

Pertanggungjawaban Bank sebagai Penyelenggara *Mobile Banking* atas Kehilangan Dana Nasabah Akibat *Phishing* dan Mekanisme Penyelesaian Sengketa

Agnesia Atika Putri^{*1}, Rizky Pratama Putra Karo Karo²

^{1,2} Program Studi Magister Hukum, Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma, Indonesia.

Email: ¹aatikaputri.ap87@gmail.com, ²rizkykarokaro@unsurtya.ac.id

Abstrak

Perkembangan layanan mobile banking memberikan kemudahan dalam transaksi keuangan, tetapi sekaligus meningkatkan risiko kejahatan siber, khususnya phishing yang dapat menyebabkan kehilangan dana nasabah. Penelitian ini bertujuan menganalisis pertanggungjawaban bank sebagai penyelenggara layanan mobile banking atas kehilangan dana nasabah akibat phishing serta mekanisme penyelesaian sengketa dalam pemulihan hak nasabah. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan empiris sebagai pendukung. Pendekatan penelitian meliputi pendekatan perundang-undangan, konseptual, dan kasus, dengan bahan hukum yang diperoleh melalui studi kepustakaan serta gambaran penerapan ketentuan hukum dalam praktik penyelesaian sengketa. Hasil penelitian menunjukkan bahwa pertanggungjawaban bank dan nasabah atas kehilangan dana akibat phishing belum memiliki batas yang diatur secara khusus dan komprehensif dalam satu ketentuan hukum. Analisis pertanggungjawaban didasarkan pada ketentuan perbankan, perlindungan konsumen, transaksi elektronik, serta pengaturan penyelenggaraan layanan perbankan digital, dengan mempertimbangkan prinsip kehati-hatian, kewajiban keamanan sistem, kontribusi kesalahan, dan hubungan sebab akibat. Penggunaan PIN atau OTP tidak dapat dijadikan satu-satunya dasar untuk membebaskan kerugian kepada nasabah karena autentikasi dapat terjadi melalui manipulasi dan social engineering. Mekanisme penyelesaian sengketa melalui pengaduan internal bank, Otoritas Jasa Keuangan (OJK), Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK), dan litigasi telah tersedia, tetapi masih menghadapi kendala berupa ketidakseimbangan penguasaan bukti, keterbatasan akses terhadap data elektronik, biaya, dan lamanya proses. Penelitian ini menyimpulkan bahwa diperlukan standar pertanggungjawaban yang lebih jelas, pembagian beban pembuktian yang proporsional, penguatan perlindungan konsumen, serta mekanisme penyelesaian sengketa yang lebih cepat, adil, dan memberikan kepastian hukum bagi nasabah.

Kata kunci: *phishing; mobile banking; pertanggungjawaban bank; perlindungan nasabah; penyelesaian sengketa*

Abstract

The development of mobile banking services provides convenience in financial transactions while simultaneously increasing the risk of cybercrime, particularly phishing, which may result in the loss of customer funds. This study aims to analyze the legal liability of banks as providers of mobile banking services for customer fund losses caused by phishing and the dispute resolution mechanisms available for restoring customer rights. This study employs normative legal research with an empirical approach as supporting data. The research approaches include statutory, conceptual, and case approaches, with legal materials obtained through a literature review as well as an overview of the application of legal provisions in the practice of dispute resolution. The results show that the liability of banks and customers for losses caused by phishing has not been specifically and comprehensively regulated within a single legal provision. The analysis of liability is based on banking regulations, consumer protection regulations, electronic transaction regulations, and regulations governing digital banking services, while considering the prudential principle, system security obligations, the contribution of each party's fault, and the causal relationship between the conduct and the resulting loss. The use of a PIN or One-Time Password (OTP) cannot be regarded as the sole basis for imposing liability on customers because authentication may occur through manipulation and social engineering. Dispute resolution mechanisms through internal bank complaints, the Financial Services Authority (OJK), the Alternative Dispute Resolution Institution for the Financial Services Sector (LAPS SJK), and litigation are available, but they still face obstacles, including unequal access to evidence, limited access to electronic data, costs, and lengthy procedures. This study concludes that clearer liability standards, a proportionate allocation of the burden of proof, stronger consumer protection, and faster, fairer dispute resolution mechanisms are required to provide legal certainty for customers.

Keywords: *phishing; mobile banking; bank liability; customer protection; dispute resolution*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi dalam sektor perbankan melalui pemanfaatan layanan digital, salah satunya *mobile banking*. Layanan ini memungkinkan nasabah melakukan transaksi keuangan secara mandiri tanpa harus datang ke kantor bank sehingga memberikan kemudahan, efisiensi, kecepatan, dan fleksibilitas. Peningkatan penggunaan *mobile banking* juga sejalan dengan semakin luasnya akses internet dan penggunaan *smartphone* dalam kehidupan masyarakat (Mutiasari, 2020). Digitalisasi tersebut memberikan manfaat bagi bank dan nasabah, tetapi sekaligus menghadirkan risiko baru berupa gangguan keamanan sistem, penyalahgunaan data, dan kejahatan berbasis teknologi informasi (Abubakar & Handayani, 2022; Tambunan & Nasution, 2023).

Salah satu bentuk kejahatan siber yang berkaitan dengan layanan *mobile banking* adalah *phishing*. Kejahatan ini dilakukan dengan memanipulasi korban agar memberikan informasi pribadi atau data autentikasi perbankan melalui pesan, surat elektronik, tautan palsu, maupun aplikasi yang menyerupai layanan resmi bank (Budiono et al., 2025). Modus tersebut dapat melibatkan permintaan kode One Time Password (OTP) atau data *login* untuk memperoleh akses terhadap rekening korban. Fenomena ini menunjukkan bahwa keamanan transaksi digital tidak hanya berkaitan dengan perilaku pengguna, tetapi juga dengan kemampuan sistem perbankan dalam mengantisipasi dan memitigasi tindakan penipuan.

Kerugian yang timbul dari *phishing* dapat berupa berkurangnya atau hilangnya dana dalam rekening nasabah. Persoalan hukum muncul ketika transaksi yang menyebabkan kerugian tersebut dilakukan tanpa sepengetahuan atau persetujuan pemilik rekening. Dalam kondisi demikian, bank dan nasabah dapat memiliki pandangan yang berbeda mengenai pihak yang harus menanggung kerugian. Bank dapat menilai bahwa nasabah telah lalai karena memberikan informasi rahasia, sedangkan nasabah dapat beranggapan bahwa bank mempunyai kewajiban menyediakan sistem transaksi yang aman serta melindungi dana yang dipercayakan kepadanya (Kusuma, 2019).

Permasalahan tersebut menjadi lebih kompleks ketika penggunaan OTP dijadikan dasar untuk menentukan adanya persetujuan atau kelalaian nasabah. Dalam praktik *phishing*, nasabah dapat memberikan OTP akibat manipulasi atau rekayasa sosial (*social engineering*) tanpa menyadari bahwa informasi tersebut akan digunakan oleh pihak yang tidak berwenang untuk melakukan transaksi. Dengan demikian, keberhasilan autentikasi menggunakan OTP tidak serta-merta menunjukkan adanya persetujuan sadar dari nasabah terhadap transaksi. Nasabah pada umumnya tidak memiliki akses terhadap *log* transaksi, data perangkat, sistem autentikasi, maupun mekanisme keamanan internal bank. Sebaliknya, informasi teknis tersebut berada dalam penguasaan bank sebagai penyelenggara layanan sehingga terdapat ketidakseimbangan dalam proses pembuktian (Ahmad et al., 2022; Mukhra et al., 2024). Oleh karena itu, penilaian terhadap tanggung jawab tidak cukup hanya didasarkan pada fakta bahwa OTP digunakan, tetapi perlu mempertimbangkan proses terjadinya *phishing*, kontribusi kesalahan masing-masing pihak, keamanan sistem bank, serta hubungan kausal antara tindakan para pihak dan kerugian yang timbul.

Kondisi tersebut berkaitan dengan kedudukan nasabah sebagai konsumen jasa keuangan. Teori perlindungan konsumen memandang konsumen sebagai pihak yang relatif lebih lemah dibandingkan pelaku usaha, baik dari aspek informasi, kemampuan ekonomi, maupun posisi tawar dalam hubungan kontraktual (Kusumadewi & Sharon, 2022). Dalam layanan *mobile banking*, ketimpangan tersebut terlihat dari keterbatasan nasabah dalam mengakses teknologi, data transaksi, dan mekanisme keamanan yang digunakan bank. Perspektif ini penting untuk menilai apakah pembebanan kerugian kepada nasabah telah mencerminkan keseimbangan hak dan kewajiban para pihak. Perspektif perlindungan konsumen tersebut penting untuk menilai keseimbangan hak dan kewajiban para pihak, khususnya ketika nasabah mengalami kerugian akibat transaksi yang terjadi melalui rekayasa sosial.

Secara normatif, perlindungan nasabah didukung oleh berbagai ketentuan yang berkaitan dengan perbankan, perlindungan konsumen, transaksi elektronik, dan penyelenggaraan teknologi informasi perbankan. Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan menjadi salah satu dasar pengaturan kegiatan perbankan dan penerapan

prinsip kehati-hatian. Perlindungan nasabah sebagai konsumen jasa keuangan juga berkaitan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen serta Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Aspek transaksi elektronik berkaitan dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sedangkan penyelenggaraan teknologi informasi perbankan antara lain diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Bank berkewajiban menjalankan kegiatan berdasarkan prinsip kehati-hatian serta menjaga keamanan layanan dan data nasabah. Pengaturan mengenai penyelenggaraan teknologi informasi oleh bank juga memberikan kewajiban terkait manajemen risiko, keamanan sistem, autentikasi transaksi, dan mitigasi risiko teknologi informasi (Wisuda, 2022; Rodli, 2021; Wardhono et al., 2024). Ketentuan tersebut belum memberikan pengaturan yang secara khusus dan komprehensif menentukan batas pertanggungjawaban bank dan nasabah ketika kerugian terjadi akibat *phishing*, terutama ketika nasabah memberikan OTP karena rekayasa sosial dan transaksi tetap berhasil melalui sistem autentikasi bank.

Ketiadaan batas yang lebih jelas tersebut dapat dianalisis melalui teori pertanggungjawaban hukum. Pertanggungjawaban dalam hukum perdata berkaitan dengan adanya perbuatan, kesalahan, kerugian, dan hubungan kausal antara perbuatan dengan kerugian (Fazriah, 2023). Dalam hubungan bank dan nasabah, pendekatan tersebut diperlukan untuk menentukan apakah kerugian berasal dari kelalaian bank, kelemahan sistem, tindakan pihak ketiga, kelalaian nasabah, atau kombinasi dari beberapa faktor (Fonda & Hoesein, 2022; Runtunuwu et al., 2025). Dengan demikian, teori pertanggungjawaban digunakan untuk menganalisis pembagian tanggung jawab berdasarkan kewajiban hukum, kontribusi kesalahan, serta hubungan kausal masing-masing pihak.

Selain persoalan tanggung jawab, pemulihan hak nasabah juga menghadapi persoalan dalam mekanisme penyelesaian sengketa. Penyelesaian dapat ditempuh melalui pengaduan kepada bank, otoritas terkait, lembaga alternatif penyelesaian sengketa, maupun jalur litigasi. Namun, dalam praktiknya, proses tersebut dapat menghadapi hambatan berupa waktu penyelesaian, biaya, keterbatasan pengetahuan hukum, dan kesulitan memperoleh bukti elektronik (Renyaaan, 2022). Teori penegakan hukum menegaskan bahwa keberhasilan suatu aturan tidak hanya bergantung pada keberadaan norma, tetapi juga pada pelaksanaannya dalam praktik serta dukungan sarana, aparat, dan kesadaran hukum masyarakat (Waluyo, 2016). Sementara itu, teori penyelesaian sengketa memberikan kerangka untuk menilai penggunaan jalur litigasi maupun non-litigasi dalam memperoleh penyelesaian yang efektif (Tamba & Mukharom, 2023). Oleh karena itu, efektivitas penyelesaian sengketa dalam penelitian ini tidak hanya dilihat dari tersedianya jalur pengaduan, tetapi juga dari kemampuannya memberikan pembuktian yang seimbang dan memulihkan hak nasabah secara efektif.

Penelitian terdahulu menunjukkan bahwa kajian mengenai *phishing* pada layanan *mobile banking* masih memiliki ruang untuk dikembangkan. Hendarto dan Prasetyawati (2024) membahas tanggung jawab bank dalam mengantisipasi dan menangani kerugian nasabah akibat *phishing*, tetapi belum secara khusus menganalisis pembagian tanggung jawab ketika nasabah memberikan OTP akibat rekayasa sosial. Rinaldi dan Wijaya (2025) membahas penegakan hukum terhadap pembobolan dana nasabah dengan fokus pada pihak internal bank, sedangkan Yosefine et al. (2023) mengkaji perlindungan hukum terhadap nasabah BTPN Jenius yang mengalami *phishing*. Penelitian-penelitian tersebut belum secara utuh menghubungkan pemberian OTP akibat rekayasa sosial dengan pembagian tanggung jawab antara bank dan nasabah, persoalan ketidakseimbangan penguasaan bukti, serta mekanisme penyelesaian sengketa dalam pemulihan dana nasabah.

Berdasarkan kesenjangan tersebut, kebaruan penelitian ini terletak pada analisis pertanggungjawaban bank sebagai penyelenggara layanan *mobile banking* dan nasabah secara proporsional ketika kehilangan dana terjadi akibat *phishing*, khususnya dalam kondisi nasabah memberikan OTP karena rekayasa sosial. Analisis tersebut dilakukan dengan mempertimbangkan kewajiban keamanan bank, kontribusi kesalahan nasabah, hubungan kausal, ketidakseimbangan penguasaan bukti, serta mekanisme penyelesaian sengketa yang dapat ditempuh untuk memulihkan hak nasabah.

Berdasarkan uraian tersebut, penelitian ini diarahkan untuk menganalisis pertanggungjawaban hukum bank sebagai penyelenggara layanan *mobile banking* atas kehilangan dana nasabah akibat *phishing*, khususnya ketika OTP diberikan akibat rekayasa sosial, serta mekanisme penyelesaian sengketa yang efektif untuk memulihkan hak nasabah yang dirugikan. Penelitian menggunakan penelitian hukum normatif dengan pendekatan empiris sebagai pendukung melalui kajian terhadap peraturan perundang-undangan, asas dan teori hukum, literatur, serta praktik penyelesaian sengketa yang relevan. Dengan pendekatan tersebut, penelitian diharapkan dapat memberikan analisis mengenai pembagian pertanggungjawaban bank dan nasabah secara proporsional serta kebutuhan mekanisme penyelesaian sengketa yang mampu memberikan keadilan dan kepastian hukum.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif. Penelitian hukum normatif digunakan untuk menganalisis norma hukum yang mengatur hubungan antara bank dan nasabah, khususnya mengenai pertanggungjawaban bank, perlindungan hukum nasabah, keamanan layanan *mobile banking*, serta penyelesaian sengketa akibat kehilangan dana yang disebabkan oleh *phishing*. Penelitian ini tidak menggunakan wawancara atau pengumpulan data lapangan secara langsung, melainkan bertumpu pada analisis terhadap bahan hukum dan literatur yang relevan.

Pendekatan penelitian dilakukan melalui pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*) dalam arti penelaahan terhadap pola permasalahan dan penyelesaian sengketa kehilangan dana nasabah akibat *phishing* yang ditemukan dalam literatur dan sumber hukum yang tersedia, bukan melalui penelitian lapangan. Pendekatan perundang-undangan digunakan dengan menelaah ketentuan yang berkaitan dengan perbankan, perlindungan konsumen, transaksi elektronik, serta pengaturan mengenai penyelenggaraan layanan perbankan digital. Peraturan yang menjadi bahan analisis meliputi Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, serta Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Pendekatan konseptual digunakan untuk menganalisis konsep pertanggungjawaban hukum, perlindungan konsumen, keamanan layanan perbankan, dan penyelesaian sengketa. Pendekatan kasus digunakan untuk memahami karakteristik permasalahan *phishing* dalam layanan *mobile banking*, khususnya mengenai transaksi yang dilakukan setelah nasabah memberikan data autentikasi akibat rekayasa sosial serta persoalan pembagian tanggung jawab antara bank dan nasabah sebagaimana dibahas dalam sumber hukum dan literatur yang dianalisis.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer terdiri atas peraturan perundang-undangan dan ketentuan regulator yang berkaitan langsung dengan kegiatan perbankan, perlindungan konsumen jasa keuangan, transaksi elektronik, keamanan sistem, dan penyelenggaraan teknologi informasi perbankan. Bahan hukum sekunder berupa buku, jurnal ilmiah, hasil penelitian, serta pendapat ahli yang berkaitan dengan pertanggungjawaban hukum, perlindungan konsumen, kejahatan *phishing*, dan penyelesaian sengketa perbankan. Bahan hukum tersier digunakan sebagai bahan pendukung untuk memberikan pemahaman terhadap istilah dan konsep yang digunakan dalam penelitian.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan penelusuran sumber pada basis data dan laman publikasi ilmiah serta sumber resmi lembaga pemerintah dan regulator. Literatur ilmiah ditelusuri menggunakan kata kunci antara lain "*phishing*", "*mobile banking*", "*pertanggungjawaban bank*", "*perlindungan nasabah*", "*keamanan perbankan digital*", "*social engineering*", dan "*penyelesaian sengketa perbankan*". Penelusuran literatur difokuskan pada publikasi yang relevan dengan permasalahan penelitian, terutama literatur yang membahas pertanggungjawaban bank, kehilangan dana nasabah, *phishing*, OTP, rekayasa sosial, perlindungan konsumen, serta mekanisme penyelesaian sengketa. Literatur yang dipilih kemudian diseleksi berdasarkan relevansi

substansi, keterkaitan dengan objek penelitian, kredibilitas sumber, dan kemutakhiran publikasi, dengan tetap menggunakan sumber hukum dan literatur yang lebih lama apabila memiliki kedudukan sebagai sumber hukum, teori, atau rujukan primer yang masih relevan.

Bahan hukum yang telah dikumpulkan kemudian diinventarisasi, diidentifikasi, dan diklasifikasikan berdasarkan dua pokok permasalahan penelitian, yaitu pertanggungjawaban hukum bank dan perlindungan nasabah serta mekanisme penyelesaian sengketa atas kehilangan dana akibat *phishing*. Untuk sumber yang membahas perkara atau penyelesaian sengketa, informasi yang relevan mengenai pola kejadian, bentuk kerugian, posisi bank dan nasabah, serta pertimbangan hukum digunakan sebagai bahan pendukung analisis.

Analisis dilakukan secara kualitatif yuridis, yaitu dengan menghubungkan ketentuan hukum yang berlaku dengan konsep dan teori hukum serta permasalahan yang menjadi objek penelitian. Analisis diarahkan untuk menentukan hubungan antara tindakan nasabah, kewajiban bank dalam menjaga keamanan layanan, terjadinya kerugian, dan hubungan kausal di antara faktor-faktor tersebut. Dengan metode tersebut, penelitian tidak semata-mata menentukan pihak yang harus menanggung kerugian, tetapi menganalisis batas pertanggungjawaban bank dan nasabah secara proporsional berdasarkan kewajiban hukum, tingkat kelalaian, serta faktor penyebab terjadinya kerugian.

3. HASIL DAN PEMBAHASAN

3.1. Pertanggungjawaban Hukum Bank dan Perlindungan Hukum Nasabah atas Kehilangan Dana Akibat *Phishing*

Perkembangan layanan *mobile banking* memberikan kemudahan bagi nasabah dalam melakukan transaksi perbankan, namun pada saat yang sama meningkatkan risiko terjadinya kejahatan siber, salah satunya *phishing*. Dalam kasus *phishing*, pelaku memanfaatkan teknik manipulasi untuk memperoleh data pribadi dan data autentikasi nasabah, termasuk PIN, *password*, maupun One Time Password (OTP). Persoalan pertanggungjawaban hukum muncul ketika data autentikasi tersebut berhasil diperoleh melalui rekayasa sosial (*social engineering*) dan kemudian digunakan untuk melakukan transaksi yang mengakibatkan hilangnya dana nasabah.

Penggunaan OTP dalam suatu transaksi tidak dapat secara otomatis dipersamakan dengan persetujuan sadar nasabah terhadap transaksi tersebut. OTP merupakan bagian dari mekanisme autentikasi yang digunakan untuk memverifikasi transaksi, tetapi dalam modus *phishing* kode tersebut dapat diperoleh melalui manipulasi terhadap nasabah. Oleh karena itu, keberhasilan proses autentikasi tidak dengan sendirinya membuktikan bahwa nasabah secara sadar dan bebas menyetujui transaksi yang kemudian menimbulkan kerugian. Penilaian tersebut perlu dikaitkan dengan kewajiban bank dalam menyediakan sistem yang aman, kewajiban nasabah dalam menjaga kerahasiaan data autentikasi, serta rangkaian peristiwa yang menyebabkan transaksi terjadi.

Secara normatif, hubungan antara bank dan nasabah didasarkan pada kewajiban bank untuk menjalankan kegiatan usaha berdasarkan prinsip kehati-hatian serta memberikan perlindungan terhadap kepentingan nasabah. Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan menjadi salah satu dasar dalam menilai kewajiban bank dalam menjalankan kegiatan perbankan. Sementara itu, perlindungan nasabah sebagai konsumen jasa keuangan berkaitan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Dalam penyelenggaraan layanan digital, Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum juga menjadi dasar untuk menilai kewajiban bank dalam pengelolaan risiko dan keamanan teknologi informasi.

Pengaturan tersebut menunjukkan bahwa keamanan layanan perbankan digital merupakan bagian dari kewajiban penyelenggara layanan. Bank tidak hanya berkewajiban menyediakan sarana transaksi, tetapi juga harus menerapkan pengamanan sistem, manajemen risiko, dan langkah mitigasi terhadap risiko teknologi informasi (Wisuda, 2022; Rodli, 2021; Wardhono et al., 2024). Ketika transaksi akibat *phishing* terjadi, penilaian terhadap tanggung jawab bank tidak cukup hanya melihat apakah sistem

mencatat penggunaan OTP, tetapi juga perlu melihat apakah bank telah menjalankan kewajiban keamanan dan pengelolaan risiko secara memadai.

Kondisi tersebut juga berkaitan dengan kedudukan nasabah sebagai konsumen jasa keuangan. Teori perlindungan konsumen memandang konsumen sebagai pihak yang relatif lebih lemah dibandingkan pelaku usaha, baik dari aspek informasi, kemampuan ekonomi, maupun posisi tawar dalam hubungan kontraktual (Kusumadewi & Sharon, 2022). Dalam layanan *mobile banking*, ketimpangan tersebut terlihat dari keterbatasan nasabah dalam mengakses teknologi, data transaksi, dan mekanisme keamanan yang digunakan bank. Ketidakseimbangan tersebut juga terlihat dalam proses pembuktian karena data *log* transaksi, data perangkat, sistem autentikasi, dan informasi keamanan pada umumnya berada dalam penguasaan bank. Oleh sebab itu, perlindungan konsumen perlu ditempatkan sebagai salah satu pertimbangan dalam menentukan pembagian tanggung jawab antara bank dan nasabah.

Ketiadaan batas yang lebih jelas tersebut dapat dianalisis melalui teori pertanggungjawaban hukum. Pertanggungjawaban dalam hukum perdata berkaitan dengan adanya perbuatan, kesalahan, kerugian, dan hubungan kausal antara perbuatan dengan kerugian (Fazriah, 2023). Dalam hubungan bank dan nasabah, pendekatan tersebut diperlukan untuk menentukan apakah kerugian berasal dari kelalaian bank, kelemahan sistem, tindakan pihak ketiga, kelalaian nasabah, atau kombinasi dari beberapa faktor (Fonda & Hoessein, 2022; Runtunuwu et al., 2025). Pembagian tanggung jawab harus didasarkan pada kontribusi masing-masing pihak terhadap timbulnya kerugian, bukan semata-mata pada fakta bahwa transaksi berhasil menggunakan mekanisme autentikasi.

Berdasarkan analisis tersebut, pembagian tanggung jawab antara bank dan nasabah dapat dirumuskan melalui beberapa parameter. Bank dapat dipandang bertanggung jawab secara dominan atau penuh apabila kerugian terutama disebabkan oleh kebocoran data atau kelemahan sistem keamanan yang berada dalam lingkup penguasaan bank, atau apabila bank tidak menerapkan pengamanan dan pengelolaan risiko yang seharusnya. Tanggung jawab bank dapat bersifat sebagian apabila terdapat kontribusi kesalahan dari bank dan nasabah secara bersamaan, misalnya ketika nasabah memberikan OTP akibat rekayasa sosial tetapi terdapat pula kelemahan pada sistem deteksi atau pengamanan transaksi bank. Sebaliknya, tanggung jawab bank dapat menjadi terbatas atau tidak dibebankan apabila bank telah memenuhi kewajiban keamanan dan nasabah dengan sengaja atau karena kelalaian berat memberikan data autentikasi tanpa adanya manipulasi atau keadaan yang dapat dikaitkan dengan kelemahan sistem bank.

Parameter tersebut tidak dimaksudkan sebagai persentase pembagian kerugian yang bersifat tetap, melainkan sebagai kerangka analisis untuk menentukan pihak yang memiliki kontribusi kausal terhadap kerugian dalam setiap peristiwa. Oleh karena itu, pemberian OTP akibat rekayasa sosial perlu dibedakan dari pemberian data autentikasi secara sadar dan tanpa manipulasi. Dalam kondisi rekayasa sosial, adanya tindakan dari nasabah tidak serta-merta menghapus kewajiban bank untuk membuktikan bahwa sistem keamanan dan mekanisme mitigasi risiko telah dijalankan secara memadai.

Matriks tersebut menunjukkan bahwa penggunaan OTP tidak dapat dijadikan satu-satunya parameter dalam menentukan pihak yang bertanggung jawab. Faktor yang harus dinilai meliputi sumber kebocoran atau akses data, efektivitas sistem keamanan dan deteksi transaksi, bentuk manipulasi terhadap nasabah, tingkat kehati-hatian nasabah, serta hubungan kausal antara tindakan para pihak dan kerugian.

Dalam transaksi akibat *phishing*, posisi nasabah yang memberikan OTP karena rekayasa sosial perlu dibedakan dari nasabah yang secara sadar memberikan data autentikasi tanpa adanya manipulasi. Rekayasa sosial dapat menyebabkan nasabah bertindak berdasarkan informasi yang keliru sehingga unsur kesalahan perlu dinilai secara lebih hati-hati. Dengan demikian, bank tidak dapat semata-mata menggunakan keberhasilan autentikasi sebagai alasan untuk membebaskan seluruh kerugian kepada nasabah, tetapi juga harus menunjukkan bahwa kewajiban pengamanan sistem dan mitigasi risiko telah dilaksanakan.

Pertanggungjawaban tersebut juga harus mempertimbangkan tindakan pihak ketiga sebagai pelaku *phishing*. Kejahatan dilakukan oleh pihak yang berada di luar hubungan kontraktual antara bank dan nasabah, tetapi keberadaan pihak ketiga tidak serta-merta menghapus hubungan hukum antara bank dan nasabah.

Tabel 1. Matriks Pembagian Pertanggungjawaban Bank dan Nasabah

Kondisi	Kontribusi Bank	Kontribusi Nasabah	Arah Pertanggungjawaban
Kebocoran data atau kelemahan sistem keamanan bank	Tinggi	Tidak ada	Bank bertanggung jawab secara penuh berdasarkan hubungan kausal dan kewajiban hukumnya
Transaksi tidak wajar gagal dideteksi atau dimitigasi oleh sistem bank	Tinggi	Rendah	Bank bertanggung jawab secara dominan apabila kegagalan tersebut berkaitan dengan kerugian
Nasabah memberikan OTP akibat rekayasa sosial (<i>social engineering</i>)	Perlu dinilai berdasarkan keamanan sistem dan mitigasi <i>fraud</i>	Ada tindakan faktual, tetapi tingkat kesalahan harus dinilai	Tanggung jawab ditentukan secara proporsional berdasarkan kontribusi kesalahan dan hubungan kausal
Nasabah memberikan OTP secara sadar tanpa manipulasi	Rendah apabila kewajiban keamanan telah dipenuhi	Tinggi	Nasabah dapat menjadi pihak yang bertanggung jawab secara dominan
Nasabah mengabaikan peringatan keamanan yang memadai dari bank	Rendah apabila bank telah memenuhi kewajibannya	Tinggi	Tanggung jawab nasabah dapat menjadi dominan
Kelemahan keamanan bank dan kelalaian nasabah terjadi secara bersamaan	Ada	Ada	Tanggung jawab dapat dibebankan secara proporsional sesuai kontribusi masing-masing pihak

Yang perlu dianalisis adalah apakah tindakan pihak ketiga tersebut merupakan penyebab yang sepenuhnya berada di luar kemampuan pencegahan bank atau terdapat kelemahan dalam sistem bank yang turut memungkinkan terjadinya kerugian.

Dengan demikian, pertanggungjawaban bank dan nasabah dalam kehilangan dana akibat *phishing* tidak dapat ditentukan berdasarkan satu indikator tunggal. Penentuan tanggung jawab harus dilakukan secara kasus per kasus dengan mempertimbangkan kewajiban hukum masing-masing pihak, kontribusi kesalahan, keamanan sistem, proses terjadinya rekayasa sosial, penggunaan OTP, serta hubungan kausal antara tindakan para pihak dan kerugian yang timbul.

3.2. Mekanisme Penyelesaian Sengketa antara Bank dan Nasabah dalam Pemulihan Hak Nasabah

Penyelesaian dapat ditempuh melalui pengaduan kepada bank, Otoritas Jasa Keuangan (OJK), lembaga alternatif penyelesaian sengketa, maupun jalur litigasi. Namun, dalam praktiknya, proses tersebut dapat menghadapi hambatan berupa waktu penyelesaian, biaya, keterbatasan pengetahuan hukum, dan kesulitan memperoleh bukti elektronik (Renyaaan, 2022). Teori penegakan hukum menegaskan bahwa keberhasilan suatu aturan tidak hanya bergantung pada keberadaan norma, tetapi juga pada pelaksanaannya dalam praktik serta dukungan sarana, aparat, dan kesadaran hukum masyarakat (Waluyo, 2016). Sementara itu, teori penyelesaian sengketa memberikan kerangka untuk menilai penggunaan jalur litigasi maupun non-litigasi dalam memperoleh penyelesaian yang efektif (Tamba & Mukharom, 2023).

Mekanisme pertama adalah pengaduan kepada bank sebagai penyelenggara layanan. Pengaduan internal merupakan tahap awal yang penting karena bank memiliki akses terhadap data transaksi, *log* sistem, informasi perangkat, dan data autentikasi yang diperlukan untuk melakukan penelusuran. Dalam

perlindungan konsumen jasa keuangan, mekanisme pengaduan juga berkaitan dengan kewajiban pelaku usaha jasa keuangan untuk menerima dan menangani pengaduan konsumen sesuai dengan ketentuan perlindungan konsumen sektor jasa keuangan.

Apabila penyelesaian melalui bank tidak memberikan hasil yang dapat diterima nasabah, penyelesaian dapat dilanjutkan melalui Otoritas Jasa Keuangan (OJK) sesuai dengan kewenangan yang diberikan oleh peraturan perundang-undangan. OJK memiliki fungsi pengaturan dan pengawasan sektor jasa keuangan serta kewenangan dalam perlindungan konsumen dan masyarakat di sektor jasa keuangan. Dasar pengaturan perlindungan konsumen tersebut antara lain terdapat dalam Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. OJK berperan dalam pengawasan dan fasilitasi perlindungan konsumen sesuai kewenangannya, tetapi tidak dapat diposisikan secara otomatis sebagai lembaga yang memutus seluruh sengketa perdata antara bank dan nasabah seperti pengadilan.

Selain OJK, nasabah dapat menggunakan mekanisme penyelesaian sengketa melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK). Mekanisme ini merupakan jalur penyelesaian sengketa di luar pengadilan yang dapat digunakan dalam sengketa antara konsumen dan pelaku usaha jasa keuangan sesuai dengan ketentuan yang berlaku dan kewenangan LAPS SJK. Penyelesaian melalui LAPS SJK dapat memberikan alternatif yang lebih sederhana dibandingkan proses litigasi, terutama dalam hal efisiensi waktu dan biaya, dengan tetap memperhatikan persyaratan dan prosedur yang ditentukan.

Mekanisme litigasi melalui pengadilan merupakan jalur penyelesaian apabila sengketa tidak dapat diselesaikan melalui pengaduan internal maupun mekanisme non-litigasi, atau apabila pihak yang dirugikan memilih menggunakan upaya hukum melalui pengadilan. Dalam proses litigasi, pembuktian menjadi aspek penting karena pihak yang bersengketa harus menunjukkan dasar tuntutan, bentuk kerugian, kesalahan, dan hubungan kausal. Persoalan ketidakseimbangan penguasaan bukti elektronik menjadi relevan karena sebagian besar data teknis transaksi berada pada pihak bank.

Setiap mekanisme memiliki fungsi dan batas yang berbeda. Pengaduan internal bank berfungsi sebagai tahap awal penanganan permasalahan dan penelusuran transaksi; OJK menjalankan fungsi pengaturan, pengawasan, dan perlindungan konsumen sesuai kewenangannya; LAPS SJK menyediakan alternatif penyelesaian sengketa di luar pengadilan; sedangkan pengadilan memberikan penyelesaian melalui mekanisme litigasi dan putusan yang mempunyai kekuatan hukum sesuai ketentuan hukum acara.

Dalam perkara kehilangan dana akibat *phishing*, pilihan mekanisme penyelesaian sengketa perlu mempertimbangkan karakteristik permasalahan, terutama kebutuhan untuk memperoleh bukti elektronik dan menentukan kontribusi kesalahan antara bank dan nasabah. Pengaduan internal kepada bank menjadi penting karena tahap tersebut memungkinkan penelusuran transaksi dan pengamanan data. Apabila tidak tercapai penyelesaian, mekanisme OJK atau LAPS SJK dapat digunakan sesuai kewenangan dan persyaratan masing-masing, sedangkan litigasi dapat ditempuh apabila diperlukan penentuan hak dan kewajiban para pihak melalui proses peradilan.

Berdasarkan pembahasan tersebut, penyelesaian sengketa kehilangan dana akibat *phishing* tidak hanya bergantung pada tersedianya jalur hukum, tetapi juga pada kemampuan mekanisme tersebut dalam memberikan akses terhadap bukti, menentukan pertanggungjawaban secara proporsional, dan memulihkan hak nasabah. Oleh karena itu, efektivitas penyelesaian sengketa perlu ditempatkan dalam kerangka perlindungan konsumen, dengan tetap mempertahankan keseimbangan antara kewajiban bank untuk menjamin keamanan layanan dan kewajiban nasabah untuk menjaga kerahasiaan data autentikasi.

4. KESIMPULAN

Pertanggungjawaban bank atas kehilangan dana nasabah akibat *phishing* dalam layanan *mobile banking* belum memiliki pengaturan yang secara khusus dan komprehensif mengenai batas pembagian tanggung jawab antara bank dan nasabah. Ketidakjelasan terutama terletak pada belum adanya parameter yang secara tegas menentukan sejauh mana penggunaan PIN atau OTP akibat rekayasa sosial dapat dikategorikan sebagai kelalaian nasabah dan sejauh mana kelemahan sistem, kegagalan deteksi transaksi tidak wajar, serta kewajiban keamanan bank menjadi dasar pertanggungjawaban bank. Oleh

karena itu, penggunaan PIN atau OTP tidak dapat menjadi satu-satunya dasar untuk membebaskan kerugian kepada nasabah apabila autentikasi tersebut diperoleh melalui *phishing* atau rekayasa sosial.

Pembagian tanggung jawab perlu ditentukan secara proporsional berdasarkan sumber kelemahan keamanan, hubungan sebab akibat antara tindakan para pihak dan kerugian, perilaku atau tingkat kelalaian nasabah, kemampuan bank dalam mencegah dan mendeteksi transaksi tidak wajar, serta respons bank setelah terjadinya pengaduan. Tanggung jawab bank dapat menjadi dominan apabila kerugian berkaitan dengan kelemahan sistem atau kegagalan memenuhi kewajiban keamanan, sedangkan tanggung jawab nasabah dapat menjadi dominan apabila kerugian terutama disebabkan oleh kelalaian berat atau tindakan sadar nasabah setelah kewajiban keamanan bank terpenuhi.

Mekanisme penyelesaian sengketa melalui pengaduan internal bank, OJK, LAPS SJK, dan litigasi telah tersedia, tetapi efektivitas pemulihan hak nasabah masih dipengaruhi oleh persoalan pembuktian elektronik, posisi tawar para pihak, waktu, dan biaya penyelesaian. Oleh karena itu, diperlukan penguatan regulasi dan standar penanganan sengketa *phishing* yang memberikan parameter pembagian tanggung jawab secara lebih jelas serta mendorong penilaian terhadap proses terjadinya transaksi, bukan hanya validitas penggunaan PIN atau OTP.

Dengan demikian, penguatan perlindungan nasabah perlu diarahkan pada kejelasan standar keamanan dan respons bank, keseimbangan pembuktian, serta mekanisme penyelesaian sengketa yang mampu menilai kontribusi masing-masing pihak secara proporsional sehingga tercapai kepastian hukum, keadilan, dan pemulihan kerugian yang efektif.

DAFTAR PUSTAKA

- Ahmad, H., Anggraini, S., & Iswahyudi, G. (2022). Perlindungan Hukum Terhadap Keamanan Rahasia Bank dalam Menjaga Kepentingan Nasabah Perbankan. *Jurnal Hukum Dan Pranata Sosial Islam*, 4(2), 337–350. <https://doi.org/10.37680/almanhaj.v4i2.1800>
- Ansyah, R. (2023). Penyelesaian sengketa asuransi melalui mediasi di Lembaga Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK). *Taqnin: Jurnal Syariah dan Hukum*, 5(2), 142–158. <https://doi.org/10.30821/taqnin.v5i02.13442>
- Budiono, Fadillah, & Arinudin (2025), *The Dangers of Phishing to Personal Data Security*, *Formosa Journal of Applied Sciences*, 4(3), 831–844, DOI 10.55927/fjas.v4i3.61.
- Fazriah, D. (2023). Tanggung jawab atas terjadinya wanprestasi yang dilakukan oleh debitur pada saat pelaksanaan perjanjian. *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat*, 1(2), 1–25. <https://journal.forikami.com/index.php/dassollen/issue/view/5>
- Fonda, H., & Hoessein, Z. A. (2022). Pertanggungjawaban Bank dalam Menjamin Keamanan Data Nasabah di Era Digitalisasi Perbankan. *Jurnal Retentum*, 4(1), 34–47. Retrieved from <http://dx.doi.org/10.46930/retentum.v7i1.5271>
- Hasanudin, T. A. (2026). Perlindungan nasabah dan tanggung jawab bank dalam penanggulangan kejahatan digital berbasis *social engineering*: Analisis hukum perbankan Indonesia. *IJBL: Indonesia of Journal Business Law*, 5(1), 99–115. <https://doi.org/10.47709/ijbl.v5i1.7476>
- Hendarto, V. A., & Prasetyawati, E. (2024). Tanggung jawab bank dalam mengantisipasi dan menangani kerugian nasabah akibat *scam* melalui link *phishing* pada mobile banking. *Iuris Studia: Jurnal Kajian Hukum*, 5(3), 759–765. <https://doi.org/10.55357/is.v5i3.714132>
- Kusumadewi, Y., & Sharon, G. (2022). *Hukum perlindungan konsumen*. Lembaga Fatimah Azzahrah.
- Maheswara, D. A., & Hana, Y. (2024). Perlindungan hukum akibat kerugian transaksi aplikasi mobile banking bagi nasabah perbankan berdasarkan hukum perbankan. *Jurnal Multidisiplin Ilmu Akademik*, 1(6), 136–146. <https://doi.org/10.61722/jmia.v1i6.2886>
- Mukhra, U. H., Makruf, J. J., Kesuma, M., Nizam, A., & Siregar, M. R. (2024). *Mobile Banking dalam Persepsi Privasi Nasabah*. Aceh: Syiah Kuala University Press. <https://jurnal.unmer.ac.id/index.php/mlj>

- Mulyadi, R., Rahmat, D., & Pratama, R. (2026). Tanggung jawab hukum pihak bank atas kerugian nasabah akibat kejahatan *phishing*. *Jurnal Greenation Sosial dan Politik*, 4(1), 14–26. <https://doi.org/10.38035/jgsp.v4i1.60785>
- Mutiasari & Soemarso (2020), *Analisis Kepuasan Nasabah atas Kualitas Layanan Internet Banking pada PT Bank Pembangunan Daerah Jawa Tengah Kantor Cabang Pati*, KEUNIS, 8(2), 120–134, DOI 10.32497/keunis.v8i2.2112
- Nur, M. S., & Sukma, D. P. (2025). Analisis perlindungan hukum dan tanggung jawab perdata bank terhadap nasabah korban *phishing* berdasarkan Undang-Undang No. 8 Tahun 1999. *Verstek: Jurnal Hukum Acara*, 13(3), 501–516. <https://doi.org/10.20961/jv.v13i3.103869>
- Rahmawati, D., & Tien, M. A. (2023). Perlindungan hukum atas kerugian nasabah yang disebabkan bobolnya mobile banking menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. *Al-Manhaj: Jurnal Hukum dan Pranata Sosial Islam*, 5(1), 1239–1248. <https://doi.org/10.37680/almanhaj.v5i2.2908>
- Renyaan, W. (2022). *Peranan Lembaga Mediasi Perbankan Dalam Penyelesaian Sengketa Non Litigasi*. Sumatera Barat: CV Azka Pustaka, hlm. 71 - 76.
- Runtunuwu, G. T. J., Wewenggang, F. S., & Mamengko, R. S. (2025). Tinjauan yuridis pertanggungjawaban pihak bank terhadap kasus *card trapping* yang dialami oleh nasabah. *Lex Crimen*, 13(1). <https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/62289/49633>
- Simanjuntak, J. L., & Simanjuntak, K. (2023). Alternatif penyelesaian sengketa klaim asuransi di BMAI dan LAPS SJK. *Unes Law Review*, 5(4), 3393–3413. <https://doi.org/10.31933/unesrev.v5i4.675>
- Tamba, T., & Mukharom. (2023). Efektivitas peran mediator dalam penyelesaian sengketa nonlitigasi dalam bidang bisnis maupun hukum. *JIMPA: Jurnal Ilmiah Mahasiswa Perbankan Syariah*, 3(2), 445–460. <https://doi.org/10.36908/jimpa.v3i2.247>
- Waluyo, B. (2016). *Penegakan hukum di Indonesia*. Sinar Grafika.
- Widjana, N. P. J. M. P., Antari, P. E. D., Kurniawan, I. G. A., & Rama, B. G. A. (2025). Pertanggungjawaban bank terhadap kerugian nasabah akibat pencurian dana melalui *phishing*. *Locus: Jurnal Konsep Ilmu Hukum*, 5(3), 451–459. <https://doi.org/10.56128/jkih.v5i3.649>
- Yosefine, Agustina, & Agus (2023), *Perlindungan Hukum terhadap Nasabah BTPN Jenius akibat Tindakan Phishing*, *Yustisia Tirtayasa: Jurnal Tugas Akhir*, 3(1), 57–72, DOI 10.51825/yta.v3i1.17650.