Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora
Volume. 4, Nomor. 1, Maret 2026
e-ISSN :2988-2273 ; p-ISSN :2988-2281, Hal. 406-418
DOI: https://doi.org/10.59059/mandub.v4i1.3564
Tersedia: https://journal.staiypiqbaubau.ac.id/index.php/Mandub

Perlindungan Hukum Nasabah atas Kerugian Akibat *Social Engineering* dalam Layanan Perbankan Digital: Parameter Operasional, Struktur Pembuktian, dan Model Pembebanan Kerugian Berjenjang

Nirin Cristin Slavina Nadeak[1*], Rani Apriani[2]
[1-2]Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Singaperbangsa Karawang, Indonesia
Email: nirinnnadeak12@gmail.com[1], rani.apriani@fh.unsika.ac.id[2]

**Penulis Korespondensi: nirinnnadeak12@gmail.com*

Abstract*. The expansion of digital banking has widened customers' exposure to social engineering, including phishing, vishing, and the takeover of OTPs and PINs. A recurring legal problem is who should bear the loss when a customer discloses credentials because of psychological manipulation, while the bank holds the authentication infrastructure, transaction data, and fraud-detection capacity. Earlier studies have discussed causally grounded proportional liability, the relativity of bank liability, and the need to restructure customer-protection constructs, but they have not yet formulated operational parameters for assigning fault, an evidentiary structure, or a tiered loss-allocation model. This normative legal study uses statutory, conceptual, and case approaches, and the analysis is prescriptive. It formulates seven parameters for determining liability and a six-stage tiered model that distinguishes dominant bank liability, proportional liability, and dominant customer liability. The study concludes that disclosure of an OTP or PIN does not automatically shift the entire loss to the customer. Liability should be determined by weighing each party's contribution to the loss, the bank's compliance with its security duties, and the causal link between failed mitigation and the loss.*

Keywords*: Customer Protection; Cybercrime; Digital Banking; Social Engineering; Strict Liability*.

Abstrak. Transformasi layanan perbankan digital memperluas kemudahan transaksi sekaligus risiko kejahatan siber berbasis *social engineering*, seperti *phishing*, *vishing*, dan pengambilalihan OTP/PIN. Persoalan hukumnya adalah siapa yang menanggung kerugian ketika nasabah memberikan kredensial akibat manipulasi psikologis, sementara bank memiliki sistem keamanan dan kemampuan mendeteksi transaksi menyimpang. Penelitian terdahulu telah membahas tanggung jawab proporsional berbasis hubungan kausal, relativitas tanggung jawab bank, dan penataan ulang konstruksi pelindungan nasabah, tetapi belum merumuskan parameter operasional penentuan kesalahan, struktur pembuktian, dan model pembebanan kerugian secara berjenjang. Penelitian hukum normatif ini menggunakan pendekatan perundang-undangan, konseptual, dan kasus dengan analisis preskriptif. Hasilnya adalah tujuh parameter penentuan tanggung jawab dan model enam tahap yang membedakan tanggung jawab bank dominan, tanggung jawab proporsional, dan tanggung jawab nasabah dominan. Penelitian menyimpulkan bahwa pemberian OTP/PIN tidak otomatis membebankan seluruh kerugian kepada nasabah. Tanggung jawab perlu ditentukan dengan menimbang kontribusi kesalahan masing-masing pihak, kepatuhan bank terhadap kewajiban keamanan, dan hubungan kausal antara kegagalan mitigasi dan kerugian.

Kata Kunci: *Cybercrime*; Perbankan Digital; Perlindungan Konsumen; Rekayasa Sosial; Tanggung Jawab Mutlak.

1. PENDAHULUAN

Perkembangan teknologi digital telah mendorong perubahan fundamental dalam penyelenggaraan layanan perbankan. Dalam satu dekade terakhir, layanan perbankan mengalami pergeseran dari interaksi yang berpusat pada kantor cabang menuju mobile banking, internet banking, dan berbagai bentuk pembayaran digital yang memungkinkan nasabah melakukan transaksi tanpa tatap muka. Transformasi tersebut memberikan kemudahan, kecepatan, dan efisiensi dalam bertransaksi, tetapi sekaligus menghadirkan bentuk

Naskah Masuk: 27 Januari 2026; Revisi: 23 Februari 2026; Diterima: 24 Maret 2026; Terbit: 31 Maret 2026

risiko baru bagi bank dan nasabah. Oleh karena itu, digitalisasi perbankan tidak hanya berkaitan dengan pengembangan produk dan layanan, tetapi juga harus disertai dengan penguatan manajemen risiko, keamanan teknologi informasi, serta pelindungan konsumen (Otoritas Jasa Keuangan [OJK], 2020, 2021).

Perubahan lanskap layanan perbankan tersebut turut diikuti oleh perkembangan kejahatan siber yang semakin memanfaatkan kelemahan manusia sebagai sasaran serangan. Salah satu bentuknya adalah social engineering, yaitu teknik manipulasi psikologis yang digunakan untuk memengaruhi korban agar memberikan informasi atau melakukan tindakan tertentu yang menguntungkan pelaku (Hadnagy, 2018). Dalam praktik perbankan digital, social engineering dapat dilakukan melalui penyamaran sebagai petugas bank, kurir, penyedia layanan, atau instansi resmi dengan menggunakan pesan singkat, panggilan telepon, media sosial, maupun tautan palsu. Korban kemudian diarahkan untuk memberikan informasi rahasia seperti one-time password (OTP), PIN, kata sandi, atau kredensial perbankan lainnya. Setelah memperoleh informasi tersebut, pelaku dapat mengambil alih akses rekening dan memindahkan dana. Persoalan menjadi semakin kompleks karena transaksi yang dilakukan menggunakan kredensial nasabah yang benar secara sistem dapat terlihat sebagai transaksi yang telah melalui mekanisme autentikasi yang sah.

Maraknya penipuan berbasis manipulasi digital menunjukkan bahwa risiko transaksi perbankan tidak lagi hanya berasal dari kegagalan teknis sistem, tetapi juga dari interaksi antara sistem teknologi dan perilaku pengguna. Kondisi tersebut mendorong OJK membentuk Indonesia Anti-Scam Centre (IASC) sebagai mekanisme penanganan dan koordinasi terhadap penipuan transaksi keuangan. Kehadiran IASC menunjukkan bahwa penipuan digital telah berkembang menjadi persoalan yang membutuhkan respons kelembagaan dan tidak dapat semata-mata dibebankan kepada individu korban (OJK, 2026). Dengan demikian, perkembangan social engineering menimbulkan pertanyaan penting mengenai pembagian tanggung jawab antara bank sebagai penyelenggara layanan keuangan dan nasabah sebagai pengguna layanan.

Persoalan hukum utama muncul ketika nasabah sendiri memasukkan atau memberikan OTP, PIN, atau kredensial lainnya setelah berhasil dimanipulasi oleh pelaku. Dalam praktik penyelesaian sengketa, fakta bahwa kredensial diberikan oleh nasabah dapat digunakan sebagai dasar untuk menyatakan bahwa kerugian merupakan akibat kelalaian nasabah. Namun, pemberian kredensial dalam situasi manipulasi tidak selalu dapat disamakan dengan tindakan nasabah yang secara sadar dan bebas menerima risiko transaksi. Pada saat yang sama, fakta bahwa transaksi telah melewati autentikasi tidak dengan sendirinya menghilangkan kewajiban

bank untuk menerapkan sistem keamanan, melakukan pemantauan terhadap transaksi yang tidak wajar, dan mengambil langkah mitigasi ketika terdapat indikasi penipuan. Dengan demikian, keberadaan OTP atau autentikasi yang valid perlu dianalisis bersama dengan konteks bagaimana kredensial tersebut diperoleh dan apakah bank telah memenuhi kewajiban keamanan serta pelindungan nasabah.

Ketimpangan penguasaan informasi dan teknologi antara bank dan nasabah semakin memperkuat persoalan tersebut. Bank memiliki penguasaan terhadap infrastruktur sistem, data historis transaksi, mekanisme autentikasi, teknologi pendeteksian anomali, serta kemampuan untuk melakukan pemblokiran atau penghentian transaksi tertentu. Sebaliknya, nasabah pada umumnya memiliki keterbatasan dalam memahami karakteristik teknis sistem keamanan perbankan dan dapat mengalami kesulitan membedakan komunikasi resmi dengan komunikasi palsu yang dirancang secara meyakinkan. Dalam perspektif analisis ekonomi terhadap hukum kecelakaan, pembebanan tanggung jawab dapat diarahkan kepada pihak yang mampu mencegah atau mengurangi risiko dengan biaya yang relatif paling rendah (*cheapest cost avoider*) (Calabresi, 1970; Shavell, 1987). Perspektif tersebut memberikan dasar untuk mempertanyakan apakah pemberian OTP atau PIN oleh nasabah secara otomatis harus dipandang sebagai alasan yang membebaskan bank dari tanggung jawab.

Kerangka hukum positif Indonesia memberikan sejumlah dasar untuk menilai persoalan tersebut. Pasal 29 ayat (4) Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 mewajibkan bank untuk menyediakan informasi mengenai kemungkinan timbulnya risiko kerugian sehubungan dengan transaksi nasabah. Sementara itu, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan hak kepada konsumen atas kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa serta mengatur tanggung jawab pelaku usaha terhadap kerugian konsumen. Ketentuan tersebut menunjukkan bahwa hubungan antara bank dan nasabah tidak hanya dapat dilihat dari perspektif hubungan kontraktual, tetapi juga dari perspektif pelindungan konsumen (Undang-Undang Nomor 8 Tahun 1999).

Dalam konteks transaksi elektronik, Undang-Undang Informasi dan Transaksi Elektronik juga memberikan kerangka mengenai tanggung jawab penyelenggara sistem elektronik. Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 pada prinsipnya mengatur bahwa penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya, dengan pengecualian tertentu apabila dapat dibuktikan adanya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna. Ketentuan ini

menjadi relevan untuk menilai hubungan antara kewajiban bank sebagai penyelenggara sistem dan perilaku nasabah sebagai pengguna ketika terjadi transaksi yang merugikan akibat social engineering.

Pada tingkat regulasi sektoral, OJK juga telah mengembangkan kerangka pengaturan mengenai pelindungan konsumen, layanan digital, dan penyelenggaraan teknologi informasi oleh bank. Peraturan OJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan menegaskan pentingnya pelindungan konsumen dalam penyelenggaraan kegiatan sektor jasa keuangan. Sementara itu, Peraturan OJK Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum serta Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum memberikan kerangka bagi penyelenggaraan layanan dan teknologi informasi perbankan. Rangkaian regulasi tersebut menunjukkan bahwa keamanan sistem dan pelindungan nasabah merupakan bagian integral dari penyelenggaraan layanan perbankan digital. Namun demikian, regulasi tersebut belum memberikan formula sederhana untuk menentukan pembagian tanggung jawab ketika kerugian terjadi akibat kombinasi antara tindakan nasabah yang tertipu dan kemungkinan kelemahan mitigasi yang dilakukan bank.

Persoalan pembagian tanggung jawab tersebut juga telah menjadi perhatian dalam penelitian terdahulu. Mulyadi et al. (2026) menunjukkan bahwa meskipun phishing dilakukan oleh pihak ketiga, bank tetap dapat dimintai pertanggungjawaban apabila terdapat hubungan kausal antara kelemahan sistem mitigasi bank dan kerugian yang dialami nasabah. Hasanudin (2026) menyoroti batas tanggung jawab bank dalam menghadapi kejahatan digital berbasis social engineering dan menekankan pentingnya penguatan konstruksi hukum pelindungan nasabah. Widjana et al. (2025) menunjukkan bahwa pertanggungjawaban bank terhadap kerugian nasabah akibat phishing bersifat relatif karena perlu mempertimbangkan letak kesalahan dan kelalaian masing-masing pihak. Sementara itu, Chairunnisa et al. (2024) membedakan konstruksi pelindungan hukum terhadap nasabah berdasarkan karakteristik kejahatan *hacking* dan *phishing* dalam kerangka hukum positif Indonesia.

Temuan penelitian terdahulu tersebut memperlihatkan bahwa tanggung jawab bank tidak dapat ditentukan hanya berdasarkan siapa yang secara langsung memberikan OTP atau PIN. Tanggung jawab perlu dikaitkan dengan tindakan para pihak, kewajiban hukum bank, tingkat keamanan sistem, kemampuan mendeteksi transaksi yang tidak wajar, serta hubungan kausal antara tindakan atau kelalaian masing-masing pihak dengan kerugian yang terjadi. Persoalan ini juga memperoleh relevansi dalam praktik peradilan, sebagaimana terlihat dalam perkara yang berkaitan dengan hilangnya dana nasabah akibat transaksi yang dipersoalkan, sehingga

memperlihatkan bahwa validitas transaksi secara teknis tidak selalu identik dengan terbebasnya bank dari persoalan tanggung jawab hukum (Pengadilan Negeri Makassar, 2023).

Meskipun penelitian terdahulu telah membahas tanggung jawab bank akibat phishing dan social engineering, masih terdapat ruang kajian mengenai bagaimana menentukan proporsi tanggung jawab ketika kesalahan atau kelalaian bank dan nasabah hadir secara bersamaan. Penelitian sebelumnya pada umumnya menitikberatkan pada dasar pertanggungjawaban bank, bentuk pelindungan hukum, atau kebutuhan pembaruan regulasi. Belum banyak kajian yang secara sistematis merumuskan parameter yang dapat digunakan untuk menentukan kapan tindakan nasabah cukup untuk membebaskan bank dari tanggung jawab, kapan kegagalan bank dalam melakukan mitigasi tetap menimbulkan tanggung jawab, bagaimana beban pembuktian seharusnya didistribusikan, serta bagaimana kerugian dapat dibebankan berdasarkan kontribusi kesalahan masing-masing pihak.

Berdasarkan kesenjangan tersebut, kebaruan penelitian ini terletak pada perumusan parameter operasional untuk menentukan tanggung jawab bank dan nasabah, struktur pembuktian, serta model pembebanan kerugian secara berjenjang dalam kasus social engineering. Parameter tersebut mencakup tindakan dan tingkat kehati-hatian nasabah, kepatuhan bank terhadap kewajiban keamanan dan pelindungan konsumen, kemampuan sistem dalam mendeteksi transaksi anomali, respons bank setelah muncul indikasi transaksi mencurigakan, serta hubungan kausal antara kegagalan mitigasi dengan kerugian nasabah. Pendekatan tersebut diharapkan dapat menghasilkan kerangka analisis yang lebih objektif dalam menentukan pembagian tanggung jawab dan tidak semata-mata mendasarkan penilaian pada fakta bahwa nasabah telah memasukkan OTP atau PIN.

Dengan demikian, penelitian ini bertujuan untuk menganalisis: (1) dasar pertanggungjawaban bank dan nasabah atas kerugian akibat social engineering dalam layanan perbankan digital; (2) parameter yang dapat digunakan untuk menentukan proporsi tanggung jawab masing-masing pihak; (3) struktur pembuktian dalam menentukan kesalahan, kelalaian, dan hubungan kausal; serta (4) model pembebanan kerugian yang proporsional berdasarkan kontribusi kesalahan bank dan nasabah. Kajian tersebut diharapkan dapat memberikan kontribusi bagi pengembangan hukum perbankan digital, khususnya dalam mewujudkan keseimbangan antara kepastian hukum, pelindungan nasabah, dan tanggung jawab bank dalam menghadapi perkembangan kejahatan berbasis *social engineering*.

2. METODE

Penelitian ini adalah penelitian hukum normatif yang menelaah norma tentang pelindungan nasabah, keamanan layanan perbankan digital, tanggung jawab bank, transaksi elektronik, dan penyelesaian sengketa konsumen sektor jasa keuangan. Pendekatan yang dipakai ada tiga. Pendekatan perundang-undangan menelaah undang-undang serta peraturan OJK dan Bank Indonesia yang relevan. Pendekatan konseptual menelaah konsep *strict liability*, *proportional liability*, *contributory negligence*, *duty of care*, dan kelalaian institusional. Pendekatan kasus menelaah putusan pengadilan dan putusan lembaga penyelesaian sengketa mengenai kerugian nasabah akibat *phishing*, *vishing*, dan pengambilalihan OTP/PIN.

Bahan hukum primer berupa undang-undang, peraturan pemerintah, peraturan OJK, peraturan Bank Indonesia, dan putusan. Bahan hukum sekunder berupa buku dan artikel jurnal ilmiah, termasuk empat penelitian terdahulu di atas. Bahan hukum tersier berupa kamus hukum dan ensiklopedia. Sebagai pembanding, penelitian ini juga merujuk dua kerangka pembagian kerugian penipuan di yurisdiksi lain, yaitu Inggris dan Singapura. Seluruh bahan dianalisis secara preskriptif, yaitu tidak berhenti menjelaskan hukum yang berlaku, tetapi merumuskan bagaimana tanggung jawab bank dan nasabah seharusnya ditentukan dalam sengketa *social engineering*.

3. HASIL DAN PEMBAHASAN

Konstruksi Pertanggungjawaban Bank dan Nasabah dalam Kejahatan Social Engineering

Dasar pertanggungjawaban perdata dalam perkara ini dapat ditarik dari dua jalur. Jalur pertama adalah hubungan kontraktual. Hubungan bank dan nasabah lahir dari perjanjian, sehingga kegagalan bank memenuhi prestasi, termasuk prestasi menjaga keamanan dana, dapat dikualifikasikan sebagai wanprestasi. Jalur kedua adalah perbuatan melawan hukum, ketika bank melanggar kewajiban hukum atau kepatutan yang diharuskan terhadap kepentingan nasabah. Pada kedua jalur, unsur yang menentukan adalah kesalahan dan hubungan kausal. Karena itu pertanyaan intinya adalah apa sesungguhnya yang menyebabkan kerugian, dan bukan sekadar siapa yang menekan tombol terakhir.

Dari sisi nasabah, perhatian utama tertuju pada ketentuan bahwa kelalaian pengguna dapat membebaskan penyelenggara sistem elektronik. Kelalaian di sini perlu dibedakan dari sekadar keterlibatan dalam rangkaian peristiwa. Nasabah yang menyerahkan OTP kepada orang yang ia yakini sebagai petugas bank, setelah menerima pesan atau panggilan yang dirancang menyerupai komunikasi resmi, berada dalam situasi yang berbeda dari nasabah yang

mengabaikan peringatan eksplisit di aplikasi, menggunakan perangkat yang telah dimodifikasi sehingga keamanannya terbuka, atau menyerahkan kredensialnya secara sukarela kepada pihak ketiga. Karena itu fakta penyerahan kredensial hanya menjadi titik awal pengujian. Fakta itu belum menjadi kesimpulan bahwa nasabah bertanggung jawab penuh.

Dari sisi bank, kewajiban hukumnya lebih luas daripada menyediakan autentikasi. Ketentuan penyelenggaraan teknologi informasi oleh bank umum menuntut tata kelola, manajemen risiko, dan pengamanan informasi, sedangkan ketentuan layanan digital menempatkan keamanan, pemantauan, dan penanganan pengaduan sebagai bagian dari penyelenggaraan layanan. Dalam kerangka pelindungan konsumen, bank juga wajib menyediakan edukasi dan informasi risiko serta menangani pengaduan secara layak. Dengan demikian, bank yang transaksinya lolos autentikasi belum otomatis memenuhi seluruh kewajibannya. Ia masih harus menunjukkan bahwa sistem pemantauan transaksi bekerja pada tingkat yang wajar, bahwa peringatan dan verifikasi tambahan diberikan ketika pola transaksi menyimpang, dan bahwa laporan nasabah ditindaklanjuti dengan cepat. Arah ini sejalan dengan Putusan Pengadilan Negeri Makassar Nomor 248/Pdt.G/2023/PN Mks, yang menilai tindakan bank setelah menerima permintaan pemblokiran dari nasabah korban *phishing* dan menyatakan bank melakukan perbuatan melawan hukum. Putusan tersebut diuraikan lebih lanjut pada bagian 3.2.

Perlu dijelaskan pula mengapa model ini tidak mengadopsi *strict liability* murni. Beban kerugian penuh pada bank tanpa memandang kesalahan memang melindungi nasabah, tetapi mengabaikan insentif nasabah untuk berhati-hati dan berpotensi menimbulkan *moral hazard*. Sebaliknya, aturan yang membebankan semua kerugian kepada nasabah begitu OTP diberikan membiarkan bank tidak berinvestasi pada deteksi anomali, padahal bank berada pada posisi terbaik untuk melakukannya. Doktrin *contributory negligence* yang meniadakan seluruh ganti rugi karena adanya kelalaian korban juga dianggap terlalu keras, dan sistem hukum modern cenderung beralih ke pembagian kerugian menurut kontribusi masing-masing pihak (*comparative fault*). Atas dasar ini, jalan tengahnya adalah pertanggungjawaban berbasis kesalahan dengan pembebanan proporsional, yang memerlukan alat ukur yang jelas. Tanpa parameter, “proporsional” mudah menjadi semata-mata keputusan diskresioner.

Kecenderungan serupa terlihat dalam kebijakan di luar negeri. Di Inggris, sejak Oktober 2024 pengatur sistem pembayaran mewajibkan penyedia jasa pembayaran mengganti kerugian korban *authorised push payment fraud*, yaitu penipuan ketika korban sendiri yang mengotorisasi pembayaran, dengan batas ganti rugi dan pembagian biaya antara bank pengirim dan bank penerima. Singapura sejak Desember 2024 menerapkan *Shared Responsibility*

Framework untuk penipuan *phishing*, yang membagi kewajiban secara berurutan kepada bank dan penyedia telekomunikasi dan baru membebankan kerugian kepada konsumen apabila kewajiban para penyelenggara telah dipenuhi. Kedua kerangka itu menunjukkan bahwa penyerahan kredensial oleh korban tidak lagi diperlakukan sebagai jawaban akhir, melainkan sebagai salah satu variabel dalam uji tanggung jawab.

Parameter Operasional Penentuan Tanggung Jawab Bank dan Nasabah

Berdasarkan analisis norma dan konsep di atas, penelitian ini mengusulkan tujuh parameter. Parameter pertama adalah kelalaian nasabah, yang dinilai dari ada tidaknya penyerahan kredensial secara sukarela dan sadar, pengabaian peringatan keamanan yang jelas, penggunaan perangkat atau tautan yang secara patut dapat dikenali berisiko, serta sejauh mana pelaku berhasil menyamarkan diri sebagai pihak resmi. Parameter kedua adalah kepatuhan bank terhadap kewajiban keamanan, yaitu kecukupan autentikasi, pengamanan sistem, dan edukasi risiko menurut standar regulasi yang berlaku saat kejadian. Parameter ketiga adalah deteksi anomali, yaitu seberapa jauh transaksi menyimpang dari pola normal nasabah dari sisi nominal, frekuensi, perangkat, lokasi, atau penerima, dan apakah penyimpangan itu semestinya terdeteksi oleh sistem yang wajar.

Parameter keempat adalah respons bank, yaitu kecepatan pemblokiran, penahanan dana, dan investigasi setelah nasabah melapor atau setelah transaksi mencurigakan teridentifikasi. Parameter kelima adalah hubungan kausal, yaitu apakah kerugian tetap akan terjadi seandainya bank menjalankan mitigasi yang semestinya. Parameter keenam adalah kemampuan mencegah kerugian, yaitu pihak yang secara realistis lebih mampu mencegah kerugian dengan biaya lebih rendah. Parameter ketujuh adalah besarnya kontribusi kesalahan, yaitu bobot relatif sumbangan masing-masing pihak terhadap terjadinya dan membesarnya kerugian.

Pentingnya parameter respons bank dan hubungan kausal tampak dalam Putusan Pengadilan Negeri Makassar Nomor 248/Pdt.G/2023/PN Mks antara Muhammad Rafie Baharuddin dan PT Bank Sulselbar. Nasabah dalam perkara tersebut menjadi korban *phishing* dan memberikan kode OTP setelah menerima pesan yang mengatasnamakan bank. Menurut pemberitaan perkara, nasabah mengetahui adanya transaksi yang tidak dikehendakinya sekitar pukul 15.42 WITA dan menghubungi bank untuk meminta pemblokiran sekitar pukul 15.51 WITA, tetapi transaksi lanjutan masih terjadi hingga sekitar pukul 16.04 WITA sehingga kerugian mencapai Rp131.485.906. Pengadilan menyatakan bank melakukan perbuatan melawan hukum, menghukum bank membayar ganti kerugian sebesar Rp131.485.906, dan menetapkan uang paksa Rp500.000 per hari apabila bank terlambat membayar setelah putusan berkekuatan hukum tetap. Kajian Aprianti atas putusan ini juga menyimpulkan bahwa

pengadilan mempertimbangkan kegagalan bank menindaklanjuti permintaan pemblokiran dengan segera.

Putusan tersebut mendukung model yang diusulkan dalam dua hal. Pertama, fakta bahwa nasabah menjadi korban *phishing* dan menyerahkan OTP tidak mengakhiri pemeriksaan atas tanggung jawab bank, karena pengadilan juga menilai apa yang dilakukan bank setelah menerima laporan. Jeda antara laporan dan pemblokiran menjadi fakta yang relevan secara hukum, dan di titik itulah parameter keempat (respons bank) dan kelima (hubungan kausal) bekerja, yaitu apakah transaksi lanjutan dapat dicegah seandainya bank memblokir dengan segera. Kedua, putusan ini memperlihatkan keterbatasan praktik yang ada. Ganti rugi yang dijatuhkan sama dengan seluruh jumlah kerugian, dan tidak diberitakan adanya pembagian berdasarkan kontribusi para pihak. Hal itu menunjukkan kebutuhan atas parameter yang eksplisit agar pembebanan kerugian tidak berhenti pada pilihan antara bank menanggung seluruhnya atau nasabah menanggung seluruhnya, yang justru hendak dijawab oleh model enam tahap dalam penelitian ini.

Ketujuh parameter tersebut dapat dipakai untuk menempatkan sebuah sengketa pada salah satu dari tiga tingkat tanggung jawab sebagaimana disajikan pada Tabel 1.

Tabel 1. Tingkat Tanggung Jawab Bank dan Nasabah.

Tingkat	Kondisi yang dominan	Akibat pembebanan kerugian
I. Bank dominan	Nasabah mengikuti prosedur keamanan; transaksi memiliki anomali signifikan; sistem bank gagal mendeteksi atau tidak memitigasi.	Bank menanggung sebagian besar atau seluruh kerugian; kontribusi nasabah diperhitungkan secara terbatas.
II. Proporsional	Nasabah lalai dalam batas tertentu dan bank juga gagal memitigasi; keduanya berkontribusi.	Kerugian dibagi menurut bobot kontribusi masing-masing pihak.
III. Nasabah dominan	Bank membuktikan sistem keamanan dan mitigasi memadai; nasabah mengabaikan peringatan atau bertindak langsung menyebabkan kerugian.	Nasabah menanggung sebagian besar kerugian; bank menanggung bagian terbatas jika masih ada kekurangan respons.

Ketiga tingkat ini bukan kategori kaku. Pembagian ini berfungsi sebagai kerangka penalaran yang menuntun pengambil keputusan agar menimbang semua parameter secara sistematis, bukan hanya parameter pertama. Penetapan angka persentase untuk tiap tingkat sebaiknya menjadi kewenangan regulator atau lembaga penyelesaian sengketa melalui pedoman, karena rentang yang terlalu rigid dapat mengabaikan keunikan kasus. Pedoman semacam itu juga akan memberi kepastian hukum bagi bank dan nasabah, yang selama ini menghadapi putusan yang sulit diprediksi.

Struktur Pembuktian dan Model Pembebanan Kerugian Berjenjang

Hukum acara perdata pada prinsipnya mengharuskan pihak yang mendalilkan suatu hak atau peristiwa membuktikannya. Prinsip ini bertemu dengan ketentuan khusus dalam hukum perlindungan konsumen yang membalik beban pembuktian unsur kesalahan kepada pelaku usaha, yang dapat terbebas apabila membuktikan bahwa kesalahan ada pada konsumen. Ketentuan UU ITE tentang kelalaian pengguna sebagai pengecualian tanggung jawab penyelenggara sistem elektronik juga mengarah ke pembuktian yang bergeser. Dari norma-norma tersebut, struktur pembuktian dapat dirumuskan secara berimbang dan dengan memperhatikan siapa yang menguasai bukti.

Bank, yang menguasai log transaksi, data autentikasi, dan konfigurasi sistem, semestinya membuktikan beberapa hal. Pertama, bahwa sistem keamanannya memenuhi kewajiban regulasi. Kedua, bahwa transaksi telah melalui mekanisme autentikasi yang berlaku. Ketiga, bahwa sistem pendeteksi anomali bekerja dan hasil penilaiannya atas transaksi yang disengketakan. Keempat, bahwa langkah mitigasi telah diambil sejak laporan diterima. Nasabah, yang menguasai pengalaman langsung atas peristiwa, perlu menunjukkan bahwa ia menjadi korban manipulasi, misalnya melalui tangkapan layar pesan, catatan panggilan, atau laporan kepolisian. Nasabah juga perlu menunjukkan bahwa ia melaporkan kejadian dengan segera dan tidak mengabaikan peringatan keamanan yang jelas. Pembagian ini tidak berarti nasabah harus membuktikan semuanya sendiri, karena ketimpangan akses informasi justru menuntut bank menyerahkan data yang diperlukan untuk menilai tanggung jawabnya.

Atas dasar struktur pembuktian itu, penentuan beban kerugian dapat dijalankan secara berjenjang dalam enam tahap. Tahap pertama mengidentifikasi kontribusi kesalahan nasabah, yaitu apa yang dilakukan nasabah, dalam kondisi apa, dan apakah tindakan itu dapat dimaklumi mengingat tingkat manipulasi. Tahap kedua mengidentifikasi kewajiban keamanan bank yang berlaku pada saat kejadian. Tahap ketiga menguji apakah sistem bank mendeteksi, atau seharusnya mendeteksi, transaksi anomali. Tahap keempat menguji hubungan kausal antara kegagalan bank dan kerugian, dengan pertanyaan apakah kerugian dapat dicegah atau dikurangi bila bank bertindak sesuai standar. Tahap kelima menentukan tingkat tanggung jawab berdasarkan hasil tahap-tahap sebelumnya. Tahap keenam menetapkan besaran kerugian yang ditanggung masing-masing pihak, termasuk kemungkinan bank hanya menanggung sebagian karena nasabah terlambat melapor atau mengabaikan peringatan.

Model ini mengubah pertanyaan sengketa. Pertanyaan yang tadinya hanya "apakah bank bertanggung jawab?" menjadi "dalam kondisi apa bank bertanggung jawab, bagaimana hal itu dibuktikan, dan berapa bagian kerugian yang harus ditanggungnya?" Bagi hakim dan lembaga

penyelesaian sengketa, urutan tahapan ini memberikan struktur putusan yang dapat diuji. Bagi bank, model ini memberi insentif nyata untuk memperkuat deteksi anomali dan respons cepat, karena investasi itu langsung mengurangi bagian kerugian yang harus ditanggung. Bagi nasabah, model ini tetap menuntut kehati-hatian karena kelalaian yang nyata tetap diperhitungkan.

4. KESIMPULAN

Pertanggungjawaban atas kerugian yang timbul akibat *social engineering* tidak dapat ditentukan semata-mata berdasarkan fakta bahwa nasabah memberikan OTP atau PIN kepada pelaku. Penentuan pihak yang bertanggung jawab perlu mempertimbangkan kontribusi kesalahan masing-masing pihak sekaligus kewajiban keamanan yang melekat pada bank, mengingat bank memiliki kendali atas sistem dan infrastruktur layanan perbankan, sedangkan nasabah bertanggung jawab sepanjang terbukti melakukan kelalaian yang nyata. Untuk menentukan pembebanan tanggung jawab secara adil, terdapat tujuh parameter yang perlu dipertimbangkan, yaitu tingkat kelalaian nasabah, kepatuhan bank terhadap kewajiban keamanan, kemampuan bank dalam mendeteksi anomali transaksi, respons bank setelah munculnya indikasi transaksi mencurigakan, hubungan kausal antara tindakan para pihak dan kerugian, kemampuan masing-masing pihak dalam mencegah kerugian, serta besarnya kontribusi kesalahan masing-masing pihak. Parameter tersebut selanjutnya dapat diterapkan melalui model pembebanan tanggung jawab yang terdiri atas enam tahap analisis dan menghasilkan tiga tingkat pertanggungjawaban, yaitu tanggung jawab bank secara dominan, tanggung jawab secara proporsional, dan tanggung jawab nasabah secara dominan. Dalam penerapannya, pembuktian juga perlu mempertimbangkan penguasaan alat bukti, sehingga beban pembuktian ditempatkan pada pihak yang secara lebih nyata menguasai dan memiliki akses terhadap bukti yang relevan. Dengan pendekatan tersebut, pertanggungjawaban atas kerugian akibat *social engineering* dapat ditentukan berdasarkan penilaian yang menyeluruh terhadap perilaku nasabah, kewajiban dan kemampuan bank, serta hubungan sebab akibat antara kelalaian para pihak dengan timbulnya kerugian.

Saran

Bagi OJK dan pembentuk regulasi, perlu disusun pedoman yang lebih jelas mengenai parameter tanggung jawab bank dan nasabah dalam kasus *social engineering*, termasuk mekanisme pembuktian dan rentang pembagian kerugian, dengan memperhatikan pengalaman kerangka tanggung jawab bersama di yurisdiksi lain. Bagi bank, perlu penguatan sistem deteksi transaksi anomali, pemantauan waktu nyata, mekanisme pemblokiran cepat, autentikasi

berlapis, dan penanganan pengaduan yang responsif. Bagi nasabah, kewajiban menjaga OTP, PIN, kata sandi, dan perangkat tetap berlaku, tetapi kewajiban itu tidak semestinya dijadikan dasar otomatis untuk membebankan seluruh kerugian kepada nasabah bila bank juga gagal menjalankan mitigasi.

DAFTAR PUSTAKA

Agustina, R. (2003). *Perbuatan melawan hukum*. Program Pascasarjana FHUI.

Aprianti, N. K. D. (n.d.). Batas pertanggungjawaban bank terhadap kerugian nasabah akibat tindakan phising. *Kertha Semaya: Journal Ilmu Hukum*. https://ojs.unud.ac.id/index.php/kerthasemaya/article/view/114466

Calabresi, G. (1970). *The costs of accidents: A legal and economic analysis*. Yale University Press.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan hukum terhadap nasabah atas kejahatan phising dan hacking pada layanan bank digital ditinjau berdasarkan hukum positif Indonesia. *Hakim: Jurnal Ilmu Hukum dan Sosial, 2*(1). https://journal.stekom.ac.id/index.php/Hakim/article/download/1535/1055

detikSulsel. (n.d.-a). Bank Sulselbar dihukum ganti rugi Rp131 juta terkait dana nasabah raib. *detik.com*. https://www.detik.com/sulsel/hukum-dan-kriminal/d-7097675/bank-sulselbar-dihukum-ganti-rugi-rp-131-juta-terkait-dana-nasabah-raib

detikSulsel. (n.d.-b). Bank Sulselbar digugat nasabah gegara tabungan Rp131 juta di rekening raib. *detik.com*. https://www.detik.com/sulsel/hukum-dan-kriminal/d-6863598/bank-sulselbar-digugat-nasabah-gegara-tabungan-rp-131-juta-di-rekening-raib

Dobbs, D. B., Hayden, P. T., & Bublick, E. M. (2011). *The law of torts* (2nd ed.). West.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

Harahap, M. Y. (2016). *Hukum acara perdata*. Sinar Grafika.

Hasanudin, T. A. (2026). Perlindungan nasabah dan tanggung jawab bank dalam penanggulangan kejahatan digital berbasis social engineering: Analisis hukum perbankan Indonesia. *Indonesia Journal of Business Law, 5*(1). https://doi.org/10.47709/ijbl.v5i1.7476

Indonesia. (1992). *Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan*.

Indonesia. (1998). *Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan*.

Indonesia. (1999). *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*.

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

Kitab Undang-Undang Hukum Perdata.

Marzuki, P. M. (2017). *Penelitian hukum* (edisi revisi). Kencana.

Monetary Authority of Singapore, & Infocomm Media Development Authority. (n.d.). *Shared responsibility framework guidelines*. https://www.mas.gov.sg/

Mulyadi, R., Rahmat, D., & Pratama, R. K. (2026). Tanggung jawab hukum pihak bank atas kerugian nasabah akibat kejahatan phising. *Jurnal Greenation Sosial dan Politik, 4*(1). https://doi.org/10.38035/jgsp.v4i1.607

Otoritas Jasa Keuangan. (2020). *Roadmap pengembangan perbankan Indonesia 2020–2025*.

Otoritas Jasa Keuangan. (2021). *Cetak biru transformasi digital perbankan*.

Otoritas Jasa Keuangan. (2022a). *Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*.

Otoritas Jasa Keuangan. (2022b). *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum*.

Otoritas Jasa Keuangan. (2023a). *Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum*.

Otoritas Jasa Keuangan. (2023b). *Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*.

Otoritas Jasa Keuangan. (n.d.). *Indonesia Anti-Scam Centre*. https://iasc.ojk.go.id/

Payment Systems Regulator. (2023). *Faster payments APP scams: Requiring reimbursement* (Policy Statement PS23/3). https://www.psr.org.uk/

Pengadilan Negeri Makassar. (2023). *Putusan Nomor 248/Pdt.G/2023/PN Mks: Muhammad Rafie Baharuddin melawan PT Bank Sulselbar*.

Shavell, S. (1987). *Economic analysis of accident law*. Harvard University Press.

Shidarta. (2006). *Hukum perlindungan konsumen Indonesia*. Grasindo.

Sjahdeini, S. R. (1993). *Kebebasan berkontrak dan perlindungan yang seimbang bagi para pihak dalam perjanjian kredit bank di Indonesia*. Institut Bankir Indonesia.

Widjana, N. P. J. M. P., Antari, P. E. D., Kurniawan, I. G. A., & Ari Rama, B. G. (2025). Pertanggungjawaban bank terhadap kerugian nasabah akibat pencurian dana melalui phising. *Locus: Jurnal Konsep Ilmu Hukum, 5*(3). https://doi.org/10.56128/jkih.v5i3.649