Reslaj: Religion Education Social Laa Roiba Journal

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Perlindungan Hukum Terhadap Nasabah Atas Kejahatan *Phising* pada *Mobile Banking* Perspektif Maqashid Syariah: Studi Kasus di BSI KCP Gatot Subroto

Siti Rahayu[1], Fatimah Zahara[2]
Universitas Islam Negeri Sumatera Utara, Indonesia
siti0204223050@uinsu.ac.id [1], fatimahzahara@uinsu.ac.id [2]

ABSTRACT

The development of mobile banking services offers convenience to customers but also increases the risk of cybercrimes, such as phishing, which can lead to financial losses. This study aims to analyze the legal protections and bank liability regarding losses suffered by customers who fell victim to phishing while using the BSI KCP Gatot Subroto mobile banking service, as well as to examine the issue from the perspective of maqashid sharia (the objectives of Sharia). The research employs an empirical-juridical method utilizing qualitative, conceptual, and statutory approaches. Data were gathered through literature reviews and interviews with BSI KCP Gatot Subroto customer service staff and customers who had been victims of phishing. The findings indicate that protection is provided through preventive measures—such as education and system security enhancements—and repressive measures, including complaint handling, investigations, and the blocking of account access. However, the recurrence of phishing incidents in 2023, 2024, and 2025 suggests that these protective measures have not been fully effective. In the cases studied, the bank attributed the losses to customer negligence without conducting a transparent assessment of the bank's own security system effectiveness. From the perspective of maqashid sharia, such protection relates to the principle of hifz al-mal (preservation of wealth), although its implementation has not yet been fully optimal.

Keywords : Legal Protection, Phishing, Mobile Banking, Maqashid Sharia.

ABSTRAK

Perkembangan layanan *mobile banking* memberikan kemudahan bagi nasabah, tetapi juga meningkatkan risiko kejahatan siber, seperti *phishing* yang dapat menimbulkan kerugian finansial. Penelitian ini bertujuan menganalisis perlindungan hukum, tanggung jawab bank terhadap kerugian nasabah korban *phishing* pada layanan *mobile banking* BSI KCP Gatot Subroto, serta tinjauannya berdasarkan perspektif *maqashid syariah*. Penelitian ini menggunakan metode yuridis empiris dengan pendekatan kualitatif, konseptual, dan perundang-undangan. Data diperoleh melalui studi kepustakaan serta wawancara dengan *Customer Service* BSI KCP Gatot Subroto dan nasabah korban *phishing*. Hasil penelitian menunjukkan bahwa perlindungan diberikan melalui upaya preventif berupa edukasi dan peningkatan keamanan sistem, serta upaya represif melalui penanganan pengaduan, investigasi, dan pemblokiran akses rekening. Namun, terulangnya kasus *phishing* pada tahun 2023, 2024, dan 2025 menunjukkan bahwa perlindungan tersebut belum sepenuhnya efektif. Dalam kasus yang diteliti, bank membebankan kerugian kepada nasabah atas dasar kelalaian pribadi tanpa penilaian terbuka terhadap efektivitas sistem keamanan bank. Dalam perspektif *maqashid syariah*, perlindungan tersebut berkaitan dengan prinsip *hifz al-mal* atau perlindungan harta, meskipun penerapannya belum sepenuhnya optimal.

Reslaj: Religion Education Social Laa Roiba Journal

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Kata kunci : Perlindungan Hukum, *Phishing, Mobile Banking, Maqashid Syari'ah.*

PENDAHULUAN

Mobile banking atau *m-banking* merupakan layanan perbankan berbasis aplikasi pada perangkat seluler yang memungkinkan nasabah melakukan berbagai transaksi keuangan tanpa harus datang ke kantor bank. Layanan ini memberikan kemudahan, menghemat waktu, dan menekan biaya transaksi (Siti Masrohatin et al., 2025). Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong penggunaan perangkat mobile dalam berbagai aktivitas, termasuk transaksi keuangan. Namun, kemudahan tersebut juga meningkatkan risiko terjadinya *cybercrime* atau kejahatan siber.

Salah satu bentuk *cybercrime* yang sering terjadi dalam layanan perbankan digital adalah phishing, yaitu tindakan penipuan melalui pesan, email, atau situs palsu yang mengatasnamakan lembaga resmi untuk memperoleh data pribadi atau mengakses akun korban secara tidak sah. Data yang menjadi sasaran dapat berupa User ID, PIN, nomor rekening, nomor kartu kredit, maupun informasi keamanan lainnya (Tuti Warsiti & Markoni, 2022). Modus *phishing* dapat dilakukan melalui berbagai media, salah satunya pesan *WhatsApp* yang berisi tautan palsu dan dibuat seolah-olah berasal dari pihak bank.

Seperti kasus yang dialami nasabah ditahun 2025, seorang nasabah BSI KCP Gatot Subroto bernama Budi mengalami kerugian sebesar Rp30.000.000 akibat dugaan *phishing*. Peristiwa tersebut bermula ketika Budi mengklik tautan yang dikirim melalui pesan *WhatsApp* dan mengatasnamakan pihak bank. Budi memasukkan PIN maupun *username* melalui *link* tersebut. Setelah mengklik tautan tersebut, terjadi transaksi yang tidak dikenali oleh Budi sehingga menyebabkan saldo rekeningnya berkurang sebesar Rp30.000.000. Kasus ini menunjukkan bahwa risiko *phishing* tidak hanya berkaitan dengan kelalaian nasabah dalam menjaga data pribadi, tetapi juga berkaitan dengan keamanan layanan digital dan kemampuan sistem bank dalam mencegah serta mendeteksi akses atau transaksi yang tidak sah.

Setelah ditelusuri lebih lanjut kasus yang dialami Budi bukanlah satu-satunya kasus *phishing* yang terjadi pada nasabah BSI KCP Gatot Subroto. Berdasarkan data penelitian, pada tahun 2023 telah terjadi kasus *phishing* yang mengakibatkan kerugian nasabah sekitar Rp20.000.000. Kemudian pada tahun 2024 kembali terjadi kasus serupa dengan kerugian yang lebih besar, yaitu sekitar Rp60.000.000. Pada tahun 2025, Budi juga mengalami kerugian setelah mengakses tautan *phishing* yang mengatasnamakan layanan bank. Dalam ketiga kasus tersebut, bank telah menerima pengaduan dan melakukan penanganan sesuai prosedur yang berlaku, namun kerugian tetap tidak dapat dipulihkan sepenuhnya oleh nasabah. Hal ini menunjukkan bahwa perlindungan hukum yang seharusnya diberikan bank kepada nasabah, baik berdasarkan ketentuan peraturan perundang-undangan maupun prinsip *maqashid syariah*, khususnya *hifz al-mal* (perlindungan harta),

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

belum terpenuhi secara optimal, terutama dalam aspek pencegahan dan perlindungan yang efektif.

Berulangnya kasus *phishing* juga menunjukkan adanya kelemahan dalam penerapan manajemen risiko dan keamanan layanan digital. POJK Nomor 11/POJK.03/2022 dan POJK Nomor 21 Tahun 2023 mewajibkan bank untuk menerapkan tata kelola teknologi informasi, sistem keamanan, serta mitigasi risiko yang efektif. Namun, fakta terjadinya kasus berulang menunjukkan bahwa sistem peringatan dini, deteksi transaksi mencurigakan, dan perlindungan terhadap akses ilegal belum berjalan optimal. Hal ini memperkuat indikasi bahwa perlindungan hukum dari sisi regulasi belum sepenuhnya diimplementasikan dalam praktik operasional bank (Otoritas Jasa Keuangan, 2023).

Permasalahan lain muncul dalam penentuan tanggung jawab atas kerugian nasabah. Dalam kasus Budi, kerugian dibebankan sepenuhnya kepada nasabah dengan alasan kelalaian pribadi. Namun, penilaian ini belum sepenuhnya transparan karena tidak dijelaskan secara terbuka apakah sistem keamanan bank telah bekerja secara maksimal atau terdapat celah yang turut berkontribusi terhadap terjadinya kerugian. Akibatnya, terdapat ketidakseimbangan dalam perlindungan hukum karena nasabah ditempatkan sebagai pihak yang paling bertanggung jawab, sementara kewajiban bank dalam menyediakan sistem yang aman belum sepenuhnya dievaluasi secara objektif.

Maqashid syariah merupakan salah satu konsep penting dalam hukum Islam yang mengarah pada tujuan ditetapkannya syariat, yaitu untuk mewujudkan kemaslahatan dan mencegah kemudaratan. Menurut Al-Syatibi, tujuan utama syariat adalah menjaga lima unsur pokok kehidupan, yaitu agama (*hifz al-din*), jiwa (*hifz al-nafs*), akal (*hifz al-'aql*), keturunan (*hifz al-nasl*), dan harta (*hifz al-mal*). Dalam konsep tersebut, hukum tidak hanya dinilai berdasarkan terpenuhinya ketentuan secara formal, tetapi juga berdasarkan kemampuannya dalam mewujudkan kemaslahatan dan mencegah terjadinya kerugian atau kemudaratan. (Alwi, 2022).

Permasalahan *phishing* dapat dikaji melalui perspektif *maqashid syariah*, khususnya prinsip *hifz al-mal* atau perlindungan terhadap harta. Prinsip ini menekankan pentingnya menjaga harta dari kehilangan, penyalahgunaan, dan kerugian yang tidak adil. Dalam konteks layanan *mobile banking*, penerapan *hifz al-mal* menuntut adanya perlindungan yang tidak hanya dilakukan setelah terjadinya kerugian, tetapi juga melalui edukasi yang efektif, sistem keamanan yang andal, pengelolaan risiko yang memadai, serta penanganan yang adil terhadap nasabah korban *phishing*. Dengan demikian, pembebanan kerugian kepada nasabah perlu dikaji secara objektif dengan mempertimbangkan tidak hanya tindakan nasabah, tetapi juga efektivitas perlindungan dan sistem keamanan yang diterapkan oleh pihak bank.

Menurut uraian tersebut dapat disimpulkan bahwa perlindungan hukum yang diberikan oleh BSI KCP Gatot Subroto terhadap nasabah korban *phishing* masih belum optimal, baik ditinjau dari Undang-Undang Perlindungan Konsumen maupun dari perspektif *maqashid syariah*. Oleh karena itu, penelitian ini tidak hanya

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

mengkaji bentuk perlindungan yang diberikan, tetapi juga menilai efektivitasnya dalam mencegah kerugian, keadilan dalam penentuan tanggung jawab, serta kesesuaiannya dengan prinsip *hifz al-mal* dalam Islam.

Penelitian ini memiliki keterkaitan dengan beberapa penelitian terdahulu. Pertama, penelitian yang ditulis oleh Mohammad Dluha dengan judul "Bentuk Perlindungan Hukum Terhadap Nasabah Bank Pengguna Layanan *Internet Banking* Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen". Penelitian tersebut membahas bentuk perlindungan hukum terhadap nasabah pengguna layanan *internet banking* berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Kedua, penelitian yang ditulis oleh Salsabila Chairunnisa, Tarsisius Murwadji, dan Nun Harrieti dengan judul "Perlindungan Hukum Terhadap Nasabah atas Kejahatan *Phishing* dan *Hacking* pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia". Penelitian tersebut berfokus pada bentuk pertanggungjawaban bank digital serta perlindungan hukum terhadap nasabah yang mengalami kerugian akibat kejahatan phishing dan hacking berdasarkan hukum positif Indonesia. Penelitian tersebut menggunakan pendekatan yuridis normatif dan menitikberatkan pada pengaturan hukum serta tanggung jawab bank secara umum.

Perbedaan penelitian ini terletak pada objek, lokasi, pendekatan, dan fokus kajian. Penelitian ini secara khusus mengkaji perlindungan hukum terhadap nasabah korban *phishing* pada layanan *mobile banking* BSI KCP Gatot Subroto berdasarkan kondisi di lapangan. Penelitian ini tidak hanya menganalisis bentuk perlindungan hukum, tetapi juga menilai efektivitas upaya preventif dan represif yang dilakukan oleh pihak bank. Terulangnya kasus phishing pada tahun 2023, 2024, dan 2025 menjadi indikator untuk menilai efektivitas perlindungan yang diberikan kepada nasabah.

Penelitian ini menggunakan perspektif *Maqashid Syariah*, khususnya prinsip *hifz al-mal*, untuk menilai apakah perlindungan yang diberikan telah mencerminkan perlindungan terhadap harta, keadilan, kemaslahatan, serta pencegahan kerugian bagi nasabah. Dengan demikian, kebaruan penelitian ini terletak pada kajian empiris mengenai efektivitas perlindungan hukum terhadap nasabah korban *phishing* yang dianalisis melalui perspektif *hifz al-mal*. Penelitian ini diharapkan dapat menjadi bahan evaluasi bagi bank dalam meningkatkan edukasi, keamanan layanan, dan penanganan terhadap nasabah korban *phishing.*

Tujuan penelitian ini adalah untuk menganalisis bentuk perlindungan hukum terhadap nasabah Bank Syariah Indonesia KCP Gatot Subroto yang menjadi korban kejahatan *phishing* pada layanan *digital banking*. Selain itu, penelitian ini juga bertujuan untuk mengetahui tanggung jawab *bank* dalam memberikan keamanan terhadap transaksi digital nasabah serta menganalisis kasus tersebut berdasarkan perspektif *maqashid syariah*, khususnya dalam perlindungan harta (*hifz al-mal*).

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian yuridis empiris dengan pendekatan kualitatif. Penelitian yuridis empiris digunakan untuk mengetahui penerapan perlindungan hukum terhadap nasabah Bank Syariah Indonesia (BSI) yang menjadi korban kejahatan *phishing* pada layanan *mobile banking*. Jenis penelitian yuridis membantu membangun dasar teori, sementara jenis penelitian empiris memberikan gambaran nyata mengenai pelaksanaan hukum dalam praktik melalui data lapangan yang relevan (Wiraguna, 2024). Penelitian ini juga menggunakan pendekatan konseptual (*conceptual approach*) dengan mengkaji permasalahan berdasarkan konsep *Maqashid Syariah*, khususnya prinsip *hifz al-mal* yang berfokus pada perlindungan harta, serta pendekatan perundang-undangan (*statute approach*) dengan menelaah peraturan yang berkaitan dengan perlindungan nasabah dan layanan perbankan digital (Aris,2021). Penelitian ini merupakan penelitian lapangan (*field research*) yang bertujuan memperoleh data primer secara langsung dari narasumber. Data primer dikumpulkan melalui wawancara semi-terstruktur dengan *Customer Service* BSI KCP Gatot Subroto dan nasabah yang pernah mengalami kejahatan *phishing*. Wawancara dilakukan untuk memperoleh informasi mengenai bentuk perlindungan hukum, penanganan, serta upaya pencegahan terhadap kejahatan phishing.

Penelitian ini menggunakan data sekunder dan data primer yang diperoleh dari peraturan perundang-undangan, buku, jurnal ilmiah, dan sumber lain yang relevan. Data yang diperoleh kemudian dianalisis secara kualitatif dengan cara mengolah, mengelompokkan, dan menginterpretasikan data hasil wawancara serta menghubungkannya dengan ketentuan hukum dan konsep *Maqashid Syariah*, khususnya *hifz al-mal.*

HASIL DAN PEMBAHASAN

Bentuk Kejahatan *Phising* Pada Layanan *Digital Banking*

Phishing merupakan salah satu bentuk kejahatan siber yang dilakukan dengan memanfaatkan situs atau tautan palsu yang dibuat menyerupai situs resmi. Pelaku menggunakan situs tersebut untuk mengelabui korban agar memasukkan data pribadi atau informasi penting, seperti *username, password, PIN,* kode *OTP,* dan data keuangan. Data yang diperoleh kemudian digunakan untuk mengakses akun atau melakukan tindakan yang merugikan korban. *Phishing* dapat dilakukan melalui berbagai media, salah satunya melalui *e-mail* yang berisi tautan menuju situs palsu (Nurfahda et al., 2024).

Teknik *phishing* mulai dikenal pada tahun 1987 oleh Hewlett Packard *(HP) Group Interex.* Istilah *phishing* kemudian digunakan pada tahun 1990-an ketika seorang *hacker* bernama Khan C. Smith menggunakan metode tersebut untuk memperoleh *username* dan *password* pengguna *American Online (AOL)* (Putra Y, 2021).

Phishing memanfaatkan kurangnya kewaspadaan korban melalui berbagai cara. Pelaku dapat mengirimkan *e-mail* atau pesan palsu yang mengatasnamakan

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

lembaga resmi dan berisi tautan menuju situs tiruan. Selain itu, pelaku dapat membuat situs yang menyerupai situs bank, media sosial, atau penyedia layanan lainnya untuk memperoleh data korban. Phishing juga dapat dilakukan melalui SMS atau aplikasi pesan instan dengan mengirimkan tautan maupun permintaan informasi sensitif. Dalam menjalankan aksinya, pelaku sering menggunakan *social engineering* dengan memanfaatkan informasi korban agar pesan terlihat meyakinkan. Pelaku juga dapat memanipulasi emosi korban melalui ancaman pemblokiran akun, pemberitahuan transaksi mencurigakan, atau penawaran hadiah agar korban bertindak tergesa-gesa dan memberikan informasi pribadinya (Rahmawati et al., 2024*).*

Permasalahan *phishing* juga terjadi pada nasabah BSI KCP Gatot Subroto. Berdasarkan data penelitian, kasus *phishing* telah terjadi secara berulang pada tahun 2023, 2024, dan 2025. Pada tahun 2023, seorang nasabah mengalami kerugian sekitar Rp20.000.000 akibat tindak kejahatan *phishing*. Selanjutnya, pada tahun 2024 kembali terjadi kasus serupa yang mengakibatkan kerugian nasabah sekitar Rp60.000.000. Kemudian, pada tahun 2025, seorang nasabah bernama Budi mengalami kerugian sebesar Rp30.000.000 akibat mengakses tautan yang mengatasnamakan layanan resmi BSI.

Kasus Budi ini bermula nasabah menerima pesan digital yang mengatasnamakan pihak BSI dan memuat tautan yang menyerupai situs resmi bank. Karena mengira tautan tersebut merupakan bagian dari layanan resmi BSI, nasabah kemudian mengakses tautan tersebut dan memasukkan data pribadi serta informasi yang diminta pada halaman tersebut. Setelah data dimasukkan, pihak yang tidak bertanggung jawab diduga memperoleh akses terhadap informasi nasabah dan melakukan transaksi tanpa sepengetahuan maupun persetujuan nasabah. Akibat peristiwa tersebut, nasabah mengalami kerugian sebesar Rp30.000.000,00 (tiga puluh juta rupiah).

Peristiwa tersebut menunjukkan bahwa modus *phishing* dapat dilakukan dengan memanfaatkan kemiripan tampilan dan identitas suatu situs dengan layanan resmi bank. Nasabah yang tidak mengetahui bahwa tautan tersebut merupakan situs palsu dapat menganggap informasi yang diterimanya sebagai informasi resmi dan mengikuti instruksi yang diberikan. Dengan demikian, *phishing* tidak hanya memanfaatkan kelemahan teknis, tetapi juga memanfaatkan kepercayaan dan kurangnya pemahaman pengguna terhadap keamanan layanan digital.

Ketiga kasus *phishing* yang terjadi pada tahun 2023, 2024, dan 2025 menunjukkan bahwa kejahatan digital masih menjadi risiko yang dihadapi oleh nasabah BSI KCP Gatot Subroto. Meskipun kronologi dan jumlah kerugian dalam setiap kasus berbeda, seluruh peristiwa tersebut sama-sama mengakibatkan kerugian finansial bagi nasabah. Terjadinya kasus secara berulang juga menunjukkan bahwa perlindungan terhadap nasabah tidak hanya perlu dilakukan setelah terjadinya kerugian, tetapi harus didukung oleh upaya pencegahan yang efektif agar nasabah mampu mengenali dan menghindari berbagai bentuk *phishing.*

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Perlindungan Hukum dan Pertanggungjawaban Pihak Bank Terhadap Nasabah atas Kejahatan *Phising* Pada *Mobile Banking*

Perlindungan hukum merupakan suatu bentuk pengayoman yang diberikan terhadap hak asasi manusia yang mengalami pelanggaran atau kerugian akibat tindakan pihak lain, sehingga masyarakat dapat memperoleh dan menikmati hak-hak yang telah dijamin oleh hukum. Dalam hal ini, negara mempunyai peran yang sangat penting dalam memberikan perlindungan kepada warga negaranya. Perlindungan hukum terhadap masyarakat menjadi salah satu tanggung jawab negara untuk mewujudkan keadilan, keamanan, serta keselamatan bagi seluruh warga. Selain itu, pelaksanaan perlindungan hukum oleh negara juga memiliki peranan penting dalam menjaga ketertiban dan stabilitas kehidupan berbangsa dan bernegara (Arya Prayoga et al., 2023).

Perlindungan merupakan salah satu fungsi hukum yang bertujuan mewujudkan keadilan serta kesejahteraan bagi masyarakat. Perlindungan hukum bagi rakyat Indonesia merupakan bentuk penerapan prinsip pengakuan dan penghormatan terhadap harkat dan martabat manusia yang bersumber pada Pancasila. Pada dasarnya, setiap hubungan hukum memerlukan adanya perlindungan hukum. Perlindungan hukum bagi rakyat terdiri dari dua bentuk, yaitu:

1. Perlindungan hukum preventif, yaitu perlindungan hukum yang bertujuan mencegah terjadinya sengketa atau permasalahan hukum.
2. Perlindungan hukum represif, yaitu perlindungan hukum yang diberikan untuk menyelesaikan sengketa atau permasalahan hukum yang telah terjadi (Nur Hasanah, 2022).

Salah satu tujuan hukum adalah memberikan kepastian hukum kepada setiap subjek hukum, termasuk nasabah sebagai pengguna layanan bank digital. Dalam hal ini, nasabah berhak memperoleh perlindungan hukum atas dana yang dimilikinya serta jaminan kepastian apabila mengalami kerugian akibat kejahatan seperti *phishing* maupun *hacking*. Selain itu, kepastian hukum juga diperlukan agar nasabah merasa terlindungi dan memiliki keyakinan bahwa hak-haknya tetap dijamin serta kejadian serupa dapat dicegah di masa yang akan datang (Chairunnisa et al., 2024).

Secara yuridis perlindungan hukum terhadap nasabah dapat dikaitkan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang menegaskan bahwa setiap konsumen berhak memperoleh kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa (Indonesia, 1999). Dalam konteks permasalahan ini, nasabah BSI sebagai pengguna layanan *mobile banking* termasuk subjek yang berhak memperoleh perlindungan atas penggunaan layanan digital perbankan agar terhindar dari risiko penyalahgunaan data pribadi maupun kerugian finansial akibat kejahatan siber.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, terdapat hak-hak konsumen untuk memperoleh kenyamanan dan keamanan dalam mengkonsumsi barang dan/atau jasa, serta hak untuk memperoleh ganti rugi

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

sebagaimana diatur dalam Pasal 4 huruf (a). Selain itu, pada Pasal 4 huruf (d) juga disebutkan "hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan". Aturan ini dapat memberikan kesempatan kepada nasabah BSI dalam menggunakan *mobile banking* untuk menyampaikan kekurangan-kekurangan dari pelayanan yang diberikan. Sebagai timbal balik, pihak bank berkewajiban untuk mendengarkan pendapat maupun keluhan dari nasabah sebagai pengguna layanan *mobile banking*. Data pribadi merupakan salah satu hal yang berkaitan erat dengan kepercayaan dari pihak nasabah (Kamila & Efendi, 2023).

Kasus *phishing* yang menyebabkan adanya transaksi tanpa sepengetahuan nasabah juga berkaitan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024. Pengaturan tersebut memberikan dasar hukum terhadap perlindungan sistem elektronik, keamanan data, serta penyalahgunaan akses digital oleh pihak yang tidak bertanggung jawab. Dalam kasus nasabah BSI KCP Gatot Subroto, dugaan adanya akses ilegal terhadap akun *mobile banking* yang berujung pada hilangnya dana nasabah menunjukkan bahwa keamanan transaksi elektronik menjadi aspek penting yang harus diperhatikan dalam perlindungan hukum terhadap pengguna layanan digital.

Berdasarkan Pasal 1 angka 2 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), dalam layanan perbankan, nasabah dapat dikategorikan sebagai konsumen karena menggunakan jasa bank untuk memenuhi kebutuhan transaksi dan pengelolaan keuangan. Penerapan UUPK menimbulkan kewajiban bagi bank sebagai pelaku usaha untuk beritikad baik, memberikan informasi yang benar, jelas, dan jujur, memberikan pelayanan secara adil dan tidak diskriminatif, serta menjamin pelayanan perbankan sesuai dengan standar dan ketentuan yang berlaku (Dluha & Ariska, 2021). Kewajiban tersebut menunjukkan bahwa perlindungan nasabah tidak hanya berkaitan dengan penyelesaian pengaduan, tetapi juga mencakup upaya pencegahan dan pengamanan dalam penyelenggaraan layanan perbankan.

Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah juga menjadi dasar dalam penyelenggaraan kegiatan usaha yang sehat, aman, dan berdasarkan prinsip kehati-hatian. Penerapan prinsip kehati-hatian tersebut berkaitan dengan kewajiban bank dalam mengelola risiko, termasuk risiko operasional dan risiko teknologi informasi yang dapat timbul dalam penggunaan layanan perbankan digital. Oleh karena itu, bank syariah perlu menerapkan manajemen risiko melalui pengamanan sistem, perlindungan data nasabah, pemantauan transaksi, serta pencegahan dan penanganan terhadap risiko kejahatan siber.

Apabila terjadi kebocoran data atau akses tidak sah terhadap rekening nasabah pada Bank Syariah Indonesia, penyelesaiannya dapat mengacu pada ketentuan mengenai perlindungan konsumen, kerahasiaan data, keamanan sistem elektronik, prinsip kehati-hatian, dan pengelolaan risiko. Ketentuan tersebut

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

menjadi dasar untuk menilai bentuk perlindungan serta tanggung jawab bank dalam menjaga keamanan data dan dana nasabah (Keliat et al., 2023).

Hal ini menunjukkan bahwa diperlukan regulasi yang tegas serta pengawasan yang optimal dari OJK agar bank syariah senantiasa mematuhi prosedur, prinsip kehati-hatian, dan standar operasional yang berlaku. Dengan demikian, kepercayaan masyarakat terhadap lembaga perbankan syariah dapat terjaga, sekaligus memberikan jaminan keamanan terhadap dana yang disimpan oleh nasabah (Nasution & Zulham, 2024).

Penerapan Perlindungan Hukum Preventif oleh BSI KCP Gatot Subroto

Perlindungan hukum preventif merupakan perlindungan yang dilakukan sebelum terjadinya pelanggaran atau kerugian. Dalam layanan perbankan digital, perlindungan preventif bertujuan untuk mencegah nasabah menjadi korban kejahatan *phishing* melalui pemberian informasi dan edukasi mengenai keamanan transaksi serta cara mengenali modus penipuan (Alfian, 2023).

Berdasarkan hasil wawancara, BSI KCP Gatot Subroto melakukan upaya pencegahan *phishing* melalui penyebaran flyer di lingkungan kantor bank dan video singkat yang dibagikan melalui media sosial. Informasi tersebut berisi imbauan agar nasabah tidak mudah percaya terhadap pesan atau tautan yang mengatasnamakan BSI serta tidak memberikan data rahasia, seperti User ID, kata sandi, PIN, dan kode OTP kepada pihak lain (Handayani, wawancara, 2026).

Upaya tersebut menunjukkan bahwa pihak bank telah memberikan informasi kepada nasabah. Namun, edukasi yang dilakukan masih terbatas karena hanya disampaikan melalui *flyer* dan video singkat tanpa adanya edukasi secara langsung kepada nasabah. Akibatnya, pihak bank tidak dapat memastikan bahwa seluruh nasabah telah membaca dan memahami informasi mengenai bahaya *phishing*.

Apabila dikaitkan dengan Pasal 4 huruf c Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen,(UU Nomor 8 Tahun, 1999) konsumen berhak memperoleh informasi yang benar, jelas, dan jujur mengenai barang dan/atau jasa yang digunakan. Selain itu, Pasal 7 huruf b Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen mewajibkan pelaku usaha untuk memberikan informasi yang benar, jelas, dan jujur mengenai barang dan/atau jasa yang diberikan. Dalam layanan perbankan digital, ketentuan tersebut dapat dikaitkan dengan kewajiban bank untuk memberikan informasi yang jelas mengenai penggunaan layanan serta risiko keamanan yang dapat merugikan nasabah.

Hal tersebut dapat dilihat dari terjadinya kasus *phishing* secara berulang di BSI KCP Gatot Subroto pada tahun 2023, 2024, dan 2025. Pada tahun 2023, nasabah mengalami kerugian sebesar Rp20.000.000, kemudian pada tahun 2024 terjadi kembali kasus *phishing* dengan kerugian sebesar Rp60.000.000, dan pada tahun 2025 Budi mengalami kerugian sebesar Rp30.000.000. Terulangnya kasus tersebut menunjukkan bahwa penyebaran *flyer* belum cukup efektif untuk mencegah nasabah menjadi korban *phishing.*

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Pihak BSI KCP Gatot Subroto perlu meningkatkan upaya preventif melalui edukasi secara langsung dan berkala kepada nasabah. Edukasi dapat dilakukan ketika nasabah datang ke kantor bank, terutama saat pembukaan rekening atau aktivasi layanan *mobile banking*. Pihak bank juga dapat memberikan penjelasan singkat mengenai ciri-ciri pesan dan tautan *phishing* serta langkah yang harus dilakukan apabila menerima pesan mencurigakan. Dengan demikian, perlindungan preventif tidak hanya dilakukan melalui penyebaran informasi, tetapi juga dapat meningkatkan pemahaman dan kewaspadaan nasabah terhadap kejahatan *phishing*.

Penerapan Perlindungan Hukum Represif oleh BSI KCP Gatot Subroto

Perlindungan hukum represif merupakan perlindungan yang diberikan setelah terjadinya pelanggaran atau kerugian. Perlindungan ini bertujuan untuk menangani pengaduan, menyelesaikan permasalahan, serta memberikan pemulihan terhadap kerugian yang dialami oleh nasabah. Dalam kasus *phishing*, perlindungan represif dapat dilakukan melalui pemeriksaan transaksi, pengamanan rekening, penelusuran aliran dana, pemblokiran rekening tujuan, serta pemberian bantuan dalam proses penyelesaian pengaduan (Zennia, 2021).

Berdasarkan hasil wawancara, setelah Budi mengetahui adanya transaksi yang tidak pernah dilakukannya, Budi segera melaporkan kejadian tersebut kepada BSI KCP Gatot Subroto. Pihak bank kemudian melakukan pengecekan terhadap mutasi rekening dan riwayat transaksi untuk mengetahui aliran dana yang hilang. Pihak BSI juga membantu mengamankan akses *mobile banking* Budi agar tidak terjadi transaksi lain yang dapat menambah kerugian (Handayani, wawancara, 2026).

Setelah melakukan pengecekan internal, pihak BSI mengarahkan Budi untuk membuat laporan resmi kepada pihak kepolisian. Pihak bank juga memberikan dokumen yang diperlukan sebagai bukti pendukung dalam proses pelaporan. Selain itu, BSI melakukan koordinasi dengan pihak BRI untuk meminta pemblokiran terhadap rekening tujuan transaksi (Handayani, wawancara, 2026). Tindakan tersebut merupakan bentuk perlindungan hukum represif karena dilakukan setelah terjadinya kejahatan *phishing* dan bertujuan untuk menindaklanjuti pengaduan serta mencegah terjadinya kerugian yang lebih besar (Undang-Undang No.10 Tahun 1998 tentang Perbankan).

Meskipun pihak bank telah melakukan penanganan, dana Budi sebesar Rp30.000.000 tidak dapat dipulihkan karena telah lebih dahulu dipindahkan oleh pelaku ke beberapa dompet digital (*e-wallet*), sehingga aliran dana menjadi sulit untuk ditelusuri (Budi, wawancara, 2026). Selain itu, pihak BSI tidak memberikan ganti rugi karena Budi dinilai telah lalai dengan memasukkan User ID, kata sandi, dan kode OTP ke dalam tautan palsu yang mengatasnamakan BSI (Handayani, wawancara, 2026).

Apabila dikaitkan dengan Pasal 19 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen,(Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen) pelaku usaha pada dasarnya bertanggung jawab

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

memberikan ganti rugi atas kerugian yang dialami konsumen. Namun, dalam kasus *phishing*, penentuan tanggung jawab perlu mempertimbangkan penyebab kerugian serta tingkat kesalahan dari masing-masing pihak. Dalam kasus Budi, tindakan memasukkan data rahasia ke dalam tautan palsu memang menjadi faktor terjadinya kerugian. Akan tetapi, penentuan bahwa kerugian sepenuhnya menjadi tanggung jawab nasabah juga perlu mempertimbangkan efektivitas sistem keamanan, penerapan manajemen risiko, serta bentuk perlindungan yang telah diberikan oleh pihak bank.

Permasalahan ini menjadi penting karena kasus *phishing* di BSI KCP Gatot Subroto tidak hanya terjadi pada tahun 2025, tetapi juga telah terjadi pada tahun 2023 dengan kerugian sekitar Rp20.000.000 dan pada tahun 2024 dengan kerugian sekitar Rp60.000.000. Terulangnya kasus *phishing* dalam beberapa tahun menunjukkan bahwa upaya perlindungan yang diterapkan belum sepenuhnya mampu mencegah dan mengurangi risiko kerugian nasabah. Kondisi tersebut juga menjadi alasan perlunya evaluasi terhadap efektivitas sistem pengamanan dan penerapan manajemen risiko pada layanan *mobile banking*.

Pihak bank tidak hanya perlu menilai kesalahan dari tindakan nasabah, tetapi juga perlu melakukan pemeriksaan terhadap kemungkinan adanya kelemahan dalam sistem keamanan, seperti kemampuan sistem dalam mendeteksi transaksi yang tidak biasa, kecepatan pemblokiran transaksi, serta efektivitas sistem dalam mencegah akses tidak sah. Dengan demikian, penentuan pihak yang bertanggung jawab tidak hanya didasarkan pada kesalahan nasabah, tetapi juga mempertimbangkan apakah pihak bank telah menjalankan kewajiban pengamanan dan manajemen risiko secara optimal.

Berdasarkan hal tersebut, upaya represif yang dilakukan oleh BSI KCP Gatot Subroto telah berjalan melalui penerimaan pengaduan, pemeriksaan transaksi, pengamanan akses mobile banking, pemberian dokumen pendukung, koordinasi pemblokiran rekening, dan pendampingan dalam proses pelaporan kepada kepolisian (Undang-Undang No.10 Tahun 1998 tentang Perbankan). Namun, perlindungan tersebut belum sepenuhnya efektif karena dana nasabah tidak berhasil dipulihkan dan seluruh kerugian dibebankan kepada nasabah berdasarkan hasil pemeriksaan internal pihak bank.

Pihak BSI perlu meningkatkan sistem pemantauan terhadap transaksi yang tidak biasa, mempercepat proses pemblokiran dan penelusuran dana, serta melakukan evaluasi secara berkala terhadap sistem keamanan dan manajemen risiko. Selain itu, perlu adanya mekanisme pemeriksaan yang lebih terbuka dalam menentukan tingkat kelalaian antara nasabah dan pihak bank. Dengan demikian, perlindungan hukum represif tidak hanya sebatas menerima dan menangani pengaduan, tetapi juga dapat memberikan pemulihan, kepastian, dan perlindungan yang lebih adil kepada nasabah.

Terkait dengan pertanggungjawaban finansial, pihak BSI tidak memberikan kompensasi atau ganti rugi atas kerugian yang dialami oleh Budi. Pihak bank menilai bahwa kerugian tersebut terjadi akibat kelalaian Budi karena telah mengklik tautan

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

yang dikirimkan melalui WhatsApp dan memasukkan data pribadi serta data rahasia perbankan, seperti User ID, kata sandi, dan kode OTP, ke dalam laman palsu yang mengatasnamakan BSI. Menurut pihak bank, tindakan tersebut merupakan bentuk kelalaian nasabah dalam menjaga kerahasiaan data perbankan karena BSI tidak pernah meminta nasabah untuk memberikan kode OTP maupun kata sandi melalui pesan, *WhatsApp*, atau tautan tertentu (Handayani, wawancara, 2026).

Penentuan bahwa kerugian sepenuhnya disebabkan oleh kelalaian nasabah tidak seharusnya hanya didasarkan pada hasil pemeriksaan internal pihak bank. Dalam menentukan pihak yang bertanggung jawab, perlu dilakukan penilaian secara objektif terhadap penyebab terjadinya kerugian serta tingkat kesalahan atau kelalaian dari masing-masing pihak. Penilaian tersebut tidak hanya melihat tindakan Budi yang memasukkan data rahasia ke dalam tautan palsu, tetapi juga perlu mempertimbangkan efektivitas edukasi yang diberikan oleh bank, kecukupan sistem keamanan *mobile banking*, kemampuan sistem dalam mendeteksi transaksi yang tidak wajar, serta penerapan manajemen risiko oleh pihak bank.

Hal ini penting karena kasus *phishing* di BSI KCP Gatot Subroto telah terjadi secara berulang, yaitu pada tahun 2023, 2024, dan 2025. Terulangnya kasus tersebut menunjukkan bahwa masih terdapat risiko yang perlu dievaluasi dalam penerapan perlindungan nasabah dan sistem pengamanan layanan digital. Oleh karena itu, pembebanan seluruh kerugian kepada nasabah tanpa adanya pemeriksaan yang menyeluruh terhadap kemungkinan kelemahan pada sistem keamanan atau penerapan perlindungan oleh pihak bank dapat menimbulkan persoalan mengenai keadilan dan kepastian hukum.

POJK Nomor 22 Tahun 2023 pada dasarnya mengatur bahwa Pelaku Usaha Jasa Keuangan (PUJK) bertanggung jawab atas kerugian konsumen yang timbul akibat kesalahan, kelalaian, atau perbuatan yang bertentangan dengan ketentuan yang dilakukan oleh PUJK. Namun, PUJK dapat dikecualikan dari tanggung jawab apabila dapat membuktikan adanya keterlibatan, kesalahan, kelalaian, atau perbuatan konsumen yang bertentangan dengan ketentuan Otoritas Jasa Keuangan, 2023). Dengan demikian, adanya kelalaian dari nasabah tidak cukup hanya dinyatakan oleh pihak bank, tetapi harus didasarkan pada pembuktian dan pemeriksaan yang jelas terhadap seluruh faktor yang menyebabkan terjadinya kerugian.

Kasus Budi ini merupakan tindakan memasukkan User ID, kata sandi, dan kode OTP ke dalam tautan palsu memang dapat menjadi dasar untuk menilai adanya kelalaian dari pihak nasabah. Namun, penilaian tersebut perlu disertai dengan pemeriksaan terhadap pelaksanaan kewajiban bank dalam memberikan edukasi, menjaga keamanan layanan digital, serta menerapkan manajemen risiko. Hal ini diperlukan untuk mengetahui apakah kerugian benar-benar sepenuhnya disebabkan oleh tindakan nasabah atau terdapat faktor lain yang juga perlu menjadi tanggung jawab pihak bank.

Pasal 19 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen mengatur kewajiban pelaku usaha untuk memberikan ganti rugi atas

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

kerugian yang dialami konsumen. Oleh karena itu, penolakan pemberian ganti rugi perlu disertai dengan alasan dan dasar penilaian yang jelas agar nasabah memperoleh kepastian mengenai mengapa kerugian tersebut tidak menjadi tanggung jawab bank. Dalam hal terdapat perbedaan pendapat mengenai pihak yang bertanggung jawab, nasabah juga harus memperoleh kesempatan untuk menempuh mekanisme penyelesaian sengketa yang tersedia, sehingga penentuan tanggung jawab tidak hanya berhenti pada keputusan internal pihak bank.

Upaya represif yang dilakukan oleh BSI telah mencakup penerimaan pengaduan, pemeriksaan transaksi, pengamanan rekening, koordinasi pemblokiran, serta pendampingan dalam proses pelaporan. Namun, perlindungan tersebut belum sepenuhnya memberikan pemulihan kepada Budi karena dana yang hilang tidak berhasil dikembalikan dan tidak diberikan kompensasi. Oleh karena itu, diperlukan mekanisme pemeriksaan yang lebih terbuka dan objektif dalam menentukan tingkat kesalahan antara bank dan nasabah. Penentuan tanggung jawab tidak hanya didasarkan pada tindakan nasabah, tetapi juga perlu mempertimbangkan efektivitas perlindungan, sistem keamanan, dan manajemen risiko yang diterapkan oleh pihak bank.

Mengenai keamanan layanan digital, BSI telah menerapkan sistem autentikasi berlapis pada aplikasi *mobile banking*, seperti penggunaan *face recognition*, *fingerprint*, kata sandi, dan metode pengamanan lainnya. Penerapan sistem tersebut merupakan bagian dari upaya bank dalam mengelola risiko teknologi informasi serta menjaga keamanan akses dan transaksi nasabah. Hal ini sejalan dengan POJK Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, yang mewajibkan bank untuk menerapkan manajemen risiko teknologi informasi secara menyeluruh dan berkelanjutan (Otoritas Jasa Keuangan, 2016).

Penerapan sistem keamanan tersebut belum dapat dinilai sepenuhnya efektif dalam memberikan perlindungan kepada nasabah. Hal ini dapat dilihat dari terjadinya kasus *phishing* secara berulang di BSI KCP Gatot Subroto pada tahun 2023, 2024, dan 2025. Terulangnya kasus tersebut menunjukkan bahwa pengamanan layanan digital dan penerapan manajemen risiko masih perlu dievaluasi, terutama dalam mendeteksi aktivitas atau transaksi yang tidak wajar serta mencegah penyalahgunaan data nasabah.

Berdasarkan hasil penelitian, BSI KCP Gatot Subroto telah melakukan upaya perlindungan hukum secara preventif dan represif. Upaya preventif dilakukan melalui penyebaran *flyer* dan video singkat di media sosial mengenai bahaya *phishing* serta pentingnya menjaga kerahasiaan data perbankan. Namun, upaya tersebut masih terbatas karena belum disertai dengan edukasi secara langsung kepada nasabah. Sementara itu, upaya represif dilakukan melalui penerimaan dan penanganan pengaduan, pemeriksaan riwayat transaksi, pengamanan akses *mobile banking*, koordinasi pemblokiran rekening tujuan, serta pemberian dokumen pendukung untuk pelaporan kepada pihak kepolisian (Handayani, wawancara, 2026).

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Bank syariah memiliki tanggung jawab untuk menjaga keamanan data nasabah sebagai bentuk kepatuhan terhadap prinsip kehati-hatian dan peraturan yang berlaku. Di era digital, perlindungan data menjadi hal yang sangat penting karena risiko kebocoran dan penyalahgunaan data semakin tinggi (Nurhaliza et al., 2025).

Perlindungan hukum yang diberikan oleh BSI KCP Gatot Subroto belum cukup hanya dinilai dari telah dilaksanakannya prosedur preventif dan represif. Perlindungan tersebut juga perlu dinilai berdasarkan efektivitasnya dalam mencegah terulangnya kasus, melindungi keamanan dana nasabah, serta memberikan penyelesaian yang adil ketika terjadi kerugian. Oleh karena itu, pihak bank perlu meningkatkan edukasi secara langsung dan berkala, memperkuat sistem pendeteksian transaksi tidak wajar, mempercepat proses pemblokiran dan penelusuran dana, serta menerapkan mekanisme yang lebih terbuka dalam menentukan tanggung jawab antara bank dan nasabah.

Berbeda dengan akad *Wadi'ah* bank juga bertanggung jawab untuk memberikan penggantian secara penuh atas kehilangan dana nasabah apabila kerugian tersebut terjadi dalam pengelolaan oleh pihak bank. Hal ini karena akad *Wadi'ah* merupakan bentuk titipan dana dari nasabah kepada bank, sehingga bank memiliki kewajiban untuk menjaga serta mengembalikan dana tersebut sesuai ketentuan yang berlaku (Fitri & Damayanti, 2023).

Pelaksanaan perlindungan hukum terhadap nasabah korban *phishing*, terdapat beberapa hambatan yang dihadapi oleh pihak BSI KCP Gatot Subroto. Pertama, edukasi kepada nasabah masih terbatas pada penyebaran *flyer* dan video singkat di media sosial sehingga belum seluruh nasabah memahami modus dan cara menghindari phishing. Kedua, pelaku dapat dengan cepat memindahkan dana ke rekening lain atau dompet digital sehingga proses penelusuran dan pemulihan dana menjadi sulit. Ketiga, penentuan tanggung jawab atas kerugian masih didasarkan pada hasil pemeriksaan internal pihak bank, sehingga diperlukan penilaian yang lebih objektif terhadap tingkat kelalaian bank dan nasabah. Hambatan tersebut menyebabkan perlindungan yang diberikan belum sepenuhnya efektif dalam mencegah terulangnya kasus dan memulihkan kerugian nasabah.

Analisis Perspektif *Maqashid Syariah* Terhadap Perlindungan Nasabah

Maqashid merupakan bentuk jamak (*jama'*) dari *maqshud* yang berasal dari kata kerja *qashada* yang berarti menuju, tujuan, kehendak, dan kesengajaan. Dalam ilmu Nahwu, kata *maqshud-maqashid* disebut sebagai *maf'ul bih*, yaitu sesuatu yang menjadi objek, sehingga dapat dimaknai sebagai "tujuan" atau "beberapa tujuan". Sementara itu, *asy-syari'ah* berasal dari kata *syara'a* yang berarti "jalan menuju sumber air sebagai sumber kehidupan". Dengan demikian, secara terminologis, *al-maqashid asy-syari'ah* dapat dipahami sebagai tujuan-tujuan dalam ajaran Islam atau maksud Allah dalam menetapkan syariat Islam (Zahara, 2020).

Menurut pandangan Abu Ishaq al-Shatibi, m*aqashid syariah* mengacu pada kesatuan hukum Islam baik dari segi dasar pembentukannya maupun tujuan

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

penerapannya. Konsep ini menegaskan bahwa setiap hukum dalam Islam memiliki tujuan untuk mewujudkan kemaslahatan, menjaga kesejahteraan, serta membawa kebaikan bagi umat manusia (Anshari & Permata, 2024).

Al-Maqashid pada bagian *al-Maqashid* Imam As-Syatibi memberikan penjelasan mengenai tujuan Allah dalam membuat syariat, bahwasannya Allah menciptakan syariat dengan tujuan untuk menjaga kemaslahatan bagi manusia baik di dunia maupun di akhirat (Al-Syatibi, 1996).

Syariat juga dipahami sebagai hukum taklifi yang wajib dijalankan sesuai ketentuan yang telah ditetapkan. Dalam penjelasannya, Imam As-Syatibi menekankan dua hal penting. Pertama, suatu taklif yang berada di luar kemampuan manusia tidak dianggap sah secara syar'i karena Islam tidak membebankan sesuatu yang tidak mampu dilaksanakan oleh manusia. Kedua, meskipun dalam pelaksanaan taklif dapat ditemukan adanya *masyaqqah* atau kesulitan, syariat pada hakikatnya ditetapkan untuk memberikan manfaat dan kemudahan bagi mukallaf, bukan justru menimbulkan kesulitan yang memberatkan (Alfarizi & Permata, 2026).

Konsep *maqashid syariah* bertujuan untuk mewujudkan kemaslahatan dan kesejahteraan bagi manusia, termasuk dalam perlindungan terhadap nasabah pada layanan *digital banking*. Kesejahteraan tersebut dapat tercapai apabila lima unsur utama *maqashid syariah*, yaitu perlindungan agama (*hifz ad-din*), jiwa (*hifz an-nafs*), akal (*hifz al-'aql*), keturunan (*hifz an-nasl*), dan harta (*hifz al-mal*) dapat dijaga secara seimbang (Al-Syatibi, 1996). Dalam konteks perbankan syariah, perlindungan nasabah tidak hanya berkaitan dengan keamanan transaksi, tetapi juga mencakup perlindungan hak, kenyamanan, serta keamanan nasabah dalam menggunakan layanan digital banking (Alwi et al., 2022).

Adapun kelima unsur *maqashid syariah* dalam menjaga keamanan nasabah yaitu:

1. Perlindungan Nasabah terhadap Agama (*Hifz ad-Din*), Pihak bank telah berupaya menjalankan pelayanan berdasarkan nilai amanah dan tanggung jawab, tetapi perlindungan yang diberikan masih perlu ditingkatkan agar lebih adil dan memberikan kemaslahatan. (Cinta Rahmi et al., 2024).
2. Perlindungan Nasabah terhadap Jiwa (*Hifz an-Nafs*), Pengamanan rekening dan penanganan pengaduan telah dilakukan, tetapi kasus phishing yang berulang menunjukkan bahwa rasa aman nasabah belum sepenuhnya terjamin.
3. Perlindungan Nasabah terhadap Akal (*Hifz al-'Aql*), Edukasi melalui flyer dan video singkat telah dilakukan, tetapi masih terbatas sehingga perlu ditingkatkan melalui edukasi langsung kepada nasabah.
4. Perlindungan Nasabah terhadap Keturunan (*Hifz an-Nasl*), Kerugian akibat phishing dapat memengaruhi kesejahteraan keluarga nasabah sehingga diperlukan perlindungan yang lebih efektif.
5. Perlindungan Nasabah terhadap Harta (*Hifz al-Mal*), Pihak bank telah melakukan penanganan, tetapi perlindungan harta belum optimal karena kasus phishing masih berulang dan dana Budi sebesar Rp30.000.000 belum dapat dipulihkan.

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Prinsip *hifz al-mal* menekankan bahwa harta harus dijaga dari kehilangan, penyalahgunaan, penipuan, maupun pengambilan secara tidak sah. Dalam layanan perbankan digital, prinsip tersebut dapat diterapkan melalui penyediaan sistem keamanan yang memadai, pemberian edukasi kepada nasabah, pencegahan terhadap kejahatan digital, serta penanganan yang cepat apabila terjadi transaksi yang tidak sah. Dengan demikian, perlindungan terhadap harta tidak hanya dilakukan setelah nasabah mengalami kerugian, tetapi juga melalui upaya pencegahan agar kerugian tersebut tidak terjadi.

Berdasarkan hasil penelitian, penerapan prinsip *hifz al-mal* tersebut belum sepenuhnya terpenuhi. Hal ini dapat dilihat dari masih terjadinya kasus *phishing* secara berulang di BSI KCP Gatot Subroto pada tahun 2023, 2024, dan 2025. Terulangnya kasus tersebut menunjukkan bahwa upaya pencegahan dan perlindungan terhadap harta nasabah belum berjalan secara optimal. Edukasi yang hanya dilakukan melalui *flyer* dan video singkat juga belum cukup untuk memastikan bahwa seluruh nasabah memahami bahaya serta cara menghindari *phishing*. Dalam perspektif *maqashid syariah*, perlindungan terhadap harta seharusnya tidak hanya dinilai dari telah dilaksanakannya prosedur oleh pihak bank. Perlindungan juga perlu dilihat dari hasil dan manfaat yang diperoleh nasabah. Apabila pihak bank telah melakukan penanganan sesuai prosedur, tetapi dana nasabah tetap hilang, tidak dapat dipulihkan, dan seluruh kerugian dibebankan kepada nasabah tanpa adanya penilaian yang terbuka terhadap tanggung jawab masing-masing pihak, maka perlindungan terhadap harta belum sepenuhnya memberikan kemaslahatan dan keadilan.

Perlindungan hukum terhadap nasabah korban *phishing* di BSI KCP Gatot Subroto dalam perspektif *maqashid syariah* dapat dikatakan telah diterapkan, tetapi belum sepenuhnya terpenuhi. Prinsip *hifz al-mal* telah terlihat melalui adanya upaya edukasi, pengamanan rekening, pemeriksaan transaksi, koordinasi pemblokiran, dan pendampingan kepada nasabah. Namun, perlindungan tersebut belum optimal karena kasus *phishing* masih berulang, edukasi kepada nasabah masih terbatas, dana Budi tidak dapat dipulihkan, dan belum terdapat mekanisme yang jelas serta terbuka dalam menentukan tanggung jawab antara pihak bank dan nasabah.

Perbankan syariah juga harus mampu memberikan gambaran yang lebih konkret dalam menerapkan prinsip-prinsip maqashid syariah pada kegiatan operasionalnya. Hal tersebut dapat dilakukan melalui penerapan prinsip keadilan, perlindungan terhadap kepentingan nasabah, serta menghindari transaksi yang bertentangan dengan syariat Islam. Dengan adanya penerapan prinsip-prinsip tersebut, kepercayaan masyarakat terhadap komitmen bank syariah dalam menjalankan nilai-nilai Islam, khususnya dalam memberikan perlindungan kepada nasabah, dapat semakin meningkat (Amelia Andini et al., 2025).

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa kejahatan *phishing* pada layanan *mobile banking* dapat menyebabkan kerugian finansial dan

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

mengancam keamanan data nasabah. Di BSI KCP Gatot Subroto, kasus *phishing* terjadi berulang pada tahun 2023, 2024, dan 2025 dengan jumlah kerugian yang berbeda.Perlindungan hukum yang diberikan BSI KCP Gatot Subroto dilakukan melalui upaya preventif berupa edukasi keamanan digital dan peningkatan sistem keamanan, serta upaya represif berupa penanganan pengaduan, investigasi transaksi, pengamanan rekening, pemblokiran rekening tujuan, dan pendampingan pelaporan kepada kepolisian. Namun, perlindungan tersebut belum sepenuhnya efektif karena edukasi masih terbatas dan kasus phishing masih terus berulang.

Kasus Budi ini menjelaskan bank membebankan kerugian kepada nasabah dengan alasan kelalaian dalam menjaga kerahasiaan User ID, kata sandi, dan kode OTP sehingga tidak diberikan kompensasi. Penetapan tersebut didasarkan pada pemeriksaan internal bank dan belum disertai mekanisme yang terbuka dalam menilai kemungkinan adanya kelemahan sistem keamanan bank. Dalam perspektif *maqashid syariah*, perlindungan terhadap nasabah korban *phishing* sejalan dengan prinsip *hifz al-mal* atau perlindungan harta serta mendukung terwujudnya kemaslahatan. Namun, penerapannya belum optimal karena kasus masih berulang, edukasi belum maksimal, dan kerugian nasabah belum dapat dipulihkan. Oleh karena itu, diperlukan peningkatan literasi digital, penguatan sistem keamanan, transparansi dalam penentuan tanggung jawab, dan pengawasan berkelanjutan agar perlindungan nasabah menjadi lebih efektif dan adil.

DAFTAR PUSTAKA

Alfarizi, A., & Permata, C. (2026). Implementasi Force Majeure Sebagai Dasar Penyelesaian Pembiayaan Perbankan Syariah Perspektif Maqasid Al Syariah. *Qanun: Journal of Islamic Laws and Studies*, *4*(3), 1424–1437. https://doi.org/10.58738/qanun.v4i3.1264

Al-Syatibi, A. I. (1996). *Al-Muwafaqot Fi Ushulis Syari'at* (Jilid 2). https://kapasan-darulfalah.blogspot.com/2013/06/download-kitab-al-muwafaqot-asy-syathibi.html

Alwi, M., Kara, M. H., Abdullah, M. W., Fachrurrazy, M., Ekonomi, F., & Islam, B. (2022). KONSEP MAQASID AS SYARIAH DALAM PERBANKAN SYARIAH. *Journal of Islamic Economic Law* , *7*(2), 56–80. http://ejournal-iainpalopo.ac.id/alamwal

Amelia Andini, P., Stiawan, D., & Islam Negeri Abdurrahman Wahid, U. K. (2025). Implementasi Maqasid Syariah pada Perbankan Syariah dan Pengaruhnya Terhadap Minat Masyarakat di Indonesia. *Jurnal Sahmiyya*, *4*(2).

Anshari, M., & Permata, C. (2024). Deforestasi Hutan Lindung dalam Proyek Strategis Nasional Food Estate: Perspektif Maqashid Syariah. *Al Qalam: Jurnal Ilmiah Keagamaan Dan Kemasyarakatan*, *18*(3), 2031. https://doi.org/10.35931/aq.v18i3.3499

Aris Prio, dkk. (2021). Pengantar Metodologi Penelitian Hukum. Yogyakarta: Pustakabarupress

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Arya Prayoga, D., Anom Husodo, J., & Elok Puri Maharani, A. (2023). Perlindungan Hukum Terhadap Hak Warga Negara Dengan Berlakunya Undang-Undang Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional. *Jurnal Demokrasi Dan Ketahanan Nasional* , *2*(2).

Budi. (2025). Wawancara Nasabah Korban Phishing. BSI KCP Gatot Subroto Medan, [12 Juni 2026].

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Jurnal Ilmu Hukum Dan Sosial*, *2*(1), 1–16. https://doi.org/10.51903/hakim.v2i1.1535

Cinta Rahmi, Ahmad Aulia Rohman, Azzahra Elvina Sari, Salsa Layyinun Nadhifah, & Muhammad Rusydi Azmi. (2024). PENERAPAN MAQASHID SYARIAH DALAM PERBANKAN SYARIAH DI INDONESIA STUDI KASUS: PADA BANK BSI (BANK SYARIAH INDONESIA). *JURNAL ILMIAH RESEARCH AND DEVELOPMENT STUDENT*, *2*(2), 01–09. https://doi.org/10.59024/jis.v2i2.711

Dluha, M., & Ariska, Y. I. (2021). Bentuk Perlindungan Hukum Terhadap Nasabah Bank Pengguna Layanan Internet Banking Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. *Jurnal Hukum Politik Dan Agama*, *1*(2).

Fitri, L., & Damayanti, Y. E. (2023). Peningkatan Pemahaman Nasabah melalui Penerapan Akad Wadi'ah pada Bank Madani Syari'ah. *Tepis Wiring: Jurnal Pengabdian Masyarakat*, *2*(2), 31–41. https://doi.org/10.33379/tepiswiring.v2i2.2901

Handayani, Suci Tri. (2025). Wawancara Customer Service BSI KCP Gatot Subroto Medan. [12 Juni 2026].

Indonesia. (1999). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 8 TAHUN 1999 TENTANG PERLINDUNGAN KONSUMEN*.

Kamila, Z., & Efendi, R. (2023). *Perlindungan Hukum Atas Kehilangan Saldo Pengguna E-Wallet Dana di Tinjau Dari Fatwa DSN MUI No.16/Dsn Mui/Ix/2017 Tentang Uang Elektronik Syariah (Studi Kasus Pengguna E-Wallet Dana di Kecamatan Medan Tembung, Kota Medan)*. *6*(2). https://doi.org/10.31933/unesrev.v6i2

Keliat, V. U., Pratiwi Siregar, A., Zulkifli, S., & Purba, I. (2023). ANALISIS UPAYA DAN PERAN PERLINDUNGAN HUKUM TERHADAP KASUS PERETASAN DATA BANK SYARIAH INDONESIA. *Jurnal Ilmu Hukum Prima*.

Nasution, N. T., & Zulham, Z. (2024). PERTANGGUNGJAWABAN BANK SYARI'AH ATAS KEHILANGAN DANA NASABAH PERSPEKTIF PERATURAN OTORITAS JASA KEUANGAN. *Legal Standing : Jurnal Ilmu Hukum*, *8*(1), 239–249. https://doi.org/10.24269/ls.v8i1.8866

Nur Hasanah, A. (2022). Perlindungan Hukum Bagi Kreditur Pada Gugatan Actio Pauliana. *Jurnal Hukum Tata Negara Dan Politik Islam*, *9*(2).

Volume 8 Nomor 8 (2026) 1563 – 1581 P-ISSN 2656-274x E-ISSN 2656-4691
DOI: 10.47476/reslaj.v8i8.13444

Nurfahda, A. F., Annasyanda Jelita Putri, Nayottama Aryasuta Yardi, & Fitra Deni. (2024). ANALISIS PENIPUAN ONLINE DALAM BENTUK PHISING MENURUT PERSPEKTIF HUKUM INDONESIA. *Sahid Banking Journal* , *4*(1). https://jurnal.febi-inais.ac.id/index.php/SahidBankingJ

Nurhaliza, S., Islam, U., Sumatera, N., Amelia, U., Ningsih, S., Negeri, U. I., Utara, S., & Nurbaiti, U. (2025). KEAMANAN DATA NASABAH BANK SYARIAH. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 651–662. https://doi.org/10.61722/jmia.v2i1.3907

Otoritas Jasa Keuangan. (2016). Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko pada Pemanfaatan Teknologi Informasi oleh Bank Umum. Jakarta: OJK.

Otoritas Jasa Keuangan. (2023). Peraturan Otoritas Jasa Keuangan Nomor 21/2023 tentang Layanan Digital oleh Bank Umum. Jakarta: OJK.

Otoritas Jasa Keuangan. (2023). Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Jakarta: OJK.

Putra Y, V. F. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. *Jurist-Diction*, *4*(6). https://doi.org/10.20473/jd.v4i6.31857

Rahmawati, D., Viendyasari, M., Lumakto Rienzy Kholifatur, G., Anindhita, W., Ameliah Syavia Bachna, R., Adienda, A., Indang Trihandini, D., Rer Nat Rosari Saleh, Mk., Ruslan Ramli, M., Bachtiar, Y. A., & Siregar, B. (2024). *WASPADA KEJAHATAN PHISHING ATTACK!* Literasi Nusantara Abadi Grup. www.penerbitlitnus.co.id

Republik Indonesia. (1998). Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Jakarta: Sekretariat Negara.

Republik Indonesia. (1999). Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Jakarta: Sekretariat Negara.

Siti Masrohatin, Muhammad Yunus, Firman Maulana, & M.Abu Wildan Hidayatullah. (2025). Strategi Meningkatkan Kualiatas Pelayanan Nasabah Melalui Mobile Banking BYOND BY BSI. *Jurnal Penelitian Nusantara*, *1*, 465–472. https://doi.org/10.59435/menulis.v1i3.138

Tuti Warsiti, & Markoni. (2022). PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN CYBER CRIME BERBENTUK PHISING DALAM TRANSAKSI PERDAGANGAN INTERNATIONAL. *Jurnal Multidisiplin Indonesia*, *X*(X). https://jmi.rivierapublishing.id/index.php/rp

Wiraguna, S. A. (2024). Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia. *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum*, *3*(3). https://doi.org/10.59818/jps.v3i3.1390

Zahara, F. (2020). The Analysis of Maqashid Syariah on the Use of Fiat Money and Dinar Dirham. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, *3*(2), 1216–1226. https://doi.org/10.33258/birci.v3i2.964