Jurnal Cendekia Hukum Indonesia
Vol. 2 No. 1 April 2026

DOI: https://doi.org/10.71417/jchi.v2i1.205
https://hukum.journalpustakacendekia.com/index.php/JCHI

Perlindungan Hukum Nasabah Korban Pembobolan Rekening melalui *Social Engineering* di Era *Open Banking*

Imelda Fitria Labibah[1], Nenden Zahwalia[2], Dewi Gita Christine Lumbantoruan[3], Sevi Dianasari[4], Baidhow[5]
[12345]Ilmu Hukum, Universitas Negeri Semarang

Alamat: Jl. Raya Banaran, Sekaran, Kec. Gn. Pati, Kota Semarang
Korespondensi penulis: imeldafl212@students.unnes.ac.id

Abstract. *The development of open banking in Indonesia has made digital financial services more accessible while simultaneously increasing the risk of cybercrime, particularly social engineering. This type of crime exploits psychological manipulation to obtain customers' authentication information such as PINs, passwords, and OTP codesresulting in significant financial losses. This study aims to analyze the forms of legal protection for customers who are victims of account breaches through social engineering, as well as the legal liability of banks in the era of open banking based on Indonesian banking regulations. The research method used is a normative legal analysis employing a statutory approach and a conceptual approach. The research findings indicate that legal protection for customers is dualistic, encompassing preventive protection through the bank's obligation to implement adequate cybersecurity systems based on POJK No. 11/POJK.03/2022 and POJK No. 22 of 2023, as well as repressive protection in the form of compensation mechanisms and dispute resolution under the Consumer Protection Act and the -Personal Data Protection Act. Bank liability may arise from three legal bases, namely contractual breach, negligence, and the principle of consumer protection. In an open banking ecosystem involving third parties, banks retain a duty of oversight; therefore, the bank's liability does not automatically cease even if losses result from weaknesses in a technology partner's system. This study concludes that stricter regulatory harmonization and improved customer digital literacy are necessary to strengthen comprehensive legal protections in the era of digital banking.*

Keywords: *The Open Banking Era, Victims of Account Hacking, Legal Protection, Social Engineering*

Abstrak. Perkembangan *open banking* di Indonesia membawa kemudahan akses layanan keuangan digital sekaligus meningkatkan risiko kejahatan siber, khususnya *social engineering*. Kejahatan ini memanfaatkan manipulasi psikologis untuk memperoleh informasi autentikasi nasabah seperti PIN, kata sandi, dan kode OTP, sehingga mengakibatkan kerugian finansial yang signifikan. Penelitian ini bertujuan menganalisis bentuk perlindungan hukum bagi nasabah korban pembobolan rekening melalui *social engineering* serta pertanggungjawaban hukum bank dalam era *open banking* berdasarkan regulasi perbankan Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual

Received April 21, 2026; Revised April 23, 2026; Accepted April 23, 2026
*Imelda Fitria Labibah, imeldafl212@students.unnes.ac.id

(*conceptual approach*). Hasil penelitian menunjukkan bahwa perlindungan hukum bagi nasabah bersifat dualistik, meliputi perlindungan preventif melalui kewajiban bank menerapkan sistem keamanan siber yang memadai berdasarkan POJK Nomor 11/POJK.03/2022 dan POJK Nomor 22 Tahun 2023, serta perlindungan represif berupa mekanisme ganti rugi dan penyelesaian sengketa berdasarkan Undang-Undang Perlindungan Konsumen dan Undang-Undang Perlindungan Data Pribadi. Pertanggungjawaban bank dapat timbul dari tiga dasar hukum, yaitu wanprestasi kontraktual, kelalaian (*negligence*), dan prinsip perlindungan konsumen. Dalam ekosistem *open banking* yang melibatkan pihak ketiga, bank tetap memiliki kewajiban pengawasan (*duty of oversight*) sehingga tanggung jawab bank tidak serta merta gugur meskipun kerugian terjadi akibat kelemahan sistem mitra teknologi. Penelitian ini menyimpulkan bahwa diperlukan harmonisasi regulasi yang lebih tegas serta peningkatan literasi digital nasabah guna memperkuat perlindungan hukum secara komprehensif di era perbankan digital.

Kata Kunci: Era *Open Banking*, Korban Pembobolan Rekening, Perlindungan Hukum, *Social Engineering*

LATAR BELAKANG

Perkembangan teknologi informasi telah mendorong transformasi besar dalam sektor keuangan, khususnya dalam sistem layanan perbankan digital. Inovasi teknologi tersebut melahirkan konsep *open banking*, yaitu sistem yang memungkinkan pertukaran data keuangan nasabah secara aman antara bank dan pihak ketiga melalui *Application Programming Interface (API)*. Sistem ini memberikan kemudahan bagi masyarakat untuk mengakses berbagai layanan keuangan secara lebih cepat, efisien, dan terintegrasi. Namun demikian, perkembangan tersebut juga menimbulkan risiko keamanan siber yang dapat mengancam data dan dana nasabah, terutama melalui berbagai bentuk kejahatan digital yang semakin kompleks (Cahyadi & Gorda, 2019).

Salah satu bentuk kejahatan siber yang semakin sering terjadi dalam sektor perbankan digital adalah *social engineering*. Kejahatan ini merupakan teknik manipulasi psikologis yang digunakan oleh pelaku untuk memperoleh informasi sensitif milik korban seperti PIN, password, maupun kode OTP yang berkaitan dengan akses rekening bank. Berbeda dengan peretasan sistem secara langsung, *social engineering* memanfaatkan kelengahan atau ketidaktahuan korban sehingga mereka secara sukarela memberikan informasi penting kepada pelaku. Dalam praktiknya, modus *social engineering* berkembang melalui berbagai media digital seperti pesan singkat, panggilan telepon, email, maupun tautan palsu yang dikenal sebagai phishing. Pelaku sering menyamar sebagai pihak bank atau lembaga resmi untuk meyakinkan korban agar memberikan

informasi pribadi yang bersifat rahasia. Kondisi ini menyebabkan banyak nasabah mengalami kerugian finansial akibat transaksi yang tidak mereka lakukan secara langsung (Az-zahra & Labib, 2024).

Meningkatnya kasus pembobolan rekening melalui *social engineering* menunjukkan bahwa keamanan sistem perbankan digital tidak hanya bergantung pada teknologi yang digunakan oleh bank, tetapi juga pada tingkat literasi digital dan kesadaran keamanan dari pengguna layanan. Dalam konteks ini, nasabah sebagai konsumen jasa keuangan berada pada posisi yang relatif rentan karena keterbatasan pemahaman terhadap berbagai risiko keamanan transaksi digital. Oleh karena itu, perlindungan hukum terhadap nasabah menjadi aspek penting dalam menjaga kepercayaan masyarakat terhadap sistem perbankan digital (Ayunda & Rusdianto, 2021). Dalam sistem hukum perbankan Indonesia, perlindungan terhadap nasabah merupakan bagian dari penerapan prinsip kehati-hatian (*prudential banking principle*) yang wajib dilaksanakan oleh setiap bank dalam menjalankan kegiatan usahanya. Bank memiliki kewajiban untuk menjaga keamanan dana nasabah serta memastikan bahwa sistem teknologi informasi yang digunakan dalam layanan perbankan digital dapat beroperasi secara aman dan terpercaya (Atsari et al., 2023).

Regulasi mengenai perlindungan konsumen di sektor jasa keuangan telah diatur dalam berbagai peraturan perundang-undangan, antara lain Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, serta berbagai peraturan yang dikeluarkan oleh Otoritas Jasa Keuangan. Regulasi tersebut bertujuan untuk memberikan kepastian hukum serta menjamin bahwa nasabah sebagai pengguna layanan perbankan memperoleh perlindungan yang memadai dalam setiap aktivitas transaksi keuangan digital (Astrini, 2015). Namun demikian, dalam praktik penyelesaian kasus pembobolan rekening melalui *social engineering* sering muncul perdebatan mengenai pihak yang harus bertanggung jawab atas kerugian yang dialami nasabah. Pihak bank sering berpendapat bahwa kerugian tersebut terjadi karena kelalaian nasabah yang memberikan informasi rahasia kepada pihak lain. Sementara itu, dari perspektif perlindungan konsumen, bank tetap memiliki tanggung jawab untuk memastikan keamanan sistem layanan serta memberikan perlindungan terhadap dana nasabah (Ervian & S, 2025).

Selain itu, implementasi konsep *open banking* yang melibatkan integrasi sistem antara bank dan berbagai pihak ketiga juga menimbulkan kompleksitas baru dalam aspek

tanggung jawab hukum. Keterlibatan berbagai aktor dalam ekosistem keuangan digital berpotensi menimbulkan permasalahan terkait keamanan data, pembagian tanggung jawab, serta mekanisme penyelesaian sengketa apabila terjadi kerugian pada nasabah (Siregar & Putra, 2025). Oleh karena itu, penting untuk menganalisis secara komprehensif mengenai bentuk perlindungan hukum bagi nasabah korban pembobolan rekening melalui *social engineering* serta pertanggungjawaban hukum bank dalam era *open banking* berdasarkan regulasi perbankan di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*), yaitu penelitian yang dilakukan dengan mengkaji dan menganalisis norma-norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, serta prinsip-prinsip hukum yang berkaitan dengan objek penelitian. Pendekatan ini dipilih karena penelitian bertujuan menganalisis konstruksi hukum perlindungan nasabah dan pertanggungjawaban bank dalam kerangka regulasi perbankan Indonesia yang berlaku, tanpa melakukan pengujian empiris di lapangan.

Pendekatan yang digunakan dalam penelitian ini meliputi dua pendekatan utama. Pertama, pendekatan perundang-undangan (*statute approach*), yaitu dengan menelaah seluruh peraturan perundang-undangan yang bersangkut paut dengan isu hukum yang diteliti, di antaranya Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, serta berbagai Peraturan Otoritas Jasa Keuangan yang relevan, antara lain POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, POJK Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum, dan POJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Kedua, pendekatan konseptual (*conceptual approach*), yaitu menelaah pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum, khususnya yang berkaitan dengan konsep pertanggungjawaban hukum, perlindungan konsumen, keamanan siber, dan ekosistem *open banking*.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas tiga kategori. Pertama, bahan hukum primer, yaitu peraturan perundang-undangan yang berlaku di Indonesia yang berkaitan langsung dengan objek penelitian, sebagaimana telah disebutkan di atas. Kedua, bahan hukum sekunder, berupa literatur hukum, buku-buku teks, jurnal ilmiah hukum, artikel ilmiah, maupun penelitian terdahulu yang memiliki relevansi dengan permasalahan yang dikaji. Ketiga, bahan hukum tersier, yaitu bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus hukum, ensiklopedia, dan sumber daring resmi dari lembaga-lembaga terkait.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), yaitu dengan menginventarisasi, mengklasifikasikan, dan menganalisis bahan-bahan hukum yang relevan secara sistematis. Analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode interpretasi hukum, meliputi interpretasi gramatikal, interpretasi sistematis, dan interpretasi teleologis, guna memperoleh pemahaman yang komprehensif mengenai norma-norma hukum yang mengatur perlindungan nasabah dan pertanggungjawaban bank dalam konteks kejahatan *social engineering* di era *open banking*.

HASIL DAN PEMBAHASAN

Bentuk Perlindungan Hukum bagi Nasabah Korban Pembobolan Rekening melalui *Social Engineering* di Era *Open Banking* Berdasarkan Regulasi Perbankan Indonesia

1. Perlindungan Hukum Preventif melalui Kerangka Regulasi Perbankan Digital

Perlindungan hukum dalam sistem perbankan Indonesia pada dasarnya bersifat dualistik, yakni mencakup dimensi preventif dan represif. Perlindungan preventif bertujuan mencegah terjadinya kerugian sebelum sengketa atau pelanggaran terjadi, sementara perlindungan represif bermaksud memulihkan hak yang telah dilanggar. Dalam konteks era *open banking* yang ditandai dengan keterbukaan antarmuka pemrograman aplikasi (API) antara bank dan pihak ketiga, potensi celah keamanan yang dapat dieksploitasi melalui rekayasa sosial (*social engineering*) menjadi semakin signifikan. Nasabah perbankan dalam hal ini menempati posisi sebagai pihak yang paling

rentan, mengingat manipulasi psikologis yang dilakukan pelaku memanfaatkan ketidaktahuan dan kepercayaan nasabah untuk memperoleh akses ilegal terhadap akun dan dana mereka (Rahmahdhani et al., 2023).

Secara regulatoris, kerangka hukum perlindungan preventif bagi nasabah perbankan di Indonesia ditopang oleh sejumlah instrumen hukum yang saling melengkapi. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan meletakkan kewajiban dasar bank untuk menerapkan prinsip kehati-hatian (*prudential banking principle*) sebagaimana diatur dalam Pasal 2 dan Pasal 29 Ayat (2), yang mengharuskan bank menjaga kesehatan operasional sekaligus melindungi kepentingan nasabah dari potensi kerugian (Siswanto & Lenita, 2024). Kewajiban ini memiliki implikasi langsung terhadap tanggung jawab bank dalam memastikan keamanan sistem digital yang dioperasikannya, termasuk perlindungan terhadap ancaman siber yang menggunakan manipulasi manusia sebagai vektornya.

Merespons perkembangan ancaman di era perbankan digital, Otoritas Jasa Keuangan (OJK) menerbitkan Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Regulasi ini mewajibkan bank untuk menjaga ketahanan siber melalui serangkaian proses terstruktur, meliputi identifikasi aset, ancaman dan kerentanan; perlindungan aset sistem informasi; deteksi insiden siber; serta penanggulangan dan pemulihan pasca insiden (Irmawati et al., 2024). Kewajiban ini secara implisit mencakup perlindungan terhadap serangan berbasis rekayasa sosial yang menargetkan data autentikasi nasabah seperti PIN, OTP, dan kata sandi. Kerangka keamanan siber yang ditentukan oleh POJK ini menjadi fondasi perlindungan preventif yang paling langsung relevan dalam konteks *open banking*, di mana aliran data nasabah yang terbuka antara bank dan mitra teknologi pihak ketiga memperbesar permukaan serangan potensial.

Dimensi perlindungan preventif turut diperkuat melalui Peraturan OJK Nomor 21 Tahun 2023 tentang Layanan Digital oleh Bank Umum, yang mengatur mekanisme kerja sama layanan digital antara bank dengan mitra teknologi, termasuk penggunaan API terbuka sebagai fondasi utama praktik *open banking*. Meskipun OJK secara eksplisit mengakui bahwa belum terdapat payung hukum tunggal yang secara khusus mengatur *open banking*, Kepala Eksekutif Pengawas Perbankan OJK menegaskan bahwa konsep *open banking* pada prinsipnya telah tercantum dalam POJK Nomor 21 Tahun 2023, serta

didukung pengaturan aspek perlindungan dan pengelolaan data dalam POJK No. 11/POJK.03/2022. Pendekatan regulasi yang bersifat prinsipil ini, sambil mendorong kolaborasi bank dengan pelaku teknologi, tetap meletakkan aspek keamanan dan perlindungan data nasabah sebagai landasan utama.

Perlindungan preventif selanjutnya juga diwujudkan melalui kewajiban edukasi dan literasi keuangan digital yang dibebankan kepada bank. Berdasarkan Peraturan OJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan yang berlaku sejak 20 Desember 2023, terdapat tujuh prinsip utama perlindungan konsumen yang salah satunya mencakup kewajiban edukasi keuangan yang memadai dan perlindungan aset, privasi, serta data konsumen. Regulasi ini secara tegas mengharuskan Pelaku Usaha Jasa Keuangan (PUJK), termasuk bank, untuk memastikan keamanan sistem informasi dan ketahanan siber (Prayascita & Adnyani, 2026). Bank tidak hanya wajib membangun infrastruktur keamanan teknis, tetapi juga wajib secara aktif membangun kapasitas nasabahnya untuk mengenali dan menghindari modus *social engineering* seperti phishing, vishing, dan smishing yang marak terjadi di era *open banking*.

2. Perlindungan Hukum Represif yakni Tanggung Jawab Bank dan Mekanisme Ganti Rugi

Ketika perlindungan preventif gagal dan nasabah telah menjadi korban pembobolan rekening akibat *social engineering*, hukum Indonesia menyediakan sejumlah mekanisme perlindungan represif yang bertujuan memulihkan kerugian yang dialami. Instrumen hukum pertama yang dapat ditempuh adalah ketentuan tanggung jawab perdata berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Pasal 19 Ayat (1) dan (2) undang-undang ini menegaskan bahwa pelaku usaha, termasuk bank sebagai penyedia jasa, bertanggung jawab memberikan ganti rugi atas kerugian konsumen yang diakibatkan oleh penggunaan jasa tersebut. Ganti rugi dapat berupa pengembalian dana, penggantian jasa, atau kompensasi lain sesuai ketentuan yang berlaku (Fuady, 2016).

Persoalan krusial yang kerap menjadi titik sengketa dalam kasus pembobolan rekening melalui *social engineering* adalah pertanyaan mengenai siapa yang menanggung beban kesalahan: bank ataukah nasabah itu sendiri. Doktrin hukum yang berlaku umum menggariskan bahwa tanggung jawab bank tidak dapat dikesampingkan apabila kerugian

terjadi akibat kelalaian atau kelemahan sistem keamanan bank. Sebaliknya, apabila kerugian semata-mata disebabkan oleh kesalahan nasabah sendiri, seperti secara sukarela membocorkan PIN, OTP, atau data autentikasi lainnya kepada pihak ketiga, maka bank dapat terbebas dari tanggung jawab penuh (Kristy & Lie, 2026). Namun, pembagian tanggung jawab ini tidaklah mutlak. Dalam praktik *social engineering*, nasabah dimanipulasi secara psikologis sehingga tidak sepenuhnya bertindak atas kehendak bebas, melainkan di bawah tekanan rekayasa pelaku. Kondisi ini menuntut interpretasi hukum yang lebih nuansatif terkait kausalitas dan distribusi tanggung jawab antara bank dan nasabah.

Dalam kerangka POJK No. 22 Tahun 2023, ketentuan Pasal 29 Ayat (1) POJK Nomor 1/POJK.07/2023 mempertegas tanggung jawab bank atas kerugian konsumen yang disebabkan oleh kesalahan atau kelalaian pengurus, pegawai, atau pihak ketiga yang bekerja untuk kepentingan lembaga tersebut. Ketentuan ini sangat relevan dalam konteks *open banking*, di mana bank menggandeng mitra pihak ketiga (*third-party providers/TPP*) dalam penyelenggaraan layanan berbasis API. Apabila serangan *social engineering* berhasil karena adanya kelemahan pada sistem mitra pihak ketiga yang bekerja sama dengan bank, tanggung jawab bank tidak serta merta gugur. Bank tetap memiliki kewajiban pengawasan (*duty of oversight*) terhadap keamanan mitra teknologinya dalam ekosistem *open banking* (Rahmahdhani et al., 2023).

Perlindungan represif turut diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 12 Ayat (1) UU PDP secara tegas mengatur hak subjek data pribadi untuk menggugat dan memperoleh ganti rugi atas pelanggaran terhadap data pribadinya. Dalam kasus pembobolan rekening melalui *social engineering*, data pribadi nasabah seperti nomor kartu, kode OTP, dan data biometric yang merupakan objek eksploitasi utama. Oleh karena itu, nasabah korban berpotensi menempuh jalur gugatan perdata berdasarkan UU PDP secara kumulatif dengan gugatan berdasarkan UU Perlindungan Konsumen, guna memaksimalkan pemulihan kerugian yang dideritanya (Wiedyasari & Yuspin, 2022). Meskipun demikian, implementasi UU PDP dalam sektor perbankan masih menghadapi tantangan berupa lemahnya penegakan hukum dan rendahnya kesadaran nasabah akan hak-haknya.

Mekanisme penyelesaian sengketa dalam sistem perlindungan represif perbankan di Indonesia dapat ditempuh melalui beberapa jalur. Pertama, pengaduan kepada bank

yang bersangkutan sebagai mekanisme internal. Kedua, eskalasi pengaduan kepada OJK apabila penyelesaian di tingkat bank tidak memuaskan, mengacu pada POJK No. 22 Tahun 2023 yang memperkuat kewenangan OJK dalam penanganan pengaduan konsumen. Ketiga, penyelesaian sengketa melalui Lembaga Alternatif Penyelesaian Sengketa (LAPS) sektor jasa keuangan, yang menyediakan forum mediasi dan arbitrase yang lebih efisien dibandingkan litigasi pengadilan. Keempat, jalur pidana melalui pelaporan kepada kepolisian berdasarkan Pasal 362 KUHP dan ketentuan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE, di mana pelaku *social engineering* yang menimbulkan kerugian materiil dapat diancam pidana penjara hingga 12 tahun dan denda hingga Rp12 miliar (Utami, 2024).

Pertanggungjawaban Hukum Bank terhadap Nasabah Korban Pembobolan Rekening melalui *Social Engineering* di Era *Open Banking*

1. Konsep Pertanggungjawaban Hukum dalam Hubungan Bank dan Nasabah

Pertanggungjawaban hukum merupakan konsekuensi yang timbul ketika suatu pihak melakukan perbuatan yang menimbulkan kerugian bagi pihak lain, baik karena pelanggaran terhadap perjanjian maupun karena perbuatan melawan hukum. Dalam konteks kegiatan perbankan, konsep pertanggungjawaban hukum menjadi penting karena bank mengelola dana masyarakat yang dipercayakan kepadanya. Oleh karena itu, hubungan antara bank dan nasabah tidak hanya bersifat administratif, tetapi juga memiliki dimensi hukum yang menimbulkan hak dan kewajiban bagi kedua belah pihak (Fuady, 2016).

Hubungan hukum antara bank dan nasabah pada dasarnya lahir dari suatu perjanjian. Ketika seseorang membuka rekening pada suatu bank, maka secara hukum terbentuk hubungan kontraktual yang mengikat kedua belah pihak. Dalam hubungan tersebut, nasabah mempercayakan pengelolaan dan penyimpanan dananya kepada bank, sedangkan bank berkewajiban memberikan layanan perbankan yang aman serta menjaga kerahasiaan dan keamanan dana nasabah. Hubungan hukum antara bank dan nasabah pada dasarnya merupakan hubungan keperdataan yang didasarkan pada perjanjian penyimpanan dana, sehingga bank memiliki kewajiban untuk menjaga kepercayaan nasabah sebagai bagian dari prinsip kepercayaan (*fiduciary relationship*) dalam kegiatan perbankan.

Dalam praktik perbankan modern, tanggung jawab bank tidak hanya terbatas pada pengelolaan dana nasabah secara administratif, tetapi juga mencakup kewajiban untuk menyediakan sistem layanan yang aman dan dapat diandalkan. Hal ini sejalan dengan penerapan prinsip kehati-hatian (*prudential banking principle*) yang mewajibkan bank untuk menjalankan kegiatan usahanya secara hati-hati guna menjaga stabilitas sistem perbankan serta melindungi kepentingan nasabah. Prinsip kehati-hatian tersebut menuntut bank untuk memastikan bahwa sistem teknologi informasi yang digunakan dalam layanan perbankan digital memiliki standar keamanan yang memadai sehingga dapat meminimalkan risiko terjadinya penyalahgunaan data maupun pembobolan rekening.

Selain didasarkan pada hubungan kontraktual, pertanggungjawaban hukum bank juga dapat timbul dari kelalaian dalam menjalankan kewajiban pelayanan kepada nasabah. Apabila bank tidak mampu menyediakan sistem keamanan yang memadai atau gagal mencegah terjadinya transaksi tidak sah yang merugikan nasabah, maka bank dapat dimintai pertanggungjawaban atas kerugian tersebut. Dalam perspektif hukum perlindungan konsumen, bank dipandang sebagai pelaku usaha yang memiliki kewajiban untuk memberikan perlindungan terhadap konsumen pengguna jasa keuangan, termasuk dalam hal menjamin keamanan transaksi dan kerahasiaan data nasabah (Ayunda & Rusdianto, 2021).

Perkembangan teknologi digital dalam sektor perbankan turut memperluas ruang lingkup tanggung jawab bank. Penerapan layanan perbankan digital seperti mobile banking, internet banking, dan integrasi sistem *open banking* membuka peluang terjadinya berbagai bentuk kejahatan siber, salah satunya melalui teknik *social engineering*. Dalam kasus tersebut, meskipun pelaku kejahatan memanfaatkan kelengahan nasabah untuk memperoleh informasi rahasia seperti kode OTP atau kata sandi, tanggung jawab bank tetap perlu dianalisis secara hukum untuk menilai sejauh mana bank telah menjalankan kewajiban pengamanan sistem serta memberikan edukasi kepada nasabah mengenai risiko keamanan digital.

2. Bentuk Pertanggungjawaban Bank terhadap Kerugian Nasabah akibat *Social Engineering*

Perkembangan layanan perbankan digital telah memberikan kemudahan bagi masyarakat dalam melakukan berbagai transaksi keuangan secara cepat dan efisien.

Namun demikian, perkembangan tersebut juga diikuti dengan meningkatnya risiko kejahatan siber, salah satunya melalui teknik *social engineering*. Kejahatan ini dilakukan dengan cara memanipulasi psikologis korban agar secara sukarela memberikan informasi sensitif seperti kata sandi, PIN, maupun kode OTP yang digunakan untuk mengakses layanan perbankan digital. Dalam situasi tersebut, muncul persoalan hukum mengenai sejauh mana bank dapat dimintai pertanggungjawaban atas kerugian yang dialami oleh nasabah akibat pembobolan rekening melalui metode tersebut (Az-zahra & Labib, 2024).

Secara umum, bentuk pertanggungjawaban bank terhadap kerugian nasabah dapat dianalisis melalui beberapa pendekatan hukum, yaitu pertanggungjawaban berdasarkan hubungan kontraktual, pertanggungjawaban akibat kelalaian, serta pertanggungjawaban berdasarkan prinsip perlindungan konsumen. Ketiga pendekatan tersebut menjadi dasar dalam menentukan apakah bank memiliki kewajiban untuk mengganti kerugian yang dialami oleh nasabah dalam kasus pembobolan rekening melalui *social engineering*.

Pertama, pertanggungjawaban kontraktual yang timbul dari hubungan perjanjian antara bank dan nasabah. Ketika nasabah membuka rekening dan menggunakan layanan perbankan, secara hukum terbentuk perjanjian antara kedua belah pihak yang mengatur hak dan kewajiban masing-masing. Dalam hubungan tersebut, bank memiliki kewajiban untuk menyediakan sistem layanan yang aman serta menjaga dana nasabah dari potensi penyalahgunaan. Apabila bank gagal memenuhi kewajiban tersebut sehingga menimbulkan kerugian bagi nasabah, maka bank dapat dianggap melakukan wanprestasi terhadap perjanjian yang telah disepakati. Dengan demikian, bank dapat dimintai pertanggungjawaban untuk memberikan ganti rugi atas kerugian yang dialami oleh nasabah (Hermansyah, 2014).

Kedua, pertanggungjawaban berdasarkan kelalaian (*negligence*). Dalam praktik perbankan digital, bank memiliki kewajiban untuk menerapkan sistem keamanan teknologi informasi yang memadai guna mencegah terjadinya penyalahgunaan layanan perbankan. Apabila bank tidak menerapkan sistem pengamanan yang memadai, tidak melakukan pengawasan terhadap aktivitas transaksi yang mencurigakan, atau tidak memberikan edukasi yang cukup kepada nasabah mengenai risiko keamanan digital, maka bank dapat dianggap lalai dalam menjalankan kewajibannya. Kelalaian tersebut dapat menjadi dasar bagi nasabah untuk menuntut pertanggungjawaban bank atas kerugian yang timbul akibat pembobolan rekening (Fitriani et al., 2024).

Ketiga, pertanggungjawaban berdasarkan prinsip perlindungan konsumen. Dalam perspektif hukum perlindungan konsumen, nasabah bank dipandang sebagai konsumen yang menggunakan jasa yang disediakan oleh pelaku usaha, yaitu bank. Oleh karena itu, bank memiliki kewajiban untuk memberikan perlindungan kepada nasabah dalam menggunakan layanan perbankan, termasuk menjamin keamanan sistem transaksi dan kerahasiaan data nasabah. Undang-Undang Perlindungan Konsumen mengatur bahwa pelaku usaha bertanggung jawab untuk memberikan ganti rugi atas kerugian yang dialami konsumen akibat penggunaan jasa yang diberikan. Dengan demikian, apabila kerugian nasabah terjadi akibat kelemahan sistem keamanan atau kurangnya perlindungan yang diberikan oleh bank, maka bank dapat dimintai pertanggungjawaban berdasarkan prinsip perlindungan konsumen.

Namun demikian, dalam praktik penyelesaian sengketa sering muncul perdebatan mengenai pembagian tanggung jawab antara bank dan nasabah dalam kasus *social engineering*. Pihak bank umumnya berpendapat bahwa kerugian tersebut terjadi karena kelalaian nasabah yang memberikan informasi rahasia kepada pihak lain. Di sisi lain, dari perspektif perlindungan konsumen, bank tetap memiliki tanggung jawab untuk memastikan bahwa sistem keamanan layanan perbankan mampu mendeteksi dan mencegah transaksi yang mencurigakan (Astrini, 2015). Oleh karena itu, penentuan tanggung jawab dalam kasus pembobolan rekening melalui *social engineering* perlu dianalisis secara komprehensif dengan mempertimbangkan sejauh mana bank telah menerapkan standar keamanan sistem serta memberikan edukasi kepada nasabah mengenai risiko keamanan transaksi digital.

Dengan demikian, bentuk pertanggungjawaban bank terhadap kerugian nasabah akibat *social engineering* tidak dapat ditentukan secara sederhana, melainkan harus dianalisis berdasarkan berbagai aspek hukum yang meliputi hubungan kontraktual antara bank dan nasabah, tingkat kelalaian yang terjadi, serta kewajiban bank dalam memberikan perlindungan kepada nasabah sebagai konsumen jasa keuangan. Analisis tersebut menjadi penting terutama dalam era *open banking*, di mana integrasi sistem antara bank dan berbagai pihak ketiga berpotensi meningkatkan kompleksitas dalam penentuan tanggung jawab apabila terjadi kerugian pada nasabah.

3. Analisis Pertanggungjawaban Bank dalam Kasus *Social Engineering* di Era *Open Banking*

Perkembangan teknologi keuangan telah mendorong munculnya konsep *open banking*, yaitu sistem yang memungkinkan pertukaran data keuangan nasabah antara bank dan pihak ketiga melalui teknologi *Application Programming Interface (API)*. Konsep ini bertujuan untuk meningkatkan efisiensi layanan keuangan serta memperluas akses masyarakat terhadap berbagai produk dan layanan keuangan digital. Namun demikian, penerapan *open banking* juga menimbulkan tantangan baru dalam aspek keamanan sistem serta perlindungan data nasabah, khususnya terkait dengan meningkatnya risiko kejahatan siber seperti *social engineering*.

Dalam kasus pembobolan rekening melalui teknik *social engineering*, pelaku biasanya memanfaatkan manipulasi psikologis untuk memperoleh informasi sensitif milik korban, seperti kode OTP, PIN, atau kata sandi layanan perbankan digital. Meskipun tindakan tersebut dilakukan oleh pihak ketiga yang tidak memiliki hubungan langsung dengan bank, persoalan hukum tetap muncul mengenai sejauh mana bank dapat dimintai pertanggungjawaban atas kerugian yang dialami oleh nasabah. Dalam konteks ini, analisis tanggung jawab bank perlu mempertimbangkan beberapa aspek, yaitu tingkat keamanan sistem perbankan, kewajiban bank dalam memberikan edukasi kepada nasabah, serta mekanisme pengawasan terhadap aktivitas transaksi yang mencurigakan.

Dari perspektif hukum perbankan, bank memiliki kewajiban untuk menerapkan prinsip kehati-hatian dalam menjalankan kegiatan usahanya, termasuk dalam penyelenggaraan layanan perbankan digital. Prinsip tersebut menuntut bank untuk menerapkan sistem manajemen risiko yang efektif serta memastikan bahwa infrastruktur teknologi informasi yang digunakan mampu melindungi dana dan data nasabah dari potensi penyalahgunaan. Apabila bank tidak menerapkan standar keamanan yang memadai atau gagal mendeteksi aktivitas transaksi yang mencurigakan, maka bank berpotensi dianggap lalai dalam menjalankan kewajibannya sehingga dapat dimintai pertanggungjawaban atas kerugian yang dialami oleh nasabah.

Namun demikian, dalam praktiknya tanggung jawab bank tidak dapat dilepaskan dari peran nasabah sebagai pengguna layanan perbankan digital. Banyak kasus *social engineering* terjadi karena nasabah secara sukarela memberikan informasi rahasia kepada pihak yang tidak berwenang akibat kurangnya pemahaman mengenai risiko keamanan digital. Oleh karena itu, dalam menentukan tanggung jawab hukum bank perlu dilakukan penilaian terhadap tingkat kelalaian yang dilakukan oleh masing-masing pihak. Apabila

kerugian terjadi semata-mata karena kelalaian nasabah yang memberikan informasi sensitif kepada pihak lain, maka bank dapat berpendapat bahwa tanggung jawab tersebut tidak sepenuhnya berada pada pihak bank.

Di sisi lain, dalam perspektif perlindungan konsumen, bank tetap memiliki tanggung jawab untuk memastikan bahwa layanan perbankan digital yang disediakan memiliki sistem keamanan yang memadai serta dilengkapi dengan mekanisme perlindungan terhadap nasabah. Hal ini termasuk penyediaan sistem fraud detection, pemberian peringatan terhadap transaksi yang mencurigakan, serta edukasi kepada nasabah mengenai risiko kejahatan siber. Dengan demikian, meskipun nasabah memiliki kewajiban untuk menjaga kerahasiaan data pribadinya, bank tetap berkewajiban untuk memberikan perlindungan maksimal terhadap dana dan data nasabah dalam penggunaan layanan perbankan digital (Shidarta, 2014).

Dalam konteks *open banking*, kompleksitas tanggung jawab hukum semakin meningkat karena keterlibatan berbagai pihak dalam ekosistem layanan keuangan digital, seperti perusahaan teknologi finansial (*fintech*), penyedia layanan pembayaran, serta penyedia infrastruktur teknologi. Integrasi sistem antara bank dan pihak ketiga melalui API berpotensi menimbulkan risiko kebocoran data atau penyalahgunaan informasi apabila tidak disertai dengan sistem pengamanan yang memadai. Oleh karena itu, diperlukan kejelasan mengenai pembagian tanggung jawab antara bank dan pihak ketiga dalam hal terjadi kerugian pada nasabah akibat penyalahgunaan data atau kegagalan sistem dalam ekosistem *open banking* (Siregar & Putra, 2025).

Dengan demikian, analisis pertanggungjawaban bank dalam kasus pembobolan rekening melalui *social engineering* di era *open banking* perlu dilakukan secara komprehensif dengan mempertimbangkan berbagai faktor, termasuk tingkat keamanan sistem perbankan, kelalaian nasabah, serta keterlibatan pihak ketiga dalam penyediaan layanan keuangan digital. Pendekatan tersebut diperlukan untuk memastikan adanya keseimbangan antara perlindungan terhadap nasabah sebagai konsumen jasa keuangan dan kewajiban nasabah dalam menjaga keamanan informasi pribadi yang berkaitan dengan akses terhadap layanan perbankan digital.

KESIMPULAN DAN SARAN

Perlindungan hukum bagi nasabah korban pembobolan rekening melalui *social engineering* di era *open banking* pada dasarnya bersifat dualistik, yaitu preventif dan represif. Perlindungan preventif diwujudkan melalui kewajiban bank menerapkan sistem keamanan siber yang komprehensif sebagaimana diatur dalam POJK Nomor 11/POJK.03/2022, POJK Nomor 21 Tahun 2023, dan POJK Nomor 22 Tahun 2023, termasuk identifikasi ancaman, perlindungan aset informasi, pemulihan insiden, serta edukasi nasabah mengenai risiko kejahatan siber. Sementara itu, perlindungan represif disediakan melalui mekanisme pengaduan internal bank, eskalasi ke OJK, penyelesaian melalui LAPS, gugatan perdata berdasarkan UU Perlindungan Konsumen dan UU PDP, hingga jalur pidana melalui UU ITE, meskipun efektivitasnya masih menghadapi kendala rendahnya literasi digital dan lemahnya penegakan hukum. Terkait pertanggungjawaban hukum, bank tetap memikul tanggung jawab berdasarkan prinsip kontraktual, kelalaian (*negligence*), dan perlindungan konsumen, meskipun sering terjadi perdebatan terkait kelalaian nasabah dalam menjaga data pribadi. Bank tidak dapat melepaskan diri dari tanggung jawab karena berkewajiban menyediakan sistem keamanan yang memadai, mekanisme *fraud detection*, serta edukasi yang cukup, dan dalam konteks *open banking*, bank juga memiliki *duty of oversight* terhadap pihak ketiga sesuai POJK Nomor 1/POJK.07/2023. Oleh karena itu, diperlukan harmonisasi regulasi yang lebih komprehensif, kejelasan pembagian tanggung jawab antara bank dan penyedia layanan pihak ketiga, serta peningkatan literasi digital untuk mewujudkan perlindungan hukum yang lebih efektif bagi nasabah di era perbankan digital.

DAFTAR PUSTAKA

Astrini, D. A. (2015). Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime. *Lex Privatum*, *1*, 149–160.

Atsari, A. W., Sulatri, K., & Mashuri, M. (2023). *Perlindungan Hukum Bagi Nasabah Perbankan Terhadap Kesalahan Layanan Mobile Banking Dari Sistem Teknologi Informasi Perbankan*. *5*(1), 59–72.

Ayunda, R., & Rusdianto. (2021). Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence Dalam Aktifitas Perbankan Di Indonesia. *Jurnal Komunikasi Hukum*, *7*, 663–677.

Az-Zahra, I., & Labib, Z. M. (2024). *Perlindungan Hukum Bagi Nasabah Dalam Kasus*

Phising Dan Siber Perbankan Di Indonesia Intania. *10*(2), 405–425.

Cahyadi, I. K. P., & Gorda, A. A. . N. S. R. (2019). Perlindungan Hukum Terhadap Nasabah Dari Ancaman Kejahatan Perbankan Skimming Melalui Layanan Electronic Banking (Studi Kasus Di Bank Rakyat Indonesia Kantor Wilayah Denpasar). *Jurnal Analisis Hukum*, *2*(September), 167–180.

Ervian, A. N., & S, S. A. (2025). *Perlindungan Hukum Terhadap Nasabah Atas Kebocoran Data Pribadi Dalam Layanan Perbankan Digital Di Indonesia*. 8785–8793.

Fitriani, S. A., Sasra, A. D., Harjuno, M., & Raharjo, A. (2024). *Analisis Perlindungan Data Pribadi Nasabah Perbankan Terhadap Penggunaan Layanan Mobile Banking*. *9*(4), 300–308.

Fuady, M. (2016). *Hukum Perbankan Modern*. Citra Aditya Bakti.

Hermansyah. (2014). *Hukum Perbankan Nasional Indonesia*. Kencana.

Irmawati, E., Pieries, J., & Widiarty, W. S. (2024). *Perlindungan Hukum Atas Data Pribadi Nasabah Bank Pengguna Mobile Banking Dalam Perspektif Uu No 27 Tahun 2022 Tentang Kebocoran Data*. *5*(1).

Kristy, A. A., & Lie, G. (2026). *Peran Regulasi Serta Pengawasan Dalam Mencegah Kebocoran Data Nasabah Pada Sektor Perbankan*. *9*, 39–46.

Prayascita, I. A. P. G., & Adnyani, N. K. S. (2026). *Implementasi Perlindungan Hukum Nasabah Pada Layanan Perbankan Digital : Analisis Regulasi Ojk*.

Rahmahdhani, D. N., Irwan, M., Nasution, P., Suci, S., & Sundari, A. (2023). *Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking*. *2*(2).

Shidarta. (2014). *Hukum Perlindungan Konsumen Indonesia*. Grasindo.

Siregar, A. N., & Putra, M. A. P. (2025). Kajian Hukum : Penegakan Perlindungan Data Pribadi Nasabah Bank Dalam Skema Bancassurance Oleh: *Jurnal Media Akademik (Jma)*, *3*(7).

Siswanto, & Lenita, M. D. (2024). Prinsip Kehati-Hatian Nasabah Perbankan Dalam Menjaga Keamanan Bisnis Dari Social Engineering Fraud. *Justitiable - Jurnal Hukum*, *7*(1), 1–18.

Utami, G. W. (2024). *Perlindungan Terhadap Nasabah Akibat Serangan Ciber : Studi Di Bank Syariah Indonesia Kc Pekalongan Pemuda*. *4*(1).

Wiedyasari, A. B., & Yuspin, W. (2022). *Protection Of Customer Personal Data Of Bank Syariah Indonesia Reviewed From Pojk Number 6/Pojk.07/2022*. 1–17.