhadap kewajiban perlindungan konsumen.
6. Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU PK) UU PK memberikan landasan hukum bagi nasabah yang mengalami kerugian akibat tindak kejahatan phishing. Bank sebagai penyedia layanan perbankan digital memiliki tanggung jawab untuk memastikan keamanan sistem mereka dan memberikan informasi yang jelas mengenai risiko transaksi daring. Jika bank tidak memberikan perlindungan yang memadai, maka nasabah yang dirugikan dapat menuntut ganti rugi berdasarkan ketentuan dalam UU PK.

Perlindungan Hukum Bagi Nasabah dalam Sistem Perbankan Digital

Kelajahatan phishing yang dilakukan melalui tautan palsu di sistem perbankan digital sering kali menyebabkan nasabah kehilangan banyak uang. Oleh karena itu, memastikan bahwa korban kejahatan ini dilindungi secara hukum menjadi komponen yang sangat penting dari sistem hukum Indonelsia. Perlindungan hukum preventif dan represif membekalkan perlindungan hukum terhadap pelanggan yang menjadi korban phishing (Nervia, 2025).

a. Perlindungan Hukum Preventif

Upaya yang dilakukan sebelum kejahatan terjadi untuk mencegah atau meminimalkan risiko yang dihadapi oleh pelanggan. Upaya ini mencakup peraturan yang ketat, edukasi kepada masyarakat, dan peningkatan keamanan digital lembaga keuangan. Untuk melindungi nasabah dari serangan siber, termasuk phishing, Bank Indonelsia (BI) dan Otoritas Jasa Keuangan (OJK) telah menetapkan berbagai peraturan yang berkaitan dengan keamanan transaksi digital.

1. Pelraturan Bank Indonelsia (PBI) No. 22/20/PBI/2020 tentang Keamanan Sistem Pembayaran menetapkan bahwa penyedia layanan pembayaran digital harus menerapkan standar keamanan yang tinggi untuk melindungi informasi pelanggan.

2. Menurut POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, lembaga keuangan diwajibkan untuk memberitahu klien mereka tentang risiko kejahatan siber. Ini termasuk mengajarkan mereka cara menemukan tautan scam berbahaya.

Peningkatan pengetahuan digital nasabah perbankan adalah upaya pencegahan tambahan. Banyak korban phishing tertipu karena mereka tidak memahami modus kejahatan siber. Oleh karena itu, otoritas perbankan harus memberitahu orang tentang pentingnya menjaga kerahasiaan data pribadi dan mengidentifikasi tanda-tanda phishing.

b. Perlindungan Hukum Reprasif

Perlindungan hukum yang reprasif adalah tindakan yang dilakukan oleh penegak hukum dan organisasi terkait setelah terjadi pelanggaran atau pelanggaran hukum. Ini adalah bagian dari sistem hukum yang bertujuan untuk mengembalikan hak-hak korban yang dirugikan dan memastikan bahwa pelaku pelanggaran dihukum dengan cara yang sesuai dengan undang-undang dan peraturan yang berlaku.

Perlindungan hukum reprasif berperan penting dalam menjaga ketertiban masyarakat dan mencegah terjadinya tindak pidana. Dalam konteks ini, perlindungan hukum reprasif tidak hanya berfokus pada pembelian keladilannya kepada korban melalui proses pengadilan, tetapi juga mencakup penanganan, penyelidikan, tuntutan, dan kriminalisasi terhadap pelaku. Semua proses tersebut dilakukan berdasarkan asas hukum yang menjunjung tinggi keladilannya, kepastian hukum, dan perlindungan hak asasi manusia.

Nasabah memiliki hak untuk mengajukan gugatan hukum perdata terhadap bank jika terbukti bank gagal menjaga keamanan sistem perbankan online secara memadai berdasarkan (Nervia. dkk, 2025):

1. Pasal 19 Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999), pelaku usaha wajib mengganti kerugian konsumen yang mengalami kerugian akibat kelalaiannya.
2. Nasabah dapat menuntut ganti rugi berdasarkan Pasal 1365 KUH Perdata tentang Perbuatan Melawan Hukum, apabila dapat dibuktikan bahwa bank telah lalai atau melakukan kesalahan.

Pembahasan

Kelajahatan dunia maya seperti phishing telah berkembang menjadi masalah yang signifikan di era digital yang semakin canggih, khususnya bagi industri perbankan dan kliennya. Phishing adalah jenis kelajahatan dunia maya yang melibatkan penipuan terhadap korban agar membocorkan informasi pribadi dengan menggunakan situs web, email, atau komunikasi palsu yang tampak berasal dari organisasi yang sah. Kelajahatan ini secara langsung memengaruhi privasi pengguna dan keamanan uang dan biasanya mengakibatkan pengguna sistem keuangan digital.

Pelngaturan Pelrtanggungjawaban Hukum Bank atas Kelrugian Nasabah Akibat Kelajahatan Phishing

Selcara normatif, pelrtanggungjawaban perdata bank atas kerugian nasabah akibat kelajahatan phishing tidak berdiri pada satu rezim hukum tunggal, melainkan tersebar dalam beberapa instrumen hukum yang saling melengkapi. Pelngaturan tersebut menunjukkan adanya pergeseran paradigma dari tanggung jawab berbasis kesalahan (fault liability) menuju tanggung jawab berbasis risiko (risk-based liability), khususnya dalam sektor jasa keuangan digital.

Dalam perspektif hukum perdata umum, dasar pertanggungjawaban bank dapat ditelusuri dari ketentuan Pasal 1365 KUH Perdata, yang mengatur perbuatan melawan hukum. Bank sebagai pelaku usaha jasa keuangan dapat dimintai pertanggungjawaban apabila terbukti melakukan perbuatan melawan hukum, baik melalui tindakan aktif maupun kelalaian (omission), yang menimbulkan kerugian bagi nasabah. Kelalaian tersebut dapat berupa kegagalan bank dalam menerapkan prinsip kehati-hatian, lemahnya sistem pengamanan transaksi elektronik, maupun lambannya respons terhadap laporan nasabah ketika terjadi indikasi kejahatan siber.

Pengaturan yang lebih spesifik terdapat dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang menempatkan nasabah bank sebagai konsumen dan bank sebagai pelaku usaha. Pasal 19 UU Perlindungan Konsumen secara tegas mewajibkan pelaku usaha untuk memberikan ganti rugi atas kerugian konsumen yang timbul akibat penggunaan jasa yang diperdagangkan. Dalam konteks phishing, meskipun kejahatan dilakukan oleh pihak ketiga, bank tetap berada dalam posisi strategis karena sistem layanan elektronik dan infrastruktur transaksi berada di bawah penguasaannya.

Selanjutnya, UU ITE (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 serta UU No. 1 Tahun 2024) memperkuat tanggung jawab penyelenggara sistem elektronik, termasuk bank, untuk menjamin keandalan, keamanan, dan perlindungan data pribadi pengguna. Pasal 15 UU ITE menegaskan bahwa penyelenggara sistem elektronik bertanggung jawab atas pelanggaran sistem secara andal dan aman. Kegagalan dalam memenuhi kewajiban ini membuka ruang pertanggungjawaban perdata apabila kerugian nasabah dapat dikaitkan dengan lemahnya sistem pengamanan.

Pengaturan yang semakin eksplisit muncul dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menempatkan bank sebagai pengelola data pribadi. Dalam rezim ini, kebocoran data, penyalahgunaan data autentikasi, atau kegagalan melindungi data nasabah yang berujung pada phishing dapat menjadi dasar pertanggungjawaban perdata tanpa harus selalu membuktikan kesalahan subjektif, sepanjang dapat dibuktikan adanya kegagalan pengelolaan data secara layak.

Di tingkat regulasi, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU PPSK) kini mempertegas kewajiban Penyelenggara ITSK (Inovasi Teknologi Sektor Keuangan) dan perbankan dalam menjaga keandalan sistem serta perlindungan konsumen secara menyeluruh. POJK Nomor 6 /POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan serta PBI No. 22/20/PBI/2020 tentang Keamanan Sistem Pembayaran secara tegas mewajibkan bank untuk menjamin keamanan sistem pembayaran, mekanisme pengaduan yang responsif, perlindungan terhadap kerugian konsumen, serta meningkatkan edukasi kepada konsumen. Regulasi ini menegaskan bahwa tanggung jawab bank tidak hanya berfokus pada pelayanan, tetapi juga mencakup pengelolaan risiko teknologi informasi dan kejahatan siber.

Dengan demikian, secara normatif, pengaturan pertanggungjawaban perdata bank atas kerugian akibat phishing tersebar dalam rezim hukum perdata, perlindungan konsumen, hukum siber, perlindungan data pribadi, serta regulasi sektor jasa keuangan yang secara sistematis menempatkan bank sebagai subjek hukum yang memiliki tanggung jawab tinggi terhadap keamanan nasabah.

Letak Pertanggungjawaban Hukum Pihak Bank atas Kerugian Nasabah Akibat Kejahatan Phishing

Berdasarkan Putusan No. 248/Pdt.G/2023/PN Makassar, letak pertanggungjawaban perdata bank tidak semata-mata ditentukan oleh fakta bahwa pelaku phishing adalah pihak ketiga (hackler), melainkan pada ada atau tidaknya kelalaian bank dalam menjalankan kewajiban hukum dan profesionalnya. Putusan ini menekankan pendekatan kausalitas

fungsional, yakni menilai sejauh mana tindakan atau kelalaian bank berkontribusi terhadap terjadinya kerugian nasabah.

Dalam perkara a quo, pengugat telah melaporkan adanya indikasi kejahatan phishing kepada pihak bank melalui call center. Namun, kerugian tetap berlangsung dalam rentang waktu tertentu sebelum sistem diblokir secara efektif. Fakta ini menunjukkan adanya jeda respons (respons delay) yang relevan secara hukum. Dalam konteks Pasal 1365 KUH Perdata, kelambanan tersebut dapat ditafsirkan sebagai bentuk kelalaian, karena bank memiliki kemampuan teknis dan kewenangan penuh untuk mengelola dan mengamankan transaksi keuangan.

Lebih jauh, pengakuan bank yang menimbulkan ganti rugi sebagian kepada nasabah memiliki makna yuridis penting. Secara doktrinal, tindakan tersebut dapat ditafsirkan sebagai pengakuan implisit adanya kontribusi kesalahan atau setidaknya kegagalan sistem pengamanan internal. Hal ini sejalan dengan prinsip presumption of liability dalam perlindungan konsumen sektor jasa keuangan, di mana beban pembuktian tidak sepenuhnya diletakkan pada nasabah.

Tetap pertanggungjawaban hukum bank dalam kasus phishing juga berkaitan erat dengan prinsip kehati-hatian (prudential principle). Bank sebagai lembaga yang menghimpun dan mengelola dana masyarakat memiliki standar kewajiban yang lebih tinggi dibanding pelaku usaha biasa. Oleh karena itu, meskipun phishing diawali oleh kelalaian nasabah (misalnya memberikan OTP), tanggung jawab bank tidak otomatishapus sepanjang dapat dibuktikan bahwa sistem keamanan, edukasi konsumen, atau mekanisme pengendalian transaksi tidak optimal.

Dalam perspektif UU PDP, tanggung jawab bank semakin diperluas karena bank berkewajiban menjamin keamanan data autentikasi nasabah. Apabila phishing berhasil karena lemahnya sistem verifikasi berlapis atau kegagalan deteksi transaksi abnormal, maka kerugian nasabah dapat dikualifikasikan sebagai akibat dari kegagalan pengendalian data pribadi.

Dengan demikian, tetap pertanggungjawaban hukum bank atas kerugian nasabah akibat phishing berada pada titik pertemuan antara kelalaian operasional, kegagalan sistem keamanan, dan tidak optimalnya perlindungan konsumen, bukan semata-mata pada perbuatan pidana pihak ketiga. Putusan PN Makassar tersebut memperlihatkan celendungan pengadilan untuk menempatkan bank sebagai pihak yang tetap memikul tanggung jawab proporsional, sejauh kerugian nasabah memiliki hubungan kausal dengan kelalaian atau kelemahan sistem bank.

KESIMPULAN

Kesimpulan

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa:

1. Pengaturan pertanggungjawaban hukum pihak bank atas kerugian nasabah akibat kejahatan phishing di Indonesia telah diatur secara komprehensif dalam berbagai rezim hukum, baik hukum perdata umum, perlindungan konsumen, hukum sipil, perlindungan data pribadi, maupun regulasi sektor jasa keuangan. KUH Perdata melalui Pasal 1365 memberikan dasar pertanggungjawaban atas perbuatan melawan hukum, sementara Undang-Undang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta POJK dan PBI terkait menegaskan kewajiban bank untuk menjamin keamanan sistem elektronik, melindungi data nasabah, dan memberikan ganti rugi atas kerugian yang timbul dalam penyelenggaraan layanan jasa keuangan digital.

2. Berdasarkan analisis Putusan No. 248/Pdt.G/2023/PN Makassar, leltak pelrtanggungjawaban hukum bank tidak selmata-mata ditelntukan oleh fakta bahwa kejahatan phishing dilakukan oleh pihak keltiga, mellainkan pada ada atau tidaknya kellalaian bank dalam melnjalankan prinsip kelhati-hatian, pelngamanan sistelm transaksi ellektronik, selrta relspons ylang celpat dan elfelktif telrhada pelngaduan nasabah. Putusan telrselbut melnunjukkan bahwa pelngadilan celndelrung melnelmpatkan bank selbagai pihak ylang teltap melmikul tanggung jawab pelrdata selcara proporsional apabila kelrugian nasabah meliliki hubungan kausal delngan kellelmahan sistelm atau keltelrlambatan tindakan bank, melskipun telrdapat unsur kellalaian dari pihak nasabah.

Delngan delmikian, pelrtanggungjawaban hukum bank atas kelrugian akibat phishing berada pada irisan antara tanggung jawab belrbasis kelsalahan dan tanggung jawab belrbasis risiko. Bank selbagai pelnyellelenggara sistelm ellektronik dan pelngelndali data pribadi dituntut untuk melnelrapkan standar pelrlindungan ylang tinggi telrhada nasabah. Kelsimpulan ini melnelgaskan pelrlunya pelnguatan relgulasi telknis, pelnngkatan sistelm kelamanan, selrta konsistelni pelnelgakan hukum guna melmbelri kelpastian hukum dan pelrlindungan ylang elfelktif bagi nasabah dalam melnghadapi keljahatan sibelr di selktor pelrbankan.

Saran

1. Telrkait pelngaturan pelrtanggungjawaban hukum bank, dipelrlukan pelnguatan dan harmonisasi relgulasi lintas relzim hukum agar standar kelwajiban bank dalam melnelgah dan melnangani keljahatan phishing meljadi lelbih jellas dan opelrasional. Pelmbelntuk kelbijakan dan relgulator selktor jasa keuangan pelrlu melrumuskan peldoman telknis ylang telgas melngelnai kelamanan sistelm ellektronik, pelrlindungan data pribadi, selrta melkanismel ganti rugi nasabah, selhingga pelngaturan pelrtanggungjawaban pelrdata bank tidak hanya belrsifat normatif, teltapi juga melmbelri kelpastian hukum dalam praktik pelnyellelenggaraan laylanan pelrbankan digital.
2. Telrkait leltak pelrtanggungjawaban hukum bank dalam praktik pelradilan, bank pelrlu melnngkatan pelnelrapan prinsip kelhati-hatian mellalui pelnguatan sistelm kelamanan transaksi, relspons ylang celpat dan elfelktif telrhada pelngaduan nasabah, selrta eldukasi belrkellanjutan melngelnai risiko phishing. Di sisi lain, aparat pelnelgak hukum diharapka konsisteln melnelrapkan pelndelkatan proporsional dalam melnilai kellalaian dan hubungan kausal antara kelrugian nasabah dan tindakan bank, selbagaimana telrcelrmin dalam Putusan PN Makassar, guna melwujudkan kelselimbangan antara pelrlindungan nasabah dan kelpastian hukum bagi pelrbankan.

REFERENSI

- Altansa, Fadlil, dan Diding Rahmat. "Analisis YLuridis Kelwelngan Jaksa dalam Pelnelgakan Hukum Tindak Pidana Informasi dan Transaksi ELlektronik." Lelx Laguelns: Jurnal Kajian Hukum dan Keladilan 2, no. 1 (Felbruari 2024): 1–13.
- Bank Muamalat Indonelsia. "Apa itu phising: Pelngelrtian, ciri-ciri, dan cara melnghindarinyla." Diaksels 23 Januari 2026.
- CNN Indonelsia. "Selrangan Phishing Melnngkat 40 Pelrseln Selpanjang 2023, Celk Targeltnyla." CNN Indonelsia, 13 Marelt 2024. Tanggal aksels 8 Oktobelr 2025.
- deltikcom. 2023. "Bank Sulsellbar dihukum ganti rugi duit nasabah Rp 131 juta ajukan banding." Deltik Sulsell, 20 Delselmbelr 2023. Diaksels 25 Januari 2026.

- ELkawati, Dian. "Pelindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan." *UNELS Law Review* 1, no. 2 (2018): 157-171.
- Helndarto, Vanyla Agatha, dan EIndang Prasetyawati. "Tanggung Jawab Bank Dalam Mengantisipasi Dan Mengurangi Kerugian Nasabah Akibat Scam Melalui Link Phishing Pada Mobile Banking." *Iuris Studia: Jurnal Kajian Hukum* 5, no. 3 (2024): 759-765.
- Julianti, Lis, dan Anak Agung Putu Wiwik Sugiantari. "Tanggung Jawab Hukum Pihak Perbankan Dalam Pencurian Data Pribadi Nasabah Dengan Teknik "Phishing" Pada Transaksi Perbankan." In *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasarwati Denpasar* 2020, vol. 1, no. 1, pp. 96-105. 2021.
- Karo, Rizki Pratama Putra Karo. "Hate Speech: Penyelimpangan terhadap UU ITE, Kelambatan Berpercepat dan Nilai-Nilai Keladilan Bermartabat." *Jurnal Lemhannas RI* 10, no. 4 (2022): 52-65.
- Kitab Undang-undang Hukum Pidana (KUHP)
- Kompas.com. "Kronologi Lengkap Raibnya Dana Rp 1 Miliar SPPG Bandung Barat Dapur." *Kompas.com*, 5 November 2025. Tanggal akses 6 November 2025.
- Lelkahelna, Clariella LZ, Gracel H. Tamporangoy, dan Susan Lawotjo. "Tanggung Jawab Hukum Pihak Perbankan Terhadap Nasabah Akibat Tindakan Kejahatan Skimming." *Lex Administratum* 11, no. 4 (2023).
- Mishkin, Frederic S. *The economics of money, banking, and financial markets*. Pearson education, 2007.
- Mishkin, Frederic S., and Stanley G. Eakins. "Financial Markets and Institutions 7e." (2011).
- Nelvia, Clara, Kresnientia Aiko Wardhana, Priscilia Angell Seli, Talitha Livia Talim, dan Waynelhard Braynel Hizkia. "Analisis Yuridis Terhadap Kejahatan Phishing Dalam Sistem Perbankan Digital Melalui Scam Link Berbahaya." *Ikon--Jurnal Ilmiah Ilmu Komunikasi* 29, no. 2 (2025): 13-30.
- Otoritas Jasa Keuangan. *Buku 2: Perbankan (Seluruh Litelasi Keuangan)*. Jakarta: Otoritas Jasa Keuangan, 2019.
- Pengadilan Negeri Makassar. (2023). Putusan Nomor 248/Pdt.G/2023/PN Mks tentang Gugatan Perbuatan Melawan Hukum antara Muhammad Rafiel Baharuddin melawan Direktur Utama PT Bank Sulselbar. Direktorat Putusan Mahkamah Agung Republik Indonesia.
- Peraturan Bank Indonesia (PBI) No. 22/20/PBI/2020 tentang Kelambatan Sistem Pembayaran
- POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan
- POJK Nomor 6 /POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Keuangan
- Sitorus, Nanang Tomi. "Urgensi Penegakan Hukum Terhadap Perbuatan Phishing Sebagai Upaya Pencegahan Kejahatan Siber." *Riau Law Journal* 8, no. 1: 83-94.
- Thamrin, Abdullah, and Wahjuputri Sintha. "Bank dan Lembaga Keuangan Edisi 2." Jakarta: Mitra Wacana Media (2018).
- Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
- Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Undang-undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU PPSK)
- Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
- Yustitiana, Rhelita. "Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia

Dikaitkan Delngan Telori ELfelktivitas Hukum." Jurnal Hukum Visio Justisia 1, no. 1 (2021): 98-126.

Yuhelson. Buku Pengantar Hukum Perbankan di Indonesia. 2019.