

Perlindungan Hukum Nasabah Terhadap Kejahatan Siber Pada Layanan Mobilebanking Di Indonesia: Studi Kasus Phishing Melalui SMS/Whatsapp Yang Menguras Rekening Nasabah

Halwi Hasia Dinata¹, Putri Wulandari², Ratih Agustin Wulandari³

^{1,2} Jurusan, Fakultas, Institusi Program Studi Hukum, Fakultas Hukum dan
³ Ekonomi Bisnis, Universitas Dharma Indonesia

Email: Halwihasiadinata134@gmail.com, wulandariagustin88@gmail.com

Published: September, 2026

ABSTRAK

Perkembangan teknologi informasi telah mendorong transformasi layanan perbankan ke arah digital melalui penggunaan *mobile banking* yang memberikan kemudahan, kecepatan, dan efisiensi dalam bertransaksi. Di sisi lain, kemajuan tersebut juga meningkatkan risiko terjadinya kejahatan siber, salah satunya melalui modus *phishing* yang dilakukan dengan mengirimkan tautan palsu melalui SMS atau WhatsApp untuk memperoleh data pribadi, informasi perbankan, serta kode autentikasi nasabah. Kejahatan ini mengakibatkan pengurasan rekening nasabah dan menimbulkan kerugian finansial yang tidak sedikit. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap nasabah sebagai korban kejahatan siber pada layanan *mobile banking* di Indonesia serta mengkaji tanggung jawab bank dalam memberikan perlindungan kepada nasabah berdasarkan ketentuan hukum yang berlaku. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Bahan hukum yang digunakan meliputi Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, serta peraturan Otoritas Jasa Keuangan yang mengatur perlindungan konsumen sektor jasa keuangan. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah telah diatur melalui mekanisme preventif dan represif, namun implementasinya masih menghadapi berbagai kendala, antara lain rendahnya literasi digital masyarakat, semakin berkembangnya teknik rekayasa sosial (*social engineering*), serta belum optimalnya mekanisme penyelesaian pengaduan dan pemberian ganti kerugian kepada korban. Oleh karena itu, diperlukan penguatan sistem keamanan *mobile banking*, peningkatan edukasi keamanan digital kepada masyarakat, optimalisasi pengawasan oleh Otoritas Jasa Keuangan, serta peningkatan koordinasi antara bank, regulator, dan aparat penegak hukum guna memberikan kepastian hukum dan perlindungan yang lebih efektif bagi nasabah sebagai pengguna layanan perbankan digital.

Kata Kunci: Perlindungan Hukum, Nasabah, *Mobile Banking*, Kejahatan Siber, *Phishing*, SMS, Whatsapp

ABSTRACT

The rapid development of information technology has accelerated the digital transformation of the banking sector through mobile banking services, providing customers with greater convenience, speed, and efficiency in conducting financial transactions. However, this advancement has also increased the risk of cybercrime, particularly phishing attacks carried out through SMS and WhatsApp messages containing fraudulent links designed to obtain customers' personal data, banking credentials, and authentication codes. Such cybercrimes often result in unauthorized access to customer

accounts and significant financial losses. This study aims to analyze the legal protection provided to customers who become victims of cybercrime in mobile banking services in Indonesia and to examine the legal responsibilities of banks in protecting customers based on the applicable legal framework. This research employs a normative juridical method using statutory, conceptual, and case approaches. The legal materials analyzed include Law Number 10 of 1998 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection, Law Number 27 of 2022 concerning Personal Data Protection, the Law on Electronic Information and Transactions and its amendments, as well as regulations issued by the Financial Services Authority concerning consumer protection in the financial services sector. The findings indicate that legal protection for customers has been regulated through preventive and repressive mechanisms. Nevertheless, its implementation still faces several challenges, including low levels of digital literacy, the increasing sophistication of social engineering techniques, and the lack of optimal complaint handling and compensation mechanisms for victims. Therefore, strengthening mobile banking security systems, improving public awareness of cybersecurity, enhancing supervision by the Financial Services Authority, and reinforcing coordination among banks, regulators, and law enforcement agencies are essential to ensuring greater legal certainty and more effective protection for customers using digital banking services.

Keywords: Legal Protection, Customers, Mobile Banking, Cybercrime, Phishing, SMS, Whatsapp

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0>

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan terhadap berbagai sektor kehidupan, termasuk sektor perbankan. Transformasi digital yang terjadi dalam industri perbankan mendorong lahirnya berbagai layanan berbasis teknologi, salah satunya adalah *mobile banking*. Layanan ini memungkinkan nasabah melakukan berbagai transaksi keuangan, seperti transfer dana, pembayaran tagihan, pembelian produk digital, hingga investasi hanya melalui telepon pintar tanpa harus datang ke kantor bank. Kehadiran *mobile banking* memberikan kemudahan, efisiensi waktu, dan fleksibilitas bagi masyarakat dalam mengakses layanan perbankan. Selain meningkatkan kualitas pelayanan, digitalisasi perbankan juga menjadi salah satu upaya meningkatkan inklusi keuangan di Indonesia melalui pemanfaatan teknologi digital. Menurut Budi Agus Riswandi (2005), perkembangan layanan *internet banking* memberikan kemudahan bagi konsumen karena transaksi perbankan dapat dilakukan kapan saja dan di mana saja. Namun, kemudahan tersebut juga diikuti dengan munculnya berbagai persoalan hukum, terutama berkaitan dengan keamanan informasi, perlindungan nasabah, serta kemungkinan terjadinya kejahatan siber. Riswandi menegaskan bahwa perkembangan layanan perbankan berbasis internet membutuhkan sistem hukum yang efektif dan dapat diandalkan untuk mencegah serta menanggulangi berbagai bentuk penyimpangan dan kejahatan siber dalam kegiatan perbankan.

Di balik berbagai kemudahan tersebut, perkembangan teknologi digital juga memunculkan berbagai risiko baru, khususnya meningkatnya kejahatan siber (*cybercrime*) yang menasar sektor perbankan. Kejahatan siber merupakan setiap perbuatan melawan hukum yang memanfaatkan sistem elektronik, jaringan internet, maupun teknologi informasi sebagai sarana melakukan tindak pidana. Salah satu bentuk kejahatan siber yang sering terjadi pada layanan *mobile banking* adalah *phishing*. Modus *phishing* dilakukan dengan cara mengelabui korban melalui pesan singkat (SMS), aplikasi WhatsApp, surat elektronik (*email*), maupun media sosial yang berisi tautan (*link*) palsu menyerupai situs resmi bank. Ketika korban memasukkan data pribadi, seperti nomor kartu, *User ID*,

PIN, kata sandi, kode OTP (*One Time Password*), atau data autentikasi lainnya, pelaku memperoleh akses untuk mengendalikan rekening korban dan melakukan transaksi tanpa izin sehingga mengakibatkan kerugian finansial. Dalam konteks ini, Budi Agus Riswandi (2005) menjelaskan bahwa perkembangan layanan perbankan melalui internet tidak hanya memberikan manfaat bagi nasabah, tetapi juga menimbulkan peluang terjadinya pelanggaran dan kejahatan yang dapat merugikan bank maupun nasabah. Oleh karena itu, aspek keamanan menjadi salah satu persoalan penting dalam penyelenggaraan layanan perbankan berbasis teknologi.

Kasus *phishing* melalui SMS dan WhatsApp semakin relevan untuk dikaji seiring dengan meningkatnya penggunaan layanan perbankan digital di Indonesia. Pelaku memanfaatkan rendahnya literasi digital masyarakat dengan mengirimkan pesan yang seolah-olah berasal dari pihak bank, seperti pemberitahuan perubahan tarif transaksi, pembaruan sistem, pemblokiran rekening, atau peningkatan keamanan akun. Pesan tersebut biasanya disertai tautan menuju halaman palsu yang memiliki tampilan menyerupai situs resmi bank sehingga korban sulit membedakan keasliannya. Setelah data autentikasi berhasil diperoleh, pelaku dapat melakukan pengambilalihan akun *mobile banking* dan memindahkan dana korban. Modus ini merupakan bentuk *social engineering* yang tidak hanya menyerang kelemahan sistem teknologi, tetapi juga memanfaatkan kelengahan dan kurangnya pemahaman pengguna terhadap keamanan digital. Penelitian Az-zahra dan Labib (2025) menunjukkan bahwa digitalisasi perbankan memang memberikan kemudahan dan efisiensi dalam transaksi, tetapi pada saat yang sama menghadirkan risiko kejahatan siber yang menyasar data pribadi dan keamanan finansial nasabah. Karena itu, perlindungan terhadap nasabah membutuhkan kombinasi antara penguatan keamanan digital, edukasi konsumen, pengawasan regulator, dan penegakan hukum.

Meningkatnya kasus *phishing* menunjukkan bahwa keamanan layanan *mobile banking* tidak hanya bergantung pada kecanggihan teknologi yang dimiliki bank, tetapi juga memerlukan sistem perlindungan hukum yang mampu memberikan kepastian hukum bagi nasabah sebagai konsumen jasa keuangan. Dalam hubungan hukum antara bank dan nasabah, bank memiliki kewajiban untuk menyelenggarakan sistem layanan yang aman, andal, dan mampu melindungi data serta dana nasabah. Di sisi lain, nasabah juga memiliki kewajiban untuk menjaga kerahasiaan data autentikasi dan menggunakan layanan perbankan sesuai dengan ketentuan yang berlaku. Menurut Budi Agus Riswandi (2005), keamanan dan perlindungan informasi merupakan persoalan penting dalam penyelenggaraan layanan *internet banking*, karena penggunaan teknologi dalam transaksi perbankan menimbulkan risiko terhadap informasi dan keuangan nasabah. Dengan demikian, penyelenggaraan layanan perbankan digital tidak cukup hanya mengutamakan kemudahan transaksi, tetapi juga harus disertai mekanisme keamanan dan perlindungan hukum yang memadai.

Permasalahan muncul ketika terjadi pengurusan rekening akibat *phishing*, karena sering kali timbul perbedaan pendapat mengenai pihak yang harus bertanggung jawab atas kerugian yang dialami nasabah. Dalam praktiknya, bank tidak selalu memberikan penggantian kerugian apabila terbukti bahwa data autentikasi diberikan sendiri oleh nasabah kepada pihak lain melalui modus penipuan. Kondisi tersebut menimbulkan perdebatan mengenai batas tanggung jawab bank dan bentuk perlindungan hukum yang seharusnya diterima oleh nasabah. Penelitian Ni Kadek Devi Aprianti dan Putu Devi Yustisia Utami (2024) mengenai batas pertanggungjawaban bank terhadap kerugian nasabah akibat *phishing* menunjukkan bahwa pertanggungjawaban bank berkaitan dengan ada atau tidaknya kesalahan atau kelalaian dari pihak bank. Dengan demikian, persoalan

pertanggungjawaban tidak dapat dilepaskan dari penilaian mengenai penyebab kerugian, tindakan bank, serta bentuk kelalaian yang mungkin terjadi dalam penyelenggaraan layanan perbankan.

Secara teoritis, persoalan tersebut dapat dianalisis melalui konsep perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon (1987). Hadjon membedakan perlindungan hukum menjadi perlindungan preventif dan perlindungan represif. Perlindungan preventif diarahkan untuk mencegah terjadinya pelanggaran atau sengketa melalui pengaturan dan pengawasan sebelum suatu peristiwa merugikan terjadi, sedangkan perlindungan represif diberikan setelah terjadi pelanggaran atau sengketa melalui mekanisme penyelesaian hukum. Dalam konteks *mobile banking*, perlindungan preventif dapat diwujudkan melalui penerapan sistem keamanan yang memadai, perlindungan data pribadi, transparansi informasi, edukasi kepada nasabah, serta mekanisme deteksi transaksi mencurigakan. Sementara itu, perlindungan represif dapat dilakukan melalui pengaduan nasabah, penyelesaian sengketa, pemberian ganti kerugian apabila memenuhi dasar pertanggungjawaban, dan penegakan hukum terhadap pelaku *phishing*. Dengan demikian, teori Hadjon memberikan kerangka untuk menilai apakah perlindungan yang diberikan kepada nasabah telah mencakup aspek pencegahan sekaligus pemulihan setelah terjadinya kerugian.

Secara normatif, perlindungan hukum terhadap nasabah pengguna layanan *mobile banking* di Indonesia telah diatur dalam berbagai peraturan perundang-undangan. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur kewajiban bank dalam menjaga kepercayaan masyarakat dan kerahasiaan data nasabah. Selain itu, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan hak kepada konsumen untuk memperoleh keamanan, kenyamanan, dan ganti rugi apabila mengalami kerugian akibat penggunaan jasa. Perlindungan terhadap data pribadi semakin diperkuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang mengatur kewajiban dalam pemrosesan dan perlindungan data pribadi. Di samping itu, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya serta berbagai Peraturan Otoritas Jasa Keuangan mengenai perlindungan konsumen dan penyelenggaraan teknologi informasi memberikan landasan hukum bagi penyelenggaraan layanan perbankan digital yang aman dan bertanggung jawab. Penelitian Chairunnisa, Murwadi, dan Harrieti (2023) juga menunjukkan bahwa perlindungan terhadap nasabah dalam menghadapi *phishing* dan *hacking* perlu dilihat melalui kerangka hukum yang mengatur hubungan antara bank, nasabah, dan negara, termasuk kewajiban bank dalam menyediakan mekanisme penanganan pengaduan dan perlindungan terhadap nasabah.

Meskipun kerangka hukum tersebut telah tersedia, implementasi perlindungan hukum terhadap korban kejahatan siber masih menghadapi berbagai kendala. Perkembangan metode *phishing* yang semakin kompleks, rendahnya literasi keamanan digital masyarakat, proses penanganan pengaduan yang belum selalu optimal, serta belum seragamnya penerapan pertanggungjawaban terhadap kerugian nasabah menjadi faktor yang dapat memengaruhi efektivitas perlindungan hukum. Mamesah (2025) menunjukkan bahwa regulasi mengenai perlindungan nasabah dari *phishing* telah tersedia melalui berbagai ketentuan, tetapi pengaturannya masih cenderung bersifat umum dan belum secara khusus mengatur batas tanggung jawab bank dalam setiap kasus *phishing*. Penelitian tersebut juga mengidentifikasi keterbatasan teknologi keamanan, kurangnya koordinasi antara bank dan aparat penegak hukum, serta rendahnya literasi digital nasabah sebagai beberapa faktor yang menghambat penanganan kasus *phishing*.

Selain persoalan regulasi, perlindungan nasabah juga berkaitan erat dengan kewajiban bank dalam menjaga keamanan data pribadi. Tanonggi, Pusparini, Limbong, Siagan, dan Thiffani (2024)

menjelaskan bahwa serangan *phishing* menimbulkan persoalan hukum mengenai pertanggungjawaban bank terhadap data nasabah serta upaya hukum yang dapat ditempuh ketika nasabah mengalami kerugian. Hal tersebut menunjukkan bahwa perlindungan data pribadi tidak dapat dipisahkan dari perlindungan dana nasabah dalam layanan perbankan elektronik. Oleh karena itu, bank tidak hanya dituntut menyediakan teknologi yang mampu memfasilitasi transaksi, tetapi juga harus memastikan bahwa sistem tersebut memiliki mekanisme keamanan yang mampu mengurangi risiko penyalahgunaan data dan transaksi tidak sah.

Perkembangan teknologi informasi yang berlangsung cepat juga menyebabkan hukum dituntut untuk mampu mengikuti perubahan bentuk kejahatan digital. Dalam konteks tersebut, hukum tidak hanya berfungsi memberikan sanksi terhadap pelaku setelah kejahatan terjadi, tetapi juga harus memberikan perlindungan yang efektif bagi masyarakat sejak sebelum kerugian terjadi. Hal ini sejalan dengan pemikiran Philipus M. Hadjon (1987) mengenai pentingnya perlindungan preventif sebagai bentuk pencegahan sengketa dan perlindungan represif sebagai sarana penyelesaian ketika pelanggaran telah terjadi. Dengan demikian, efektivitas perlindungan hukum terhadap nasabah *mobile banking* perlu dinilai tidak hanya berdasarkan keberadaan peraturan perundang-undangan, tetapi juga berdasarkan kemampuan bank dan regulator dalam menerapkan pencegahan, merespons pengaduan, menyelesaikan sengketa, serta memberikan pemulihan terhadap korban.

Berdasarkan uraian tersebut, penelitian ini menjadi penting untuk mengkaji bagaimana bentuk perlindungan hukum yang diberikan kepada nasabah yang menjadi korban kejahatan siber pada layanan *mobile banking*, khususnya melalui modus *phishing* menggunakan SMS dan WhatsApp. Selain itu, penelitian ini juga bertujuan untuk menganalisis tanggung jawab bank dalam memberikan perlindungan kepada nasabah serta mengidentifikasi berbagai kendala dan upaya yang dapat dilakukan untuk meningkatkan efektivitas perlindungan hukum terhadap pengguna layanan perbankan digital di Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan ilmu hukum, khususnya hukum perbankan dan hukum siber, sekaligus menjadi bahan pertimbangan bagi regulator, lembaga perbankan, dan masyarakat dalam mewujudkan sistem layanan *mobile banking* yang aman, terpercaya, dan memberikan kepastian hukum bagi seluruh nasabah.

METODE

Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu penelitian hukum yang dilakukan dengan mengkaji norma-norma hukum yang berlaku melalui studi kepustakaan (*library research*). Penelitian ini bertujuan untuk menganalisis ketentuan hukum yang mengatur perlindungan hukum terhadap nasabah pengguna layanan *mobile banking* yang menjadi korban kejahatan siber, khususnya tindak pidana *phishing* melalui SMS dan WhatsApp. Fokus penelitian diarahkan pada peraturan perundang-undangan, asas hukum, teori hukum, serta literatur ilmiah yang berkaitan dengan perlindungan konsumen, hukum perbankan, hukum siber, dan perlindungan data pribadi.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan yang berkaitan dengan perbankan digital dan perlindungan konsumen, antara lain Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang

Penyelenggaraan Layanan Perbankan Digital. Pendekatan ini digunakan untuk memahami bagaimana hukum positif mengatur hak dan kewajiban antara bank dan nasabah serta bentuk perlindungan hukum yang diberikan kepada nasabah.

Pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum yang berkembang dalam doktrin dan literatur hukum, khususnya mengenai perlindungan hukum, tanggung jawab hukum (*liability*), hubungan hukum antara bank dan nasabah, serta prinsip kehati-hatian (*prudential principle*) dalam kegiatan perbankan. Pendekatan ini tidak hanya berfokus pada teks hukum, tetapi juga digunakan untuk memperoleh pemahaman yang lebih mendalam mengenai konsep dan teori yang menjadi dasar perlindungan hukum terhadap nasabah. Sementara itu, pendekatan kasus dilakukan dengan menganalisis kasus-kasus sengketa perbankan digital yang terjadi di masyarakat. Pendekatan ini digunakan untuk melihat penerapan norma hukum dalam praktik sekaligus mengidentifikasi berbagai permasalahan yang muncul dalam penyelesaian sengketa akibat kejahatan siber.

Bahan hukum yang digunakan dalam penelitian ini berupa data sekunder yang terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer merupakan sumber hukum yang memiliki kekuatan mengikat, meliputi peraturan perundang-undangan yang berkaitan dengan perbankan dan perlindungan konsumen serta peraturan yang diterbitkan oleh Otoritas Jasa Keuangan (OJK). Bahan hukum sekunder digunakan untuk memberikan penjelasan dan analisis terhadap bahan hukum primer, yang meliputi buku-buku hukum, jurnal ilmiah, artikel akademik, dan hasil penelitian terdahulu. Adapun bahan hukum tersier digunakan sebagai bahan pelengkap, seperti kamus hukum dan ensiklopedia.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan mengumpulkan dan menelaah peraturan perundang-undangan yang relevan, mengkaji berbagai literatur hukum seperti buku dan jurnal ilmiah, serta mengakses sumber elektronik yang kredibel. Pengumpulan bahan hukum tersebut dilakukan untuk memperoleh bahan yang komprehensif dan relevan dengan permasalahan penelitian.

Analisis bahan hukum dilakukan secara kualitatif, yaitu dengan mengolah dan menguraikan bahan hukum dalam bentuk penjelasan yang sistematis tanpa menggunakan analisis statistik. Analisis dilakukan melalui proses inventarisasi bahan hukum dengan mengumpulkan peraturan yang relevan, klasifikasi bahan hukum berdasarkan keterkaitannya dengan permasalahan penelitian, interpretasi terhadap ketentuan hukum yang berlaku, serta evaluasi terhadap penerapan dan efektivitas hukum dalam praktik. Penarikan kesimpulan dilakukan secara deduktif, yaitu dengan menghubungkan ketentuan hukum yang bersifat umum dengan permasalahan atau kasus yang bersifat khusus.

Sistematika analisis dilakukan dengan menghubungkan norma hukum yang berlaku dengan konsep perlindungan hukum serta fakta dan kasus yang terjadi dalam praktik. Melalui hubungan tersebut, penelitian diharapkan dapat memberikan gambaran yang utuh mengenai efektivitas perlindungan hukum terhadap nasabah pengguna layanan *mobile banking* yang menjadi korban kejahatan siber, khususnya tindak pidana *phishing* melalui SMS dan WhatsApp, serta penyelesaian sengketa perbankan digital di Indonesia.

HASIL DAN PEMBAHASAN

Bentuk Perlindungan Hukum Nasabah terhadap Kejahatan Siber pada Layanan Mobile Banking

Transformasi digital pada sektor perbankan telah mengubah pola pelayanan kepada masyarakat melalui pemanfaatan layanan *mobile banking*. Layanan tersebut memberikan berbagai kemudahan dalam melakukan transaksi keuangan secara cepat, efisien, dan fleksibel. Namun, di sisi lain perkembangan teknologi juga meningkatkan risiko kejahatan siber yang mengancam keamanan data maupun dana nasabah. Salah satu bentuk kejahatan yang paling sering terjadi adalah *phishing*, yaitu upaya memperoleh informasi rahasia milik nasabah dengan cara menyamar sebagai pihak resmi melalui SMS, WhatsApp, email, maupun media elektronik lainnya.

Perlindungan hukum terhadap nasabah merupakan bentuk jaminan negara dalam memberikan kepastian hukum kepada masyarakat sebagai pengguna jasa perbankan. Perlindungan tersebut bertujuan menciptakan rasa aman, menjaga kepercayaan masyarakat terhadap sistem perbankan nasional, serta memberikan kepastian mengenai hak dan kewajiban antara bank dengan nasabah.

Dalam hukum Indonesia, perlindungan hukum terhadap nasabah dapat dibedakan menjadi dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif merupakan upaya yang dilakukan untuk mencegah terjadinya kerugian terhadap nasabah. Bentuk perlindungan ini meliputi transparansi informasi mengenai produk dan layanan perbankan, perlindungan terhadap data pribadi nasabah, serta pemberian edukasi keuangan mengenai penggunaan layanan perbankan digital secara aman. Hal ini sejalan dengan penelitian yang menyatakan bahwa perlindungan preventif dilakukan melalui keterbukaan informasi dan perlindungan privasi konsumen.

Sementara itu, perlindungan hukum represif merupakan upaya yang diberikan setelah terjadi pelanggaran atau kerugian terhadap nasabah. Perlindungan ini dapat dilakukan melalui mekanisme pengaduan nasabah, penyelesaian sengketa antara nasabah dan pihak bank, serta penegakan hukum terhadap pihak yang melakukan pelanggaran. Dengan demikian, perlindungan hukum represif bertujuan memberikan penyelesaian dan pemulihan atas kerugian yang dialami nasabah.

Analisis Dasar Hukum Perlindungan Nasabah

Hasil penelitian menunjukkan bahwa secara normatif, Indonesia telah memiliki kerangka hukum yang cukup kuat dalam memberikan perlindungan terhadap nasabah pengguna layanan perbankan digital. Perlindungan tersebut antara lain bersumber dari Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, serta berbagai peraturan yang diterbitkan oleh Otoritas Jasa Keuangan mengenai penyelenggaraan dan perlindungan konsumen dalam layanan perbankan. Ketentuan tersebut pada dasarnya menempatkan bank sebagai pihak yang memiliki kewajiban untuk menyelenggarakan sistem perbankan yang aman, menjaga kerahasiaan dan keamanan data nasabah, serta memberikan perlindungan terhadap nasabah dalam penggunaan layanan perbankan digital.

Menurut Budi Agus Riswandi (2005), perkembangan layanan perbankan berbasis internet memberikan kemudahan bagi nasabah, tetapi juga menimbulkan risiko hukum yang berkaitan dengan keamanan transaksi dan perlindungan nasabah. Oleh karena itu, penyelenggaraan layanan perbankan berbasis teknologi harus disertai dengan sistem keamanan dan mekanisme perlindungan hukum yang memadai. Pandangan tersebut menunjukkan bahwa kewajiban bank tidak hanya

terbatas pada penyediaan fasilitas transaksi, tetapi juga mencakup upaya untuk memastikan bahwa teknologi yang digunakan mampu memberikan keamanan dan perlindungan bagi nasabah.

Dalam perspektif perlindungan hukum, Philipus M. Hadjon (1987) menjelaskan bahwa perlindungan hukum dapat diberikan dalam bentuk preventif dan represif. Perlindungan preventif bertujuan mencegah terjadinya pelanggaran atau kerugian, sedangkan perlindungan represif diberikan setelah terjadi pelanggaran untuk menyelesaikan sengketa dan memberikan pemulihan kepada pihak yang dirugikan. Apabila dikaitkan dengan layanan *mobile banking*, perlindungan preventif dapat diwujudkan melalui penerapan standar keamanan sistem, perlindungan data pribadi, pemberian informasi yang jelas kepada nasabah, serta edukasi mengenai keamanan transaksi digital. Adapun perlindungan represif dapat dilakukan melalui mekanisme pengaduan, penyelesaian sengketa, pemberian ganti kerugian sesuai dengan dasar pertanggungjawaban, serta penegakan hukum terhadap pelaku kejahatan siber.

Meskipun kerangka hukum yang tersedia relatif memadai, hasil penelitian juga menunjukkan bahwa penerapannya masih menghadapi berbagai kendala. Salah satu kendala yang ditemukan adalah belum optimalnya pengawasan terhadap penerapan standar keamanan pada layanan perbankan digital. Perbedaan tingkat kesiapan teknologi dan mekanisme keamanan antarpengyelenggara layanan dapat meningkatkan risiko terjadinya penyalahgunaan data dan transaksi tidak sah. Selain itu, lemahnya penegakan sanksi terhadap pelanggaran tertentu juga dapat mengurangi efektivitas regulasi dalam memberikan efek pencegahan.

Kendala lainnya berkaitan dengan masih terbatasnya pemahaman sebagian nasabah mengenai hak dan kewajibannya dalam menggunakan layanan perbankan digital. Dalam kasus *phishing*, misalnya, nasabah dapat menyerahkan data autentikasi kepada pelaku karena tidak mampu membedakan pesan resmi bank dengan pesan penipuan. Kondisi tersebut kemudian menimbulkan persoalan dalam menentukan tanggung jawab atas kerugian yang terjadi. Menurut Budi Agus Riswandi (2005), persoalan keamanan dalam layanan perbankan berbasis internet tidak hanya berkaitan dengan teknologi, tetapi juga dengan perilaku dan pemahaman pengguna. Dengan demikian, perlindungan nasabah tidak dapat hanya dibebankan kepada nasabah melalui kewajiban menjaga data pribadi, tetapi harus didukung oleh sistem keamanan bank, edukasi yang memadai, pengawasan regulator, dan mekanisme penyelesaian sengketa yang efektif.

Dengan demikian, hasil penelitian memperlihatkan bahwa keberadaan regulasi belum secara otomatis menjamin terciptanya perlindungan hukum yang efektif bagi nasabah. Efektivitas perlindungan hukum sangat bergantung pada konsistensi penerapan regulasi, pengawasan terhadap bank, peningkatan standar keamanan sistem, penegakan sanksi terhadap pelanggaran, serta peningkatan literasi digital dan pemahaman hukum nasabah. Perlindungan yang komprehensif diperlukan agar nasabah pengguna layanan *mobile banking* tidak hanya memperoleh perlindungan secara normatif, tetapi juga mendapatkan kepastian dan pemulihan ketika menjadi korban kejahatan siber.

Mekanisme Penyelesaian Sengketa

Penyelesaian sengketa antara nasabah dan bank akibat permasalahan dalam layanan perbankan digital dapat ditempuh melalui jalur non-litigasi maupun jalur litigasi. Jalur non-litigasi merupakan mekanisme penyelesaian sengketa di luar pengadilan yang dapat dilakukan melalui pengaduan kepada bank, mediasi, serta Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK). Nasabah juga dapat menyampaikan pengaduan kepada Otoritas Jasa

Kuangan (OJK) sesuai dengan kewenangan yang dimilikinya. Mekanisme tersebut pada dasarnya memberikan kesempatan kepada nasabah untuk memperoleh penyelesaian yang lebih sederhana tanpa harus langsung mengajukan gugatan ke pengadilan.

Dalam perspektif perlindungan konsumen, penyelesaian sengketa di luar pengadilan memiliki arti penting karena dapat memberikan akses penyelesaian yang lebih mudah bagi pihak yang berada dalam posisi yang relatif lemah. Shidarta (2006) menjelaskan bahwa konsumen pada dasarnya berada dalam posisi yang lebih lemah dibandingkan pelaku usaha karena adanya ketidakseimbangan informasi, kemampuan ekonomi, serta penguasaan terhadap produk dan layanan. Oleh karena itu, keberadaan mekanisme penyelesaian sengketa yang mudah diakses menjadi bagian penting dari perlindungan konsumen, termasuk dalam hubungan antara nasabah dan bank.

Mediasi menjadi salah satu mekanisme yang dapat digunakan untuk mempertemukan kepentingan nasabah dan bank guna mencapai penyelesaian berdasarkan kesepakatan. Dalam sengketa yang berkaitan dengan *phishing*, mediasi dapat digunakan untuk membahas kronologi transaksi, tingkat keamanan sistem bank, tindakan nasabah dalam menjaga data autentikasi, serta kemungkinan bentuk penyelesaian atau penggantian kerugian. Sementara itu, LAPS SJK memberikan alternatif penyelesaian sengketa melalui mekanisme yang dirancang secara khusus untuk sektor jasa keuangan. Keberadaan lembaga tersebut penting karena sengketa perbankan memiliki karakteristik teknis dan hukum yang membutuhkan pemahaman mengenai hubungan antara konsumen, bank, teknologi informasi, dan regulasi sektor jasa keuangan.

Selain jalur non-litigasi, nasabah juga dapat menempuh jalur litigasi melalui pengadilan umum apabila sengketa tidak dapat diselesaikan melalui mekanisme pengaduan atau penyelesaian sengketa di luar pengadilan. Jalur litigasi memberikan kesempatan kepada nasabah untuk memperoleh putusan yang memiliki kekuatan hukum mengikat. Dalam perkara kerugian akibat *phishing*, proses litigasi dapat digunakan untuk menguji ada atau tidaknya kesalahan atau kelalaian bank, tindakan nasabah, hubungan sebab akibat antara peristiwa dengan kerugian, serta dasar hukum yang dapat digunakan untuk menuntut pertanggungjawaban.

Menurut Philipus M. Hadjon (1987), perlindungan hukum represif bertujuan memberikan penyelesaian terhadap sengketa yang telah terjadi. Dalam konteks hubungan antara nasabah dan bank, mekanisme pengaduan, mediasi, LAPS SJK, maupun pengadilan merupakan bentuk perlindungan represif karena digunakan setelah terjadi permasalahan atau kerugian. Dengan demikian, tersedianya berbagai jalur penyelesaian sengketa merupakan bagian penting dari upaya memberikan perlindungan hukum kepada nasabah, terutama ketika nasabah menjadi korban kejahatan siber dalam penggunaan layanan *mobile banking*.

Namun, dalam praktiknya, penyelesaian sengketa antara nasabah dan bank masih menghadapi berbagai kendala. Salah satu kendala utama adalah proses penyelesaian yang dapat berlangsung cukup panjang, terutama apabila sengketa berlanjut hingga tahap litigasi. Selain itu, terdapat ketidakseimbangan posisi antara nasabah dan bank karena bank pada umumnya memiliki sumber daya, informasi, tenaga ahli, serta dokumentasi transaksi yang lebih lengkap dibandingkan nasabah. Kondisi tersebut dapat menyulitkan nasabah dalam membuktikan bahwa kerugian yang dialaminya berkaitan dengan kelemahan sistem atau kelalaian pihak bank.

Kendala lainnya adalah kurangnya pemahaman sebagian nasabah mengenai hak, kewajiban, dan prosedur penyelesaian sengketa. Nasabah yang menjadi korban *phishing* sering kali tidak memahami langkah yang harus segera dilakukan setelah mengetahui adanya transaksi tidak sah, termasuk mekanisme pengaduan, penyampaian bukti, dan prosedur permohonan penyelesaian

sengketa. Menurut Shidarta (2006), keterbatasan pengetahuan konsumen mengenai hak dan mekanisme perlindungan dapat menjadi salah satu faktor yang menyebabkan hak konsumen tidak dapat diperoleh secara optimal.

Berdasarkan hasil penelitian, dapat diketahui bahwa keberadaan mekanisme penyelesaian sengketa melalui jalur non-litigasi dan litigasi pada dasarnya telah memberikan pilihan bagi nasabah dalam memperoleh perlindungan hukum. Akan tetapi, tersedianya mekanisme tersebut belum sepenuhnya menjamin penyelesaian yang efektif karena masih terdapat persoalan mengenai lamanya proses, ketidakseimbangan posisi antara nasabah dan bank, serta keterbatasan pemahaman nasabah mengenai prosedur hukum. Oleh karena itu, diperlukan mekanisme penyelesaian sengketa yang lebih sederhana, cepat, transparan, dan mudah diakses agar nasabah korban *phishing* dapat memperoleh kepastian hukum dan pemulihan kerugian secara lebih efektif.

Kendala Perlindungan Hukum Nasabah

Beberapa kendala dalam perlindungan hukum terhadap nasabah pengguna layanan perbankan digital masih ditemukan dalam praktik. Kendala tersebut meliputi lemahnya implementasi regulasi, rendahnya literasi keuangan dan literasi digital masyarakat, ketimpangan posisi antara bank dan nasabah, serta kurang optimalnya pengawasan. Meskipun berbagai ketentuan hukum telah mengatur kewajiban bank dalam memberikan perlindungan kepada nasabah, keberadaan regulasi tersebut belum sepenuhnya menjamin penerapan perlindungan secara efektif.

Menurut Shidarta (2006), konsumen pada dasarnya berada dalam posisi yang relatif lebih lemah dibandingkan pelaku usaha karena adanya ketidakseimbangan informasi, kemampuan, dan sumber daya. Pandangan tersebut relevan dalam hubungan antara bank dan nasabah karena bank memiliki penguasaan yang lebih besar terhadap teknologi, informasi transaksi, sistem keamanan, serta dokumen yang berkaitan dengan aktivitas perbankan. Kondisi tersebut dapat menyulitkan nasabah ketika harus membuktikan adanya kesalahan atau kelalaian bank dalam suatu sengketa.

Rendahnya literasi keuangan dan literasi digital masyarakat juga menjadi salah satu faktor yang meningkatkan risiko terjadinya kejahatan siber. Nasabah yang tidak memahami karakteristik penipuan digital dapat dengan mudah mempercayai pesan yang mengatasnamakan bank dan menyerahkan data autentikasi kepada pelaku. Selain itu, kurangnya pengawasan terhadap penerapan standar keamanan perbankan dapat menyebabkan adanya kesenjangan antara ketentuan regulasi dan praktik penyelenggaraan layanan digital.

Dalam kasus likuidasi bank, perlindungan terhadap nasabah juga menghadapi persoalan tersendiri, terutama dalam menjamin kepastian dan keadilan bagi nasabah dalam memperoleh kembali haknya. Kondisi tersebut menunjukkan bahwa perlindungan hukum tidak hanya diperlukan ketika bank masih beroperasi, tetapi juga ketika terjadi kegagalan atau likuidasi bank. Oleh karena itu, mekanisme perlindungan harus mampu memberikan kepastian mengenai kedudukan dan hak nasabah dalam berbagai kondisi.

Studi Kasus *Phishing* Melalui SMS dan WhatsApp

Modus *phishing* melalui SMS dan WhatsApp merupakan salah satu bentuk *social engineering* yang memanfaatkan kelengahan dan aspek psikologis korban. Pelaku biasanya mengirimkan pesan yang mengatasnamakan pihak bank dengan alasan tertentu, seperti perubahan tarif transaksi, pembaruan sistem, pemblokiran rekening, informasi hadiah atau undian, maupun pemberitahuan

mengenai aktivitas keamanan akun. Pesan tersebut umumnya disertai tautan yang mengarahkan korban menuju halaman palsu yang dibuat menyerupai situs resmi bank.

Setelah membuka tautan tersebut, korban biasanya diminta memasukkan sejumlah informasi rahasia, seperti *User ID*, *password*, nomor kartu ATM, PIN, dan kode OTP (*One Time Password*). Setelah seluruh informasi diperoleh, pelaku dapat menggunakan data tersebut untuk memperoleh akses terhadap akun *mobile banking* korban dan melakukan transaksi tanpa persetujuan pemilik rekening. Dana korban kemudian dapat dipindahkan ke rekening lain dalam waktu yang relatif singkat. Dalam banyak kasus, korban baru mengetahui bahwa rekeningnya telah terkuras setelah menerima notifikasi transaksi atau ketika melakukan pengecekan saldo.

Menurut Budi Agus Riswandi (2005), perkembangan layanan perbankan berbasis internet memberikan kemudahan bagi nasabah, tetapi pada saat yang sama menimbulkan risiko terhadap keamanan transaksi dan informasi nasabah. Oleh karena itu, aspek keamanan merupakan bagian penting dalam penyelenggaraan layanan perbankan berbasis teknologi. Dalam konteks *phishing*, pendapat tersebut menunjukkan bahwa bank tidak cukup hanya menyediakan fasilitas transaksi digital, tetapi juga harus memastikan bahwa sistem yang digunakan memiliki tingkat keamanan yang memadai untuk melindungi nasabah dari berbagai bentuk penyalahgunaan.

Analisis Kasus

Berdasarkan kasus *phishing* melalui SMS dan WhatsApp tersebut, dapat diidentifikasi beberapa permasalahan utama yang berkaitan dengan perlindungan hukum nasabah. Permasalahan pertama adalah kemungkinan terjadinya kegagalan sistem (*system error*) atau kelemahan mekanisme keamanan yang memungkinkan transaksi tidak sah berlangsung. Permasalahan kedua adalah lambatnya respons bank dalam menangani laporan nasabah setelah terjadinya transaksi mencurigakan. Kecepatan respons sangat penting karena dana hasil kejahatan dapat segera dipindahkan melalui rekening lain sehingga semakin sulit untuk dilacak dan dipulihkan.

Permasalahan berikutnya adalah kurangnya transparansi mengenai proses investigasi dan mekanisme penentuan tanggung jawab atas kerugian nasabah. Nasabah sering kali tidak memperoleh informasi yang cukup mengenai bagaimana bank melakukan pemeriksaan terhadap transaksi yang disengketakan, faktor yang digunakan untuk menentukan tanggung jawab, serta alasan diterima atau ditolaknya permohonan penggantian kerugian. Selain itu, terdapat ketidakpastian hukum mengenai batas tanggung jawab bank ketika transaksi terjadi setelah nasabah secara tidak sadar memberikan data autentikasinya kepada pelaku *phishing*.

Philipus M. Hadjon (1987) menjelaskan bahwa perlindungan hukum terdiri atas perlindungan preventif dan represif. Perlindungan preventif bertujuan mencegah terjadinya pelanggaran, sedangkan perlindungan represif diberikan setelah terjadi pelanggaran atau sengketa. Berdasarkan konsep tersebut, analisis terhadap kasus *phishing* tidak hanya perlu melihat bagaimana bank memberikan penyelesaian setelah rekening nasabah dikuras, tetapi juga menilai apakah bank telah melakukan tindakan pencegahan yang memadai sebelum transaksi tidak sah terjadi.

Tanggung Jawab Bank

Berdasarkan hasil analisis, bank memiliki tanggung jawab hukum terhadap nasabah yang dapat bersumber dari hubungan kontraktual, peraturan perundang-undangan, dan prinsip tanggung jawab atas kelalaian (*negligence*). Tanggung jawab kontraktual merupakan kewajiban bank yang timbul berdasarkan hubungan hukum antara bank dan nasabah melalui perjanjian penggunaan layanan

perbankan. Bank berkewajiban memberikan layanan sesuai dengan ketentuan dan standar yang telah ditetapkan serta menjaga keamanan transaksi nasabah.

Tanggung jawab berdasarkan undang-undang merupakan kewajiban yang dibebankan kepada bank melalui berbagai peraturan perundang-undangan. Ketentuan tersebut antara lain berkaitan dengan keamanan sistem, perlindungan konsumen, kerahasiaan data, serta perlindungan data pribadi. Sementara itu, tanggung jawab berdasarkan kelalaian dapat timbul apabila kerugian nasabah terbukti disebabkan oleh kesalahan atau kelalaian bank dalam menjalankan kewajibannya.

Ahmadi Miru dan Sutarman Yodo (2015) menjelaskan bahwa pelaku usaha pada prinsipnya memiliki kewajiban untuk memberikan kompensasi atau ganti rugi apabila konsumen mengalami kerugian akibat penggunaan barang atau jasa yang diberikan. Dalam konteks layanan perbankan, prinsip tersebut dapat dikaitkan dengan kewajiban bank sebagai penyedia jasa kepada nasabah. Oleh karena itu, apabila dapat dibuktikan bahwa kerugian nasabah disebabkan oleh kegagalan sistem, lemahnya pengamanan, atau kelalaian bank, maka terdapat dasar untuk meminta pertanggungjawaban dan pemulihan kerugian sesuai dengan ketentuan hukum yang berlaku.

Meskipun demikian, tanggung jawab bank dalam kasus *phishing* tidak dapat ditentukan secara otomatis hanya karena nasabah mengalami kerugian. Penentuan tanggung jawab perlu mempertimbangkan kronologi kejadian, sistem keamanan yang diterapkan bank, tindakan nasabah dalam menjaga data autentikasi, karakteristik transaksi, serta ada atau tidaknya kesalahan dan kelalaian dari masing-masing pihak. Hal ini diperlukan karena *phishing* merupakan kejahatan yang dilakukan oleh pihak ketiga melalui manipulasi terhadap korban.

Evaluasi Efektivitas Perlindungan Hukum

Hasil penelitian menunjukkan bahwa meskipun regulasi mengenai perlindungan nasabah telah tersedia, efektivitas perlindungan hukum dalam praktik masih belum optimal. Salah satu penyebabnya adalah kurangnya kecepatan respons bank dalam menangani pengaduan nasabah. Dalam kasus *phishing*, keterlambatan penanganan dapat menyebabkan dana korban berpindah melalui beberapa rekening sehingga semakin sulit untuk diblokir dan dipulihkan.

Selain itu, mekanisme penyelesaian sengketa masih dapat membutuhkan waktu yang relatif panjang, terutama apabila sengketa berlanjut pada proses litigasi. Rendahnya literasi digital masyarakat juga menjadi faktor yang memperbesar risiko terjadinya *phishing*, sementara pengawasan dan penegakan hukum terhadap kejahatan siber masih perlu diperkuat.

Upaya perbaikan dapat dilakukan melalui peningkatan kualitas sistem keamanan perbankan digital, penguatan pengawasan oleh OJK, peningkatan edukasi kepada masyarakat, serta penyederhanaan mekanisme penyelesaian sengketa. Bank perlu meningkatkan kemampuan sistem dalam mendeteksi transaksi mencurigakan dan memberikan respons yang cepat ketika terdapat laporan dari nasabah. Di sisi lain, OJK perlu memastikan bahwa standar keamanan dan perlindungan konsumen diterapkan secara konsisten oleh penyelenggara layanan perbankan digital.

Menurut Philipus M. Hadjon (1987), perlindungan hukum yang efektif harus mencakup aspek preventif dan represif. Oleh karena itu, peningkatan keamanan sistem dan edukasi nasabah merupakan bagian dari perlindungan preventif, sedangkan pengaduan, penyelesaian sengketa, pemberian ganti rugi, dan penegakan hukum merupakan bagian dari perlindungan represif. Kedua bentuk perlindungan tersebut perlu berjalan secara beriringan agar nasabah memperoleh perlindungan sebelum maupun setelah terjadinya kerugian.

Sintesis Pembahasan

Secara keseluruhan, perlindungan hukum terhadap nasabah dalam layanan perbankan digital di Indonesia telah memiliki dasar hukum yang relatif kuat melalui berbagai peraturan mengenai perbankan, perlindungan konsumen, teknologi informasi, dan perlindungan data pribadi. Namun, masih terdapat kesenjangan antara regulasi dan implementasinya, khususnya dalam penanganan kasus *phishing*, penentuan tanggung jawab bank, kecepatan respons terhadap pengaduan, serta mekanisme pemulihan kerugian nasabah.

Dengan demikian, perlindungan hukum yang efektif tidak cukup hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh konsistensi penerapannya. Diperlukan sinergi antara regulator, pelaku usaha perbankan, aparat penegak hukum, dan masyarakat untuk meningkatkan keamanan sistem, memperkuat pengawasan, meningkatkan literasi digital, serta menyediakan mekanisme penyelesaian sengketa yang cepat dan mudah diakses. Sinergi tersebut diharapkan dapat mewujudkan sistem perbankan digital yang aman, adil, transparan, dan terpercaya serta memberikan kepastian hukum bagi nasabah yang menjadi korban kejahatan siber.

KESIMPULAN

Perlindungan hukum terhadap nasabah dalam sistem perbankan nasional telah diatur secara komprehensif melalui berbagai regulasi. Namun, dalam praktiknya masih terdapat kelemahan, khususnya dalam penyelesaian sengketa. Studi kasus pembobolan rekening menunjukkan bahwa nasabah masih berada pada posisi yang lemah. Oleh karena itu, diperlukan penguatan regulasi, peningkatan pengawasan, serta edukasi kepada masyarakat.

Namun, dalam praktiknya masih terdapat berbagai kendala, seperti lambatnya respons bank, kurangnya transparansi, serta belum optimalnya mekanisme penyelesaian sengketa. Oleh karena itu diperlukan peningkatan pengawasan oleh OJK, peningkatan kualitas layanan perbankan digital, serta peningkatan literasi digital masyarakat.

REFERENCES

- Ahmadi, M., & Yodo, S. (2015). *Hukum perlindungan konsumen* (Ed. revisi, cet. ke-9). RajaGrafindo Persada.
- Aprianti, N. K. D., & Utami, P. D. Y. (2024). Batas pertanggungjawaban bank terhadap kerugian nasabah akibat tindakan *phishing*. *Kertha Semaya: Journal Ilmu Hukum*, 12(12), 2938–2948. <https://doi.org/10.24843/KS.2024.v12.i12.p08>
- Chairunnisa, S., Murwadi, T., & Harieti, N. (2024). Perlindungan hukum terhadap nasabah atas kejahatan *phishing* dan *backing* pada layanan bank digital ditinjau berdasarkan hukum positif Indonesia. *Hakim: Jurnal Ilmu Hukum dan Sosial*, 2(1), 1–16.
- Endrawati, E. A., Kaemirawati, D. T., & Herawati, S. (2024). Perlindungan hukum sebagai upaya meningkatkan kepercayaan masyarakat terhadap perbankan: Studi kasus kejahatan perbankan di Indonesia. *Binamulia Hukum*, 13(2), 589–602. <https://doi.org/10.37893/jbh.v13i2.945>
- Hardinata, M. J., Shanty, S., Sitohang, Y. Y., Rahma, I. A., Utomo, S., & Ramadoni, S. R. (2024). Sosialisasi kebijakan bank digital: Perlindungan hukum terhadap data nasabah dari risiko serangan siber. *RENATA: Jurnal Pengabdian Masyarakat Kita Semua*, 2(2), 165–172. <https://doi.org/10.61124/1.renata.53>

- Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia: Sebuah studi tentang prinsip-prinsipnya, penanganannya oleh pengadilan dalam lingkungan peradilan umum dan pembentukan peradilan administrasi negara*. Bina Ilmu.
- Mamesah, M. (2025). Perlindungan hukum terhadap nasabah bank dari tindak pidana *phishing*. *Lex Crimen*.
- Miru, A., & Yodo, S. (2015). *Hukum perlindungan konsumen* (Ed. revisi). RajaGrafindo Persada.
- Mutiasari, A. I. (2020). Perkembangan industri perbankan di era digital. *Jurnal Ekonomi Bisnis dan Kewirausahaan*, 9(2), 32–41. <https://doi.org/10.47942/iab.v9i2.541>
- Riswandi, B. A. (2005). *Aspek hukum internet banking*. RajaGrafindo Persada.
- Shidarta. (2006). *Hukum perlindungan konsumen Indonesia* (Ed. revisi). Grasindo.
- Tanonggi, J. T., Pusparini, I., Limbong, C. P., Thiffani, G., & Siagan, S. N. (2024). Tinjauan hukum terhadap pertanggungjawaban bank kepada data nasabah dalam serangan *phishing*. *Indonesian Journal of Law*, 1(6), 186–194.
- Yunita, Y., Saimima, I. D. S., Purnama, D., & Hutagalung, A. T. (2025). Perlindungan hukum nasabah bank digital terhadap bunga yang melebihi tingkat penjaminan Lembaga Penjamin Simpanan. *Srivijaya Journal of Private Law*, 2(2), 124–138. <https://doi.org/10.28946/sjpl.v2i2.5118>

Peraturan Perundang-undangan

- Undang-Undang Republik Indonesia Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankan.
- Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan peraturan perundang-undangan yang berlaku.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Republik Indonesia Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.
- Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital.
- Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum.