Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora
Volume. 4, Nomor. 1, Maret 2026
e-ISSN :2988-2273 ; p-ISSN :2988-2281, Hal. 365-379
DOI: https://doi.org/10.59059/mandub.v4i1.3555
Tersedia: https://journal.staiypiqbaubau.ac.id/index.php/Mandub

Perlindungan Hukum Nasabah terhadap Kejahatan *Social Engineering* dalam Transaksi Perbankan Digital di Indonesia

Syakira Hilwa
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Singaperbangsa Karawang, Indonesia
Penulis Korespondensi: syakiraciwciw@gmail.com

Abstract*. The rapid development of digital banking services has made financial transactions more convenient for the public. However, it has also increased the risk of technology-based crimes, including social engineering. Unlike conventional cyberattacks, social engineering does not necessarily involve direct attacks on banking systems; instead, perpetrators manipulate customers into conducting transactions or disclosing confidential security information. This situation raises important legal issues concerning customer protection and the allocation of liability when financial losses occur. This study aims to analyze the forms of legal protection available to customers who become victims of social engineering and to examine the liability of banks in Indonesia for losses arising from digital banking transactions. The research employs a normative legal research method using both the statutory approach and the conceptual approach. The legal materials consist of legislation, regulations issued by the Financial Services Authority (Otoritas Jasa Keuangan), as well as relevant books and scholarly journals. The findings indicate that legal protection for banking customers is supported by various legal provisions, particularly those governing the security of digital banking services, consumer protection, and data security. Nevertheless, the existing legal framework still faces challenges in determining the allocation of liability between banks and customers because social engineering transactions are often conducted using the customers' own credentials. Therefore, the determination of liability should not rely solely on the use of one-time passwords (OTP), personal identification numbers (PIN), or customer credentials, but should also take into account the degree of negligence, the bank's security obligations, the characteristics of the transaction, and the contribution of each party to the resulting loss. Strengthening legal protection requires the implementation of multilayered security systems and clearer standards for allocating liability between banks and customers.*

Keywords*: Bank Liability; Customer Protection; Digital Banking; Digital Crime; Social Engineering*.

Abstrak. Peningkatan layanan perbankan digital memberikan kemudahan bagi masyarakat dalam melakukan transaksi keuangan, tetapi di sisi lain juga meningkatkan risiko kejahatan berbasis teknologi, termasuk *social engineering*. Kejahatan ini memiliki karakteristik yang berbeda karena pelaku tidak selalu menyerang sistem perbankan secara langsung, melainkan memanipulasi korban untuk melakukan transaksi atau memberikan informasi keamanan. Kondisi tersebut menimbulkan persoalan mengenai perlindungan hukum terhadap nasabah dan pembagian tanggung jawab apabila terjadi kerugian. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap nasabah yang menjadi korban *social engineering* serta tanggung jawab bank di Indonesia terhadap kerugian yang timbul akibat transaksi perbankan digital. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Bahan hukum yang digunakan meliputi peraturan perundang-undangan, peraturan Otoritas Jasa Keuangan, serta literatur dan jurnal yang relevan. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah telah didukung oleh berbagai ketentuan, khususnya yang berkaitan dengan keamanan layanan digital, pelindungan konsumen, dan keamanan data. Namun, kerangka hukum yang ada masih menghadapi persoalan dalam menentukan batas tanggung jawab antara bank dan nasabah karena transaksi *social engineering* sering kali dilakukan menggunakan kredensial nasabah. Oleh karena itu, penentuan tanggung jawab tidak seharusnya hanya didasarkan pada penggunaan OTP, PIN, atau kredensial nasabah, tetapi perlu mempertimbangkan tingkat kelalaian, kewajiban keamanan bank, karakteristik transaksi, serta kontribusi masing-masing pihak terhadap timbulnya kerugian. Penguatan perlindungan hukum diperlukan melalui penerapan sistem keamanan berlapis serta standar yang lebih jelas dalam menentukan pembagian tanggung jawab antara bank dan nasabah.

Kata Kunci: Kejahatan Digital; Perbankan Digital; Perlindungan Nasabah; *Social Engineering*; Tanggung Jawab Bank.

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

1. PENDAHULUAN

Kegiatan perbankan Indonesia telah berubah secara signifikan karena kemajuan teknologi informasi. Semakin banyak orang beralih ke layanan perbankan berbasis digital seperti mobile banking, internet banking, dan berbagai jenis transaksi elektronik lainnya, yang sebelumnya biasanya dilakukan secara langsung di kantor bank. Transaksi dapat dilakukan dengan lebih cepat, praktis, dan fleksibel karena perubahan ini memudahkan masyarakat. Namun, perubahan ini juga menimbulkan ancaman baru, terutama yang berkaitan dengan keamanan transaksi konsumen dan data pribadi. Dalam Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum, Otoritas Jasa Keuangan menyatakan bahwa pengembangan layanan digital perbankan harus mempertimbangkan manajemen risiko, keamanan data nasabah, dan perlindungan konsumen.

Social engineering adalah salah satu jenis kejahatan yang berkembang seiring dengan meningkatnya penggunaan layanan perbankan digital. Kejahatan ini dilakukan dengan menggunakan manipulasi psikologis untuk mendapatkan informasi atau tindakan tertentu dari korban. Misalnya, mereka memanfaatkan tautan palsu, pesan yang terlihat seperti layanan bank, atau meminta kode OTP, PIN, dan data pribadi. Social engineering lebih banyak memanfaatkan kelengahan dan kepercayaan korban daripada serangan yang secara langsung merusak sistem teknologi bank. Studi sosial engineering tentang industri perbankan digital menunjukkan bahwa pemahaman yang buruk tentang modus kejahatan digital dan keamanan data dapat menyebabkan kerugian klien. Namun, itu juga terkait dengan kesiapan sistem keamanan dan instruksi yang diberikan oleh bank.

Problem ini semakin serius karena data yang digunakan untuk kejahatan social engineering dapat melibatkan data pribadi dan keuangan klien. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur hak dan tanggung jawab subjek data dan pihak yang melakukan pemrosesan data pribadi, serta menetapkan data keuangan pribadi sebagai salah satu jenis data pribadi yang khusus. Oleh karena itu, perlindungan konsumen tidak hanya mencakup keamanan saldo atau transaksi, tetapi juga bagaimana data dan informasi pribadi konsumen dikelola dan dilindungi.

Sebaliknya, pelanggan memiliki status konsumen jasa keuangan, yang berarti mereka akan dilindungi sesuai dengan ketentuan perlindungan konsumen. Sekarang berlaku, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen mengatur hak dan kewajiban konsumen serta tanggung jawab pelaku usaha atas kerugian konsumen. POJK Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan memperkuat

undang-undang ini di sektor jasa keuangan dengan mengatur hak dan kewajiban konsumen, perlindungan data konsumen, dan keamanan sistem.

Terlepas dari fakta bahwa banyak ketentuan telah dibuat untuk melindungi pelanggan, masih ada pertanyaan tentang siapa yang bertanggung jawab atas kerugian yang disebabkan oleh social engineering. Dalam praktiknya, korban seringkali berada dalam situasi sulit karena transaksi dapat dilakukan menggunakan kredensial milik pelanggan sendiri setelah pelaku berhasil memanipulasi korban. Kemudian muncul pertanyaan apakah tanggung jawab sepenuhnya ditanggung oleh nasabah karena kelalaian menjaga data pribadi atau apakah bank juga bertanggung jawab jika sistem keamanan bermasalah, mendeteksi transaksi mencurigakan, dan mendidik dan melindungi pelanggan. Pentingnya pembagian tanggung jawab ini karena perlindungan konsumen dalam industri jasa keuangan tidak hanya menuntut konsumen untuk berhati-hati, tetapi juga mewajibkan pelaku usaha jasa keuangan untuk mengikuti standar perlindungan konsumen dan menjaga keamanan sistem dan informasi yang digunakan.

Oleh karena itu, kajian hukum yang tidak hanya melihat social engineering sebagai bentuk kejahatan digital perlu dilakukan, itu juga penting untuk melihat hubungan antara kewajiban nasabah untuk melindungi informasi mereka dengan kewajiban bank untuk memberikan layanan digital yang aman, mencegah risiko, dan menangani pengaduan dan klaim. Berdasarkan permasalahan tersebut, penelitian ini mengangkat judul "Perlindungan Hukum Nasabah terhadap Kejahatan *Social Engineering* dalam Transaksi Perbankan Digital di Indonesia".

2. METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan jenis penelitian hukum normatif yang berfokus pada norma dan kaidah hukum yang relevan dengan masalah yang diteliti. Penelitian hukum normatif melihat ketentuan hukum yang melindungi nasabah dalam transaksi perbankan digital, terutama dalam kasus di mana kerugian disebabkan oleh kejahatan social engineering. Metode ini tidak hanya melihat adanya undang-undang, tetapi juga menganalisis bagaimana berbagai ketentuan hukum berhubungan dan diterapkan untuk memberikan perlindungan kepada nasabah.

Peraturan dan undang-undang yang berkaitan dengan perbankan digital, perlindungan konsumen, perlindungan data pribadi, dan penyediaan layanan digital oleh bank adalah sumber hukum penelitian ini. Beberapa regulasi utama yang digunakan antara lain Undang-Undang

Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum, dan Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan**.**

POJK 21/2023 mengatur bagaimana bank menjalankan layanan digital, termasuk infrastruktur teknologi informasi dan perlindungan data pribadi. POJK 22/2023 mengatur perlindungan konsumen, hak dan kewajiban mereka, keamanan sistem informasi, dan mekanisme pengaduan dan penyelesaian sengketa.

Pendekatan Penelitian

Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*)**.** Metode perundang-undangan ini dilakukan dengan meninjau berbagai peraturan yang berkaitan dengan penyelenggaraan transaksi perbankan digital dan perlindungan hukum nasabah. Metode ini diperlukan untuk mengetahui bagaimana hukum positif Indonesia mengatur kewajiban bank, hak nasabah, perlindungan data pribadi, keamanan layanan digital, dan mekanisme penyelesaian ketika nasabah mengalami kerugian.

Sementara itu, pendekatan konseptual digunakan untuk memahami konsep hukum yang berkaitan dengan perlindungan hukum, tanggung jawab bank, keamanan transaksi digital, dan social engineering. Metode ini digunakan agar analisis tidak hanya berhenti pada bunyi peraturan, tetapi juga dapat melihat bagaimana konsep tanggung jawab dan perlindungan nasabah diterapkan dalam kasus kejahatan social engineering. POJK 21/2023 menempatkan manajemen risiko, keamanan data, dan perlindungan konsumen sebagai elemen penting dalam penyelenggaraan layanan digital perbankan.

Sumber Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan hukum yang memiliki kekuatan mengikat, terutama undang-undang yang berkaitan langsung dengan subjek penelitian. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum, dan Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan adalah bahan hukum utama dalam penelitian ini.

Bahan hukum sekunder membantu dan meningkatkan analisis bahan hukum primer. Sumber penelitian ini mencakup publikasi resmi lembaga, buku hukum, artikel, dan jurnal ilmiah tentang perbankan digital, perlindungan konsumen, keamanan data, dan social engineering. Jurnal resmi Otoritas Jasa Keuangan juga digunakan sebagai sumber karena menjelaskan bagaimana mengatur dan menerapkan transformasi digital di sektor perbankan. OJK menyatakan bahwa POJK 21/2023 adalah penyempurnaan dari undang-undang sebelumnya. Ini mengatur layanan digital, penggunaan teknologi informasi, perlindungan konsumen, dan perlindungan data pribadi.

Teknik Pengumpulan Bahan Hukum

Pengumpulan bahan hukum dilakukan melalui studi perpustakaan (*library research*), yaitu menelusuri, mengumpulkan, dan mempelajari berbagai bahan hukum yang terkait dengan masalah penelitian. Bahan hukum ini berasal dari peraturan perundang-undangan, dokumen resmi OJK, jurnal ilmiah, dan literatur hukum tentang kejahatan social engineering dan perlindungan nasabah dalam transaksi perbankan digital.

Peneliti menekankan pada sumber yang terkait langsung dengan subjek penelitian mereka selama proses pengumpulan bahan hukum. Hal ini dilakukan agar materi yang digunakan tidak hanya relevan untuk kejahatan siber tetapi juga dapat memberikan dasar yang jelas untuk menganalisis hubungan antara kewajiban bank, hak nasabah, keamanan layanan digital, perlindungan data pribadi, dan tanggung jawab atas kerugian yang disebabkan oleh *social engineering* (POJK Nomor 21 Tahun 2023; POJK Nomor 22 Tahun 2023).

Teknik Analisis Bahan Hukum

Bahan hukum yang telah dikumpulkan akan dianalisis secara kualitatif, Dengan kata lain, ketentuan hukum yang relevan dengan masalah yang diteliti diuraikan dan dihubungkan. Analisis ini dilakukan dengan membandingkan ketentuan dari berbagai undang-undang untuk melihat jenis perlindungan hukum yang diberikan kepada nasabah serta batas tanggung jawab bank terhadap kerugian yang disebabkan oleh social engineering.

Selanjutnya, hasil analisis digunakan untuk menjawab rumusan masalah secara sistematis dengan mengaitkan norma hukum dengan ciri-ciri kejahatan social engineering dalam transaksi perbankan digital. Oleh karena itu, penelitian tidak hanya menjelaskan peraturan yang berlaku, tetapi juga melihat apakah peraturan saat ini memberikan perlindungan yang memadai bagi pelanggan. Ini termasuk menentukan bagaimana tanggung jawab antara pelanggan dan bank dibagi ketika transaksi terjadi karena tindakan kriminal.

3. HASIL DAN PEMBAHASAN

Hasil dan Pembahasan

Nasabah sekarang dapat melakukan transaksi tanpa harus pergi ke kantor bank berkat perkembangan layanan perbankan digital. Namun, kemudahan ini juga diikuti dengan munculnya berbagai jenis kejahatan yang memanfaatkan kelemahan manusia dan teknologi. *Social engineering*, teknik manipulasi yang digunakan untuk mendorong korban untuk melakukan tindakan yang menguntungkan pelaku atau memberikan informasi tertentu, adalah salah satu jenis kejahatan tersebut. Karena pelaku tidak selalu perlu memasuki sistem keamanan bank secara langsung, tetapi cukup memanipulasi klien sebagai pengguna layanan, social engineering menjadi masalah dalam sektor perbankan.

Phishing, vishing, penyamaran sebagai petugas bank, pesan melalui aplikasi percakapan, dan pemberian tautan atau aplikasi palsu adalah beberapa cara *sosial engineering* dapat dilakukan. Dalam phishing, pelaku biasanya menyamar sebagai orang yang dipercaya korban dan mengarahkannya untuk membuka tautan atau memasukkan informasi rahasia. Sementara vishing dilakukan melalui komunikasi suara atau telepon dengan tujuan mendapatkan informasi. Penelitian tentang ancaman phishing pada layanan keuangan online menunjukkan bahwa metode ini menggunakan rekayasa sosial untuk meniru identitas pihak berwenang, mendorong korban untuk mengikuti perintah pelaku.

Adanya keterlibatan korban dalam proses terjadinya transaksi adalah masalah utama dalam *social engineering*. Dalam kasus social engineering, korban dapat memberikan informasi autentikasi atau melakukan tindakan tertentu setelah diyakinkan oleh pelaku; ini berbeda dengan pencurian melalui pembobolan sistem secara langsung. Dengan demikian, transaksi yang sebenarnya dilakukan oleh pelaku dapat dianggap sebagai transaksi yang dilakukan oleh nasabah secara sah. Dalam situasi seperti ini, siapa yang bertanggung jawab jika terjadi kerugian, terutama jika sistem perbankan berhasil memverifikasi kredensial yang digunakan dalam transaksi.

Oleh karena itu, social engineering bukan hanya masalah ketidakhati-hatian pelanggan. Kewajiban penyelenggara layanan termasuk menjaga keamanan layanan perbankan digital. Bank diharuskan untuk menerapkan prinsip pengendalian pengamanan data dan transaksi nasabah dalam setiap sistem elektronik yang digunakan untuk layanan digital, menurut POJK Nomor 21 Tahun 2023. Kerahasiaan, integritas, ketersediaan, autentikasi, pengendalian otorisasi, dan dokumentasi audit adalah beberapa contoh keamanan ini.

Perlindungan Hukum terhadap Nasabah Korban Social Engineering

Nasabah yang melakukan transaksi perbankan digital pada dasarnya berfungsi sebagai konsumen jasa keuangan serta pengguna rekening. Oleh karena itu, prinsip perlindungan konsumen sangat penting dalam hubungan antara bank dan nasabah. Ini semakin penting dalam layanan digital karena transaksi dilakukan melalui sistem elektronik, yang memungkinkan risiko keamanan data dan transaksi tanpa adanya interaksi langsung antara nasabah dan petugas bank.

Kewajiban bank untuk menjaga data dan transaksi pelanggan adalah salah satu cara untuk melindungi pelanggan. Menurut POJK Nomor 21 Tahun 2023, bank harus menerapkan prinsip pengendalian pengamanan data dan transaksi nasabah pada setiap sistem elektronik yang digunakan dalam layanan digital. Ketentuan ini menunjukkan bahwa kewajiban bank tidak terbatas pada menyediakan aplikasi atau fasilitas transaksi, tetapi juga mencakup penyelenggaraan sistem yang mampu menjaga keamanan data dan transaksi nasabah.

Selain itu, POJK Nomor 22 Tahun 2023 memberikan perlindungan yang lebih baik bagi konsumen yang bekerja dalam industri jasa keuangan. Pasal 19 mewajibkan Pelaku Usaha Jasa Keuangan (PUJK) untuk menjaga kerahasiaan dan keamanan data konsumen dan menerapkan prinsip perlindungan data pribadi. Ini juga berlaku ketika PUJK bekerja sama dengan pihak lain dalam mengelola data konsumen.

Berdasarkan Pasal 24 POJK Nomor 22 Tahun 2023, kewajiban PUJK untuk memastikan keamanan sistem informasi dan ketahanan siber memperkuat perlindungan tersebut. Keamanan sistem informasi mencakup pengamanan kerahasiaan, integritas, dan ketersediaan informasi, sedangkan ketahanan siber mencakup proses identifikasi ancaman dan kerentanan, perlindungan aset, deteksi insiden siber, serta penanggulangan dan pemulihan insiden siber. Ini berarti bahwa bank harus melindungi pelanggan secara preventif dan responsif ketika terjadi masalah keamanan.

Tanggung Jawab Bank terhadap Kerugian Nasabah akibat Social Engineering

Tanggung jawab bank menjadi lebih kompleks ketika transaksi yang merugikan nasabah terjadi setelah korban memberikan informasi tertentu kepada pelaku. Dalam situasi seperti itu, bank tidak dapat secara otomatis dianggap bertanggung jawab atas semua kerugian karena perlu mempertimbangkan bagaimana transaksi terjadi, informasi yang diberikan oleh pelanggan, apakah terdapat kesalahan atau kelalaian bank, dan apakah sistem bank telah mematuhi peraturan keamanan. Karena kredensial konsumen dapat diperoleh melalui manipulasi korban dalam kasus *social engineering*, penggunaan kredensial konsumen dalam

transaksi juga tidak serta-merta menunjukkan bahwa konsumen secara sadar melakukan transaksi tersebut.

Ketika transaksi yang merugikan nasabah terjadi setelah korban memberikan informasi tertentu kepada pelaku, tanggung jawab bank menjadi lebih kompleks. Bank tidak dapat secara otomatis bertanggung jawab atas semua kerugian dalam situasi seperti itu karena perlu mempertimbangkan bagaimana transaksi terjadi, informasi yang diberikan oleh pelanggan, apakah terjadi kesalahan atau kelalaian bank, dan apakah sistem bank telah mematuhi peraturan keamanan. Karena dalam kasus *social engineering*, kredensial konsumen dapat diperoleh melalui manipulasi korban, penggunaan kredensial konsumen dalam transaksi juga tidak serta-merta menunjukkan bahwa konsumen secara sadar melakukan transaksi tersebut.

Di sisi lain, nasabah juga wajib menjaga keamanan data yang digunakan dalam transaksi. Akibatnya, teknik penyelesaian kerugian yang disebabkan oleh social engineering tidak seharusnya menggunakan metode yang secara otomatis membebankan semua kerugian kepada satu pihak. Kontribusi masing-masing pihak terhadap kerugian harus dipertimbangkan. Jika nasabah secara tidak sengaja atau secara tidak sengaja memberikan OTP, PIN, atau kredensial kepada pihak lain, hal itu dapat menjadi masalah. Namun, jika terjadi kegagalan sistem pengamanan bank atau bank tidak memenuhi tanggung jawab yang ditetapkan oleh undang-undang, tanggung jawab bank juga harus dipertimbangkan dalam konteks situasi tertentu. Metode ini lebih sesuai dengan sifat social engineering, yang memang memanfaatkan interaksi antara sistem keamanan digital dan kelemahan manusia.

Analisis Perlindungan Hukum terhadap Nasabah Korban Social Engineering

Secara normatif, Indonesia memiliki sejumlah instrumen hukum yang dapat digunakan untuk melindungi klien yang menjadi korban social engineering. Rezim hukum perbankan, perlindungan konsumen, perlindungan data pribadi, dan peraturan layanan digital perbankan adalah sumber perlindungan tersebut. Misalnya, POJK Nomor 21 Tahun 2023 membuat bank harus menerapkan pengendalian untuk menjaga data dan transaksi nasabah di semua sistem elektronik yang digunakan dalam layanan digital. Sementara itu, POJK Nomor 22 Tahun 2023 secara normatif menetapkan bahwa bank memiliki kewajiban yang jelas untuk membangun sistem layanan digital yang aman. Ini karena undang-undang ini menetapkan bahwa pelaku usaha jasa keuangan harus menjaga keamanan data dan informasi konsumen serta menerapkan keamanan sistem informasi dan ketahanan siber.

Namun, apakah ada atau tidaknya aturan tidak menentukan masalahnya. Permasalahan yang lebih mendasar adalah sejauh mana aturan tersebut mampu memberikan perlindungan ketika kejahatan terjadi melalui manipulasi terhadap klien. Karena pelaku memanfaatkan

pelanggan sebagai jalan masuk, social engineering berbeda dengan pembobolan sistem secara langsung. Akibatnya, bank dapat memiliki alasan untuk menganggap transaksi sebagai transaksi yang sah ketika dilakukan menggunakan perangkat, akun, atau kredensial yang secara teknis terdaftar atas nama nasabah. Ini menimbulkan masalah hukum karena validitas autentikasi secara teknis tidak selalu berarti adanya kehendak yang sah dari pemilik rekening.

Kondisi ini menunjukkan bahwa keamanan transaksi perbankan digital tidak hanya dapat diukur dari kemampuan sistem untuk mengidentifikasi username, password, PIN, atau OTP. Meskipun sistem dapat mengidentifikasi kredensial yang benar, mereka mungkin tidak dapat memastikan bahwa orang yang menggunakan kredensial tersebut benar-benar bertindak sesuai dengan keinginan pemilik rekening. Dengan kata lain, keamanan autentikasi belum tentu identik dengan keamanan transaksi. Persoalan ini sangat penting karena social engineering bekerja dengan membuat korban menyerahkan informasi atau melakukan tindakan yang kemudian digunakan pelaku untuk melakukan transaksi. Studi mengenai perlindungan hukum terhadap social engineering juga menunjukkan bahwa ada masalah dalam menentukan tanggung jawab bank ketika transaksi terjadi melalui manipulasi terhadap nasabah.

Oleh karena itu, pertanyaan apakah nasabah memberikan OTP atau PIN kepada pelaku tidak seharusnya menjadi fokus perlindungan hukum terhadap korban social engineering. Bagaimana bank memenuhi kewajiban pengamanannya sebelum, ketika, dan setelah transaksi adalah pertanyaan yang lebih penting. Apabila bank memiliki sistem yang dapat mendeteksi pola transaksi tidak wajar tetapi tidak melakukan tindakan pengamanan yang tepat, situasi ini harus dipertimbangkan saat menentukan tanggung jawab. Sebaliknya, jika sistem bank berjalan sesuai prosedur dan kerugian hanya terjadi karena tindakan pelanggan yang secara sadar mengabaikan peringatan keamanan, hal ini juga harus dipertimbangkan.

Dengan demikian, pola pikir "nasabah memberikan OTP = nasabah pasti salah" tidak seharusnya mewakili perlindungan hukum terhadap nasabah. Pola pikir ini terlalu sederhana untuk menggambarkan karakter social engineering. Dalam menentukan siapa yang bertanggung jawab, keseluruhan rangkaian kejadian serta kewajiban hukum masing-masing pihak harus dipertimbangkan. Hal ini penting karena prinsip perlindungan konsumen tetap relevan tetapi tidak menghilangkan kewajiban konsumen untuk menjaga keamanan data pribadi mereka.

Bentuk Perlindungan Preventif terhadap Nasabah

Perlindungan preventif melindungi terhadap kerugian sebelum terjadi. Karena ciri khas kejahatan social engineering adalah memanfaatkan kelengahan, keyakinan, dan ketidaktahuan korban, perlindungan preventif sangat penting. Oleh karena itu, upaya pencegahan seharusnya

menjadi bagian dari tanggung jawab bank untuk membangun sistem perbankan digital yang aman, bukan hanya memberi tahu nasabah untuk mempertahankan OTP atau PIN.

POJK Nomor 22 Tahun 2023 mengatur keamanan sistem informasi dan ketahanan siber, termasuk identifikasi ancaman, perlindungan aset, deteksi insiden, penanggulangan, dan pemulihan. Sementara itu, POJK Nomor 21 Tahun 2023 mewajibkan bank menerapkan pengendalian pengamanan data dan transaksi, termasuk autentikasi, pengendalian otorisasi, serta pemeliharaan jejak audit. Ini menunjukkan bahwa tanggung jawab bank sebenarnya bersifat proaktif, bukan hanya menanggapi ketika nasabah kehilangan uang.

Permasalahannya adalah bahwa instruksi klien seringkali menjadi garis pertahanan yang paling mudah ditekankan dalam praktik *social engineering*. Klien diminta untuk menghindari memberikan OTP, PIN, atau password kepada orang lain. Meskipun pendidikan penting, perlindungan konsumen dapat berubah menjadi sekadar pemindahan risiko kepada konsumen jika dijadikan dasar utama untuk melepaskan tanggung jawab bank. Padahal, bank memiliki sumber daya, teknologi, dan kemampuan teknis yang jauh lebih besar daripada nasabah individu untuk menemukan transaksi mencurigakan.

Oleh karena itu, edukasi pelanggan seharusnya dimasukkan ke dalam salah satu lapisan perlindungan, bukan sebagai satu-satunya. Bank harus tetap mengembangkan sistem yang dapat mengenali transaksi yang tidak sesuai dengan standar, memberikan peringatan tambahan tentang transaksi tertentu, dan memiliki cara untuk memblokir atau menghentikan transaksi ketika ada indikasi penyalahgunaan. Karena kejahatan tersebut memanfaatkan kelemahan manusia sekaligus memanfaatkan sistem transaksi digital, pendekatan berlapis ini lebih sesuai dengan sifat social engineering.

Perlindungan Represif dan Penyelesaian Kerugian Nasabah

Ketika upaya pencegahan tidak berhasil dan klien mengalami kerugian, perlindungan represif diperlukan. Dalam situasi seperti ini, masalahnya tidak lagi sekadar mencegah pelanggaran, tetapi memastikan bahwa korban memiliki akses yang mudah ke proses pengaduan dan penyelesaian sengketa. Menurut POJK Nomor 22 Tahun 2023, konsumen memiliki hak untuk menyampaikan pengaduan kepada Pelaku Usaha Jasa Keuangan dan meminta penanganan atas masalah yang mereka hadapi.

Namun, apabila proses pemeriksaan hanya berfokus pada informasi bahwa transaksi telah dilakukan menggunakan kredensial konsumen, mekanisme pengaduan akan menjadi tidak efektif. Dalam konteks social engineering, memastikan bahwa OTP atau password digunakan dengan benar dapat berkontribusi pada keberhasilan tindakan kriminal. Oleh karena itu, pemeriksaan seharusnya tidak hanya menilai **"**siapa yang menggunakan kredensial"**,** tetapi

juga “bagaimana kredensial tersebut dapat digunakan dan apakah sistem bank telah melakukan pengamanan yang seharusnya”**.**

Permasalahan ini terkait erat dengan ketimpangan informasi yang terjadi antara bank dan konsumen. Bank dapat melihat log transaksi, informasi perangkat, waktu dan lokasi transaksi, serta pola atau lokasi transaksi. Sementara itu, kebanyakan pelanggan hanya mengetahui bahwa saldo telah berkurang setelah transaksi dilakukan. Agar klien tidak berada dalam situasi yang sulit untuk membuktikan bahwa dia adalah korban, ketidaksesuaian ini harus diperhatikan selama proses pengadilan.

Oleh karena itu, proses penyelesaian pengaduan harus digunakan tidak hanya sebagai alat administrasi, tetapi juga untuk mengungkap sebab-sebab transaksi dan menentukan siapa yang bertanggung jawab. Sangat penting untuk memberikan transparansi tentang hasil investigasi karena klien berhak untuk mengetahui mengapa pengaduan diterima atau ditolak. Ini juga dapat meningkatkan akuntabilitas bank dalam menangani kejahatan digital.

Pembagian Tanggung Jawab antara Bank dan Nasabah

Dalam hal *social engineering*, bagian yang paling kompleks adalah masalah pembagian tanggung jawab. Nasabah harus menjaga kerahasiaan data autentikasi. Namun, kewajiban tersebut secara otomatis menjadi tanggung jawab pelanggan untuk setiap transaksi yang menggunakan kredensial pelanggan. Sebaliknya, kewajiban bank untuk menyediakan sistem yang aman tidak berarti bahwa bank harus membayar semua kerugian konsumen.

Akibatnya, penentuan tanggung jawab harus dilakukan dengan mempertimbangkan bagaimana setiap pihak berkontribusi terhadap kerugian. Tidak ada perbedaan yang signifikan antara pelanggan yang secara sadar memberikan informasi rahasia tanpa melakukan manipulasi yang signifikan dan pelanggan yang tertipu oleh orang yang menyamar sebagai petugas bank. Bank juga melihat perbedaan antara transaksi yang menunjukkan pola yang sangat tidak wajar tetapi tetap diproses tanpa perlindungan tambahan.

Pendektan ini menunjukkan bahwa istilah "kelalaian nasabah" harus digunakan dengan hati-hati. Tidak semua tindakan korban yang memungkinkan pelaku mendapatkan akses dapat langsung dianggap sebagai kelalaian, menghapus seluruh tanggung jawab bank. Korban adalah hasil dari manipulasi yang dirancang oleh pelaku dalam *social engineering*. Oleh karena itu, tingkat kesadaran korban, cara manipulasi yang dilakukan, informasi yang diberikan, peringatan keamanan yang diberikan bank, dan respons sistem terhadap transaksi semuanya harus dipertimbangkan.

Sebaliknya, perlindungan konsumen juga tidak dapat diartikan sebagai jaminan bahwa bank akan bertanggung jawab atas setiap kerugian yang disebabkan oleh penipuan. Pelanggan tetap harus menggunakan layanan dengan hati-hati dan menjaga kredibilitas mereka. Oleh karena itu, lebih bijaksana untuk membagi tanggung jawab berdasarkan fakta dan tingkat kesalahan masing-masing pihak daripada memberikan tanggung jawab secara otomatis kepada masing-masing pihak.

Kelemahan Perlindungan Hukum dan Kebutuhan Penguatan Regulasi

Meskipun peraturan di Indonesia telah berkembang, masih ada masalah tentang batas tanggung jawab bank dan konsumen dalam kasus kerugian akibat *social engineering*. Bank telah diwajibkan untuk menjaga sistem, data, dan transaksi aman, tetapi kejahatan yang melibatkan manipulasi manusia membuatnya lebih sulit. Menurut penelitian terbaru tentang perlindungan hukum terhadap social engineering, munculnya modus kejahatan digital membuat penentuan tanggung jawab bank dan perlindungan nasabah menjadi lebih sulit.

Salah satu masalah yang perlu diperhatikan adalah ketidaksederhanaan kriteria untuk menentukan kapan kerugian disebabkan oleh kelalaian nasabah dan kapan kerugian dapat dikaitkan dengan kegagalan sistem keamanan bank. Namun, perbedaan ini berdampak langsung pada pihak yang menanggung kerugian. Apabila standar tersebut tidak jelas, penyelesaian kasus dapat sangat bergantung pada hasil penyelidikan internal bank, yang dapat melemahkan nasabah.

Oleh karena itu, diperlukan peningkatan perlindungan hukum bukan hanya dengan menambahkan aturan baru, tetapi juga dengan membuat prosedur pemeriksaan dan pembagian tanggung jawab yang lebih jelas. Regulasi dapat diubah untuk memberikan standar yang lebih spesifik untuk penilaian transaksi social engineering. Ini dapat mencakup hal-hal yang perlu dipertimbangkan untuk mengidentifikasi kelalaian konsumen dan kegagalan keamanan bank. Sangat penting untuk memastikan bahwa penyelesaian sengketa tidak semata-mata didasarkan pada keadaan teknis transaksi sebagai transaksi yang telah divalidasi.

Pada akhirnya, kurangnya aturan bukanlah satu-satunya masalah dalam melindungi nasabah dari kejahatan social engineering; lebih penting lagi, hukum harus dapat menangani kejahatan digital yang menggabungkan kelemahan manusia dengan teknologi perbankan. Untuk sistem yang efektif, bank dan nasabah harus diposisikan sebagai pihak yang memiliki kewajiban yang berbeda sesuai dengan kapasitas dan peran mereka. Metode ini dapat berfungsi sebagai normatif dan memberikan mekanisme yang lebih objektif untuk menentukan siapa yang bertanggung jawab atas kerugian.

4. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian mengenai perlindungan hukum nasabah terhadap kejahatan *social engineering* dalam transaksi perbankan digital di Indonesia, dapat disimpulkan bahwa meskipun dasar hukum yang cukup luas telah ditetapkan untuk melindungi nasabah yang menjadi korban social engineering, implementasinya masih sulit. Layanan digital perbankan, perlindungan konsumen sektor jasa keuangan, dan perlindungan data pribadi adalah contoh dari perlindungan ini. Bank bertanggung jawab untuk menjaga keamanan data dan transaksi pelanggan melalui penggunaan autentikasi, pengendalian akses, audit trail, keamanan sistem informasi, dan kemampuan untuk mengidentifikasi dan menanggapi ancaman. Namun, keabsahan teknis suatu transaksi yang menggunakan fitur *social engineering* yang memanfaatkan manipulasi psikologis terhadap klien tidak selalu menunjukkan kehendak nasabah yang sebenarnya. Oleh karena itu, perlindungan hukum tidak seharusnya hanya berfokus pada apakah transaksi dilakukan dengan kredensial nasabah; itu juga harus mempertimbangkan bagaimana kredensial tersebut diperoleh, bagaimana transaksi terjadi, dan seberapa baik bank telah memenuhi tanggung jawab keamanan dan pencegahan risiko mereka.

Baik bank maupun konsumen tidak dapat secara otomatis bertanggung jawab atas kerugian yang disebabkan oleh *social engineering*. Meskipun konsumen tetap harus memastikan bahwa mereka menjaga data dan informasi perbanannya aman, pemberian OTP, PIN, atau informasi lainnya karena penipuan tidak serta-merta menunjukkan bahwa seluruh kerugian adalah akibat dari kelalaian konsumen. Sebaliknya, kewajiban bank untuk menjaga keamanan sistem tidak berarti bahwa bank harus membayar semua kerugian akibat social engineering. Tanggung jawab harus diputuskan berdasarkan rangkaian peristiwa dan bagaimana masing-masing pihak berkontribusi terhadap kerugian. Oleh karena itu, penilaian yang lebih objektif diperlukan terhadap tingkat kelalaian nasabah, kekuatan sistem keamanan bank, karakteristik transaksi, dan kemampuan bank untuk menemukan transaksi yang tidak wajar. Ketiadaan aturan bukan masalah utama dalam melindungi korban social engineering; masalah lebih besar adalah bagaimana menentukan siapa yang bertanggung jawab ketika kesalahan manusia dan kegagalan sistem teknologi terjadi bersamaan.

Saran

Bank, regulator, dan konsumen harus bertanggung jawab satu sama lain untuk melindungi pelanggan dari pelanggaran social engineering. Bank harus menerapkan sistem keamanan berlapis untuk memastikan bahwa pencegahan tidak hanya bergantung pada kehati-hatian pelanggan. Ini termasuk deteksi transaksi yang mencurigakan, verifikasi tambahan, dan

pelatihan nasabah yang berkala. Sebaliknya, dalam kasus *social engineering*, otoritas keuangan dan penggubal undang-undang harus membuat aturan yang jelas tentang tanggung jawab. Ini harus mempertimbangkan tingkat kelalaian nasabah, tanggung jawab keamanan bank, dan bagaimana masing-masing pihak bertanggung jawab atas kerugian. Perlindungan hukum dapat berjalan secara merata tanpa membebankan semua risiko kepada salah satu pihak. Nasabah harus tetap menjaga kerahasiaan PIN, OTP, password, dan data keamanan lainnya serta segera melaporkan transaksi yang mencurigakan kepada bank.

DAFTAR REFERENSI

Ahmad, M. R. A., & Utari, I. S. (2025). Perlindungan hukum pengguna e-commerce: Perspektif viktimologi dalam menghadapi kejahatan siber. *Bookchapter Hukum dan Lingkungan, 1*, 967–989.

Efendi, N. A., Harahap, M. I., & Syahbudi, M. (2025). Pengaruh social engineering dan cyber crime terhadap persepsi keamanan pada aplikasi BSI Mobile. *Jurnal Manajemen Terapan dan Keuangan, 14*(3), 1237–1250.

Hasanudin, T. A. (2026). Perlindungan nasabah dan tanggung jawab bank dalam penanggulangan kejahatan digital berbasis *social engineering*: Analisis hukum perbankan Indonesia. *Indonesia of Journal Business Law, 5*(1), 99–115. https://doi.org/10.47709/ijbl.v5i1.7476

Indonesia. (1999). *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 22, Tambahan Lembaran Negara Republik Indonesia Nomor 3821.

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Kornelis, Y. (2022). Digital banking consumer protection: Developments & challenges. *Jurnal Komunikasi Hukum, 8*(1), 378–394.

Noval, S. M. R., & Soecipto, S. T. (2023). *Perlindungan hak digital: Ancaman privasi di tengah serangan social engineering*. PT RajaGrafindo Persada.

Nurrizky, A., & Nugroho, W. (2025). Analisis kebijakan Otoritas Jasa Keuangan dalam upaya menanggulangi cyber crime di sektor perbankan. *Recht Studiosum Law Review, 4*(1), 79–88.

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. (2024). *Booklet perbankan Indonesia 2024*.

Pamuji, R. A. (2018). Perlindungan hukum bagi nasabah dan tanggung jawab bank dalam kasus card skimming. *Lex Renaissance, 3*(1), 12.

Rizieq, M., & Suwarsit, S. (2024). Transformasi layanan perbankan dari antrian panjang menuju banking in your pocket. *Jurnal Multidisiplin Ilmu Akademik, 1*(6), 291–299.

Sugiarto, N., Yuliawan, I., & Irawati, A. C. (2026). Perlindungan data pribadi sebagai instrumen hukum dalam menanggulangi kejahatan perbankan. *Pendas: Jurnal Ilmiah Pendidikan Dasar, 11*(1), 68–82.

Utami, P. D. Y., & Purwanti, N. P. (2025). Strengthening legal protections against social engineering in digital banking: Challenges, gaps, and recommendations. *Masalah-Masalah Hukum, 54*(2), 214–226. https://doi.org/10.14710/mmh.54.2.2025.214-226

Wahyu, R., & Widiatno, M. W. (2025). Tanggung jawab hukum pidana penyelenggara elektronik perbankan terhadap perlindungan data pribadi nasabah. *Arus Jurnal Sosial dan Humaniora, 5*(2), 3190–3199.