

Analisis Yuridis Perlindungan Hukum bagi Nasabah atas Kerugian Kehilangan Saldo pada Aplikasi BRIMO Berdasarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Alequesty Mariani Pandu^{1*}, Orpa Juliana Nubatonis², Rini Marselin Kaesmetan³

¹⁻³ Universitas Nusa Cendana, Indonesia

Email: arnipandu279@gmail.com^{1*}, orpajubatonis@gmail.com², rinikaemetan1985@gmail.com³

*Penulis Korespondensi: arnipandu279@gmail.com

Abstract. The rapid development of digital banking has improved the efficiency and accessibility of financial services while simultaneously increasing the risk of cybercrime, particularly phishing, unauthorized access, and the loss of customers' funds. This study aims to analyze the legal protection available to customers who suffer financial losses due to balance depletion in the BRIMO application and to examine the legal liability of banks under Law Number 10 of 1998 concerning Banking. This research employed normative legal research using statutory and conceptual approaches. The legal materials consisted of primary, secondary, and tertiary legal sources analyzed through qualitative descriptive methods. The findings indicate that legal protection for banking customers is provided through preventive measures, including the application of the prudential principle, information technology risk management, personal data protection, and customer education, as well as repressive measures through dispute resolution mechanisms. However, the existing legal framework has not specifically regulated the allocation of liability in digital banking transactions. Banks may be held liable when losses result from weaknesses in security systems or failures in implementing risk management. Therefore, more specific regulations are required to strengthen legal certainty and ensure balanced legal protection for both banks and customers in the digital banking sector.

Keywords: Banking Law; BRIMO; Customer Protection; Digital Banking; Legal Liability.

Abstrak. Perkembangan layanan perbankan digital telah meningkatkan kemudahan transaksi keuangan, tetapi juga memunculkan risiko kejahatan siber, seperti *phishing*, akses tidak sah, dan kehilangan saldo nasabah. Penelitian ini bertujuan untuk menganalisis perlindungan hukum bagi nasabah yang mengalami kerugian kehilangan saldo pada aplikasi BRIMO serta mengkaji tanggung jawab bank berdasarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah diberikan melalui upaya preventif berupa penerapan prinsip kehati-hatian, manajemen risiko teknologi informasi, perlindungan data pribadi, dan edukasi kepada nasabah, serta upaya represif melalui mekanisme penyelesaian sengketa. Meskipun demikian, pengaturan yang berlaku belum mengatur secara khusus pembagian tanggung jawab dalam layanan perbankan digital. Bank dapat dimintai pertanggungjawaban apabila kerugian timbul akibat kelemahan sistem keamanan atau kegagalan penerapan manajemen risiko. Oleh karena itu, diperlukan penguatan regulasi untuk memberikan kepastian hukum dan perlindungan yang lebih efektif bagi nasabah dalam penggunaan layanan perbankan digital.

Kata Kunci: BRIMO; Hukum Perbankan; Perbankan Digital; Perlindungan Nasabah; Tanggung Jawab Bank.

1. LATAR BELAKANG

Perkembangan teknologi informasi telah mendorong perubahan yang signifikan dalam penyelenggaraan layanan perbankan di Indonesia. Bank tidak lagi berfungsi hanya sebagai lembaga penghimpun dan penyalur dana masyarakat, tetapi juga sebagai penyedia layanan keuangan berbasis digital yang mengutamakan kecepatan, kemudahan, dan efisiensi transaksi. Transformasi tersebut melahirkan berbagai inovasi, seperti internet banking dan mobile banking, yang memungkinkan nasabah melakukan aktivitas perbankan tanpa dibatasi ruang

dan waktu. Menurut Djaja (2020), digitalisasi telah menjadi bagian penting dalam modernisasi sistem perbankan nasional sehingga bank dituntut mampu menyesuaikan layanan dengan perkembangan teknologi tanpa mengabaikan aspek keamanan dan kepastian hukum.

Hubungan hukum antara bank dan nasabah lahir dari adanya perjanjian penyimpanan dana yang menimbulkan hak dan kewajiban bagi kedua belah pihak. Dalam hubungan tersebut, bank berkewajiban menjaga dana serta memberikan perlindungan terhadap kepentingan nasabah sebagai konsumen jasa keuangan. Kewajiban tersebut ditegaskan dalam Pasal 37B ayat (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan yang mewajibkan setiap bank menjamin dana masyarakat yang disimpan pada bank bersangkutan. Dari perspektif hukum perikatan, tanggung jawab tersebut merupakan konsekuensi dari adanya hubungan kontraktual sehingga bank harus melaksanakan kewajibannya dengan itikad baik dan berdasarkan prinsip kehati-hatian (Amin, 2023).

Penguatan perlindungan hukum terhadap nasabah juga semakin penting seiring meningkatnya penggunaan layanan perbankan digital. Selain diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, perlindungan tersebut diperkuat melalui Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yang mewajibkan bank menerapkan manajemen risiko teknologi informasi dan menjaga ketahanan siber. Ketentuan tersebut menunjukkan bahwa keamanan sistem elektronik merupakan bagian yang tidak terpisahkan dari tanggung jawab bank dalam memberikan layanan kepada nasabah (Romli, 2024).

Salah satu bentuk digitalisasi layanan perbankan adalah aplikasi BRIMO yang dikembangkan oleh PT Bank Rakyat Indonesia (Persero) Tbk. Aplikasi ini menyediakan berbagai layanan transaksi keuangan secara terpadu, mulai dari transfer dana, pembayaran tagihan, pembelian produk digital hingga layanan investasi. Kehadiran BRIMO memberikan kemudahan bagi masyarakat dalam melakukan transaksi secara daring. Namun demikian, kemudahan tersebut juga diikuti dengan meningkatnya risiko kejahatan siber, seperti phishing, malware, pencurian identitas, maupun penyalahgunaan data pribadi yang dapat menyebabkan hilangnya dana nasabah. Menurut Nugraheni (2024), meningkatnya intensitas serangan siber pada layanan internet banking menunjukkan bahwa penguatan sistem keamanan digital masih menjadi tantangan utama bagi industri perbankan.

Fenomena tersebut tercermin dari meningkatnya jumlah pengaduan masyarakat terkait layanan perbankan digital. Data Indonesia Anti Scam Center di bawah koordinasi Otoritas Jasa

Keuangan menunjukkan bahwa selama periode 22 November 2024 hingga 14 Januari 2026 tercatat 432.637 laporan pengaduan dengan total kerugian mencapai sekitar Rp9,1 triliun yang melibatkan lebih dari 721 ribu rekening nasabah. Tingginya angka tersebut menunjukkan bahwa perlindungan hukum terhadap pengguna layanan digital masih menghadapi berbagai tantangan, terutama berkaitan dengan efektivitas penerapan manajemen risiko dan sistem keamanan teknologi informasi oleh bank.

Permasalahan serupa juga terjadi di Provinsi Nusa Tenggara Timur. Salah satu kasus yang mendapat perhatian publik adalah hilangnya saldo sebesar Rp14.000.000 milik nasabah BRI Cabang Kuanino di Kota Kupang setelah korban membuka tautan undangan pernikahan yang dikirim melalui aplikasi WhatsApp. Setelah tautan tersebut diakses, pelaku berhasil melakukan sejumlah transaksi tanpa persetujuan pemilik rekening sehingga korban kehilangan akses terhadap aplikasi BRIMO. Di samping itu, berbagai pemberitaan juga menunjukkan adanya transaksi gagal yang menyebabkan saldo rekening terdebit meskipun proses transaksi tidak berhasil. Kondisi tersebut memperlihatkan bahwa kerugian nasabah tidak selalu disebabkan oleh kelalaian pengguna, tetapi juga dapat berkaitan dengan aspek keamanan sistem dan pengelolaan risiko layanan digital (Abdullah, 2024).

Sejumlah penelitian terdahulu lebih banyak membahas perlindungan hukum terhadap korban phishing, tanggung jawab bank atas kehilangan dana, maupun keamanan layanan digital secara umum. Namun, kajian yang secara khusus menghubungkan tanggung jawab bank atas kehilangan saldo pada aplikasi BRIMO dengan ketentuan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan serta regulasi perlindungan konsumen dan teknologi informasi masih relatif terbatas. Padahal, perkembangan kejahatan siber menuntut adanya analisis hukum yang lebih komprehensif mengenai batas pertanggungjawaban bank dan bentuk perlindungan hukum yang dapat diperoleh nasabah. Oleh karena itu, penelitian ini bertujuan menganalisis perlindungan hukum bagi nasabah yang mengalami kerugian kehilangan saldo pada aplikasi BRIMO berdasarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan sehingga dapat memberikan kontribusi terhadap pengembangan hukum perbankan digital serta menjadi bahan evaluasi bagi peningkatan perlindungan konsumen di sektor jasa keuangan.

2. KAJIAN TEORITIS

Perlindungan hukum merupakan instrumen yang disediakan negara untuk menjamin terpenuhinya hak dan kepentingan setiap subjek hukum melalui perangkat peraturan perundang-undangan maupun mekanisme penyelesaian sengketa. Perlindungan hukum pada hakikatnya tidak hanya bertujuan memberikan kepastian hukum, tetapi juga menciptakan

keadilan dan kemanfaatan bagi masyarakat. Konsep ini dikenal dalam dua bentuk, yaitu perlindungan hukum preventif yang berorientasi pada pencegahan terjadinya pelanggaran hak melalui pengaturan dan pengawasan, serta perlindungan hukum represif yang diberikan setelah terjadi sengketa melalui mekanisme penyelesaian hukum. Dalam konteks negara hukum, kedua bentuk perlindungan tersebut merupakan dasar bagi penyelenggaraan sistem hukum yang menjamin kepastian dan perlindungan terhadap hak warga negara (Romli, 2024).

Dalam sektor perbankan, perlindungan hukum diwujudkan melalui hubungan hukum antara bank dan nasabah yang lahir dari suatu perjanjian. Berdasarkan ketentuan Pasal 1313 Kitab Undang-Undang Hukum Perdata, perjanjian merupakan perbuatan hukum yang menimbulkan hak dan kewajiban bagi para pihak. Hubungan tersebut menempatkan bank sebagai pihak yang berkewajiban memberikan pelayanan yang aman, menjaga dana simpanan, serta memenuhi prestasi sebagaimana diperjanjikan dengan nasabah. Oleh karena itu, hubungan hukum antara bank dan nasabah tidak hanya bersifat kontraktual, tetapi juga mengandung tanggung jawab hukum yang lahir dari ketentuan peraturan perundang-undangan apabila terjadi kerugian akibat kelalaian atau kegagalan sistem perbankan (Amalia, 2019; Amin, 2023).

Kedudukan nasabah sebagai konsumen jasa keuangan memperoleh perlindungan melalui Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Kedua regulasi tersebut mewajibkan bank menjalankan kegiatan usahanya berdasarkan prinsip kepercayaan, prinsip kehati-hatian, prinsip kerahasiaan, serta prinsip mengenal nasabah (know your customer). Penerapan prinsip-prinsip tersebut menjadi landasan penting dalam menjaga stabilitas sistem perbankan sekaligus memberikan jaminan atas keamanan dana dan data pribadi nasabah. Prinsip kehati-hatian memiliki peran yang sangat penting karena mengharuskan bank mengidentifikasi, mengendalikan, dan meminimalkan setiap risiko yang dapat merugikan nasabah maupun lembaga perbankan (Gozali & Usman, 2024).

Perkembangan teknologi informasi telah mendorong transformasi layanan perbankan menuju sistem digital melalui internet banking dan mobile banking. Salah satu bentuk implementasinya adalah aplikasi BRIMO yang dikembangkan oleh PT Bank Rakyat Indonesia (Persero) Tbk. sebagai layanan digital terpadu yang memudahkan berbagai transaksi keuangan. Kehadiran layanan digital meningkatkan efisiensi pelayanan, namun juga memperbesar potensi terjadinya kejahatan siber, seperti phishing, pencurian identitas, malware, dan penyalahgunaan data pribadi. Oleh karena itu, penyelenggaraan layanan digital harus disertai sistem keamanan

yang memadai agar mampu menjaga kerahasiaan, integritas, dan ketersediaan informasi nasabah (Savitri, 2024).

Sejalan dengan perkembangan tersebut, penerapan manajemen risiko menjadi kewajiban yang tidak dapat dipisahkan dari penyelenggaraan layanan perbankan digital. Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 mewajibkan setiap bank menerapkan manajemen risiko teknologi informasi dan memperkuat ketahanan siber sebagai bagian dari tata kelola perbankan. Risiko keamanan siber dapat berasal dari kelemahan sumber daya manusia, proses bisnis, sistem teknologi informasi, maupun ancaman eksternal yang memanfaatkan perkembangan teknologi. Risiko tersebut tidak hanya berpotensi menimbulkan kerugian finansial bagi nasabah, tetapi juga dapat mengurangi kepercayaan masyarakat terhadap industri perbankan. Oleh karena itu, tanggung jawab bank tidak berhenti pada penyediaan layanan digital, melainkan juga mencakup kewajiban memberikan perlindungan hukum, menjamin keamanan sistem, serta menyediakan mekanisme penyelesaian kerugian apabila nasabah mengalami kehilangan dana akibat kelemahan sistem maupun serangan siber (Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum, 2021; Pesak, 2025).

3. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang berorientasi pada pengkajian norma, asas, doktrin, serta ketentuan hukum positif yang mengatur perlindungan hukum terhadap nasabah pengguna layanan perbankan digital. Penelitian hukum normatif menempatkan hukum sebagai suatu sistem norma yang dianalisis melalui studi kepustakaan (*library research*) dengan menelaah berbagai bahan hukum yang relevan untuk menjawab isu hukum yang diteliti (Muhaimin, 2020). Pendekatan ini dipilih karena penelitian berfokus pada analisis pengaturan hukum mengenai perlindungan nasabah atas kerugian kehilangan saldo pada aplikasi BRIMO berdasarkan ketentuan peraturan perundang-undangan yang berlaku. Pandangan tersebut sejalan dengan konsep penelitian hukum normatif yang menitikberatkan pada analisis terhadap norma hukum sebagai dasar penyelesaian suatu permasalahan hukum (Kristiawanto, 2022).

Penelitian menggunakan dua pendekatan, yaitu pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan melalui penelaahan terhadap berbagai regulasi yang berkaitan dengan perlindungan nasabah dan penyelenggaraan layanan perbankan digital, sedangkan pendekatan konseptual digunakan untuk mengkaji doktrin, teori, serta pandangan para ahli yang relevan sebagai landasan analisis terhadap isu hukum yang diteliti (Ahmad, 2024).

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Kitab Undang-Undang Hukum Perdata, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, serta POJK Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Bahan hukum sekunder diperoleh dari buku, artikel ilmiah, jurnal, skripsi, dan doktrin yang membahas hukum perbankan, perlindungan konsumen, pertanggungjawaban hukum, serta keamanan siber. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber informasi daring yang mendukung penafsiran terhadap bahan hukum primer dan sekunder (Suryanto, 2022).

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan menelusuri, mengidentifikasi, dan menginventarisasi berbagai literatur, peraturan perundang-undangan, serta dokumen hukum yang berkaitan dengan objek penelitian. Selanjutnya, seluruh bahan hukum diseleksi berdasarkan relevansi, diklasifikasikan menurut jenis dan hierarki sumber hukum, kemudian disusun secara sistematis untuk memudahkan proses analisis terhadap permasalahan yang diteliti (Tahir, 2023). Analisis bahan hukum dilakukan secara deskriptif-kualitatif dengan mengkaji keterkaitan antara ketentuan peraturan perundang-undangan, teori hukum, dan doktrin yang relevan. Seluruh bahan hukum dianalisis melalui proses interpretasi dan penalaran hukum untuk memperoleh argumentasi yuridis mengenai bentuk perlindungan hukum bagi nasabah serta ruang lingkup pertanggungjawaban bank atas kerugian kehilangan saldo pada aplikasi BRIMO. Hasil analisis kemudian disajikan secara sistematis untuk menghasilkan kesimpulan yang mampu menjawab rumusan masalah penelitian secara komprehensif (Kristiawanto, 2022).

4. HASIL DAN PEMBAHASAN

Perlindungan Hukum bagi Nasabah atas Kehilangan Saldo pada Aplikasi BRIMO

Perlindungan hukum terhadap nasabah pada dasarnya ditujukan untuk menjamin keamanan hak, dana, dan kepentingan nasabah dalam hubungan hukum dengan bank. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan tetap relevan dijadikan landasan perlindungan terhadap pengguna BRIMO meskipun dibentuk sebelum berkembangnya layanan mobile banking. Hal ini karena norma dalam undang-undang tersebut mencakup seluruh kegiatan penghimpunan dan pengelolaan dana masyarakat, termasuk simpanan yang diakses

melalui sarana elektronik. Dengan demikian, saldo yang ditampilkan pada aplikasi BRIMO bukanlah objek yang berdiri sendiri, melainkan representasi digital dari simpanan nasabah yang berada dalam penguasaan dan pengelolaan bank.

Pasal 1 angka 16 Undang-Undang Perbankan mendefinisikan nasabah sebagai pihak yang menggunakan jasa bank, sedangkan nasabah penyimpan merupakan pihak yang menempatkan dananya berdasarkan perjanjian dengan bank. Hubungan tersebut melahirkan kewajiban bank untuk tidak hanya menyediakan akses transaksi, tetapi juga menjaga keamanan dan integritas dana nasabah. Hubungan antara bank dan nasabah memiliki karakter kontraktual sekaligus hubungan kepercayaan karena masyarakat menyerahkan pengelolaan dananya kepada lembaga perbankan (Gozali & Usman, 2024). Oleh sebab itu, kewajiban bank tidak terbatas pada isi formulir pembukaan rekening atau syarat penggunaan aplikasi, tetapi juga mencakup kewajiban yang bersumber dari undang-undang.

Pasal 37B ayat (1) Undang-Undang Perbankan menegaskan bahwa setiap bank wajib menjamin dana masyarakat yang disimpan pada bank. Ketentuan tersebut menunjukkan bahwa perlindungan terhadap simpanan merupakan kewajiban hukum yang melekat pada fungsi bank sebagai lembaga kepercayaan. Namun, frasa “wajib menjamin” tidak serta-merta dapat ditafsirkan bahwa bank harus mengganti seluruh kerugian tanpa pemeriksaan penyebab. Jaminan tersebut harus dibaca bersama ketentuan mengenai prinsip kehati-hatian, manajemen risiko, keamanan sistem, serta kontribusi kesalahan masing-masing pihak. Bank dapat dimintai pertanggungjawaban apabila kerugian timbul akibat kelemahan sistem, kegagalan pengawasan, atau tidak terpenuhinya kewajiban perlindungan yang dibebankan oleh hukum.

Kasus yang dianalisis dalam penelitian ini berkaitan dengan nasabah DK yang mengalami kehilangan saldo sebesar Rp14.000.000 setelah membuka file undangan pernikahan yang diterima melalui WhatsApp. Setelah file tersebut diakses, terjadi sejumlah transaksi yang tidak pernah diperintahkan oleh nasabah dan akses terhadap aplikasi BRIMO tidak lagi dapat digunakan. Peristiwa ini memperlihatkan karakter serangan phishing yang memanfaatkan manipulasi psikologis dan perangkat lunak berbahaya untuk memperoleh kredensial korban. Meskipun tindakan awal berasal dari pembukaan file oleh nasabah, keberhasilan pelaku melakukan transaksi dalam waktu singkat tetap menimbulkan pertanyaan mengenai efektivitas sistem deteksi transaksi tidak wajar, verifikasi berlapis, dan respons pengamanan bank.

Perlindungan hukum dalam kasus tersebut dapat dibedakan menjadi perlindungan preventif dan represif. Perlindungan preventif pertama diwujudkan melalui penerapan prinsip kehati-hatian. Pasal 2 dan Pasal 29 ayat (2) Undang-Undang Perbankan mewajibkan bank

menyelenggarakan kegiatan usaha secara hati-hati dan mempertahankan tingkat kesehatan bank. Dalam perbankan digital, prinsip tersebut harus dimaknai lebih luas, yaitu mencakup keamanan aplikasi, autentikasi pengguna, deteksi pola transaksi abnormal, pembatasan akses, serta mekanisme penghentian transaksi yang terindikasi tidak sah. Prinsip kehati-hatian merupakan tolok ukur untuk menilai apakah bank telah melakukan tindakan pencegahan yang wajar terhadap risiko yang dapat diperkirakan (Putera, 2019).

Perlindungan preventif berikutnya berkaitan dengan kerahasiaan dan perlindungan data pribadi. Pasal 40 Undang-Undang Perbankan mewajibkan bank merahasiakan informasi nasabah penyimpan dan simpanannya. Kewajiban tersebut diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan POJK Nomor 22 Tahun 2023 yang melarang pelaku usaha jasa keuangan menyampaikan data konsumen kepada pihak lain tanpa dasar yang sah. Dalam kasus phishing, perlu dibedakan antara kebocoran data yang berasal dari sistem bank dan data yang diperoleh pelaku melalui manipulasi terhadap perangkat nasabah. Perbedaan ini penting karena menentukan dasar pertanggungjawaban. Bank harus bertanggung jawab apabila ditemukan kebocoran atau kelemahan pengamanan dari sistemnya, sedangkan nasabah dapat menanggung akibat apabila seluruh akses diperoleh akibat kelalaian pribadi tanpa adanya kegagalan sistem bank.

Aspek ketiga adalah manajemen risiko teknologi informasi. Pasal 15 ayat (1) POJK Nomor 11/POJK.03/2022 mewajibkan bank menerapkan manajemen risiko secara efektif dalam penyelenggaraan teknologi informasi, sedangkan Pasal 21 mengharuskan bank menjaga ketahanan siber. Kewajiban tersebut meliputi identifikasi, pengukuran, pemantauan, dan pengendalian risiko secara berkelanjutan. Sistem bank seharusnya mampu mengenali perpindahan perangkat, perubahan pola transaksi, transaksi berulang dalam waktu singkat, atau pengiriman dana kepada rekening yang belum pernah berinteraksi dengan nasabah. Ketidakmampuan sistem merespons pola tersebut dapat menunjukkan belum optimalnya pengelolaan risiko keamanan digital (Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum, 2021).

Perlindungan preventif juga diwujudkan melalui transparansi dan edukasi. Pasal 29 ayat (4) Undang-Undang Perbankan mewajibkan bank menyediakan informasi mengenai kemungkinan timbulnya risiko kerugian dalam transaksi. Kewajiban ini menempatkan bank sebagai pihak yang harus aktif meningkatkan literasi keamanan digital nasabah, termasuk menjelaskan modus phishing, larangan membagikan PIN atau OTP, bahaya memasang aplikasi dari sumber tidak resmi, dan prosedur yang harus ditempuh ketika terjadi transaksi mencurigakan. Edukasi tidak cukup dilakukan melalui pemberitahuan umum, tetapi perlu

disampaikan secara berkala, mudah dipahami, dan menjangkau kelompok nasabah yang memiliki literasi digital terbatas (Sihotang & Agustiawan, 2023).

Sementara itu, perlindungan represif diberikan setelah kerugian terjadi. Tahap pertama dilakukan melalui mekanisme pengaduan internal bank atau internal dispute resolution. Bank harus menerima laporan, memblokir akses yang bermasalah, menelusuri aliran dana, memeriksa log autentikasi, dan menyampaikan hasil investigasi secara transparan. Jika penyelesaian internal tidak memberikan hasil yang dapat diterima, nasabah dapat menempuh penyelesaian melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan atau Badan Penyelesaian Sengketa Konsumen. Jalur pengadilan dapat digunakan sebagai upaya terakhir melalui gugatan wanprestasi atau perbuatan melawan hukum.

Secara teknis, BRIMO telah dilengkapi dengan pengamanan berlapis berupa user ID, kata sandi, PIN transaksi, autentikasi biometrik, enkripsi, *safety mode*, dan pemantauan sistem. Fitur tersebut menunjukkan adanya upaya bank untuk memenuhi kewajiban keamanan. Namun, keberadaan teknologi keamanan tidak dengan sendirinya membuktikan bahwa kewajiban bank telah terlaksana secara efektif. Ukuran perlindungan bukan hanya kecanggihan sistem, melainkan kemampuannya mencegah, mendeteksi, dan merespons transaksi tidak sah. Oleh karena itu, kasus DK menunjukkan adanya kesenjangan antara desain keamanan dan perlindungan yang dirasakan nasabah. Kesenjangan tersebut harus diuji melalui audit transaksi dan pemeriksaan teknis, bukan semata-mata melalui pernyataan bahwa sistem bank dalam keadaan normal.

Pertanggungjawaban Bank atas Kerugian Nasabah pada Layanan BRIMO

Pertanggungjawaban hukum timbul ketika subjek hukum tidak memenuhi kewajiban atau melakukan perbuatan yang menimbulkan kerugian bagi pihak lain. Dalam hubungan perbankan digital, tanggung jawab bank mencakup keamanan teknis, penyelesaian transaksi tidak sah, keterbukaan informasi, penanganan pengaduan, serta pemulihan kerugian apabila terbukti terdapat kesalahan atau kelemahan sistem. Pertanggungjawaban tersebut merupakan konsekuensi dari posisi bank sebagai pengelola dana, penyelenggara aplikasi, dan pihak yang menguasai infrastruktur transaksi digital (Purwantono, 2024).

Tanggung jawab teknis mengharuskan bank menyediakan sistem yang andal, melakukan pembaruan keamanan, menerapkan autentikasi berlapis, menjaga ketersediaan data, serta melakukan pengujian keamanan secara berkala. Dalam hal terjadi transaksi yang tidak diakui nasabah, bank berkewajiban menelusuri riwayat transaksi, perangkat yang digunakan, alamat jaringan, metode autentikasi, perubahan kredensial, dan rekening tujuan. Hasil investigasi perlu

disampaikan secara jelas kepada nasabah agar penyelesaian tidak hanya didasarkan pada kesimpulan sepihak bahwa transaksi telah menggunakan data autentikasi yang benar.

Tanggung jawab bank juga mencakup penyediaan informasi dan penanganan pengaduan. Informasi mengenai risiko, biaya, limit transaksi, tata cara penggunaan, serta mekanisme pengamanan harus disampaikan secara benar dan tidak menyesatkan. Ketika terjadi kehilangan saldo, bank wajib menyediakan saluran pengaduan yang mudah diakses, merespons secara cepat, dan menyediakan mekanisme eskalasi. Penolakan penggantian dana tanpa memberikan hasil pemeriksaan yang dapat diverifikasi berpotensi memperlemah hak nasabah untuk memperoleh informasi dan penyelesaian yang adil.

Dari perspektif hukum perdata, tanggung jawab bank dapat didasarkan pada wanprestasi apabila bank tidak memenuhi kewajiban yang timbul dari perjanjian maupun undang-undang. Pasal 1233 KUH Perdata menegaskan bahwa perikatan lahir karena persetujuan atau undang-undang. Dengan demikian, kewajiban menjaga dana nasabah tidak hanya bersumber dari syarat penggunaan BRIMO, tetapi juga dari Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, dan regulasi OJK. Jika bank gagal memenuhi kewajiban tersebut sehingga menimbulkan kerugian, nasabah dapat mengajukan tuntutan berdasarkan Pasal 1243 KUH Perdata (Purba, 2025).

Pertanggungjawaban bank dapat dianalisis menggunakan teori tanggung jawab berdasarkan kesalahan. Berdasarkan teori ini, bank dapat dimintai pertanggungjawaban apabila terbukti melakukan kesalahan atau kelalaian, seperti tidak memiliki sistem deteksi transaksi abnormal, terlambat memblokir rekening, atau gagal melindungi data nasabah. Kendala penerapan teori ini terletak pada ketimpangan penguasaan bukti. Data teknis, log transaksi, rekaman autentikasi, dan sistem pemantauan seluruhnya dikuasai bank, sementara nasabah hanya mengetahui bahwa saldonya berkurang. Keadaan tersebut menyebabkan pembuktian kesalahan bank sulit dilakukan oleh nasabah dan memperlihatkan ketidakseimbangan posisi para pihak.

Penelitian ini juga menemukan bahwa prinsip *strict liability* relevan untuk dipertimbangkan dalam layanan perbankan digital, tetapi tidak dapat diterapkan secara otomatis pada setiap kasus. Bank menguasai sistem, jaringan, pusat data, mekanisme autentikasi, dan pemantauan transaksi sehingga memiliki kemampuan paling besar untuk mengendalikan risiko. Selain itu, bank memperoleh manfaat ekonomi dari digitalisasi berupa efisiensi operasional dan perluasan layanan. Berdasarkan pertimbangan tersebut, beban risiko selayaknya lebih besar ditempatkan pada bank apabila kerugian terjadi dalam lingkup sistem yang berada di bawah kendalinya (Pesak, 2025).

Namun, penerapan *strict liability* tetap harus mempertimbangkan kontribusi nasabah. Bank tidak semestinya dibebani tanggung jawab penuh apabila dapat membuktikan bahwa sistem telah berfungsi sesuai standar, transaksi telah melalui autentikasi yang sah, dan kerugian sepenuhnya terjadi karena nasabah menyerahkan kredensial atau mengabaikan peringatan keamanan. Sebaliknya, bank patut bertanggung jawab apabila terdapat transaksi tidak wajar yang gagal dideteksi, kelemahan autentikasi, keterlambatan pemblokiran, atau kegagalan sistem pengamanan. Karena itu, bentuk tanggung jawab yang lebih adil adalah tanggung jawab berbasis pembagian risiko dengan beban pembuktian yang lebih besar ditempatkan pada bank sebagai penguasa sistem.

Dalam kasus DK, fakta bahwa serangkaian transaksi dapat dilakukan setelah korban membuka file berbahaya belum cukup untuk langsung menentukan pihak yang bertanggung jawab. Diperlukan pemeriksaan terhadap waktu transaksi, perubahan perangkat, penggunaan OTP, lokasi akses, nilai transaksi, pola rekening tujuan, serta respons sistem terhadap aktivitas tersebut. Apabila bank mampu membuktikan bahwa seluruh prosedur keamanan berjalan, tanggung jawabnya dapat dibatasi. Sebaliknya, jika ditemukan bahwa transaksi terjadi tanpa autentikasi memadai atau sistem mengabaikan anomali yang seharusnya dapat dikenali, bank dapat dinilai lalai dan wajib memberikan ganti rugi.

Hasil analisis menunjukkan bahwa Undang-Undang Nomor 10 Tahun 1998 telah memberikan dasar umum berupa kewajiban menjamin dana, menerapkan prinsip kehati-hatian, menjaga kerahasiaan, serta memberikan informasi risiko. Akan tetapi, undang-undang tersebut belum mengatur secara rinci pembagian tanggung jawab dalam kasus phishing dan transaksi mobile banking yang tidak sah. Kekosongan ini menyebabkan penyelesaian kasus sangat bergantung pada investigasi internal bank dan kemampuan nasabah membuktikan kelemahan sistem. Kondisi tersebut berpotensi menempatkan nasabah pada posisi yang kurang seimbang.

Oleh karena itu, diperlukan pengaturan yang lebih tegas mengenai standar minimum deteksi transaksi abnormal, batas waktu pemblokiran, akses nasabah terhadap hasil investigasi, mekanisme pengembalian dana sementara, dan pembagian beban pembuktian. Penerapan tanggung jawab yang lebih ketat terhadap bank dapat menjadi instrumen untuk mendorong peningkatan keamanan, tetapi harus tetap membuka kemungkinan pembebasan atau pengurangan tanggung jawab apabila bank mampu membuktikan adanya kesalahan dominan dari nasabah. Model tersebut lebih proporsional dibandingkan penerapan tanggung jawab absolut karena menjaga perlindungan nasabah tanpa mengabaikan prinsip keadilan bagi penyelenggara layanan.

5. KESIMPULAN DAN SARAN

Kesimpulan

Perlindungan hukum terhadap nasabah yang mengalami kehilangan saldo pada aplikasi BRIMO telah diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan melalui penerapan prinsip kehati-hatian, pengelolaan risiko, perlindungan data nasabah, serta mekanisme penyelesaian sengketa. Namun, pengaturan tersebut masih bersifat umum dan belum mengatur secara khusus mengenai tanggung jawab bank dalam layanan perbankan digital. Hasil penelitian menunjukkan bahwa bank dapat dimintai pertanggungjawaban apabila terbukti terdapat kelalaian dalam menjaga keamanan sistem atau menerapkan manajemen risiko. Oleh karena itu, diperlukan penguatan regulasi agar pembagian tanggung jawab antara bank dan nasabah menjadi lebih jelas sehingga mampu memberikan kepastian hukum dan perlindungan yang lebih efektif bagi nasabah.

Saran

Bank perlu terus meningkatkan keamanan sistem BRIMO, memperkuat edukasi kepada nasabah mengenai risiko kejahatan siber, serta menyediakan mekanisme pengaduan yang cepat dan transparan. Di sisi lain, nasabah perlu lebih berhati-hati dalam menjaga kerahasiaan data pribadi dan menghindari berbagai bentuk penipuan digital, seperti phishing. Selain itu, pemerintah dan Otoritas Jasa Keuangan diharapkan menyempurnakan regulasi mengenai perlindungan nasabah pada layanan perbankan digital agar memberikan kepastian hukum yang lebih jelas terhadap penyelesaian kerugian akibat kehilangan saldo.

DAFTAR REFERENSI

- Abdullah, N. P. (2024). Analisis yuridis perlindungan nasabah bank dalam tindak pidana pencurian data melalui UU ITE dan UU Perbankan. *Media Hukum Indonesia (MHI)*, 2(4).
- Ahmad. (2024). *Buku ajar metode penelitian & penulisan hukum*. Sonpedia Publishing Indonesia.
- Amalia, E. (2019). *Hukum perikatan*. Universitas Tama Jagakarsa.
- Amin, S. N. (2023). *Buku ajar hukum perjanjian*. Deepublish Digital.
- Departemen Penelitian dan Pengaturan Perbankan, Otoritas Jasa Keuangan. (2021). *Consultative paper manajemen risiko keamanan siber bank umum*. Otoritas Jasa Keuangan.
- Djaja, B. (2020). *Hukum perbankan*. CV Andi Offset.
- Gozali, D. S., & Usman, R. (2024). *Hukum perbankan*. Sinar Grafika.
- Kitab Undang-Undang Hukum Perdata*.
- Kristiawanto. (2022). *Memahami penelitian hukum normatif*. Prenada Media.

- Muhaimin, S. (2020). *Metode penelitian hukum*. UPT Mataram University Press.
- Nugraheni, T. (2024). Analisis yuridis penerapan perlindungan hukum dalam melindungi pengguna layanan internet banking dari cyber crime. *Jurnal Hukum, Politik dan Ilmu Sosial*, 3(2). <https://doi.org/10.55606/jhps.v3i2.3715>
- Otoritas Jasa Keuangan. (2022). *Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum*.
- Otoritas Jasa Keuangan. (2023). *Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang perlindungan konsumen dan masyarakat di sektor jasa keuangan*.
- Pesak, V. Y. (2025). Tanggung jawab hukum bank umum atas risiko layanan digital berdasarkan Peraturan Otoritas Jasa Keuangan. *Lex Crimen*, 14(3).
- Purba, H. (2025). *Hukum perikatan dan perjanjian*. Sinar Grafika.
- Purwantono, R. A. (2024). *Pertanggungjawaban hukum: Regulasi dan keadilan*. PT RajaGrafindo Persada.
- Putera, A. P. (2019). *Hukum perbankan: Analisis mengenai prinsip, produk, risiko dan manajemen risiko dalam perbankan*. Scopindo Media Pustaka.
- Romli. (2024). *Perlindungan hukum*. CV Doki Course and Training.
- Savitri, P. (2024). *Transformasi digital dalam industri perbankan: Implikasi terhadap akuntansi dan teknologi informasi*. PT Nasya Expanding Management.
- Sihotang, L., & Agustiawan. (2023). Upaya meningkatkan pemahaman dan keamanan dalam penggunaan aplikasi BRIMO kepada nasabah di PT Bank Rakyat Indonesia (BRI) Kantor KCP Ahmad Yani. *Jurnal Sosial dan Pengabdian Masyarakat*, 1(1). <https://doi.org/10.59966/semar.v1i01.15>
- Suryanto. (2022). *Metode penelitian hukum: Pengantar penelitian normatif, empiris dan gabungan*. Unigres Press.
- Tahir, R. (2023). *Metode penelitian bidang hukum*. Sonpedia Publishing Indonesia.
- Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.